

## 主题研究

# 区块链与数字货币：科技如何重塑金融基础设施

### 观点聚焦

#### 投资建议

2019 年 6 月 17 日，Facebook 发布 Libra，引起各国对其长期威胁国家货币主权的担忧。10 月 25 日，习总书记在政治局学习会上明确提出，区块链是我国自主创新的下一个重要突破口。我们认为，区块链技术的发展，特别是过去一年稳定币技术的成熟，使区块链有望成为支撑金融行业下一代基础设施的核心技术。科技巨头涉足金融业务并非新事，但我们认为科技巨头利用区块链技术进军金融，使其有机会从货币这个金融体系的基础出发，彻底改变行业生态。各国监管当局如何调整监管体系以拥抱数字经济，金融企业如何利用区块链提升效率，中国企业如何在技术变革中抓住发展机遇都是非常重要的话题。我们希望这篇报告能够帮助投资人把握区块链这个颠覆性技术的未来发展脉络。

#### 理由

**稳定币的出现，使区块链有望成为金融行业下一代基础设施的核心技术。**2009 年比特币问世以来，其结算流程简单、匿名性强等优点就广受瞩目，但由于其价格波动过于剧烈，很难被用作日常生活中的交易手段。以 USDT、USDC 为代表的稳定币，通过和法定资产挂钩，在保留了加密货币优点的同时，避免了价格波动大的问题，正逐渐取代比特币成为加密资产行业的主流支付工具。此外，以稳定币技术为基础的抵押贷款等新业务也在加密资产行业中不断诞生，数字世界的新金融体系正在形成。

**Facebook 的用户规模优势和稳定币的技术优势结合，使 Libra 有望威胁国家的货币主权。**谷歌、亚马逊、脸书、苹果、阿里、腾讯等科技巨头（GAFA+AT）利用其用户规模和技术上的优势，涉足金融业务由来已久。但过去科技巨头的金融服务仍然是以现有支付体系为基础，例如苹果的 Apple Pay 等。稳定币的出现，为科技巨头构筑一个全新的跨国家支付体系提供了工具。Libra（及其它大规模稳定币）虽然短期仍然面临许多监管难题，但长期可能改变跨境汇款、移动支付等领域的现有格局，成为数字经济时代新的储值手段和价值尺度。

**各国积极完善加密资产监管体系，加速数字货币研发落地。**过去一年，美国、英国、新加坡、中国香港监管当局相继发布了各自的加密资产监管标准。Libra 发布后 4 天，全球反洗钱金融行动特别工作组（FATF）发布了全球第一个加密货币监管标准。另一方面，全球央行出现了加速发展数字货币的趋势，我国有望成为全球第一个发行央行数字货币的国家。央行数字货币的推出，除了为消费者提供的一个新的广覆盖、跨平台的支付手段以外，也会实现 1）提升央行货币政策操作的准确性，2）助推人民币国际化，以及 3）更有效的打击金融犯罪等目标。

**金融企业积极利用区块链提升服务效率。**除了稳定币以外，主要金融企业过去几年也在积极探索区块链技术。经过过去几年发展，区块链技术已经被证明适合需要“多方共享”、“高频重复”、“交易链条长”的许多金融场景。在跨境支付、交易后清算、资产证券化、电子票据、贸易融资、供应链金融等领域已经初显成效。

**中国企业占有一定先机，政策助推行业加速发展。**区块链行业目前主要包括 1）提供共识机制芯片的半导体企业，2）以太坊、Hyperledger Fabric 等开源区块链框架，3）蚂蚁金服、平安、腾讯、万向等区块链平台，以及 4）提供基于区块链服务或软件解决方案的企业。国内企业中，蚂蚁金服、中国平安、腾讯、华为、万向等公司的区块链平台技术在全球占有重要地位，且资产交易、清结算、跨境支付、电子票据等领域中也有一批优秀初创企业。我们认为总书记的发言会大幅加速我国区块链技术的落地速度，提升金融等行业的运作效率，为相关企业提供发展良机。

#### 风险

各国监管政策变化及区块链技术实际落地效果可能影响相关企业发展速度。

#### 黄乐平

分析员  
SAC 执证编号：S0080518070001  
SFC CE Ref: AUZ066  
leping.huang@cicc.com.cn

#### 王瑞平

分析员  
SAC 执证编号：S0080517120002  
SFC CE Ref: ALE841  
victor.wang@cicc.com.cn

#### 姚泽宇

分析员  
SAC 执证编号：S0080518090001  
SFC CE Ref: BJ003  
zeyu.yao@cicc.com.cn

#### 杨俊杰

分析员  
SAC 执证编号：S0080519090001  
SFC CE Ref: BOJ945  
junjie.yang@cicc.com.cn

#### 相关研究报告

- 主题研究 | 区块链研究#5：中国金融及 IT 企业如何布局区块链 (2019.01.18)
- 主题研究 | 区块链研究#4：ICO 泡沫的教训与 STO 的发展机会 (2019.01.15)
- 主题研究 | 区块链研究#3：数字货币与跨境支付 (2019.01.14)
- 主题研究 | 区块链研究#2：比特币产业链 (2018.12.06)
- 主题研究 | 区块链研究#1：比特币及其他加密资产 (2018.11.30)

资料来源：万得资讯、彭博资讯、中金公司研究部



北京 | 11月22-24日  
163期PEMA

## 股权投资基金的募投管退

主讲人：上海亿宸投资管理有限公司董事长 马卫国

## 并购战略与操作

主讲人：招商证券副董事 高涛

## 并购与基金的法律安排

主讲人：中银律师事务所主任 闫鹏和

## 并购与基金的财务规则

主讲人：毕马威会计师事务所专家团队



长按二维码报名

## 目录

<b>摘要：区块链如何重塑金融基础设施</b>	<b>4</b>
<b>争议：Libra 的挑战和机会</b>	<b>8</b>
什么是 Libra：基于联盟链的有资产抵押的稳定币	8
主要政府和国际组织对 Libra 持谨慎态度	11
Libra 的 SWOT 分析	14
优势：稳定币的技术优势+互联网公司的 DNA	14
机会：改善现有的跨境支付、移动支付体验，成为新的储值手段及虚拟世界交易工具	17
劣势：性能瓶颈尚未突破，监管与合规（AML/KYC/CFT）问题亟待解决	21
挑战：Libra 威胁国家货币主权和金融市场稳定	22
<b>探索：中国央行数字货币的路径及影响</b>	<b>23</b>
央行为什么要发行数字货币	23
中国央行数字货币可能的发展路径：部分 M0 替代，双层体系，技术中立	27
央行数字货币对金融市场及货币政策影响	29
央行数字货币对支付行业影响	31
中国央行数字货币推广：前景展望	33
<b>升级：全球监管渐明，区块链进入 3.0 时代</b>	<b>34</b>
区块链发展步入 3.0 时代	35
加密资产的法律地位逐渐明确，监管取向渐趋明朗	37
加密货币市场回暖，比特币市值占比稳步提升	39
稳定币超越比特币成为主要交易手段	41
矿机进入 7nm 时代，在网算力回升，矿池集中度稳定	43
交易所：提供衍生品交易服务成趋势，交易量真实性有待考证	47
加密货币基金：加密资产已成为一种新的另类投资资产	47
衍生品：芝加哥商品交易所等开始上线比特币期货产品	48
ICO 基本失去融资能力，加密资产借贷业务开始兴起	49
<b>展望：区块链如何赋能传统金融</b>	<b>53</b>
习近平总书记明确区块链成为自主创新下一个重要突破口	54
金融企业如何拥抱区块链	55
科技企业把握区块链发展机遇	57
主要区块链框架介绍：Hyperledger、R3	60
主要区块链平台介绍：蚂蚁、腾讯、微众、平安、万向、华为、趣链	62
其他区块链相关企业介绍：恒生电子、航天信息、众安在线	64
联盟链的主要应用场景	65
应用场景#1：跨境支付：当菲佣遇到区块链	66
应用场景#2：交易后清算：区块链增加透明度、缩短清算时间	69
应用场景#3：资产证券化（ABS）：解决“看不清”、“管不住”的问题	70
应用场景#4：电子票据：实现异地看病报销	71
应用场景#4：贸易融资：减少交易处理时间及造假风险	72
应用场景#5：供应链金融：实现核心企业信用的多级穿透	73
应用场景#6：监管科技：共享数据，消除信息孤岛	74
附录：主要区块链相关企业	77
<b>回溯：加密资产技术及产业链全景</b>	<b>78</b>
主要加密资产#1：比特币：第一个得到广泛使用的加密资产	79
主要加密资产#2：以太坊：具有智能合约功能的区块链平台	82
主要加密资产#3：稳定币：价值相对稳定的加密资产	85



产业链#1：矿机、矿工、矿池 .....	89
产业链#2：交易所和托管行 .....	92
主要企业介绍：Coinbase、Circle.....	94
区块链的核心技术及未来技术演进 .....	96

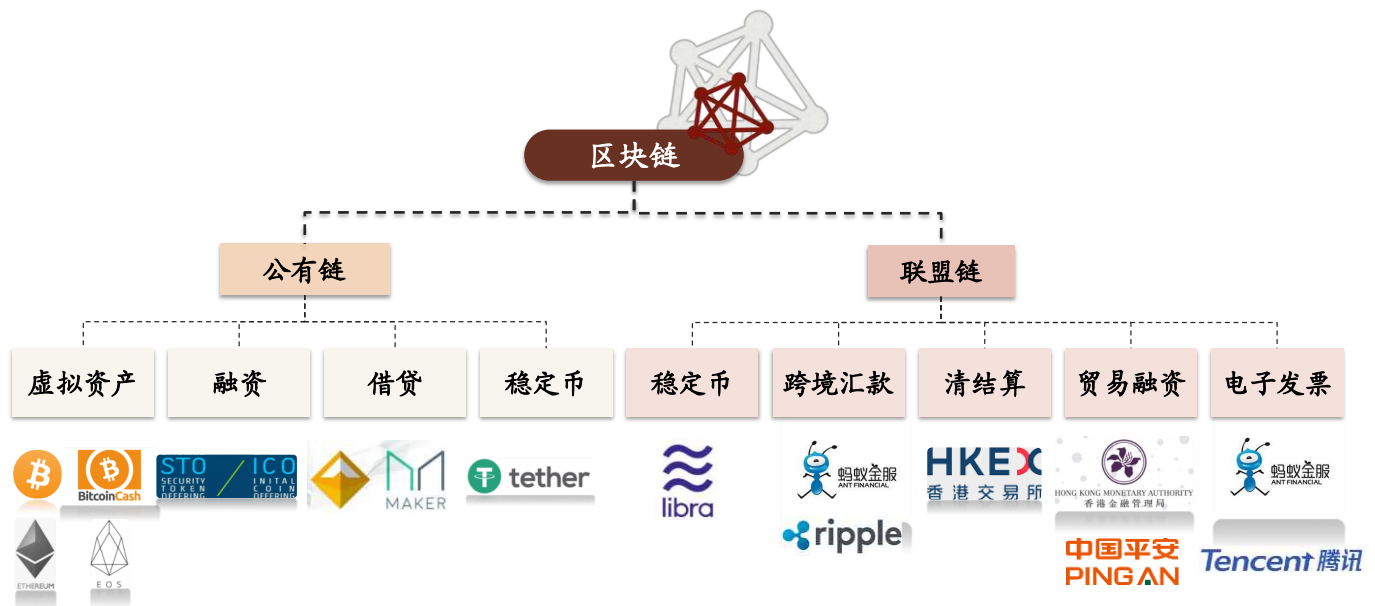


## 摘要：区块链如何重塑金融基础设施

区块链按开发者可以分为由开源社区主导的公有链,及大型 IT 或金融企业主导的联盟链。在这篇报告里,我们沿着以下脉络系统性地分析区块链及数字货币行业:

- **Libra:** 这章我们先介绍 Libra 是一种基于联盟链的有资产抵押的稳定币,并梳理了各个主要政府和国际组织对其态度,最后从优势、劣势、机会、挑战四个方面对 Libra 进行具体剖析。
- **央行数字货币:** 这章我们将介绍全球各国央行发展数字货币的背景,中国央行数字货币可能的发展路径,以及它对金融、IT 行业可能造成的影响。
- **区块链行业:** 这章我们首先回顾了区块链行业技术和应用的发展三阶段,然后梳理各国对加密资产的监管政策变化,最后对加密资产市场的市值、交易量,以及矿机、矿池、交易所、加密资产基金、借贷服务等生态链发展最新动态进行更新。
- **区块链如何赋能传统金融:** 这章我们介绍国内外主要金融企业及科技企业在区块链上的业务布局,并从区块链框架、区块链平台、区块链场景三个层次展开,进行主要案例分析。
- **区块链技术简介:** 这章我们介绍比特币、以太坊、稳定币等主要加密资产,以及矿机、矿工、矿池、交易所和托管行等主要产业链环节的技术原理和最新概况。

图表 1: 区块链的主要用途



资料来源: Wikipedia, Google news, 中金公司研究部

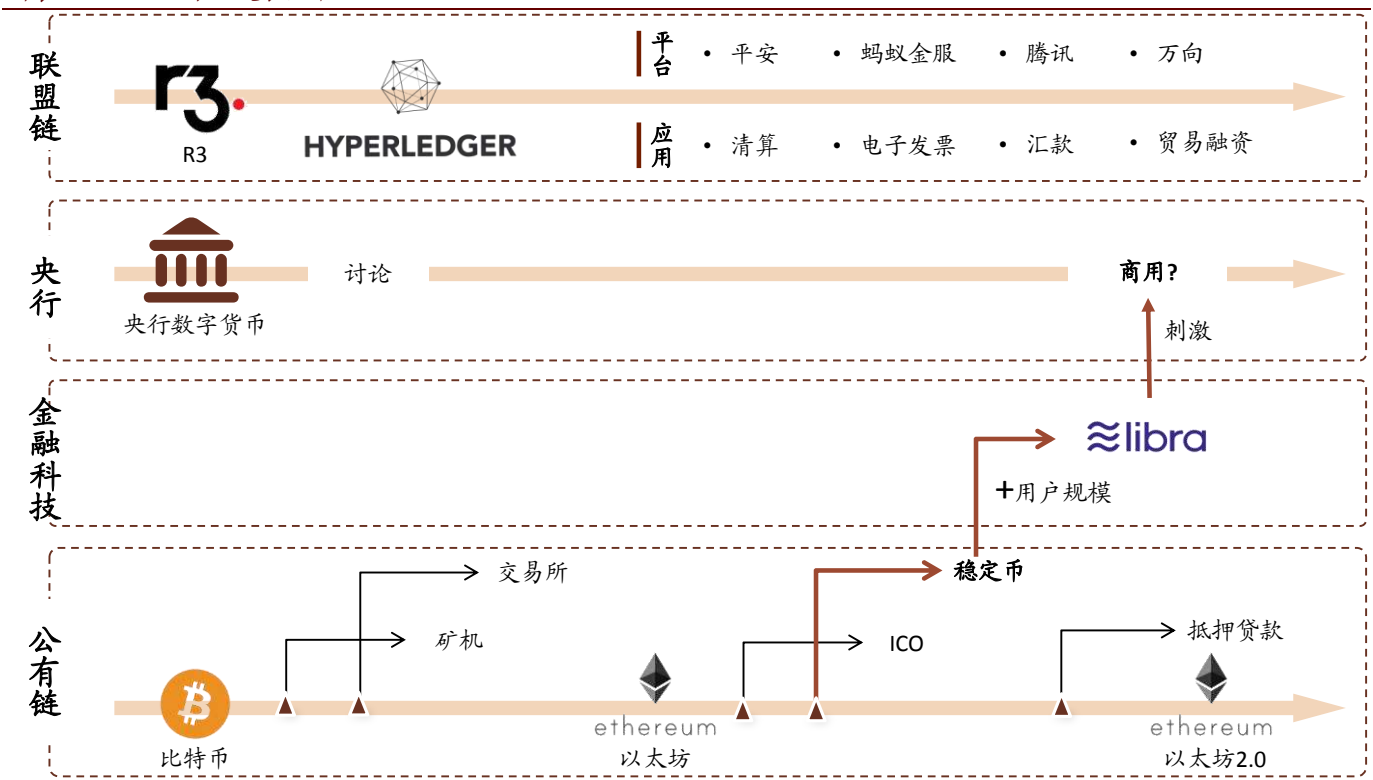




2009年，比特币的出现使人们对区块链技术产生初步概念。随后，在加密资产市场，以太币、瑞波币、EOS等各种加密资产不断涌现，同时矿机、矿池、矿工等产业链环节逐步成型。在种类繁多的加密资产中，稳定币在保留了加密货币清结算流程简单、匿名性强等优点的同时，避免了比特币存在的价格相对法币波动过大的问题，正逐渐成为加密资产行业主要的价值尺度和主流支付工具。

Facebook看到了稳定币巨大的潜力，其将稳定币技术与其庞大用户基础结合而推出的Libra，对各国的货币主权形成了挑战。Libra进一步刺激了全球央行加速数字货币研究和商业落地。近来，区块链技术已经不仅局限于加密资产行业，其在清结算、支付、电子发票、供应链金融、贸易融资等领域开始发挥积极的作用。目前，主要的区块链开源架构有Hyperledger Fabric、R3 Corda等，蚂蚁金服、平安、腾讯、万向等则是主要的区块链平台服务提供商。

图表2：区块链行业发展历程



资料来源：Libra, R3, Hyperledger, 中金公司研究部

图表3：主要货币形式的比较

	法币现金	银行存款	比特币	USDT稳定币	Libra	央行数字货币
价格稳定性	稳定	稳定	波动大	较稳定	稳定	稳定
结算流程	中等	复杂	简单	简单	简单	简单
交易速度	中等	快	慢	中等	中等	快
接受范围	国内	国内	小（币圈）	小（币圈）	全球	国内
信用背书	国家	商业银行	无	资产	资产	国家
匿名性	匿名	实名	匿名	匿名	有条件匿名	有条件匿名

资料来源：IMF, Libra, 比特币白皮书, 中金公司研究部

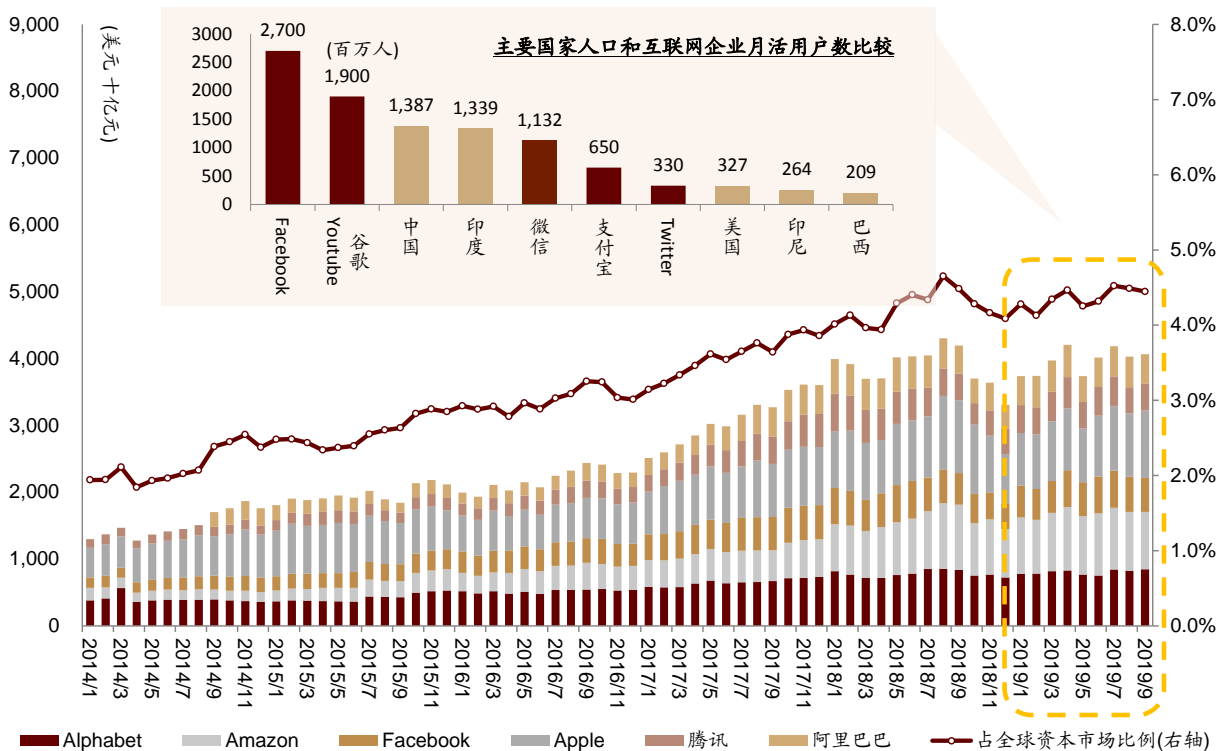


图表 4：区块链有望成为金融行业下一代基础设施的核心技术



资料来源：中金公司研究部

图表 5：全球前 6 大科技公司（GAFA+AT）总市值 2014 年至今上涨 213%，占全球资本市场比例达到 4.5%



资料来源：World Bank, Statista, 中金公司研究部；注：人口数据截止 2018 年，用户数量统计截止 2019 年 6 月



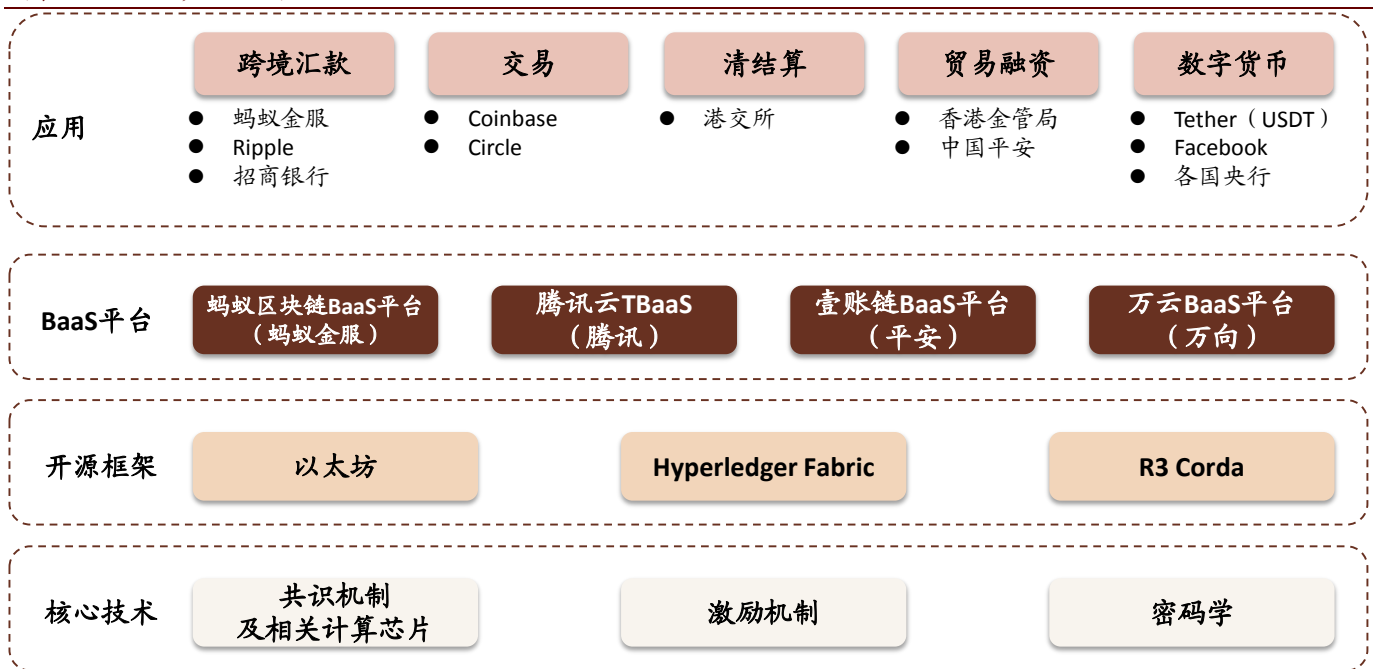
图表 6：各主要国家或地区对加密资产监督态度

	财产	证券		货币 (支付手段)	法币
		发行 (ICO)	交易		
中国	积极	消极	消极	消极	消极
中国香港	积极	中性	中性	中性	消极
美国	积极	积极	积极	中性	消极
英国	积极	中性	中性	中性	消极
日本	积极	中性	积极	积极	消极
韩国	积极	中性	中性	中性	消极
新加坡	积极	积极	积极	中性	消极

 积极
  中性
  消极

资料来源：星瀚金融，中金公司研究部；注：本表格讨论的加密资产不包括央行数字货币

图表 7：区块链产业地图



资料来源：中金公司研究部





## 争议：Libra 的挑战和机会

我们认为 Facebook 发布 Libra 白皮书是科技巨头（Big Techs）进军金融行业的一个里程碑事件。虽然从技术角度，我们不认为 Libra 相比现有的稳定币有明显突破，但 Facebook 超过 27 亿的庞大用户基础与区块链技术相结合，使 Libra 有可能挑战跨境汇款、移动支付等领域的现有格局，成为数字经济时代新的储值手段和价值尺度。目前，Libra 面临许多监管难题，短期内对实体经济影响有限，但其长期影响不可低估。建议投资人关注 FATF 等国际组织对加密资产监管政策的变化，及其对包括 Libra 在内的加密资产行业发展的影响。

**稳定币技术与庞大用户基础结合，挑战各国货币主权。** Facebook 选择了加密货币行业中常用的稳定币作为 Libra 的技术框架。稳定币在保留了加密货币清结算流程简单、匿名性强等优点的同时，避免了比特币存在的价格相对法币波动过大的问题，正逐渐成为加密资产行业主要的价值尺度。稳定币技术与 Facebook 强大的数据分析能力、全球超过 27 亿的庞大用户基础相结合，使 Libra 可能挑战各国的货币主权。具体来讲，我们认为 Libra 可能改变 1) 目前被 SWIFT 所垄断的跨境汇款市场，2) Visa、MasterCard 主导的各国移动支付市场，以及成为 3) 部分汇率波动较大国家新的储值手段，和 4) 数字资产交易中新的价值尺度。

**短期存在许多监管难题需要克服。** 主要国家政府和 G7、G20 等主要国际组织都对 Libra 持谨慎态度。目前，Libra 被指出的问题具体包括：1) Libra 的性能无法达到目前各国支付系统的性能要求；2) Libra 匿名性较强，可能无法满足各国对反洗钱（AML）/了解你的客户（KYC）的要求，容易被犯罪分子利用；3) Libra 计划采用与一篮子法定货币挂钩的抵押模式，该模式可能对各国货币政策和金融系统稳定造成一定冲击。

**Libra 长期影响不可小觑。** Libra 相关的新闻动态每天都在变化，截至 2019/10/11，Visa、MasterCard 等 6 家企业相继宣布退出 Libra 协会，但仍有 Spotify、Uber、Coinbase 等 21 家企业正式加盟 Libra 协会。2019/10/21，据路透社报道<sup>1</sup>，Libra 项目负责人 David Marcus 表示，愿意放弃原先基于一篮子货币的抵押模式，采用和美元、欧元、英镑等一系列法币单独挂钩方式，并承诺在满足美国政府所有监管要求前不在任何国家开始商用。我们认为，虽然目前很难判断 Libra 商业运营的最终形式，但即使只在部分国家商用，其规模也会远超目前加密货币市场，可能对我们的日常生活造成影响。

**关注 FATF 等机构监管政策最新发展。** 我们注意到，在 Facebook 6 月 18 日发布 Libra 白皮书之后 4 天，G20 下属的反洗钱金融行动特别工作组（Financial Action Task Force on Money Laundering, FATF）即发布了全球第一个加密货币监管标准，为其旗下的 37 个成员国提供了监管政策的参考。我们相信 Libra 的问世，正在倒逼各国金融监管当局制定加密资产相关法律法规。

### 什么是 Libra：基于联盟链的有资产抵押的稳定币

**Libra 致力于金融普惠。** 2019/6/18，Facebook 发布了 Libra 白皮书<sup>2</sup>，计划在 2020 年上半年推出基于区块链技术的数字货币 Libra。白皮书称，“Libra 的使命是建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施”。Libra 白皮书中引用世界银行数据称，目前全球仍有 17 亿人无法享用到金融服务，并且各类金融手续费对于低收入人群来说过于昂贵，而 Libra 将致力于金融普惠工作，提供一种去中心化、安全、费用低廉的世界型货币，创造一个高效的全球支付系统。

**子公司 Calibra 提供数字钱包服务。** Facebook 专门设立了子公司 Calibra，其将在 2020 年推出一款支持 Libra 的数字钱包。Calibra 数字钱包将不仅供 Messenger 和 WhatsApp 使用，还会发布独立的 iOS 和 Android 应用。Libra 的运营并非由 Facebook 独家掌控，而是由位于瑞士日内瓦的独立非营利组织 Libra 协会管理，其中 Calibra 是 Libra 协会的初始成员之一。

<sup>1</sup> <https://www.reuters.com/article/us-imf-worldbank-facebook/facebook-open-to-currency-pegged-stablecoins-for-libra-project-idUSKBN1WZONX>

<sup>2</sup> [https://libra.org/zh-CN/wp-content/uploads/sites/17/2019/06/LibraWhitePaper\\_zh\\_CN.pdf](https://libra.org/zh-CN/wp-content/uploads/sites/17/2019/06/LibraWhitePaper_zh_CN.pdf)



图表 8: Libra 协会与 Calibra 数字钱包



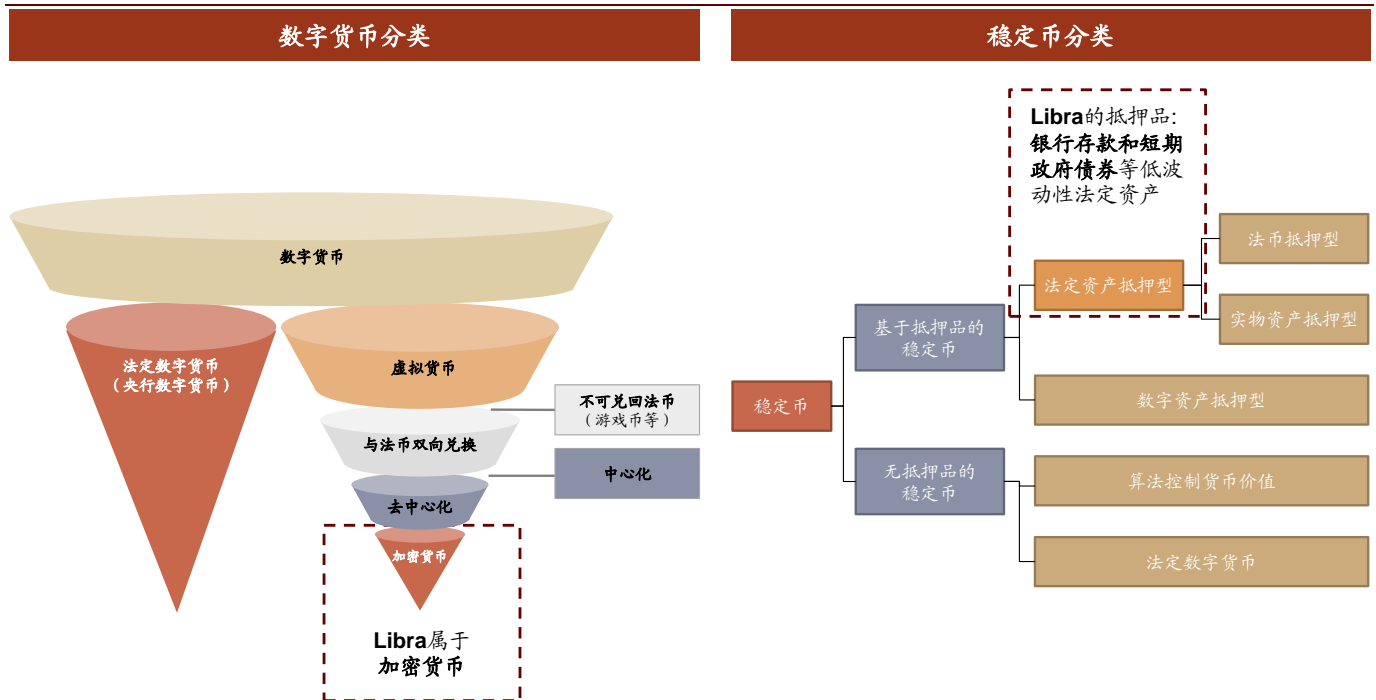
资料来源: Libra, 中金公司研究部

Libra 是一种法定资产抵押型稳定币

**Libra 初始设计为与一篮子货币挂钩。**根据白皮书，Libra 是一种法定资产抵押型稳定币，与“一篮子货币”挂钩，具有“稳定性、低通货膨胀率、全球普遍接受和可互换性”的优良特性。2019/9/21，Facebook 写给欧盟的内部信显示，Libra 计划以美元 50%、欧元 18%、日元 14%、英镑 11%、新加坡元 7%的比例挂钩五种主要货币。



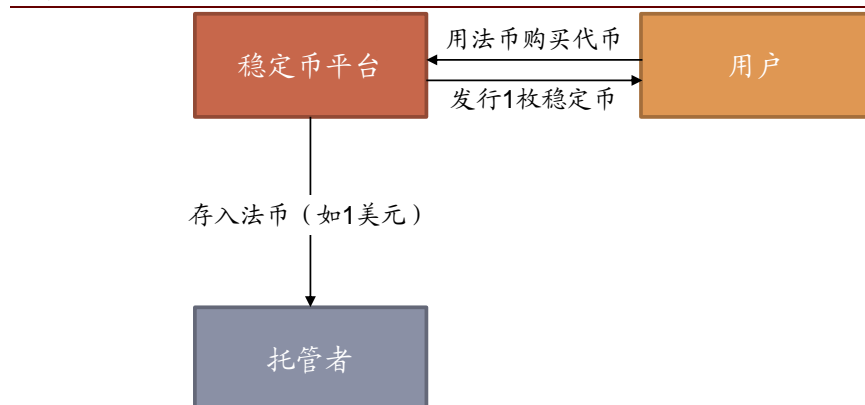
图表 9: Libra 是一种法定资产抵押型稳定币



资料来源: Libra, IMF, 链得得, 中金公司研究部

与比特币 (BTC)、以太币 (ETH) 等加密货币不同, Libra 是有法定资产抵押支持的稳定币。每当创建新的 Libra 货币时, 会有相应价值的一篮子银行存款和短期政府债券等低波动性资产作为储备支持。也不同于 USDT 等锚定美元的稳定币, Libra 并不与单一货币挂钩, 其价值随着储备资产价值的波动而波动。Libra 的储备资产在选择时将会最大限度减少其波动性, 并且其会被分散在全球各地的托管机构持有。我们认为, 这充分保证了 Libra 的稳定性和资产安全性, 使得其具备了价值尺度、贮藏手段等货币基本职能。

图表 10: 法币抵押型稳定币工作原理



资料来源: 哈希派, 中金公司研究部

Libra 可能在监管压力下选择“非合成货币”的方案。2019 年 10 月 5 日, 大型支付服务商 PayPal 宣布退出 Libra 协会; 10 月 11 日, MasterCard、Visa、Stripe、Mercado Pago, 以及大型电商 eBay 集体宣布退出 Libra 协会, 其中 Visa 和 MasterCard 均表示需要等候监管机构的明确回复。2019 年 10 月 21 日, 路透社报道<sup>3</sup>, 在各国监管的质疑以及 Visa、MasterCard 等白皮书中 Libra 协会初始成员退出的压力下, Facebook 做出了让步, 表示方案可以更灵活一些, Libra 币可以和美元、欧元、英镑等一系列法币单独挂钩, 而不是使用合成货币。

<sup>3</sup> <https://www.reuters.com/article/us-imf-worldbank-facebook/facebook-open-to-currency-pegged-stablecoins-for-libra-project-idUSKBN1WZ0NX>



图表 11: Libra 和其他主要支付手段比较

	发行主体	发行机制	发行数量	信用背书	技术路线	流通范围	交易处理速度 (TPS)	匿名性	结算途径
发行	各国政府	中心化	动态调节	国家信用	中心化结算	国家内部	高速	高速	面对面
支付	商业银行	中心化	动态调节	银行信用	中心化结算	国家内部	高速	实名	银行账户体系
用户	-	去中心化	有限, 每四年减半	无	公有链	全球	7	匿名	钱包/交易所
	Tether基金会	中心化	动态调节	资产抵押 (1:1美元)	公有链	全球	7~50	匿名	钱包/交易所
	Libra基金会	中心化	动态调节	资产抵押 (1:1挂钩多种货币、国债)	联盟链	全球	1,000	Libra匿名, 钱包实名	钱包 (Calibra)
	-	-	-	-	中心化结算	特定允许场景	高速	实名	银行账户体系

资料来源: Libra 白皮书, USDT 白皮书, 中金公司研究部

## 主要政府和国际组织对 Libra 持谨慎态度

### 美国关注 Libra 是否符合美国国家利益

美国主要关心三个维度的问题: 1) 数字货币能不能做? 数字货币会不会助力洗钱、恐怖主义问题, 以及数字货币如何纳税; 2) 数字货币是不是美国来做? Libra 是否会影响美元中心地位、美元制裁作用, Libra 协会在瑞士导致美国很难直接监管; 3) 数字货币为什么是 FB 来做? FB 侵犯用户数据隐私是由来已久的问题, 很难获得政府和民众的信任。

北京时间 7/16 晚, 美国国会针对 Facebook 提出的数字货币 Libra 和数据隐私问题召开听证会<sup>4</sup>, Facebook Calibra 团队负责人 David A. Marcus (前 PayPal 总裁) 出席听证会, 并就数据隐私、监管、反洗钱、纳税等美国国会议员关心的问题做了陈述<sup>5</sup>。在听证会上, Marcus 强调在监管问题完全解决前不会急于发行 Libra 货币, 但同时也指出虚拟货币是全球重要的发展趋势, 由 Facebook 牵头推进更加符合美国国家利益。

- ▶ **Libra 协会将会接受瑞士监管。**Libra 协会总部设在日内瓦, 因此将受到瑞士金融市场监管局 (FINMA) 的监督, 并且瑞士联邦数据保护和信息委员会 (FDPIIC) 将成为 Libra 协会的隐私监管机构。Libra 将总部设在瑞士的目的, 不是为了逃避美国监管, 而是为了更好的与国际清算银行 (BIS) 等国际金融机构保持合作。Facebook 认同美国在全球虚拟货币游戏规则制定上应拥有绝对领导地位。
- ▶ **Calibra 接受美国监管。**Calibra 是 Facebook 的 Libra 钱包服务, 可以在 Messenger、WhatsApp 等 Facebook 服务上使用。Calibra 公司是 Facebook 的子公司, 注册地在美国, 接受美国 KYC 和 AML 等监管要求。使用 Calibra 钱包前, 用户需要提交身份证明, 满足 KYC 等要求后方能开户。
- ▶ **Facebook 如何从 Libra 中受益:** Calibra 可以帮助 Facebook 平台上 9000 万中小企业客户更便捷地与超过 20 亿 Facebook 用户直接进行交易。交易量上升, 我们认为会带动 Facebook 的广告收入上升。
- ▶ **如何保证 Calibra 用户隐私:** Calibra 公司掌握所有 Calibra 平台上用户的交易数据, 但 Calibra 与 Facebook 其他服务会完全隔离, Facebook 不会利用 Calibra 数据进行任何商业行为。Facebook 正在努力解决用户隐私保护问题。
- ▶ **Facebook 发展数字货币, 符合美国国家利益。**Marcus 表示, Facebook 不牵头推进类似于 Libra 的数字货币, 也会有来自其他国家的其他公司来做。美国议员认为, 如果不受美国监管的虚拟货币率先得到普及, 将会威胁到美国国家利益。

<sup>4</sup> <https://www.banking.senate.gov/hearings/examining-facebooks-proposed-digital-currency-and-data-privacy-considerations>

<sup>5</sup> <https://www.banking.senate.gov/download/marcus-testimony-7-16-19>





- **Facebook 不对 Libra 拥有控制权。**Facebook 在 100 个成员的 Libra 协会中只拥有一票。Libra 协会创始成员正在商讨其具体的运作机制，细节决定后会正式对外发布。

#### 国际组织普遍持反对态度

- **G7:** 2019/7/18, G7 财长和央行行长会议结束后，法国财长勒梅尔<sup>6</sup>、德国财长肖尔茨<sup>7</sup>等各国财长公开表示，Libra 可能有危害国家主权、数据安全隐患等问题，其需要满足“最高标准监管”。2019/10/13, G7 稳定币工作组发布报告，反对 Libra 在满足监管要求前仓促投入使用，认为 Libra 可能造成包括全球金融体系风险在内的九种风险，需要证明其安全性。
- **G20:** 2019/10/19, G20 财长和央行行长会议上，各方达成共识，认为 Libra 在监管方面“将引发严重风险”；会议结束后，G20 发布了将 Libra 作为监管对象的协议文件，认为 Libra 存在被用于洗钱、用户保护方面的隐忧，明确表示在“对严重风险采取恰当处置”前不允许发行。
- **BIS:** 2019/6/23, 在 Libra 白皮书发布不足一周的时间内，BIS 即表示，Libra 已经超出了传统金融监管领域，对全球银行系统造成了挑战，全球监管机构可能需要“修改”规则，以应对控制“关键数字平台”（例如电子商务网站和社交网络）的参与者带来的结构性变化，并对其中的巨大风险提出警告。
- **FATF:** 2019/6/22, 反洗钱金融行动特别工作组（Financial Action Task Force on Money Laundering, FATF）发布了加密货币监管标准，为其旗下的 37 个成员国提供了监管政策的参考。2019/10/18, FATF 表示 Libra 等稳定币如果大规模推广，可能对全球反洗钱、反恐怖融资工作产生严重影响，威胁全球货币和金融体系的稳定。

#### 主要国家对 Libra 态度普遍消极

- **美国:** 1) 众议院金融服务委员会致函扎克伯格等<sup>8</sup>，要求在获得监管支持之前暂停开发 Libra 项目；2) 美联储表示，不会将 Libra 纳入议程<sup>9</sup>，因为美联储不具备此类权利。
- **中国:** 1) 央行数字货币研究所所长穆长春表示<sup>10</sup>，Libra 创造的是跨境自由流动的可兑换数字货币，离不开央行的支持和监管；2) 清华大学金融研究院院长朱民认为<sup>11</sup>，Libra 对现有金融体系、货币体系，乃至未来储备体系会造成很大冲击。
- **欧盟:** 欧盟委员会正在就 Libra 潜在的垄断行为进行调查<sup>12</sup>。
- **英国:** 1) 英国金融监管机构官员表示<sup>13</sup>，Libra 将给社会和政府带来需要密切审查问题；2) 英国金融行为管理局认为<sup>14</sup>，有关 Libra 信息不足，若无更多信息，Libra 或不被批准；3) 英国央行行长认为<sup>15</sup>，Libra 可大幅降低成本并增加金融包容性。

<sup>6</sup> <https://www.reuters.com/article/us-g7-economy-france/france-says-g7-focused-on-containing-risks-of-facebooks-libra-idUSKCN1UC0FT>

<sup>7</sup> <https://www.reuters.com/article/us-facebook-cryptocurrency-germany/germanys-scholz-sounds-alarm-on-cryptocurrencies-such-as-facebooks-libra-idUSKCN1UB199>

<sup>8</sup> <https://www.theguardian.com/technology/2019/jul/03/libra-us-congress-asks-facebook-pause-development-cryptocurrency>

<sup>9</sup> <https://www.bloomberg.com/opinion/articles/2019-07-18/federal-reserve-has-no-interest-in-regulating-facebook-s-libra>

<sup>10</sup> <http://database.caixin.com/2019-07-06/101436323.html>

<sup>11</sup> [https://www.thepaper.cn/newsDetail\\_forward\\_3810608](https://www.thepaper.cn/newsDetail_forward_3810608)

<sup>12</sup> <https://www.bloomberg.com/news/articles/2019-08-20/facebook-s-libra-currency-gets-european-union-antitrust-scrutiny>

<sup>13</sup> <https://www.reuters.com/article/us-crypto-currencies-britain-regulator/facebook-s-libra-cryptocurrency-needs-deep-thought-and-detail-uk-regulator-idUSKCN1TX1ZU>

<sup>14</sup> <https://www.reuters.com/article/us-facebook-cryptocurrency-britain/facebook-met-uk-officials-three-times-before-libra-announcement-idUSKBN1W3270>

<sup>15</sup> <https://www.theguardian.com/business/2019/aug/23/mark-carney-dollar-dominant-replaced-digital-currency>



- ▶ **俄罗斯：**1)俄罗斯杜马金融委员会主席表示<sup>16</sup>，俄罗斯将禁止在现阶段使用 Facebook 加密货币作为支付工具；2) 俄罗斯财政部副部长表示<sup>17</sup>，俄罗斯财政部不会对 Libra 发布任何特别规定，没有人会禁止。
- ▶ **印度：**据印度经济时报报道<sup>18</sup>，Libra 预计将不会在印度使用，因为该国目前规定不允许利用银行网络交易加密货币。

<sup>16</sup> <https://finance.yahoo.com/news/russia-not-legalize-facebook-cryptocurrency-183900773.html>

<sup>17</sup> <https://news.yahoo.com/russia-won-t-ban-facebook-150014101.html>

<sup>18</sup> <https://economictimes.indiatimes.com/tech/internet/facebook-may-abort-libra-launch-in-india/articleshow/69867426.cms>

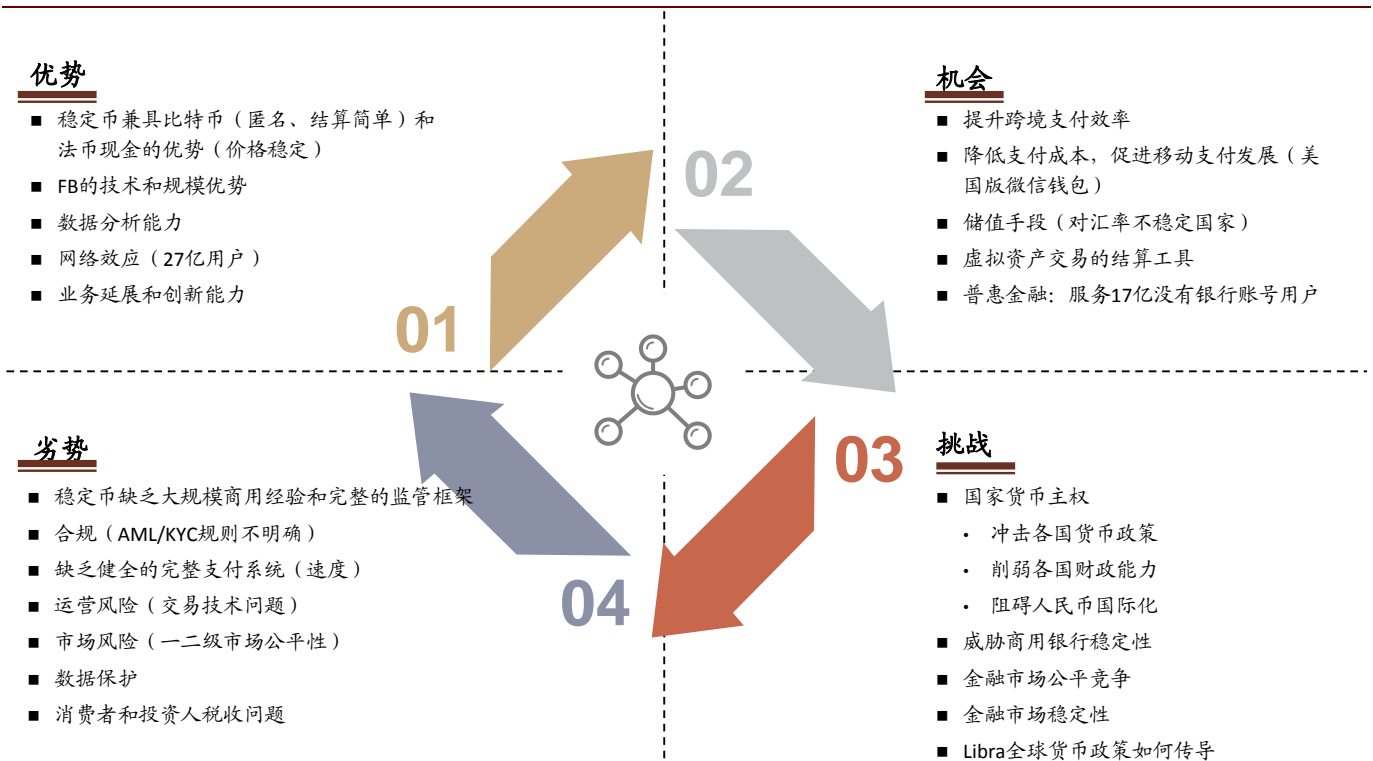




## Libra 的 SWOT 分析

我们从优势、劣势、机会、挑战四个方面，对 Libra 进行分析：

图表 12: Libra 的 SWOT 分析



资料来源：BIS, Libra, 中金公司研究部

### 优势：稳定币的技术优势+互联网公司的 DNA

#### 优势#1：稳定币兼具加密货币和传统货币的优势，有望成为高效支付工具

##### 加密货币作为交易媒介具有诸多优势：

- ▶ **降低交易和发行成本：**由于免去了诸多交易中间环节，使得整体支付成本降低；同时，省去了货币制造和流通的成本。
- ▶ **提高安全性：**去中心化的分布式账本以及共识机制的设计，使得账本信息很难丢失或被黑客攻击篡改。
- ▶ **提高效率：**交易确认即完成结算与清算，且智能合约的引入进一步提高效率。
- ▶ **匿名交易：**加密货币的匿名特性，对匿名交易需求者有一定的吸引力。

**加密货币价格波动剧烈，难具价值尺度与价值贮藏功能。**一般来说，加密货币没有政府信用背书或资产抵押（稳定币除外），其价格完全依赖于市场供需情况。自 2009 年发行以来，比特币的价格波动就十分剧烈。这就使得加密货币很难具备货币的价值尺度、价值贮藏功能。此外，加密货币还存在以下问题，使其难以真正成为通行货币：

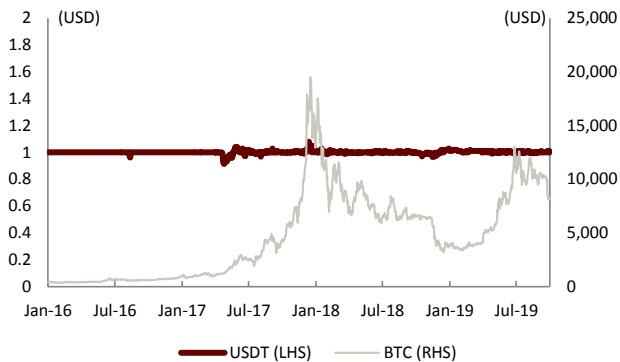
- ▶ 安全性问题，被攻击或错误转账后不可撤回交易；
- ▶ 匿名交易的特性可能被用作非法用途，如洗钱等；
- ▶ PoW 共识机制能耗高、吞吐量低，为了去中心化牺牲了效率；



- ▶ 虽然交易者匿名，但交易记录全网可见；
- ▶ 发行总量一定，通货紧缩货币难以适应经济发展需要。

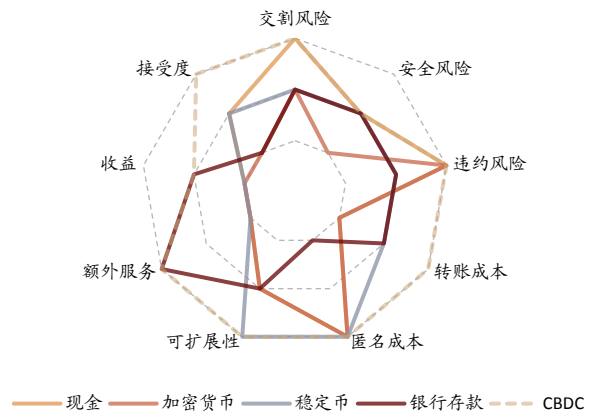
**稳定币兼具加密货币和传统货币的优势。**Libra 选择了稳定币的方案，相比比特币、以太币等公有链加密货币，稳定币直接解决了价格相对法定资产波动大的关键问题。不仅如此，稳定币保留了加密货币 1) 低违约风险、2) 低成本高效率的清算、3) 匿名性的优点，同时又拥有类似于传统货币的 1) 接受度高、2) 转账成本较低、3) 安全合规性较高的优点。

图表 13: 比特币和 USDT 稳定币价格变化



资料来源: CoinMarketCap, 中金公司研究部

图表 14: 主要货币形式的比较



资料来源: IMF, 中金公司研究部; 注: 对于每项指标, 从内到外代表吸引力低、中、高

#### 优势#2: FB 具备规模和技术优势, 能够实现稳定币规模化部署

**FB 拥有处理大规模数据的技术储备。**全球化的数字货币并非易事, 首先需要解决交易吞吐量 (TPS) 的问题。目前, 日交易量最大的稳定币 USDT 主要基于比特币 Omni 协议、以及以太坊 ERC20 协议, TPS 分别仅为 7 笔/秒、30 笔/秒, 而目前 Visa 和 MasterCard 的 TPS 都在四位数的水平。央行数字货币研究所所长穆长春表示<sup>19</sup>, 央行法定数字货币 DC/EP 的 TPS 需达到 30 万笔/秒。

因此, 全球化的数字货币基于现有的通用技术不太现实, 需要强大的研发团队重新开发。此外, 随着 TPS 的提高, 以及用户数量的增长, 数字货币系统需要处理和存储海量数据, 这对研发团队的数据处理和存储技术开发能力提出了挑战。Facebook 作为全球最大的互联网公司之一, 在全球各地拥有 27 亿用户, 建设并拥有多个大型数据中心, 对于大规模数据的处理和存储拥有强大的技术储备, 这是其能够推出 Libra 的用户和重要技术基础。

根据 BIS 关于稳定币的报告<sup>20</sup>, Facebook 等大型互联网公司发展支付业务时, 在数据分析能力 (Data Analysis)、网络效应 (Network effects) 以及业务创新能力 (Activities) 三方面具有优势:

- ▶ **数据分析能力 (Data analytics):** Facebook、Google 等大型互联网公司的营业收入主要来自于广告业务, 2018 年 Facebook、Google 的广告业务收入分别为 550 亿美元、1,163 亿美元, 分别占其占总收入的 98.5%、85.0%。为了提高广告变现能力, 这些公司积累了深厚的数据分析能力。当其将数据分析能力用于支付业务的风控等领域时, 相比传统金融机构具有明显优势。
- ▶ **网络效应 (Network effects):** 目前, Facebook 旗下的各类产品 (Facebook、Messenger、Instagram、WhatsApp) 合计月活跃用户数高达 27 亿, 远超中国、印度等主要国家

<sup>19</sup> [http://www.xinhuanet.com/money/2019-08/12/c\\_1210238504.htm](http://www.xinhuanet.com/money/2019-08/12/c_1210238504.htm)

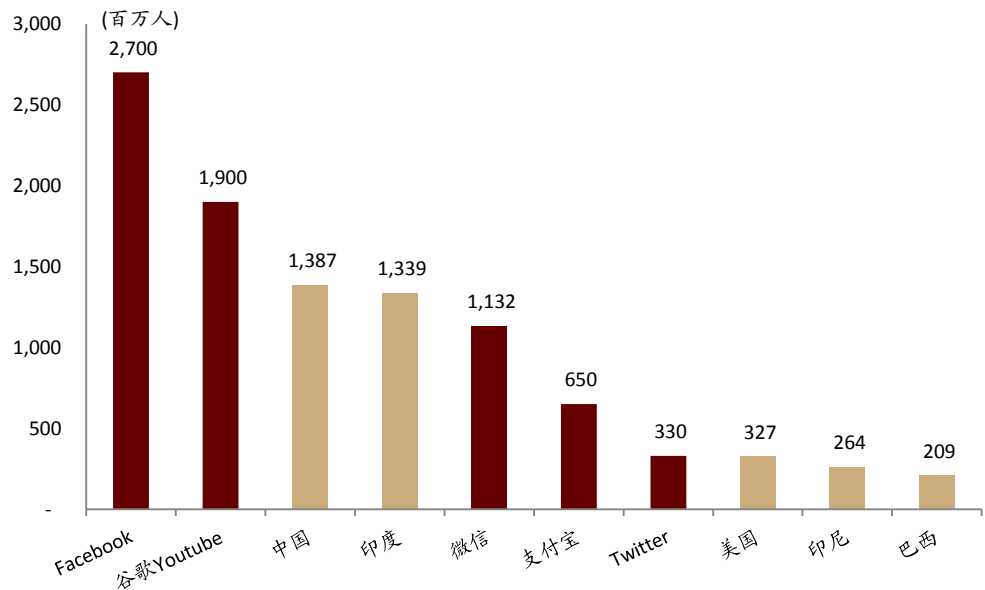
<sup>20</sup> <https://www.bis.org/cpmi/publ/d187.pdf>



人口总数。FB 的用户可以便捷地接入 FB 下属子公司推出的 Calibra 钱包,使用支付、转账等功能,我们认为这可能冲击现有的支付体系。据腾讯财报披露,截至 2Q18 微信支付的在微信(含 WeChat)用户中的渗透率达到 76%,这是微信支付在微信全球用户中的渗透率,如果仅考虑中国用户,则渗透率会更高。

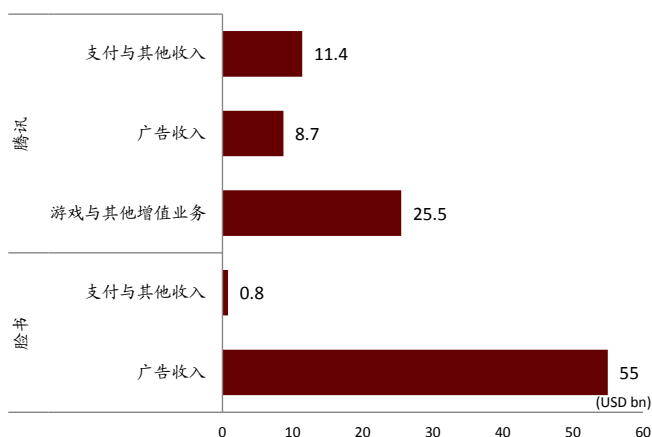
- **业务创新能力 (Activities):** 互联网公司具有较强的业务创新能力,在发展新兴业务时拥有较强的业务扩张能力和变现能力。以微信支付为例,2013 年 8 月微信支付正式上线,截至 2Q18 时月活即达到 8 亿。据艾瑞咨询数据,1Q19 中国第三方移动支付市场,支付宝、微信支付分别占据 53.8%、39.9%的份额,而银联的份额仅 0.4%。

图表 15: 主要国家人口和互联网企业月活用户数比较



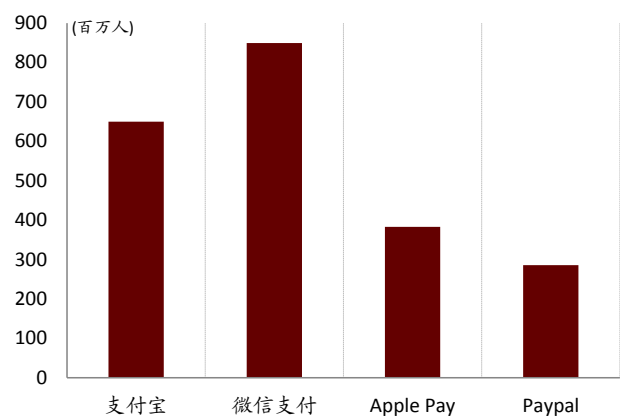
资料来源: World Bank, Statista, 中金公司研究部; 注: 人口数据截止 2018 年, 用户数量统计截止 2019 年 6 月

图表 16: 腾讯和 Facebook 2018 年收入结构比较



资料来源: 腾讯、Facebook 公司年报, 中金公司研究部

图表 17: 主要科技公司支付工具月活用户数



资料来源: Statista, 中金公司研究部; 注: 数据截止 2019 年 6 月

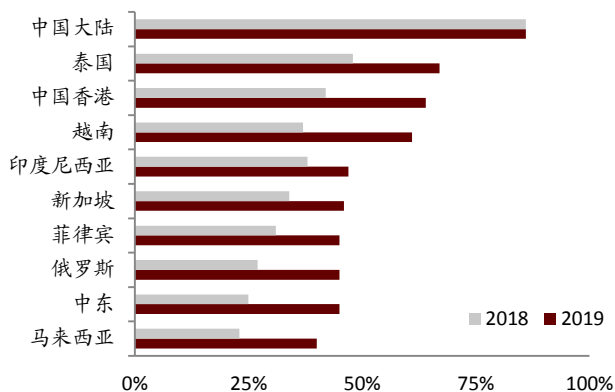


机会：改善现有的跨境支付、移动支付体验，成为新的储值手段及虚拟世界交易工具

机会#1：降低支付成本，促进移动支付发展（美国版微信钱包）

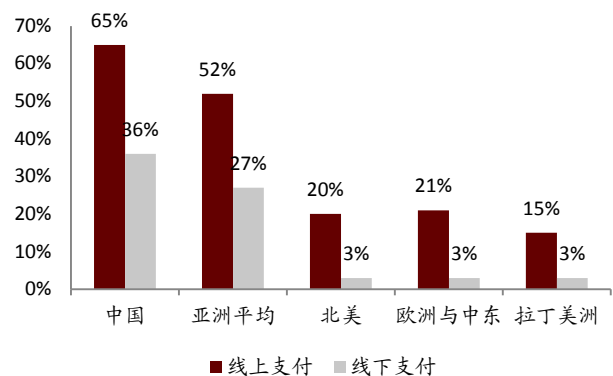
北美欧洲移动支付较为落后，FB 机会较大。北美欧洲地区移动支付还未普及，信用卡仍是其民众的主要支付方式。据普华永道统计，全球移动支付普及率前十大地区中，8 个来自亚太。Facebook Messenger 现有的转账功能，仅能从一方的借记卡，转入另一方的借记卡，且需要 1~3 个工作日。Facebook 北美和欧洲的客户占比达到 26%，考虑到北美欧洲及部分亚太地区移动支付普及率较低，我们认为如果政策和法律允许，基于 Libra 的移动支付会快速普及。

图表 18：全球移动支付前十的地区



资料来源：PwC，中金公司研究部

图表 19：2018 年电子钱包（支付软件）使用率



资料来源：WorldPay，中金公司研究部

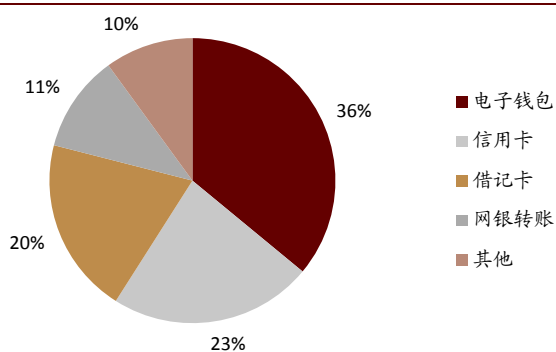
图表 20：主要第三方支付在各国落地情况

		使用范围	
		境内	全球
支付基础设施	依附	Venmo	Apple Pay, Google Pay, PayPal, Calibra
	独立	支付宝, 微信, M-Pesa	Libra

资料来源：BIS，中金公司研究部

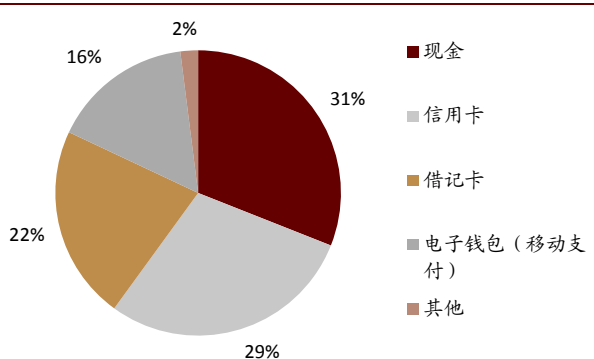
根据麦肯锡数据，2018 年全球支付市场规模达到 US\$2tn，预计到 2022 年将达到 US\$3tn。根据支付的方法不同，可以分为线上支付和线下支付：线上支付手段包括电子钱包、信用卡、借记卡、网银转账，而线下支付主要包括现金、信用卡、借记卡等。

图表 21：2018 年全球线上支付方法占比



资料来源：WorldPay，中金公司研究部

图表 22：2018 年全球线下支付方法占比

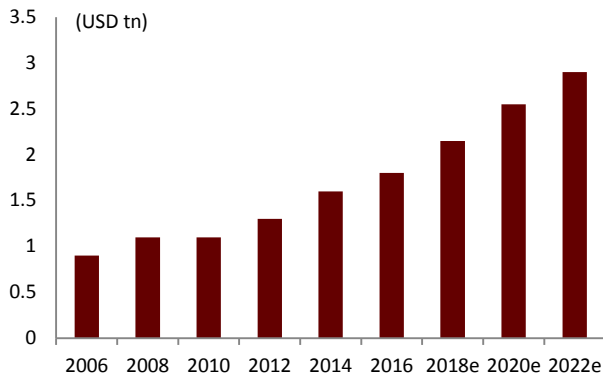


资料来源：WorldPay，中金公司研究部



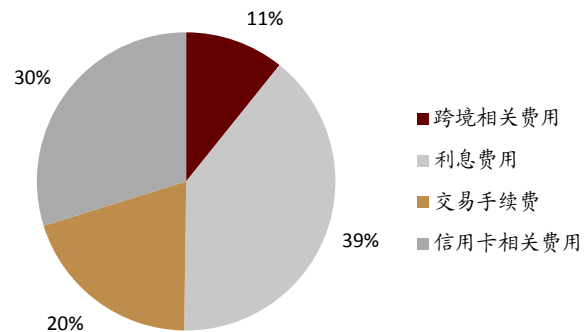
完成支付过程中产生的中间费用是支付公司盈利的方法。根据支付的收入来源不同，可以分为跨境支付费用、利息费用、交易手续费以及信用卡相关费用。

图表 23: 全球支付收入与预测



资料来源：麦肯锡，中金公司研究部

图表 24: 2018 年全球支付相关收入分类



资料来源：麦肯锡，中金公司研究部

图表 25: 当前支付行业参与方盈利模式

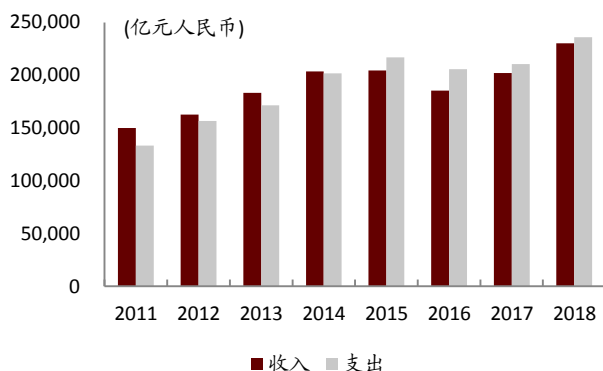
支付产业参与方	盈利模式	收益形式
银行卡组织	银行卡收单跨行交易手续费分润；ATM跨行取款收费；非金融机构支付清算；银行卡发行品牌服务（类似冠名）等	银行卡收单分润、网络服务费、品牌服务费等
商业银行	银行卡交易发卡行手续费分润；银行卡交易收单行手续费分润；电子银行转账等手续费；快捷支付手续费分润等	发卡行分润、收单行分润；转账手续费等
第三方支付	电商平台支付解决方案提供；商户交易佣金；沉淀资金利息收入（中国由于网联已取消）等	平台接入费、交易手续费；技术服务费、沉淀资金利息等

资料来源：易观，中金公司研究部

## 机会#2: 降低跨境支付成本，提升效率

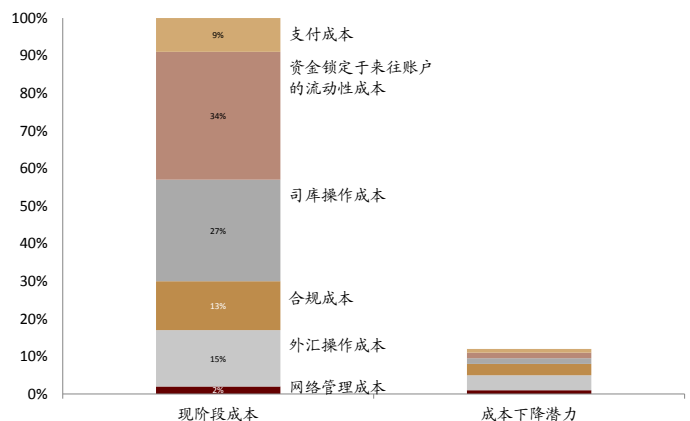
据埃森哲统计，全球每年通过银行进行的跨境支付规模达 25 万亿-30 万亿美元，全年总交易次数 100 亿-150 亿笔，每笔交易需缴纳费用 30-40 美元；IBM 预计，2020 年全球跨境支付市场规模将达 2 万亿美元。据国家外汇管理局统计，2018 年我国银行代客涉外收付款（以人民币计价）收入和支出分别达 230,186 亿元、235,986 亿元。目前跨境支付主要通过 SWIFT 进行。SWIFT 系统不仅耗时（2-3 工作日）、交易环节多、费用高（平均 30-40 美元/笔）、系统陈旧存在安全隐患，还存在所有交易数据受美国政府监控等问题。

图表 26: 2011-2018 我国银行代客涉外收付款金额



资料来源：国家外汇管理局，中金公司研究部

图表 27: 跨境支付成本分析（2013-2015 平均）



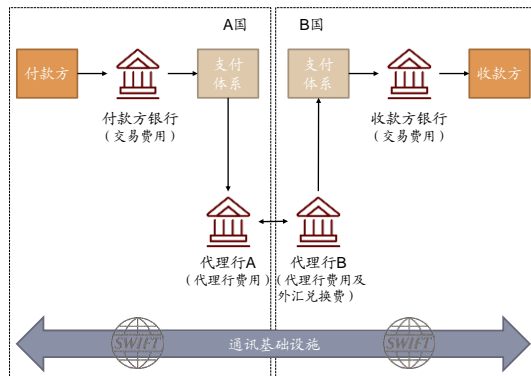
资料来源：麦肯锡，万向，中金公司研究部



根据麦肯锡 2016 年和万向区块链首席经济学家邹传伟的研究，跨境支付的主要成本来自代理银行账户的流动性成本(34%，这些资金可以用于收益更高的地方)、司库造作(27%)、外汇操作(15%)和合规(13%)。通过区块链技术，理论上可以大幅压缩 90-95% 的成本。

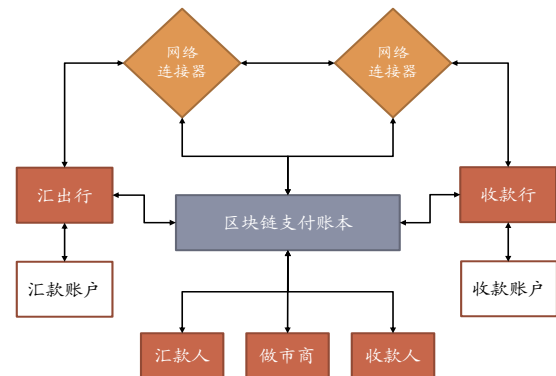
目前，支付宝、微信、以及跨境支付 SWIFT 等现有的电子支付系统，基本上全部采用银行账簿式的电子支付，而 Libra 采用了以联盟链为基础的去中心化支付系统。相比传统跨境支付存在的流程冗长、手续费高、支付账本复杂等问题，区块链跨境支付具有快速、低费率、高效率等优点。我们认为，Libra 将挑战现有支付系统，最先直接与现有跨境支付系统竞争，例如 SWIFT、Visa、PayPal 等。我们看到，SWIFT、Ripple 等跨境支付机构正积极应对挑战，例如 SWIFT 联合 R3 推出 SWIFT+code，Ripple 收购速汇金等。

图表 28: SWIFT 汇款模式



资料来源: Aite Group, 中金公司研究部

图表 29: 区块链跨境支付架构



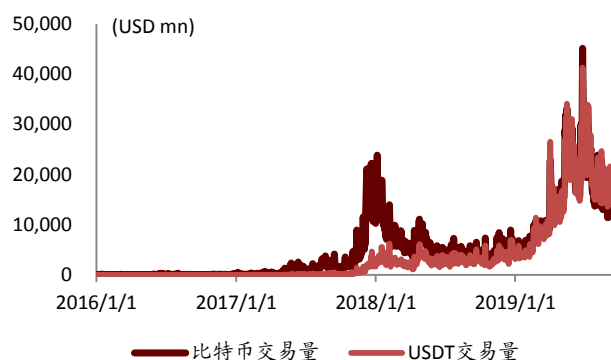
资料来源: 信通院, 中金公司研究部

另一方面在本地支付市场,我们认为 Libra 也将会以其高效率、低成本的优势,颠覆网银、支付宝、微信支付等以本地市场为主的支付系统;或者可能对这些本地支付服务扩张全球跨境支付业务版图形成阻碍。

### 机会#3: 虚拟资产交易的结算工具

目前,稳定币的交易已成为加密货币市场最活跃的交易。据 CoinMarketCap 数据,近三个月平均日交易量 189.2 亿美元,超过比特币的 169.3 亿美元,是交易量最大的加密货币。从比特币的交易对占比来看, CryptoCompare 数据显示, USDT-BTC 交易对占比特币总交易量的比例超过 75%。

图表 30: USDT 日交易量 vs. BTC 日交易量

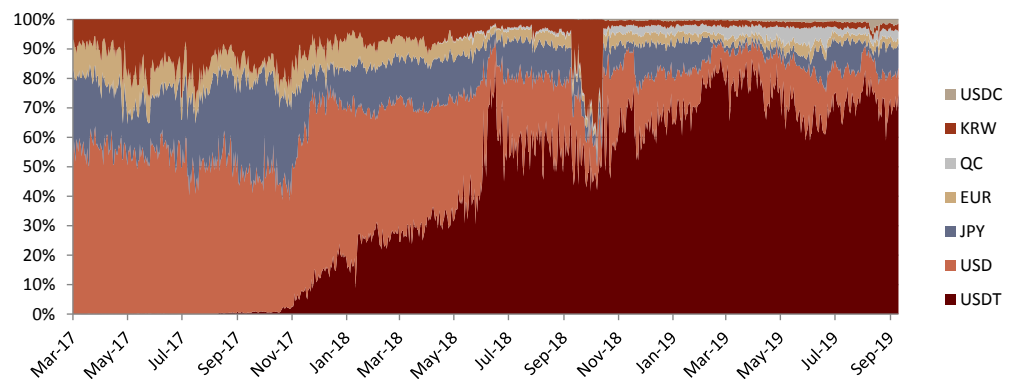


资料来源: CryptoCompare, 中金公司研究部





图表 31: 比特币交易对分布占比



资料来源: CryptoCompare, 中金公司研究部

我们认为, 稳定币流行的主要原因包括:

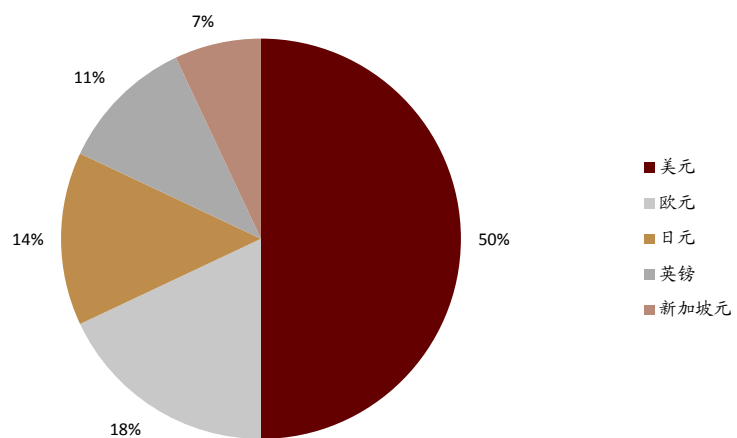
- ▶ 结算便捷性 (不用每笔交易和美元结算);
- ▶ 价值稳定性 (相对法定资产价值稳定, 加密货币市场波动大时可用作避险);
- ▶ 匿名性 (继承加密货币的优点);
- ▶ 广为接受的中间媒介 (作为法币-加密货币交换、不同加密货币互换的中间货币)。

Libra 同样拥有以上稳定币的优点, 考虑到其庞大的潜在用户量, 可能成为新的主要虚拟资产交易结算工具。

#### 机会#4: 新的储值手段 (对汇率不稳定国家民众)

Libra 的发行会抵押相应的法币, 这与 USDT 等稳定币较为相似。不同之处在于 USDT 以美元单一货币作为抵押资产, 而 Libra 会在考虑汇率、交易量等多种因素的基础上用一篮子货币和短期政府债券作为抵押资产。根据德国出版物《Der Spiegel》在今年 9 月的一份报告, Facebook 在回应德国立法委员 Fabio De Masi 问题的一封信中提出, Libra 储备资产的分配方案为: 美元 50%、欧元 18%、日元 14%、英镑 11% 和新加坡元 7%。

图表 32: Libra 抵押货币篮子权重分布

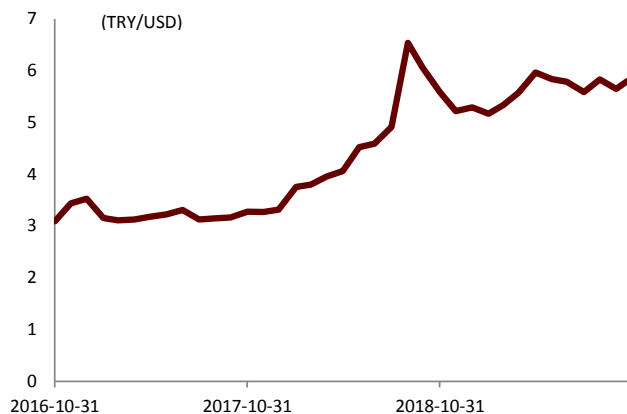


资料来源: Facebook, 中金公司研究部



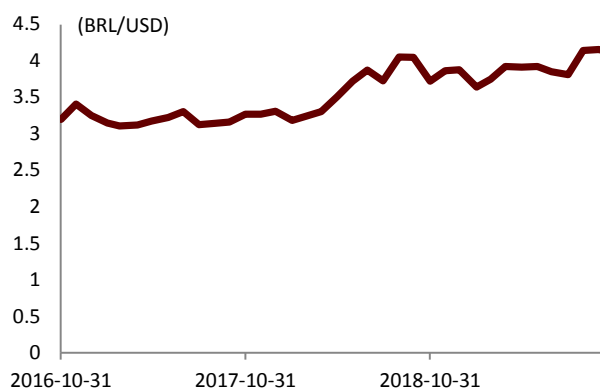
近年来，土耳其、阿根廷、印度尼西亚、巴西等新兴市场国家的货币遭遇危机，进而引发了更严重的金融风险。我们认为，对于汇率不稳定国家的民众，Libra 有可能成为良好的储值手段。相比美元，挂钩一篮子货币的 Libra 价值稳定性更高；相比黄金，Libra 更方便获取、存储与使用。

图表 33: 土耳其里拉对美元汇率变化



资料来源：万得资讯，中金公司研究部

图表 34: 巴西雷亚尔对美元汇率变化



资料来源：万得资讯，中金公司研究部

### 劣势：性能瓶颈尚未突破，监管与合规（AML/KYC/CFT）问题亟待解决

#### 劣势#1: 缺乏健全的支付系统

Libra 采用分布式记账的技术，由于是中心化发行，与比特币等完全去中心化区块链网络不同。比特币由于完全去中心化，因此每秒只能处理 7 笔交易，而 Libra 的设计每秒处理交易笔数达到 1000 笔。但随着 Libra 的逐渐普及，1000 笔/秒的处理速度远远不够，这也是 Libra 技术上未来需要克服的难题之一。

#### 劣势#2: 合规问题（AML/KYC/CFT）

由于针对 Libra 的完善监管体制尚未建立，加上数字货币流动迅速的特点，容易被犯罪分子用来进行非法交易或者洗钱。现在各个国家针对反洗钱有一套各自的监管，将来针对 Libra 洗钱和非法交易的问题，各国金融监管机构还需要出台统一政策，这也为监管增加了难度和风险。为了减轻这些风险，稳定币和其他属于稳定币生态系统的实体的提供者应遵守 AML / CFT 的最高国际标准，并应对大规模毁灭性武器扩散的融资。

反洗钱金融行动工作组（Financial Action Task Force on Money Laundering, FATF）是 AML / CFT 的国际标准制定机构，其为打击国家、金融机构以及指定的非金融企业和专业的洗钱，恐怖分子融资，扩散融资和其他非法融资提供了强大且全面的框架。2018 年 10 月，FATF 表示，其规定适用于涉及虚拟资产和虚拟资产服务提供商的金融活动，并且于 2019 年 6 月更新指南和增加了解释性注释。

Libra 协会正在考虑采用阶梯式（分层式）KYC 方法，Libra 协会中的非营利组织（如小额信贷平台 Kiva）可能起到关键作用。近期，Kiva 与塞拉利昂政府合作探索阶梯式 KYC，使用生物识别技术分配数字钱包。就 KYC 要求而言，可以根据账户的美元金额或 Libra 币金额，采取阶梯式方法，在较低财务门槛时壁垒较低，而在较高财务门槛时壁垒较高。



**劣势#3：消费者保护**

Libra 通过 Calibra 钱包进行交易。Calibra 掌握大量用户交易数据，这些数据的使用、以及与第三方共享的过程中，很难做到不侵犯用户的数据隐私。Facebook 作为 Libra 的发起人和 Libra 协会成员企业之一，侵犯用户数据隐私是由来已久的问题，因此 Libra 在消费者数据隐私问题上很难获得政府和民众的信任。

**挑战：Libra 威胁国家货币主权和金融市场稳定**

从货币角度看，Libra 属于有备抵资产的稳定币，其币值基于美元、欧元、日元、英镑和新加坡元一篮子主要货币的组合，因此具有货币基本的价值尺度、交易媒介、价值贮藏等货币的基本特征。我们认为，Libra 的这些特点使其具备了超主权货币的雏形。

图表 35: Libra 与美元对比

	美元	Libra
使用群体	全球货币，占全球交易40%	以Facebook全球27亿用户为基础
抵押资产	石油，且有美国政府背书	一篮子货币
流通场景	全球货币，占全球交易40%	初期围绕Libra协会成员的场景，之后逐步拓展
利息收入	有	无

资料来源：Libra 白皮书，中金公司研究部

Libra 有广泛的用户基础和较为稳定的价格，在一些主权货币较弱、汇率波动较大的国家，有可能形成对主权货币的替代。对于主权国家的财政政策也会形成影响。

- ▶ Libra 在一些主权货币较强的国家可能流通相对缓慢，但由于其支付场景丰富、币值相对稳定的特点，在一些主权货币弱的国家可能会快速流通甚至取代主权货币，从而给这些国家的货币政策、财政政策甚至国家经济造成非常大的冲击。
- ▶ 根据 Facebook 回应德国立法委员 Fabio De Masi 问题的一封信，Libra 储备资产的分配方案为：美元 50%，欧元 18%、日元 14%、英镑 11%和新加坡元 7%，人民币不在其中。SDR(特别提款权)纳入人民币之后，人民币占全球货币储备从 2016 年的 0.84% 上升至 2019 年的 1.84%。若 Libra 未将人民币纳入抵押货币，我们认为人民币国际化将会受阻。
- ▶ 目前，全球结算中美元占比 40%左右，而 Libra 抵押资产的一篮子货币中，美元占比可能达到 50%，其实是对美元全球地位的加强。由于 Facebook 对 Libra 的影响力较大，我们认为，不排除未来可能美元在 Libra 抵押资产中的占比会逐步增大。Facebook 总裁扎克伯格在今年 6 月美国国会听证会上直言 Libra 需要也期待和美国政府的合作。



## 探索：中国央行数字货币的路径及影响

央行数字货币（CBDC，Central Bank Digital Currency）过去几年一直是各国央行和国际清算银行（BIS）等国际金融监管当局讨论的一个重要议题。Facebook 计划发布 Libra，引发了其是否会对国家的货币主权造成挑战的讨论。包括我国央行在内的全球央行出现了加速数字货币的研究和商业落地的趋势。在这篇报告中，我们介绍全球各国央行发展数字货币的背景、中国央行数字货币可能的发展路径，以及它对金融、IT 行业可能造成的影响。

**全球央行加快数字货币研究，应对科技巨头的挑战。**随着智能手机、电子商务等快速发展，现金在发达国家日常生活中的占比不断下降。与此同时，全球仍然有 10 亿以上消费者没有银行账户。对发达国家来说，CBDC 是央行在无现金时代，为消费者提供的广覆盖、跨平台的支付手段；对新兴市场国家来说，CBDC 是普惠金融的一部分，可望大幅加速金融服务渗透率。Facebook 拟推出 Libra 的计划，也反映目前有许多支付需求没有被充分满足，正在倒逼各国央行加速数字货币研究工作。

**我国央行数字货币的发展方向：M0 替代，双层运营体系。**根据央行副行长范一飞和央行数字货币研究所所长穆长春最近的发言<sup>21</sup>，我国央行数字货币（DC/EP）未来的发展主要定位在部分定位 M0 替代，会采用“央行-商业银行/其他运营机构-货币使用者”的双发放和运营层体系。央行数字货币暂未预设技术路线，但提出最低满足每秒 30 万笔交易的要求。在匿名性上，央行数字货币实现可控匿名，即只对央行披露交易数据。

**央行数字货币不改变当前电子支付体系，关注新 DC/EP 运营资质机构等发展机会。**我们认为央行 DC/EP 的发行对当前电子支付体系的冲击较小，但可能加速商业银行、支付机构等商业机构之间的分化。获得 DC/EP 运营资质的机构直接实现货币化的空间可能有限，但随着场景应用的增加，有望为其带来客户活跃度和粘性的增加。金融 IT 服务商有望收获银行机构改造升级核心交易系统带来的商业机会。我们认为，DC/EP 推出后对政府用户有望最快产生作用，并逐步影响到企业用户；相对而言，由于现有支付体系效率很高，个人用户对 DC/EP 的使用可能进展最慢。

**央行数字货币对金融市场和货币政策的影响。**1) 数字货币的运用或帮助央行对货币供应量及其结构、流通速度、货币乘数、时空分布等方面的测算更为精确，从而提升货币政策操作的准确性。2) 助推人民币国际化：由于央行数字货币采用账户松耦合形式、减少了交易环节对账户的依赖度，由此带来和现金一样的流通性和可控匿名属性，有助于推动人民币在更广范围内的流通使用。3) 打击金融犯罪：在可控匿名机制下，央行可以对掌握的交易数据进行分析以实现审慎管理和反洗钱、反逃税、反恐怖融资等监管目标，提升金融监管效率。

### 央行为什么要发行数字货币

央行数字货币（CBDC，Central Bank Digital Currency）是最近几年各国央行和国际货币基金组织（IMF）、国际清算银行（BIS）等国际金融监管当局讨论的一个重要议题。和传统现金相比，CBDC 具有使用方便、便于监管、具备功能扩展性等优势。

<sup>21</sup> <https://www.yicai.com/news/5395409.html>; [http://www.xinhuanet.com/finance/2019-08/13/c\\_1210239239.htm](http://www.xinhuanet.com/finance/2019-08/13/c_1210239239.htm)



图表 36: 不同形态的货币特点比较

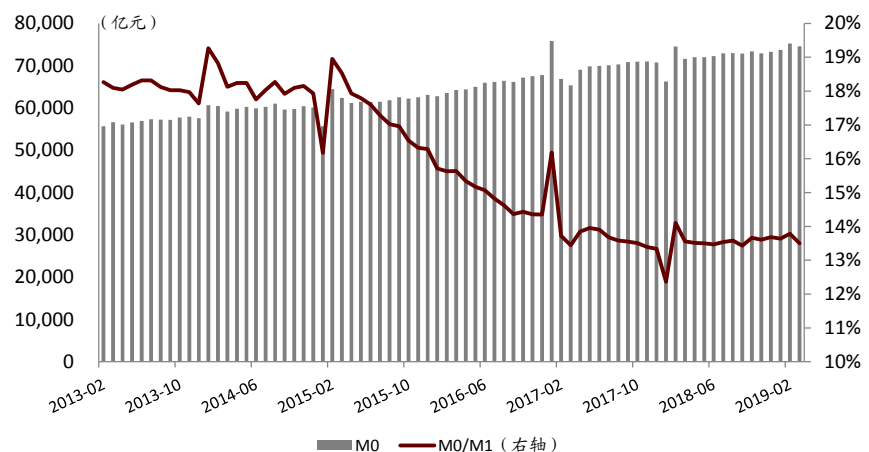
	实物现金	电子货币		央行数字货币
		银行存款	第三方支付机构账户余额	
数字化形态	否	是		是
分发机构	商业银行	商业银行	第三方支付机构	商业银行、其他机构
债务人	央行负债	商业银行负债	央行负债（备付金100%集中缴存下）	央行负债
准备金制度	无	法定及超额存款准备金	100%缴纳备付金	运营机构100%缴纳备付金
匿名性	完全匿名	实名	可控匿名	可控匿名
信用背书	国家信用	银行信用	支付机构信用	国家信用
货币供应量层次	M0	M1-M0或M2-M0	M2-M0	M0

资料来源：中国人民银行，中金公司研究部

综合 IMF、BIS、英国央行、瑞典央行等机构的研究，我们认为 CBDC 主要可能为中央银行带来以下作用：

- **适应无现金社会的发展，打破支付壁垒。**随着智能手机、电子商务、第三方支付等技术的发展，现金在日常生活中的占比不断下降。例如，中国现金（M0）占 M1 的比例从 2013 年 18% 下降到 2018 年的 13%，瑞典等北欧国家的 M0/M1 比例甚至已经降到了 5% 以下。目前，中国线下非现金支付主要通过微信钱包、支付宝等第三方机构，或者银联信用卡等进行。由于 CBDC 具有高于商业银行和第三方支付机构的信用等级，我们认为 CBDC 可能会打破支付行业的行业垄断。

图表 37: 中国 M0 与 M0/M1 变化趋势

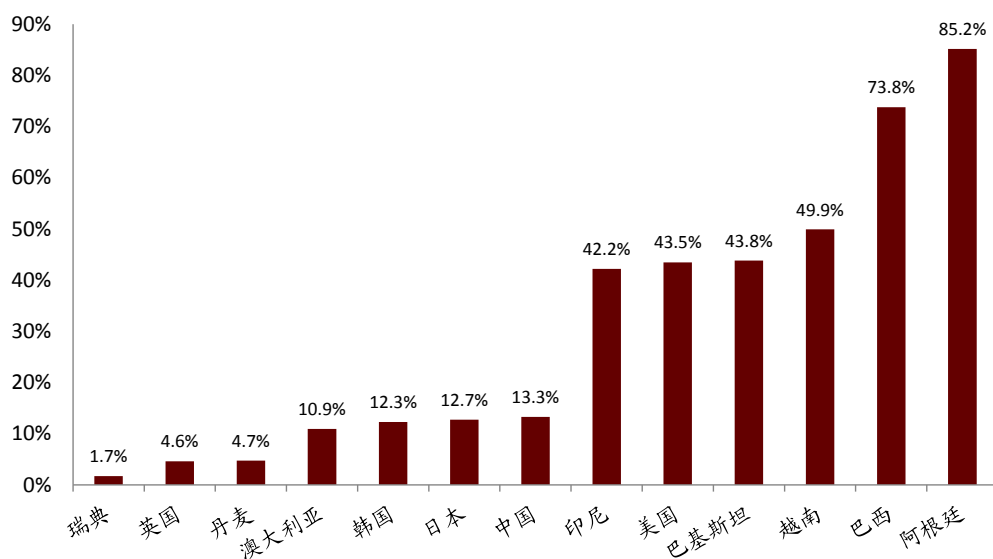


资料来源：万得资讯，中金公司研究部





图表 38: 各国 M0/M1 比较



资料来源：万得资讯，彭博资讯，中金公司研究部；注：数据截至 2019 年 9 月

- ▶ **应对“私人货币”挑战。**传统现金存在印刷或铸造、流通、回收成本，同时 ATM 建设、维持也会产生费用。此外，现金交易本身就存在监管难的问题。以比特币、Libra 为代表的非官方货币的广泛使用会进一步扩大监管盲区，发行央行数字货币有助于央行加强金融监管，打击经济犯罪。
- ▶ **扩大普惠金融。**在金融基础设施较差的发展中国家，相比于建设更多银行网点及配套设施，发展央行数字货币可以用较低成本提高银行与金融体系普及率。边远地区、贫困地区建设银行网点存在成本收益问题，而央行数字货币可以依托于手机等个人终端解决大多数需求。
- ▶ **实时精准定位，创新货币政策。**央行数字货币能够实现对每单位货币的精准追踪，从而使得央行有对货币流通和经济运行更准确的把握，有助于增强货币政策前瞻性、及时性；未来通过智能合约能够实现精准定向货币发行，提高货币政策传导的准确性。

值得注意的是，Libra 推出后，各国央行明显增加了对央行数字货币的关注度。通过调研，我们注意到中国、瑞典等国家在央行数字货币的讨论上走在比较前列。

- ▶ **中国：**中国央行 2017 年成立数字货币研究所推进 DC/EP 研发，目前已经确定施行央行-商业银行/其他金融机构-使用者的两层架构，在积极利用现有成熟的电子支付基础设施的同时，对区块链技术持开放态度；
- ▶ **瑞典：**瑞典央行针对本国无现金趋势推动电子克朗计划，技术上同时采用两种并行的方案，计划于 2021 年正式部署；
- ▶ **英国、加拿大与新加坡**央行开展了用于跨境支付的央行间通用 CBDC 的研究，提出了超级代理银行、世界通用央行数字货币等概念；
- ▶ **英国、法国：**8 月英国央行行长 Mark Carney 在美联储年度研讨会上强调了当前以美元为主导的国际货币体系风险，并勾勒出一一种替代方案：推出由多种国家货币支持的通用数字货币，这一方案得到了法国经济与财政大臣 Bruno Le Maire 的支持；
- ▶ **美国：**美联储曾在 2017 年对央行数字货币提出质疑，但 2019 年下半年以来已有多名议员和美联储官员表态应重启联储数字货币 Fedcoin 研究；
- ▶ **日本：**日本目前没有 CBDC 计划。但日央行总裁黑田东彦表示，未来央行将“关注加密资产作为支付、结算手段能否获得信任，对金融结算体系产生哪些影响”。





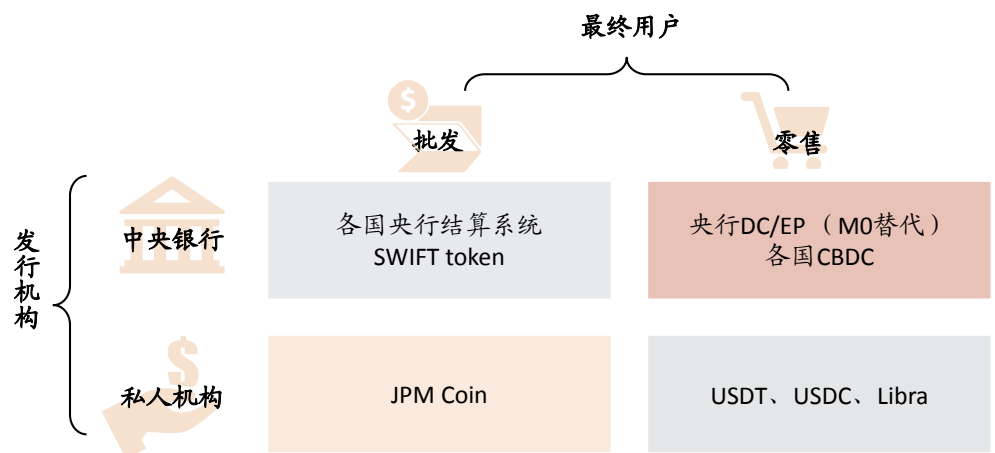
图表 39: 各国央行在央行数字货币研究方面的进展

国家	项目名称	提出时间	预计落地时间	进展状况	作用	技术路线
美国	美联储数字货币 Fedcoin	2015	未披露	考虑重启	现金替代	可能采用区块链技术，两种货币投送途径：1) 央行拥有特殊签名，能够在区块上添加代币；2) 向网络中预分配所有货币两种并行方案：1) 基于账户-类似银行存款；2) 基于价值-类似于充值型钱包。基于账户的不提供匿名性，基于价值的不提供利息。
瑞典	电子克朗 eKrona	2017	2021	2019年开始测试技术原型	现金替代	1) 利用现有电子支付技术；2) 考虑区块链技术，加载智能合约
中国	中国法定数字货币 DC/EP	2014	未披露	稳步推进	现金替代	1) 各国设立国内唯一的跨境支付代理机构取代传统的代理银行机制；2) 采用一种跨国央行数字货币，使用分布式账本作为其底层技术
英国/加拿大/新加坡	银行间跨境支付与结算升级项目	2018	未披露	处于论证阶段	跨境支付	

资料来源：美联储，中国人民银行，英格兰银行，加拿大银行，新加坡金管局，Sveriges Riksbank，中金公司研究部

根据万向首席经济学家邹传伟的报告《区块链与金融基础设施——兼论 Facebook Libra》，数字货币按照最终用户类型和发行机构，主要可以分为以下四种类型：

图表 40: 数字货币的主要类型



资料来源：邹传伟《区块链与金融基础设施——兼论 Facebook Libra》(2019)，BIS，中金公司研究部

- ▶ **金融机构发行的面向一般客户的稳定币：**目前主要包括 USDT、USDC 等基于比特币和以太坊的稳定币。Libra 也属于这一类型。
- ▶ **金融机构发行的面向其它机构客户的稳定币：**目前 JPMorgan 发行的用于金融机构之间美元清算的 JPM Coin 属于这一类别。
- ▶ **央行发行的面向一般客户的数字货币：**我国央行等规划中的 CBDC 属于这个类别。
- ▶ **央行发行的面向机构客户的数字货币：**主要目的是提高金融机构之间的清结算效率。



### 中国央行数字货币可能的发展路径：部分 M0 替代，双层体系，技术中立

央行在 2018 年 3 月的全国货币金银工作电视电话会议上提出，货币金银部门要扎实推进央行数字货币研发。2019 年 8 月，央行在下半年工作电视会议中再次提出要加快推进我国法定数字货币（DC/EP）研发步伐。我们认为，随着 Libra 在 2019 年 6 月的提出，央行数字货币的研发和推出节奏加快。

图表 41：央行 2014 年以来数字货币研发进展

时间	事件
2014	央行成立发行法定数字货币专门研究小组，论证央行发行法定数字货币的可行性。
2015	发布发行数字货币的系列研究报告，并完成发行法定数字货币原型的两轮修订。
2016	召开数字货币研讨会，进一步明确了央行发行数字货币的战略目标，确定将要发行法定数字货币。 确定使用数字票据交易平台作为法定数字货币的试点应用场景，并启动了数字票据交易平台的封闭开发工作。 公布直属单位 2017 年度工作人员招聘公告，其中留个岗位是央行数字货币研究所储备技术人才。
2017	成功测试了基于区块链的数字票据交易平台，根据央行的安排部署，上海票据交易所会同数字货币研究所，组织中钞信用卡公司、工商银行、中国银行、浦发银行和杭州银行共同开展基于区块链技术的数字票据交易平台建设相关工作。2018 年 2 月，上海票据交易所数字票据交易平台实验性生产系统成功上线试运行。 央行数字货币研究所在北京德胜国际中心 C 座 9 楼正式挂牌成立，依据招聘信息，数字研究所主要的研究内容包括数字货币法律研究、区块链开发、芯片设计等。
2018	召开 2018 年全国货币金银工作电视电话会议，会议称央行货币金银部门稳步推进了央行数字货币研发，2018 年要扎实推进央行数字货币研发。 数字货币研究所全资控股的深圳金融科技服务有限公司成立，其经营范围为“金融科技相关技术开发、技术咨询、技术转让、技术服务；金融科技相关系统建设与运行维护。” 数字货币研究所（南京）应用示范基地正式揭牌成立。该中心由南京市人民政府、南京大学、江苏银行、中国央行南京分行、中国央行数字货币研究所合作共建。 《法定数字货币模型与参考架构设计》项目在银行科技发展奖评审领导小组会议上获得一等奖
2019	召开 2019 年下半年工作电视会议，会议要求加快推进我国法定数字货币（DC/EP）研发步伐，跟踪研究国内外虚拟货币发展趋势，继续加强互联网金融风险整治。

资料来源：中国人民银行官网，新华社，中金公司研究部

#### 定位：替代部分 M0

根据范一飞和穆长春的表述，央行数字货币主要注重对 M0 的替代，主要原因是：

- ▶ M1、M2 已经实现电子化和数字化，替代 M1 和 M2 意义不大；
- ▶ 当前的 M0 容易匿名伪造，存在洗钱、恐怖融资风险；
- ▶ 现有的银行卡和互联网支付与银行账户绑定，无法实现匿名支付。

#### 运营体系：“央行-商业银行/其他运营机构-货币使用者”的双层体系

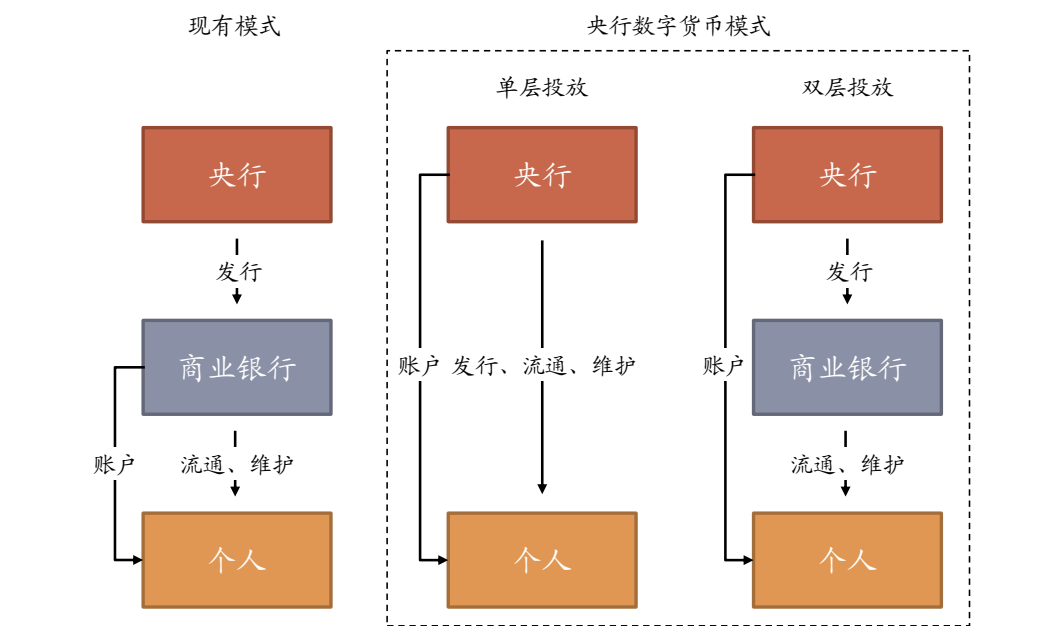
中国央行数字货币采用和人民币相同的运营体系，即“央行-商业银行/其他运营机构-货币使用者”的双层体系：商业银行及其他运营机构向央行缴纳 100% 准备金兑换数字货币，再兑换给货币使用者。双层体系的优势：

- ▶ 单层运营体系会对央行的运营带来很大挑战，可能会降低使用体验，提高风险；
- ▶ 单层运营体系可能对商业银行存款产生挤出效应。

与现行人民币体系不同的是，在“发行-分发”体系中，负责分发的不仅仅是商业银行，还有其他运营机构。这意味着除传统商业银行外，符合要求、技术实力高的市场化机构可能参与到数字货币的分发过程中。



图表 42: 现行货币模式与单、双层架构的央行数字货币模式对比



资料来源：央行数字货币研究所，中金公司研究部

#### 技术路线：考虑区块链技术，可加载智能合约

央行数字货币的货币属性要求其在高并发的使用场景能够正常使用（比如每年双 11 中，每秒交易笔数可达到 30 万笔/秒），而当前比特币仅为 7 笔/秒，ETH 为 30-50 笔/秒。Facebook 的 Libra 设计为 1000 笔/秒，这些都无法满足央行数字货币的要求。因此，央行数字货币暂未预设技术路线，可以考虑现在大部分加密资产的区块链技术，也可以采用现在电子支付技术基础上演变的新技术。

对于区块链技术中常见的可以自动执行协议的智能合约功能，范一飞提出，有利于货币职能的智能合约可以考虑，但对超出货币职能的智能合约应持审慎态度。

#### 账户与匿名性：松耦合；仅对央行披露交易数据

范一飞指出，中国央行数字货币应基于账户松耦合形式，以降低交易环节对账户的依赖。央行数字货币采用中心化运营，在松耦合模式下，交易数据每日由运营机构异步传输至央行，在保证央行掌握必要的数据以确保审慎管理和反洗钱监管的同时，也减轻了运营机构的系统负担。在匿名性上，央行数字货币将实现可控匿名，只有央行可以获得全部交易数据。



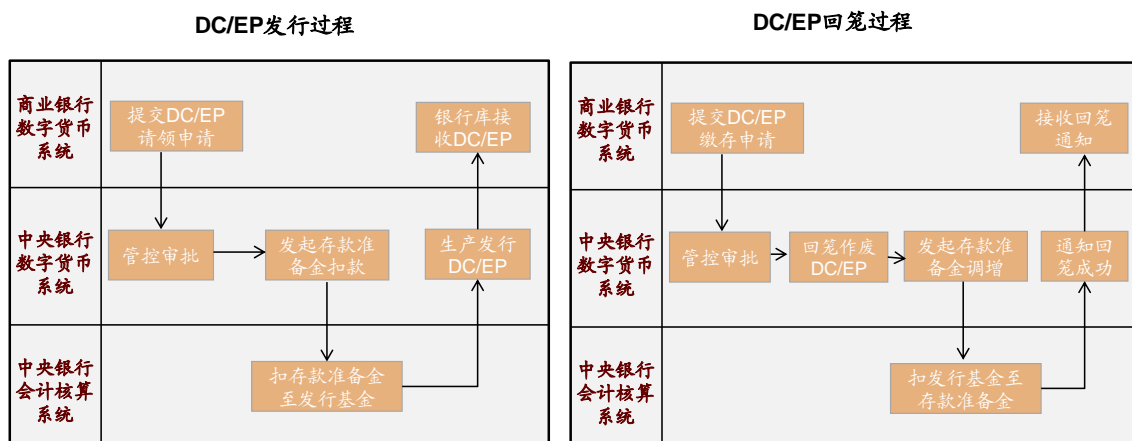
## 央行数字货币对金融市场及货币政策影响

我们认为短期 DC/EP 对现行金融市场运行及货币政策传导的影响较小，中长期若能利用数字货币的可追踪性和可编程性等特质，能够加大政策调控的颗粒度，有望实现货币政策实时传导、货币精准定向投放、逆周期调控等创新功能。

央行数字货币现阶段注重对 M0 的替代，并坚持中心化的管理模式和双层运营体系，因此其发行与回笼机制与纸币较为相似。通过“央行—商业银行（或其他商业机构）”的双层投放模式，由央行发行货币到商业机构的银行库（在此过程中商业机构需要向央行全额、100%缴纳准备金；但运送方式变为电子传送、保存仓库变成云空间），再由商业机构直接面向个人/企业提供数字货币服务。这样的安排有利于充分利用商业机构现有资源、人才、技术等优势，减少不必要的 IT 系统重复建设，并可以兼顾效率和安全、避免风险集中在单一机构以及避免“金融脱媒”。

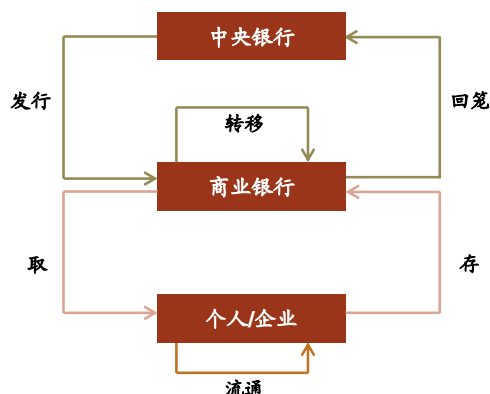
未改变现有的流通货币的债权债务关系、货币投放体系以及二元账户结构，保持央行中心管理的地位、不影响现有货币政策传导机制。与纸币相类似，数字货币作为央行负债并拥有央行的信用担保、具备无限法偿性。此外，央行数字货币不计息的机制下，不会对银行存款产生挤出效应、不会影响货币创造功能。考虑到数字货币使得存款（M2-M0）向现金（M0）的转化更加便捷，为防止恐慌事件下的金融顺周期效应（如挤兑带来的流动性危机），央行可以设置适当机制加以限制（如设置 DC/EP 的交易和余额上限）。

图表 43：数字货币的投放及回笼过程示意图



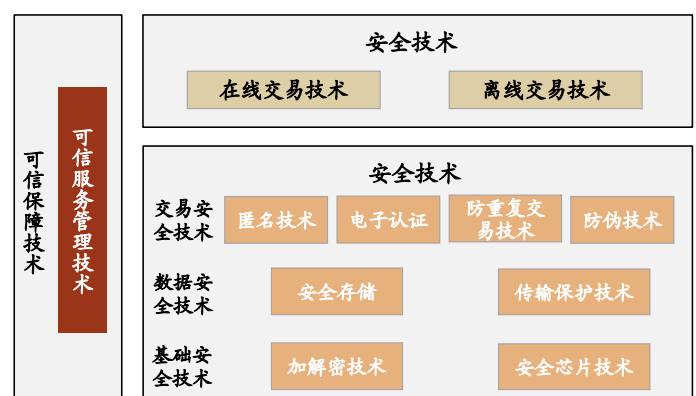
资料来源：姚前《中央银行数字货币原型系统实验研究》（2018），中金公司研究部

图表 44：数字货币二元模式运行框架



资料来源：姚前《中央银行数字货币原型系统实验研究》（2018），中金公司研究部

图表 45：数字货币应用的核心技术



资料来源：清华大学国家金融研究院，中金公司研究部

数字货币的运用不仅在于采用“数字化的铸币”方式降低了现金的存储、发行和处理成本，长远来看或对我国金融基础设施、货币政策实施、金融稳定性维护、人民币国际化

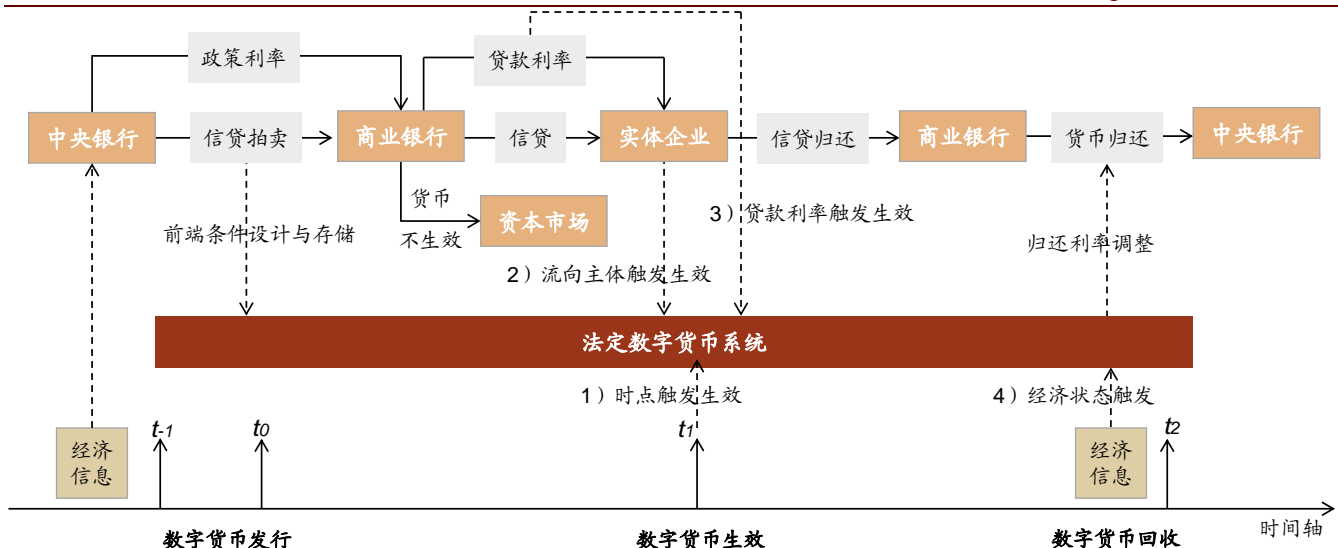


战略发挥积极作用：

- **提升货币政策的前瞻性、及时性、有效性：**数字货币的运用或帮助央行对货币供应量及其结构、流通速度、货币乘数、时空分布等方面的测算更为精确，从而提升货币政策操作的准确性。中证登总经理姚前在《法定数字货币对现行货币体制的优化及其发行设计》所提出的，数字货币的可追踪性可以帮助央行追踪和监控数字货币投放后的流转信息、获取货币全息信息，而其可编程性则可通过“前瞻条件触发（Forward Contingent）”设计，让法定货币很好地解决传导机制不畅、逆周期调控困难、货币“脱实向虚”、政策沟通不足等传统货币政策困境。此外，随着数字货币逐渐对现金的替代，也带来了负利率政策运用的可能——纸币作为一种零利率储蓄，当负利率政策实施时将存款提现为纸币，造成“零利率下限”的政策困扰，而通过对数字货币收取类似“保管费”的形式则等同负利率的效果。
- **助推人民币国际化战略：**由于央行数字货币采用账户松耦合形式、减少了交易环节对账户的依赖度，由此带来和现金一样的流通性和可控匿名属性，有助于推动人民币在更广范围内的流通使用。同时，相较于其他投资属性更重的加密资产，DC/EP以我国国家信用作为保证、价值保持相对稳定而能够得到广泛接纳。展望未来，若其他国家及国际组织亦发行数字货币，全球网络范围内的法定数字货币自由兑换亦可能出现，而数字货币点对点交易的特质有助于解决传统跨境汇兑链条长、到账慢、效率低等问题。
- **有助于通过大数据分析打击金融犯罪：**在可控匿名机制下，央行可以对掌握的交易数据进行分析以实现审慎管理和反洗钱、反逃税、反恐怖融资等监管目标，提升金融监管效率。

数字货币发行流通体系的建立亦对监管提出的挑战，需要央行不断优化总量控制、修正管理机制：1）货币结构变化、货币乘数增大——数字货币对现金的替代，使得M0向银行存款的转换更加便捷，或带来银行资金来源的扩大和货币扩张能力的提升；2）支付和交易效率的提升带来货币流通速度的加快；3）货币与其他金融资产之间的转化成本进一步降低，提高了货币需求对利率的敏感性。

图表 46：基于数字货币的可追踪性和可编程性进行货币投放的“前瞻条件触发（Forward Contingent）”设计



资料来源：姚前《法定数字货币对现行货币体制的优化及其发行设计》（2018），中金公司研究部





### 央行数字货币对支付行业影响

我们认为央行DC/EP的发行对当前电子支付体系的冲击较小，更多体现为商业银行/支付机构等商业机构之间的分化加剧，推动行业集中度的进一步提升，以及为相关金融IT企业带来业务机会。

- ▶ **运营主体猜想：**为提升央行数字货币的便捷性和服务可得性、增强公众使用意愿、结合移动支付成熟的基础设施，我们预计进行数字货币代理投放的运营主体除了商业银行之外，亦可能包括头部第三方支付机构（如支付宝、财付通）和银行卡清算组织（如银联）。在双层投放体系下，银行承担监管责任、并建立央行与运营机构以及运营机构之间的互联互通，而运营机构负责交易确认与管理及更多场景应用的开发。
- ▶ **产品形态猜想：**如果说电子货币是数字钱包中的普通数字，数字货币则是存储于数字钱包并运行在特定数字货币网络中的加密数字。我们认为，操作性较强的方案为在现有的商业银行账户/第三方支付账户/NFC智能卡上加入数字货币钱包的属性，即实现一个账户下既可以管理电子货币、亦可以管理数字货币（例如银行App中有单独的数字货币账户管理入口）。引用姚前<sup>22</sup>的比喻，银行账户下的数字货币类似于客户存放在银行的保管箱——银行不能擅自打开、保证可控匿名性，电子货币与数字货币管理上虽然存在账号使用、身份认证、资金转移等共性，但数字货币属于银行表外资产、与银行存款相区分，从而不影响现有银行核心业务系统。
- ▶ **应用场景猜想：**目前监管的普遍共识是基于央行—商业银行—非银行金融机构—单位账户—个人账户的推广路径，逐步扩大使用范围、最终完全取代实物现金。早在2016年央行和试点商业银行搭建的数字票据交易平台即运营成功，显示数字货币在数字票据场景应用的落地。未来我们认为发展空间更大的领域为小额零售业务场景，我们预计个人/企业之间支付数字货币的操作或与当前电子支付类似，包括PC/移动端的网关/快捷支付、扫码/NFC支付、或直接输入对方钱包地址转账等，支持线上/线下消费场景、兼顾在线/离线网络环境。

我们预计DC/EP主要针对纸币现金替代、对电子货币影响较小。获得DC/EP运营资质的机构的直接货币化空间可能有限，更多作用体现为场景应用的增加带来的客户活跃度和粘性的增加，带来机构之间进一步的分化。此外，我们预计金融IT服务商有望收获银行机构改造升级核心交易系统带来的商业机会。

- ▶ **M0增长趋缓、整体现金需求降低。**央行数字货币用于替代现金，属于M0范畴，而广义货币中的活期存款部分已由现有支付体系高效处理。我国银行间支付清算系统（如大小额支付系统和网上支付跨行清算系统等）、商业银行行内系统以及非银行支付机构的各类网络支付手段等运转高效，社会对于现金的需求逐渐降低。截至9月末M0货币供应量为7.4万亿元、同比仅增长4%、在M2中的比重降至不足4%。
- ▶ **预计数字货币主要对纸币进行替代、对电子货币的挤占或有限。**对于用户而言，使用DC/EP相比纸币的便捷性和安全度大幅提升，我们预计在目前移动支付渗透率快速提升的背景下、以数字钱包为载体的数字货币会以较快的速度为大众所接受。相比电子货币而言，DC/EP的优势包括交易难以篡改、可控匿名属性、更高的信用背书、支付双离线支付等，但考虑到用户对商业银行/头部支付机构已建立起的信任感、移动支付习惯的养成和逐渐固化、匿名支付需求的有限性和日益完善的网络基础设施下，叠加基于电子货币产生的理财/贷款等综合金融服务（DC/EP不计付利息），我们预计数字货币对电子货币影响有限。
- ▶ **短期带给DC/EP运营机构的直接货币化空间或有限、更多作用体现为入口地位的夯实。**不仅纸币交易不存在服务商从而没有额外收费、目前电子货币的存取/转账也大多免费，考虑到数字货币对纸币进行替代的定位，我们预计数字货币的运营本身较难进行大规模的货币化，基于其点对点的直接支付方式，亦不需跨行清算组织参与其中（如POS网络中银联负责清算转接）。但是获得DC/EP运营许可的商业银行/支付机构/清算机构通过将数字货币入口嵌入到当前账户及软件中，通过数字货币相关应用的开发和场景的开拓提升自身的用户活跃度和粘性，从而进一步扩大其较其他银行/支付机构的用户领先优势，形成强者恒强局面。在数字货币与电子货币等金融资产之间高速转化的背景下，存取现的复杂流程被进一步简化，亦可能影响存款金

<sup>22</sup> <https://www.cebnet.com.cn/20180806/102512063.html>

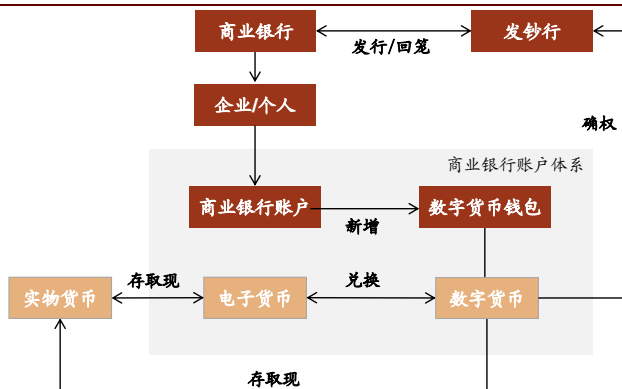




## 融机构的竞争格局。

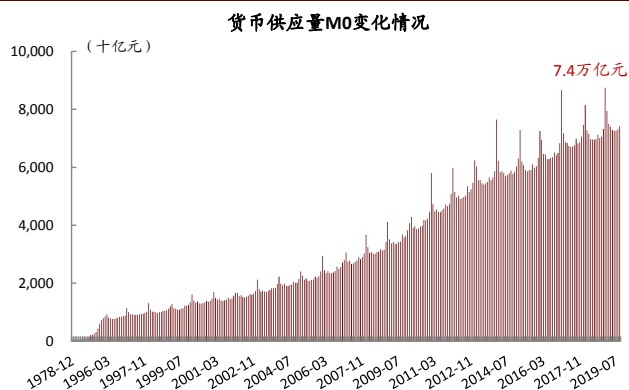
- ▶ **DC/EP 的推出料将带来银行机构核心系统升级需求，同时或对 ATM 和铸币相关公司带来一定负面冲击。**我们预计数字货币投放运营机构需要对自身系统进行改造、建立银行库和保存数字货币，其中安全加密、身份认证、分布式记账、大数据分析、安全芯片、可信云计算和隐私保护等技术的应用需求较为突出。

图表 47: 基于商业银行账户体系支持的数字货币示意图



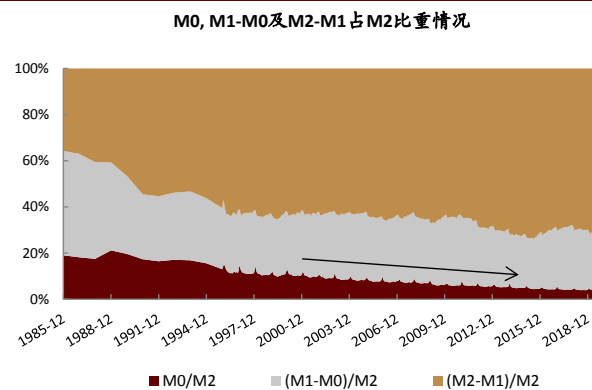
资料来源：央行数字货币研究所，中金公司研究部

图表 48: 近几年来 M0 增速显著放缓



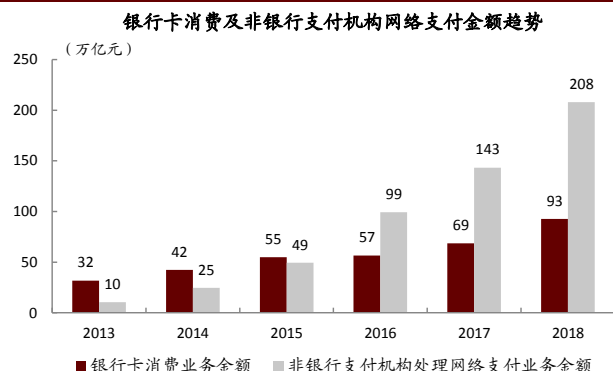
资料来源：中国人民银行，中金公司研究部

图表 49: M0 在 M2 中占比逐渐降低



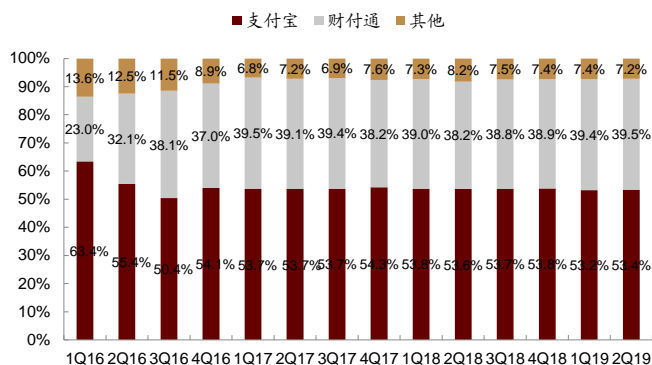
资料来源：中国人民银行，中金公司研究部

图表 50: 支付机构网络支付规模高速增长



资料来源：中国人民银行，中金公司研究部

图表 51: 移动支付中支付宝及财付通市占率遥遥领先



资料来源：易观智库，中金公司研究部



## 中国央行数字货币推广：前景展望

我们认为，对于不同类型使用者，央行数字货币的重要性存在差异。对于政府客户，央行数字货币意义较大且有条件迅速推广，随后会逐渐影响到企业和消费者。

### 政府：加强财政管理，促进效率提升

对于各级政府机构，我们认为央行数字货币在发行后会以较快速度推行。采用数字货币后，财政资金的使用的效率、透明度、交易的真实性、可追溯性将大大提高，有助于进一步规范政府购买服务、完善专项资金管理。我们预计，作为财政资金发放的数字货币，可能会通过智能合约等形式，设置更为严格的向传统货币转换的权限，以实现更完整的追溯。除此之外，推行央行数字货币有助于公共部门进行更高效的社会管理，社保资金、扶贫资金等直接向个人数字货币账户发放，能够减少运营成本。

### 企业：数字货币使用将首先集中于 G 端业务

对于企业而言，我们预计央行数字货币短期内不会被大规模使用。企业已经形成了很多金融交易的流程和架构，需要一定时间逐步地建立各类支持数字货币的财务与市场基础设施，更为重要的是，不同于行政单位，企业之间对央行数字货币概念与政策的理解存在差异，这会影响数字货币的接受速度。我们认为，通过积极的引导和市场自发的培育过程，央行数字货币会逐渐在企业层面推广，而在初期将主要在企业与政府的交易中使用。

### 消费者：短期内舒适区存在，长期内可能改变支付习惯

对于消费者群体，我们预计数字货币在短期内不会对支付习惯产生巨大影响，但存在对第三方支付的替代潜力。中国已建立了完备的电子支付基础设施，移动支付技术水平与普及率走在世界前列。使用央行的数字货币进行支付，对于普通的消费者来说，在便携性、支付成本上均没有较大的额外效益。但对于生活服务场景，当前存在各类缴费账户繁多且互相独立的痛点，且接入第三方支付软件也存在公共事业数据安全与消费者个人隐私泄露风险，我们认为央行数字货币的推行提供了另一种不依赖第三方软件的、直接与个人数字货币账户挂钩的选项。



## 升级：全球监管渐明，区块链进入 3.0 时代

2019 年年初以来，加密资产市场开始回暖，主要加密资产总市值相比年初上升约 85%。Facebook 于 6 月发布白皮书，并拟推出 Libra 币的消息，也为加密资产市场吸引了很高的关注度。尽管倍受争议，过去一年美国、英国、新加坡、中国香港等相继明确了加密资产监管政策，带动比特币期货、加密货币基金等新兴加密资产市场发展。技术方面的主要变化包括 1) 以 USDT/USDC 为代表的美元稳定币交易量超越比特币，以及 2) 以抵押贷款为代表的去中心化金融应用开始兴起，虽然其总体规模都很小，但通过了解加密资产技术和监管的发展，有利于我们把握 Libra 及央行数字货币未来可能的走向和影响。

**各国对比特币等加密资产监管政策渐趋明确。**过去一年，各国对加密资产的法律地位定义和监管取向逐渐明确。中国在法律上不认可加密资产的货币属性，也不允许任何 ICO 或虚拟货币相关交易。美国 SEC、CFTC 分别对被认定为证券、商品的加密资产业务实施监管，2018 年 10 月美国 SEC 发放了首批 STO 牌照。2019 年 9 月，美国商品期货交易委员会（CFTF）和纽约金融服务部（NYFDS）推出第一个实物交割比特币期货牌照。2019 年 1 月，英国 FCA 发布《加密货币资产指南》，明确对证券型通证提出监管。新加坡于 2019 年 1 月通过《支付服务法案》（Payment Service Act），数字货币交易所等业务可以在这个法令的监管下合规运营。香港 SFC 2019 年 9 月发布针对加密资产基金管理人的监管条例。

**比特币“虚拟黄金”地位日益巩固，稳定币取代比特币成为最主要交易手段。**2019 年以来，加密货币市场整体回升的同时，比特币的市值占市场比也同步推高，由年初的 52% 增至 10/13 的 67%，反映其日益巩固的“虚拟黄金”地位。另一方面，我们注意到，以 USDT、USDC 代表的稳定币（价格和美元挂钩的加密货币）交易量快速上升，其中 USDT 过去三个月平均日交易量已经超过比特币，成为加密货币交易中最主要的交易手段。Facebook 拟推出的 Libra 币也采用稳定币的方案，使得稳定币获得了相当高的关注度。

**ICO 基本失去融资能力，以抵押贷款为代表的去中心化金融（区块链 3.0）开始兴起。**以太坊的诞生，代表区块链行业进入 2.0 时代，并且以太坊提供的智能合约能力催生了 ICO。ICO 融资额于 2017 年 12 月最高达到单月 18 亿美元，但由于 ICO 本身无法保证资产上链真实性等问题，ICO 市场迅速萎缩，现已几乎失去功能。从 2017 年底起，以基于智能合约的抵押贷款为代表的去中心化金融（Decentralized Finance）项目上线，行业进入 3.0 时代。目前，基于智能合约的抵押贷款总金额只有 4.4 亿美金，但我们认为其代表加密货币行业一种技术趋势。

**加密资产生态链在大起大落中发展。**目前，每月通过挖矿新增相当于约 5 亿美金的比特币。Bitwise 向美国 SEC 递交的一份白皮书显示，比特币日均交易量约 2.73 亿美元（相当于上交所/港交所日均交易量的 1%/3%）。比特币的发行和交易催生了矿机、交易所、资产管理等不同业态。在整个加密资产生态链中，目前比较成熟的商业模式包括 1) 保证比特币的生产及运行的矿机、矿池等：据 Frost & Sullivan 统计，2017 年基于 ASIC 的加密货币矿机市场规模约 30 亿美元；2) 交易所、加密资产基金等：Coinbase 最新一轮融资市值达 80 亿美元，加密货币基金 AUM 达 183.2 亿美元；3) 稳定币、借贷服务等：目前借贷类 DeFi 项目总锁仓规模为 4.42 亿美元。

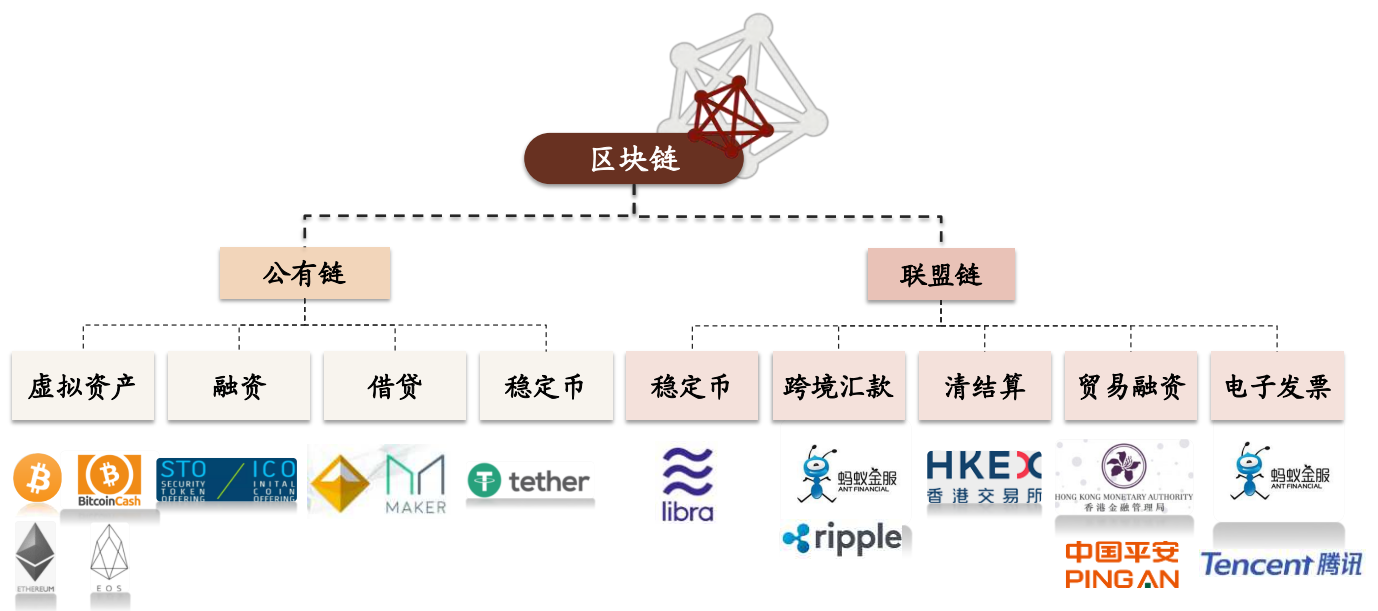


## 区块链发展步入 3.0 时代

区块链按开发者可以分为由开源社区主导的公有链,及大型 IT 或金融企业主导的联盟链。

- **公有链**: 公有链的优点是协议公开,信息透明度高,全部数据均可以被公开访问。缺点是很难在满足去中心化和安全性的同时支持很高的交易量。目前,主要的公有链有比特币、以太坊、比特币现金等。目前区块链主要的应用包括 1) 加密资产(比特币、USDT 等稳定币、比特币现金), 2) 基于区块链的融资(ICO), 3) MakerDAO 等基于加密资产的借贷服务。
- **联盟链**: 联盟链是半公开性质的区块链网络,需预先指定节点作为记账人,区块的生成由所有记账人协同决定。联盟链的优点是网络性能高,运作成本较低,但其透明度较公有链低。目前主要的联盟链框架有 Hyperledger Fabric 等。阿里巴巴、腾讯、华为、平安等中国主要 IT 企业都积极参与联盟链,但大多数联盟链现仍处于概念验证阶段。

图表 52: 区块链的主要用途

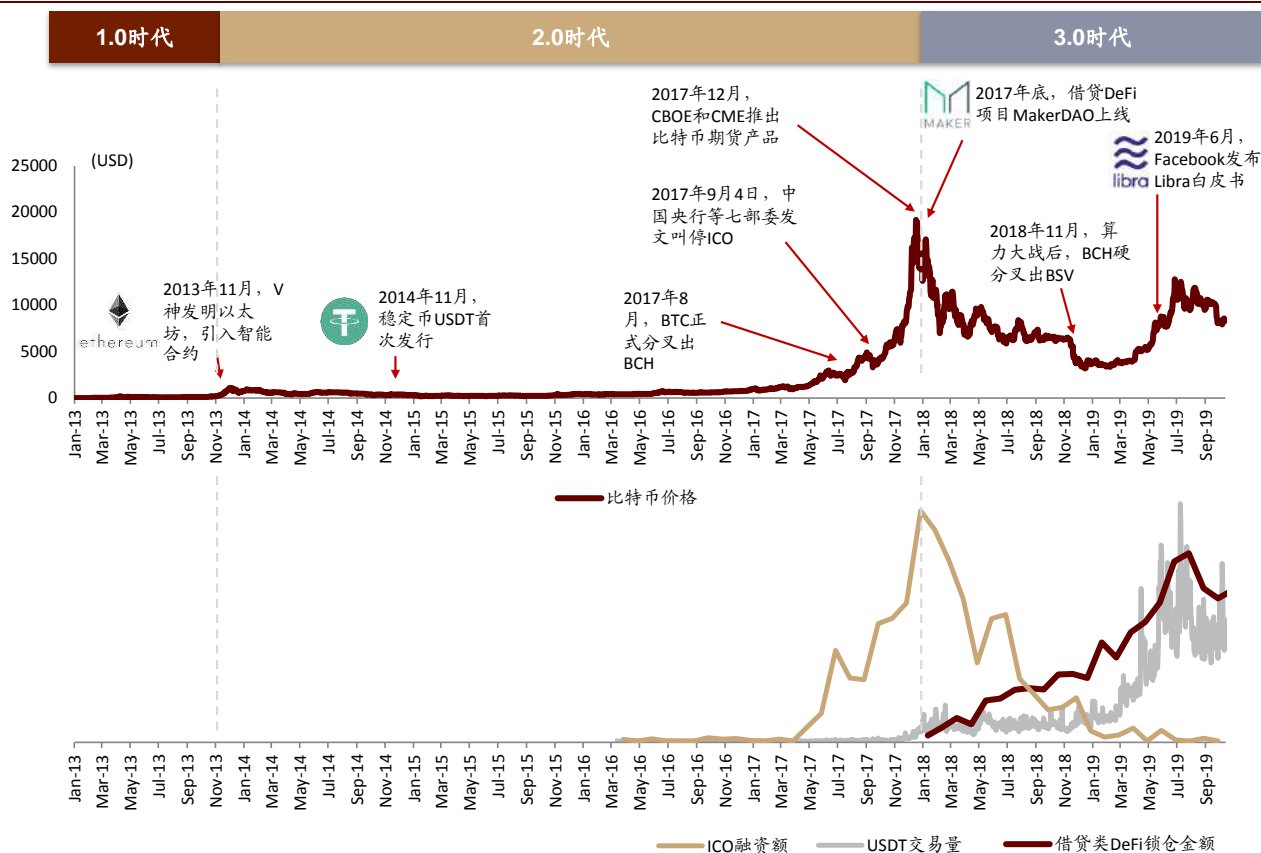


资料来源: Wikipedia, Google news, 中金公司研究部



自2008年比特币问世以来，区块链技术不断发展，从最初的比特币，到支持智能合约的以太坊，再到稳定币。与之相应的，基于区块链的应用也越来越多，种类越来越丰富。我们将区块链行业的发展，分为以下三个阶段：

图表 53：区块链行业发展历程



资料来源：CoinMarketCap, icodata, DeFi Pulse, 中金公司研究部；注：下半张图仅用作变化趋势示意，不同量之间绝对数值不可比

- **比特币发布，开启区块链 1.0 时代（2009-2013）：**2008 年，署名为“中本聪”的匿名人士发表论文《比特币：对等网络电子现金系统》，最初期望是推出一种可以自由流通的点对点电子现金。但因其价格波动剧烈、交易吞吐量低、能耗高等问题，比特币难以真正成为通行货币。比特币是发展历史最长、知名度最高的加密货币，被称为其他加密电子货币的始祖。同时，由于比特币的总量有限，其目前在加密货币市场中扮演着“数字黄金”的角色。2017 年底，随着受监管的比特币期货在 CBOE 和 CME 开始交易，比特币价格曾一度达到近 20,000 美元的高点，此后又在 2018 年 12 月跌至 3100 美元的低点。
- **以太坊推出，区块链进入 2.0 时代（2014-2017）：**2013 年 11 月，Vitalik Buterin（V 神）发布了以太坊白皮书。以太坊与比特币的最大区别，是其支持脚本语言应用开发，可以实现智能合约。以太坊出现，催生了 ICO、STO 等新型融资手段。ICO 融资额于 2017 年 12 月最高达到单月 18 亿美元，但此后受币价下跌以及各国强化监管的影响，ICO 市场迅速萎缩，现已几乎失去功能。
- **稳定币流行及 MakerDAO 上线，推动区块链 3.0 时代（2018-）：**2017 年底起，稳定币 USDT 的交易开始显著放量，2019 年以来 USDT 交易量增长迅速，目前其日交易量已经超过比特币。2017 年 12 月，借贷类 DeFi（Decentralized Finance，去中心化金融）项目 MakerDAO 上线，其中也用到了稳定币的技术。随后借贷类 DeFi 项目规模快速扩张，据 DeFi Pulse 统计数据，截至 2019/10/13，借贷类 DeFi 项目总锁仓金额为 4.42 亿美元，其中 MakerDAO 占比达 65.96%。我们认为，虽然借贷类 DeFi 项目的规模与传统的金融借贷市场相比仍有较大差距，处于早期发展阶段，但由于其平等、高效率、低费用、高透明、高可信等优点，具有较强的成长潜力。





## 加密资产的法律地位逐渐明确，监管取向渐趋明朗

过去一年，我们看到各国对加密资产的法律地位定义逐渐明确，对加密资产的监管取向也渐趋明朗。2019 年 6 月，著名的反洗钱、反恐怖主义融资政府间组织——反洗钱金融行动特别工作组（Financial Action Task Force on Money Laundering, FATF）发布了加密货币监管标准，为其旗下的 37 个成员国提供了监管政策的参考。

阻碍比特币普及的一个重要原因是其法律地位不明确。比特币普及度持续提高，但各国由于对比特币底层技术的不了解或对货币去中心化的担心等，对比特币采取了不同的态度，根据我们对各国法律条文的理解和法学专家的访谈，我们将政府对加密资产可能采取的法律定位分为财产、证券、货币和法币等四类。主要定义如下：

- **财产**：与游戏道具等类似的数字资产。所有者对虚拟货币享有财产权，盗窃加密资产违法。
- **证券**：分为发行和交易两部分。发行即 ICO（Initial Coin Offering），属于证券首次发行；交易及监管机构发放加密资产交易牌照，在监管下可合法进行加密资产买卖。
- **货币**：加密资产可用于一般支付手段进行交易，但不能作为纳税手段。
- **法币**：国家以法律形式赋予其强制流通使用的货币，可以用来纳税。

主要国家目前基本认可加密资产的财产权，但对是否是证券（发行、交易）以及适合参与加密资产投资的投资人资格意见存在分歧。在主要国家中，目前日本认可加密资产具有等同于货币的地位，即认可加密资产的支付权。所有国家目前都不承认加密资产具有等同于法币的地位。

图表 54：各主要国家或地区对加密资产监督走向

	财产	证券		货币 (支付手段)	法币
		发行 (ICO)	交易		
中国	积极	消极	消极	消极	消极
中国香港	积极	积极	积极	积极	消极
美国	积极	积极	积极	积极	消极
英国	积极	积极	积极	积极	消极
日本	积极	积极	积极	积极	消极
韩国	积极	积极	积极	积极	消极
新加坡	积极	积极	积极	积极	消极

 积极
  中性
  消极

资料来源：星瀚金融，中金公司研究部；注：本表格讨论的加密资产不包括央行数字货币

**中国**：中国在法律上不认可加密资产的货币属性，也不允许 ICO 或相关交易。2017 年 9 月 4 日，中国央行等七部委联合发布《关于防范代币发行融资风险的公告》，正式开启了对 ICO 和加密资产的强监管时代。2018 年 11 月，深圳国际仲裁院裁决的一起案件，首次认可比特币具备财产属性、受法律保护，并被认为在一定程度上弥补了现有司法判例的空缺。2019 年 3 月 21 日，北京市互联网金融行业协会公布了《关于防范以“虚拟货币”



“ICO”“STO”“稳定币”及其他变种名义进行非法金融活动的风险提示》，反映中国官方对于加密资产及相关业务的强监管态度。2019 年 10 月 10 日，支付宝和微信明确表态，禁止用户将其用于虚拟货币交易。

**中国香港：**加密资产被香港特别行政区政府视为虚拟资产，且取决于其确切特征，某些加密资产可作为股份、集体投资计划、储值支付工具或其他工具而加以监管。2017 年 12 月 11 日，香港证监会（SFC）发布的《致持牌法团及注册机构的通函：有关比特币期货合约及与加密货币相关的投资产品》指出，香港投资者提供比特币期货交易服务及其他相关服务构成监管条件，需要向 SFC 申请牌照。2018 年 11 月 1 日，香港 SFC 发布《有关针对虚拟资产投资组合的管理公司、基金分销商及交易平台营运者的监管框架的声明》，针对加密资产等虚拟资产投资发布新规。加密资产交易所成为被香港允许实行“沙盒”实验中的金融科技项目，可行性被验证后可发出正式牌照。2019 年 3 月 28 日，香港 SFC 发布《有关证券型代币发行的声明》，声明中表示证券型代币可能属于《证券及期货条例》下的“证券”，应受到监管，并且推广及分销证券型代币应申请第 1 类牌照（证券交易），证券型代币应只发售给专业投资者。2019 年 10 月 4 日，香港 SFC 正式发布了针对加密资产基金管理人的监管条例，与第 9 类牌照（资产管理）的要求基本一致，但在托管（Custody）部分针对加密资产的特点做出了额外要求。

**美国：**美国对加密资产持开放态度，认可加密资产的财产属性，交易合法，不是法币。但加密资产监管复杂，涉及较多部门，暂无系统性框架。美国证券交易委员会（SEC）、美国商品期货交易委员会（CFTC）、美国国税局（IRS）、美国财政部金融犯罪执法网络（FinCEN）都有相关法规。SEC 认为某些加密资产属于证券，它的 ICO 需要注册并受法律监管；CFTC 负责监管比特币期货交易，其认为比特币期货属于大宗商品；IRS 出于税收考虑，将比特币和其他加密资产认定为财产而非货币，并于 2019 年成立了专门团队，打击加密资产逃税；FinCEN 认为通证是货币，并且 ICO 受《银行保密法》约束。早在 2017 年 3 月，美国财政部和 SEC 就明确表示，加密数字货币交易所需要向 FinCEN 申请注册 MSB（Money Services Business）牌照。2019 年 10 月 11 日，原计划于 10 月 31 日主网上线的 Telegram 区块链项目 TON（Telegram Open Network）被美国 SEC 提起“紧急行动并获得临时限制令”。美国 SEC 认为，Gram 代币被定性为证券，Telegram 应当按 1933 年《证券法》（Securities Act of 1933）要求，完成证券要约和销售的注册，以及相关信息的披露。

**英国：**英国认为机构投资人交易加密资产合法，职责不在于监督加密资产，而是加密资产衍生品。2017 年 9 月 12 日，金融市场行为监管局（FCA）认为 ICO 是高风险、投机性强的投资活动，并将其纳入监管范围。2018 年 5 月 21 日法定交易平台 LMAX 允许机构投资人进行相关交易。FCA 计划在 2018 年底前确定加密资产监管政策，FCA 的监管职责不包括加密资产，仅限于加密资产衍生品如加密资产期货、加密资产差异合约和加密资产期权。2019 年 1 月，FCA 发布《加密货币资产指南》文件，进一步明确监管对加密资产的态度。在该文件中，FCA 指出 1）比特币、莱特币等交易型通证可用于商品和服务的买卖，无需经过银行；2）证券型通证应该纳入监管；3）除电子货币外的实用型通证不受监管。

**日本：**2017 年 4 月 1 日，日本《支付服务修正法案》正式生效，部分加密资产作为支付手段的合法性被正式认可。加密资产交换业务受到监管，要求对企业及其客户的资金或加密资产进行分开管理。2017 年 7 月 1 日，日本新版消费税正式生效，加密资产交易免除消费税。2019 年 3 月，日本通过虚拟货币相关修正案草案，将“虚拟货币”的更名为“加密资产”，并且加密资产交易所得税率最高达 45%。虽然 ICO 目前不在《支付服务修正法案》的监管范围内，但 2018 年 12 月日本金融厅（FSA）公开表示正在计划对 ICO 的监管。日本没有明确规定 ICO 具体细则，现行的比特币支付法律并不足以确定某些 ICO 活动的合法地位。

**韩国：**韩国是一个代币交易市场火爆的国家，有强化监管的趋势。2017 年 8 月韩国认为加密资产交易合法，是受法律保护的“一种交易工具或者电子保值品”，可不是法币。韩国金融服务委员会（FSC）将新设金融创新局，该部门将专注于为该区块链和金融科技行业制定政策。韩国 2017 年宣布首次代币发行（ICO）非法。然而 2018 年 5 月份，韩国政府的立法机构进而取消了这一禁令，并正式提议只要投资者保护措施到位，就允许 ICO。2018 年 7 月韩国央行（BOK）表示，加密资产很可能被用作海外汇款等有限领域的支付手段。

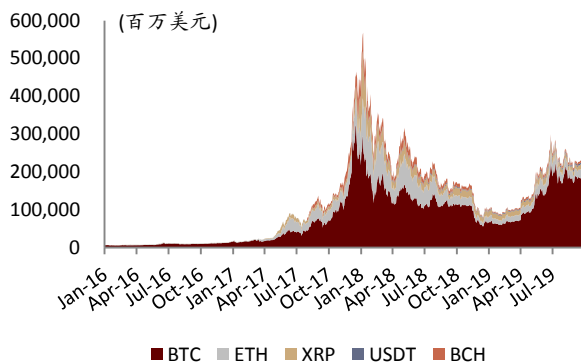


**新加坡：**新加坡既降低加密资产市场准入门槛，又积极治理不符合监管要求的加密资产。2018 年 9 月，新加坡金融管理局（MAS）将代币分为应用型代币，支付型代币以及证券型代币：1）MAS 不打算监管应用型代币；2）新加坡国税局（IRAS）于 2019 年 7 月发布草案，对支付型代币交易免征商品的服务税和增值税；3）证券型代币适用于现有的新加坡证券及期货法，比特币出售和交付需缴税。2019 年 1 月 14 日，新加坡国会审议通过《支付服务法案》（Payment Service Act），对数字货币业务的监管进行了明确，该法案规定，数字货币交易所、OTC 平台、钱包等属于支付型代币服务商，需要满足相关反洗钱规定，并申请相应牌照。

### 加密货币市场回暖，比特币市值占比稳步提升

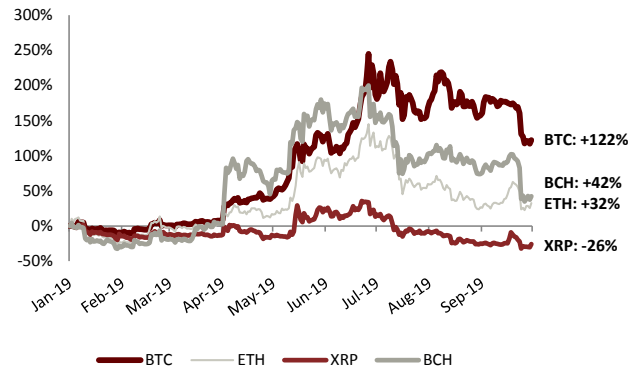
过去两年主要加密资产的价格大幅波动，2019 年以来市场回暖。以前五大加密资产（比特币、以太坊、Ripple、USDT、比特币现金）为例，其总市值从 2017/1/1 的 170 亿美金，在一年后上升 30 倍在 2018/1/7 达到顶点的 5,280 亿美金，其后开始下跌，2018/12/15 下落到 805 亿美金，和峰值比下跌 85%。2019 年年初以来，加密货币市场开始回暖，截至 2019/9/30，主要加密资产总市值上升 85%至 1,864 亿美元。

图表 55：主要加密资产市值变化



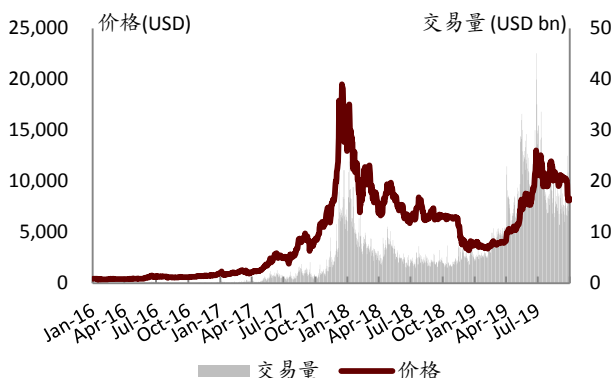
资料来源：CoinMarketCap，中金公司研究部

图表 56：2019 年年初以来主要加密资产价格变化



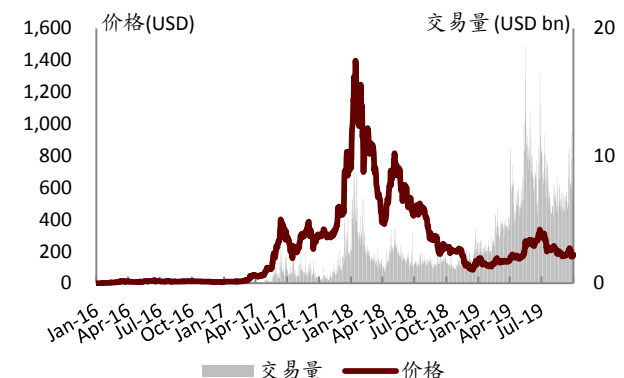
资料来源：CoinMarketCap，中金公司研究部

图表 57：比特币价格和交易量变化情况



资料来源：CoinMarketCap，中金公司研究部

图表 58：以太坊价格和交易量变化情况



资料来源：CoinMarketCap，中金公司研究部

**比特币市值占比稳步提升。**据 CoinMarketCap 数据，截至 2019/10/7，共有 2,963 种加密货币，总市值超过 2,000 亿美元。其中以比特币、以太坊为代表的公链货币，占据了加密货币总市值的绝大部分。2019 年年初以来，随着加密货币市场整体回暖以及 ICO 项目的退潮，比特币市值占比（Bitcoin Dominance）也稳步提升，由年初的 51.7%增至 2019/10/13 的 66.9%。

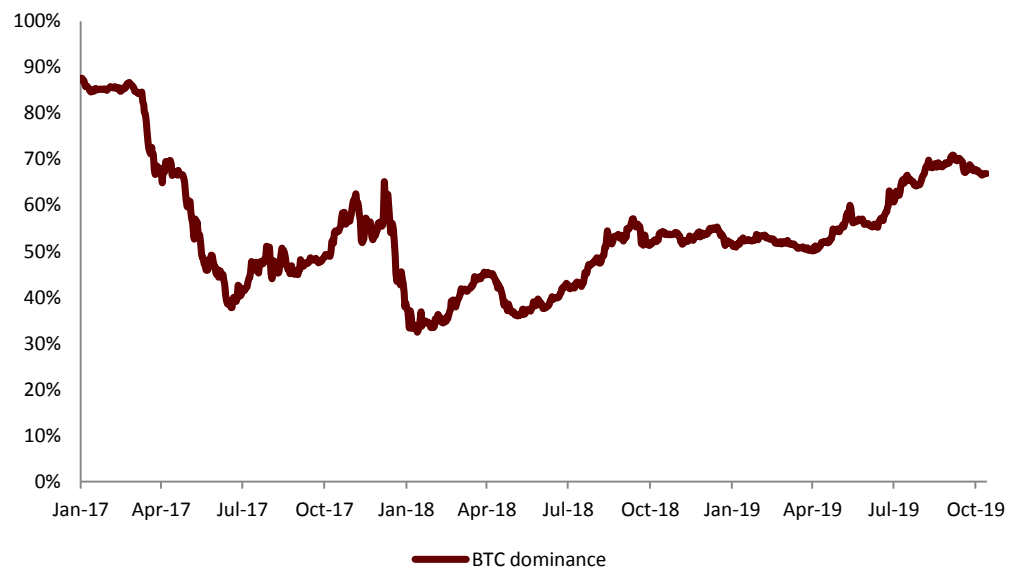


图表 59: 主要加密货币价格、市值、交易量情况

币种	价格	市值	市值占比	近3个月平均日交易量
BTC	\$8,421.13	\$151,498,178,625	66.8%	\$16,929,028,996
ETH	\$184.38	\$19,937,276,080	8.8%	\$7,078,819,526
XRP	\$0.28	\$12,070,686,389	5.3%	\$1,192,987,611
USDT	\$1.01	\$4,133,979,825	1.8%	\$18,920,568,047
BCH	\$227.09	\$4,100,003,929	1.8%	\$1,482,733,142
LTC	\$57.36	\$3,640,137,642	1.6%	\$2,804,677,605
EOS	\$3.11	\$2,914,245,619	1.3%	\$1,699,347,215
BNB	\$18.21	\$2,832,275,225	1.2%	\$222,056,881
BSV	\$88.61	\$1,582,210,652	0.7%	\$316,272,360
XLM	\$0.06	\$1,234,400,026	0.5%	\$159,393,763

资料来源: CoinMarketCap, 中金公司研究部; 截至 2019/10/13

图表 60: 比特币市值占比



资料来源: CoinMarketCap, 中金公司研究部





图表 61: 主要加密资产比较

	比特币 BTC	比特币现金 BCH	以太坊 ETH	EOS 币 EOS	Tether 币 USDT
创始人	中本聪	从比特币分叉	Vitalik Buterin (V神)	Daniel Larimer (BM)	Brock Pierce, Craig Sellars
市场规模 (10亿美元)	154.5	4.3	20.7	3.0	4.1
日交易规模 (10亿美元)	20.5	1.5	9.4	1.7	23.9
社区	比特币基金会	Bitcoin ABC 等开发团体	以太坊基金会	Block One 及 EOS 基金会	Tether Limited
虚拟资产	√	√	√	√	√
支付手段	慢	√	√	√	√
DAPP/智能合约			√	√	
哈希算法	SHA-256	SHA-256	ETHASH	SHA-256	SHA-256 或 ETHASH
共识机制	PoW	PoW	PoW	DPoS	PoW
P2P 拓扑结构	平等节点	平等节点	平等节点	21 个超级节点	平等节点
激励途径	新区块产生 + 交易费用	新区块产生 + 交易费用	新区块产生 + 交易费用	EOS 增发	-
激励形式	比特币	比特币现金	新区块产生: ETH 交易费用: Gas	EOS	-
区块容量	1M	32M	-	-	-
每秒可处理交易数	7	277	30-50	百万级	7~50
总量	2,100 万	2,100 万	无限	无限	无限
主流矿机	ASIC 矿机	ASIC 矿机	GPU 矿机	-	-

资料来源: CoinMarketCap, 各虚拟货币白皮书, 中金公司研究部; 注: 市场规模和交易量数据截至 2019/9/30

### 稳定币超越比特币成为主要交易手段

为了解决普通加密货币价格波动过于剧烈的问题, 各种形式的稳定数字货币 (Stable Coin) 陆续进入市场。稳定币不仅部分解决了比特币价格大幅波动带来的问题, 还成为连接法币与其他加密货币的重要资产。

USDT (USD Tether, 泰达币) 是由 Tether 公司发行的, 价格 1:1 锚定美元的稳定币。USDT 最初通过 Omni Layer 协议在比特币区块链上以代币形式发行, 目前部分资产在以太坊、EOS 等其他区块链网络上发行。USDT 的发行机制如下: Tether 公司每发行 1 USDT, 将有 1 美元存储在香港 Tether 公司。用户可以通过 SWIFT 电汇美元至 Tether 公司银行账户取得 USDT, 或者通过交易所换取 USDT; 反之可用 USDT 赎回美元。

**USDT 日交易量超过比特币。**2018 年底以来, 以 USDT 为代表的稳定币市值和交易量上升迅速, USDT 的平均日交易量已经超过比特币。我们认为, 主要原因如下:

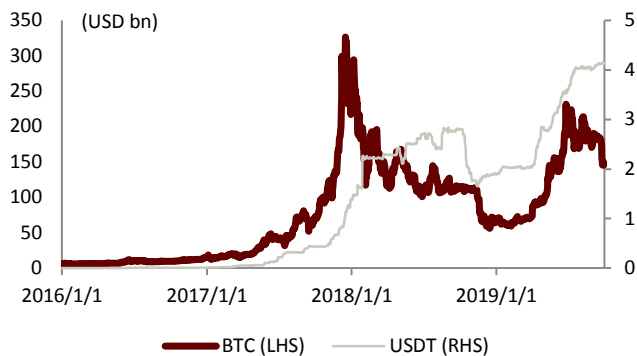
- ▶ 一方面, 在波动较为剧烈的加密货币市场行情下, 稳定币是一种良好的避险资产, 且相比法币, USDT 保留了传统加密货币匿名、便捷等优点;
- ▶ 另一方面, 由于监管要求, 大多数交易所仅支持加密货币之间的交易, 而不支持法币和数字货币的直接交易, 因此稳定币成为较好的法币-加密货币交换、不同加密货币互换的良好中间媒介。

此外, 由于 Facebook 拟推出的 Libra 币也采用稳定币的方案, 使得稳定币获得了相当高的关注度。



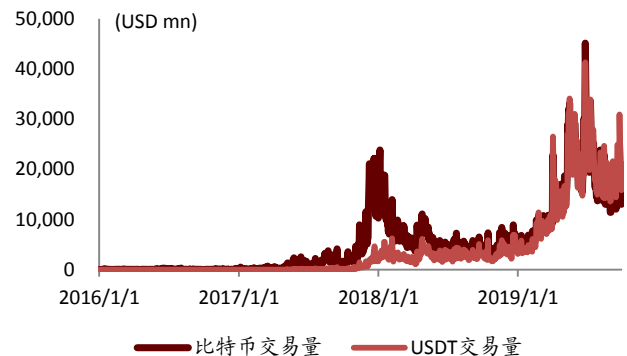


图表 62: USDT 市值 vs. BTC 市值



资料来源: CoinMarketCap, 中金公司研究部

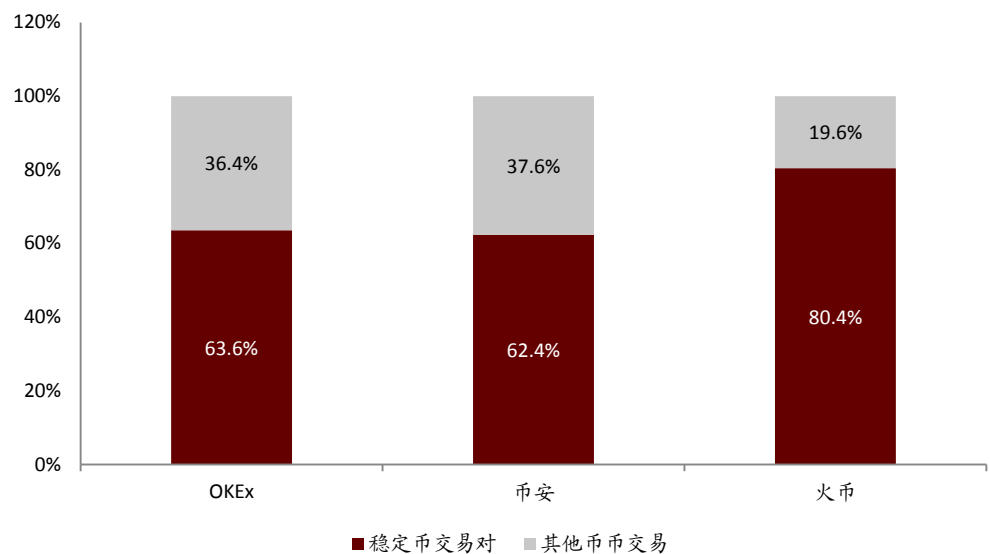
图表 63: USDT 日交易量 vs. BTC 日交易量



资料来源: CoinMarketCap, 中金公司研究部

稳定币的交易已成为加密货币市场最活跃的交易。据 CoinMarketCap 数据,近三个月平均日交易量 189.2 亿美元,超过比特币的 169.3 亿美元,是交易量最大的加密货币。从交易对占比来看,OKEx、币安、火币三大交易所中,稳定币交易对的占比分别为 64%、62%、80%(2019/10/13 数据)。从比特币的交易对占比来看,CryptoCompare 数据显示,USDT-BTC 交易对占比特币总交易量的比例超过 75%。

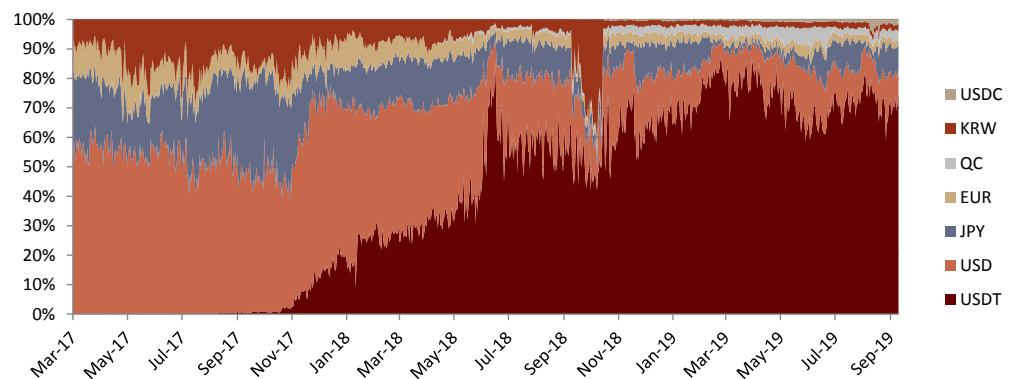
图表 64: 主要交易所稳定币交易占比 (2019/10/13)



资料来源: CoinMarketCap, 中金公司研究部



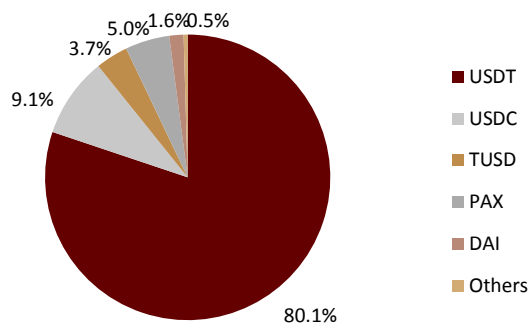
图表 65: 比特币交易对分布



资料来源: CryptoCompare, 中金公司研究部

截至 2019/10/8, 主要稳定币总市值达 51.3 亿美元, 约占加密货币总市值的 2.3%。其中, USDT 的市值和交易量在稳定币中均处于领先地位。2019/10/8, USDT 市值 41.1 亿美元, 占主要稳定币总市值的 80.1%, 在所有加密货币中位列第 4; 24h 交易量 179.5 亿美元, 占主要稳定币 24h 总交易量的 95.3%, 在所有加密货币中位列第 1。

图表 66: 主要稳定币市值分布 (2018/10/8)



资料来源: CoinMarketCap, 中金公司研究部; 注: Others 包括 GUSD、BITCNY、BITUSD 和 SUSD

图表 67: 主要稳定币 24h 交易量 (2019/10/8)

币种	24h 交易量	占比
USDT	US\$ 17,952,453,336	95.3%
PAX	US\$ 330,839,000	1.8%
TUSD	US\$ 191,953,709	1.0%
USDC	US\$ 181,524,610	1.0%
BITCNY	US\$ 169,030,158	0.9%
DAI	US\$ 2,802,678	0.0%
GUSD	US\$ 2,430,004	0.0%
EURS	US\$ 821,626	0.0%
USDS	US\$ 182,481	0.0%
BITUSD	US\$ 12,425	0.0%

资料来源: CoinMarketCap, Coincodex, 中金公司研究部

### 矿机进入 7nm 时代, 在网算力回升, 矿池集中度稳定

#### 虚拟货币成为全球半导体行业重要需求之一

虚拟货币矿机是专用于维持虚拟货币区块链网络运行时, 所需的工作量证明 (Proof of Works, PoW) 计算的计算机。矿机的特点是通过采用大量专用挖矿芯片进行并行计算, 实现远远优于 CPU/GPU 等传统通用芯片的能耗比和计算设备的性价比。比特币及以太坊等主要加密资产采用哈希运算等工作量证明的形式进行竞争记账。作为成功记账的奖励, 参与记账的节点 (矿工) 获得 1) 交易发起方支付的手续费; 2) 生成新区块时奖励的比特币。矿工主要成本包括 1) 进行哈希运算所消耗的电费; 2) 矿机的初始成本以及折旧。



图表 68: 阿瓦隆矿机



资料来源：中关村在线，中金公司研究部

图表 69: 典型矿机的主要参数，其中能耗比是最重要参数

	蚂蚁矿机S9	Avalon A921	翼比特 E9.3	蚂蚁矿机S15	蚂蚁矿机E3	蚂蚁矿机S17	Avalon A1066	翼比特E12+
额定算力 (TH/s)	13.5	20	16	28	190MH/s	56	50	50
墙上功耗 (W)	1,485	1,700	1,760	1,596	760	2520	3250	2500
能耗比 (W/TH/s)	110	85	110	57	4W/MH/s	45	65	50
芯片	BM1389	A3206	DW1228	BM1391	BM1790	BM1397	A3205	DW1233
芯片数量	189	104	144	Unknown	18	144	342	Unknown
制程	16nm	7nm	10nm	7nm	28nm	7nm	16nm	10nm
架构	ASIC	ASIC	ASIC	ASIC	ASIC	ASIC	ASIC	ASIC
计算方法	SHA-256	SHA-256	SHA-256	SHA-256	ETHASH	SHA-256	SHA-256	SHA-256
对应币种	比特币	比特币	比特币	比特币	以太坊	比特币	比特币	比特币

资料来源：中关村在线，中金公司研究部

比特币挖矿以 ASIC 矿机为主，以太坊挖矿以 GPU 为主。典型的英特尔 CPU 挖矿性能是 20 MHash/s，而英伟达 GPU 性能约为 400 MHash/s。而 2012 年的第一颗挖矿专用芯片烤猫 BE100 开始已经达到 850GH/s，到最新一代蚂蚁矿机 S17 达到 56 TH/s (1T=1024G)，哈希运算能力在不断增强，而能耗比方面，已经降到了 GPU 的 1/10,000。采用专用芯片以外的方法进行挖矿，在经济上已经不可行。例外的是，以太坊等一部分加密资产，认为 ASIC 挖矿有损加密资产社区的公平性，因此调整算法，限制 ASIC 挖矿的性能，这些加密资产的挖矿目前以 GPU 方法为主。

图表 70: 主要共识机制及其对应芯片解决方案

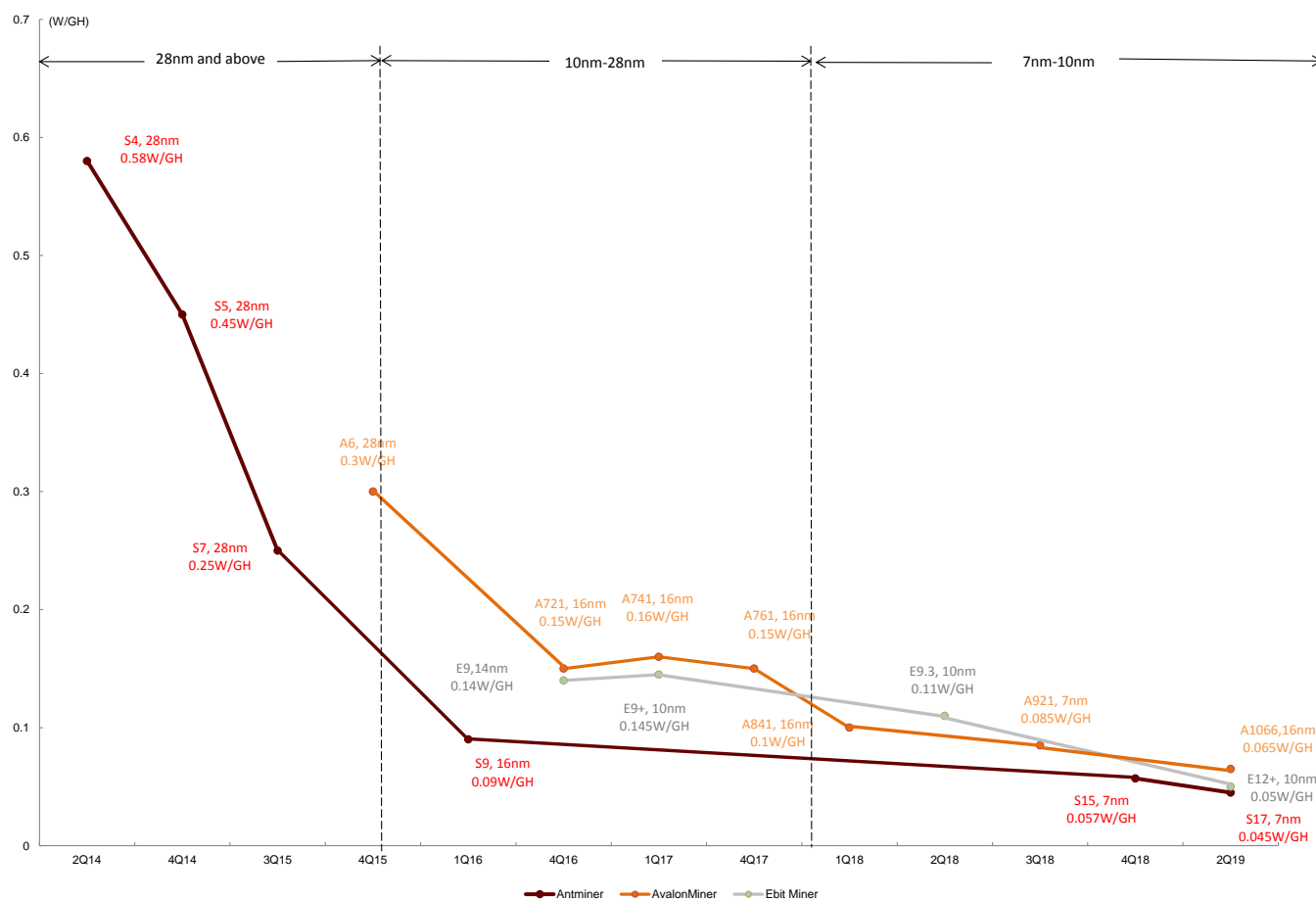
	PoW		PoS	DPoS	PBFT
区块链应用	BTC/BCH	ETH	NXT	EOS	Hyperledger Fabric
芯片解决方案	ASIC	CPU/GPU	CPU/GPU	CPU/GPU	CPU/GPU
主要厂商	嘉楠耘智、亿邦国际	英特尔、英伟达、AMD	英特尔、英伟达、AMD	英特尔、英伟达、AMD	英特尔、英伟达、AMD
2017年市场规模	30亿美元	很小	很小	很小	未知

资料来源：AMD，英伟达，英特尔，嘉楠耘智，亿邦国际，中金公司研究部

**矿机迭代追逐最新制程。**由于能耗比是矿机芯片的主要性能参数，矿机芯片一般采用最先进的半导体制造工艺进行生产。从台积电的季报业绩披露可以看到，矿机芯片与苹果手机芯片、英伟达等的 GPU 芯片一起成为 7nm 等台积电最先进工艺的主要用户。除了采用最先进的半导体生产工艺以外，矿机厂商也通过采用自己研发的低功耗 IP 等方法，降低整体功耗。



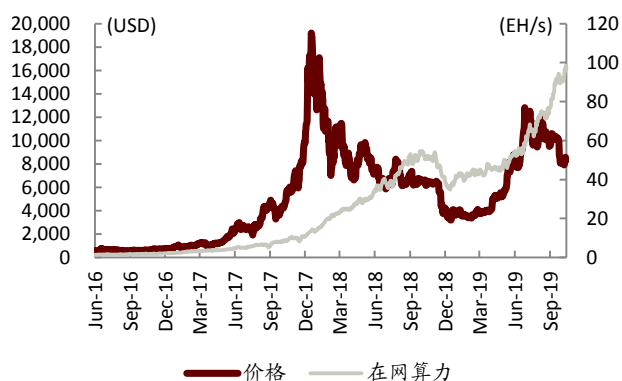
图表 71: 主流矿机性能演进



资料来源：中关村在线，中金公司研究部

在网算力持续升高，有望拉动相关半导体产业链的需求。我们注意到，比特币价格自 2019 年年初以来，涨幅超过 120%，同时比特币在网算力也上涨 133%；以太坊价格上涨 27%，在网算力上升 10%。币价的波动直接影响着加密货币相关的半导体产业链的发展。我们认为，随着币价回暖，在网算力将持续升高，拉动相关半导体产业链的需求。

图表 72: 比特币价格及在网算力



资料来源：bitcoin.com，中金公司研究部

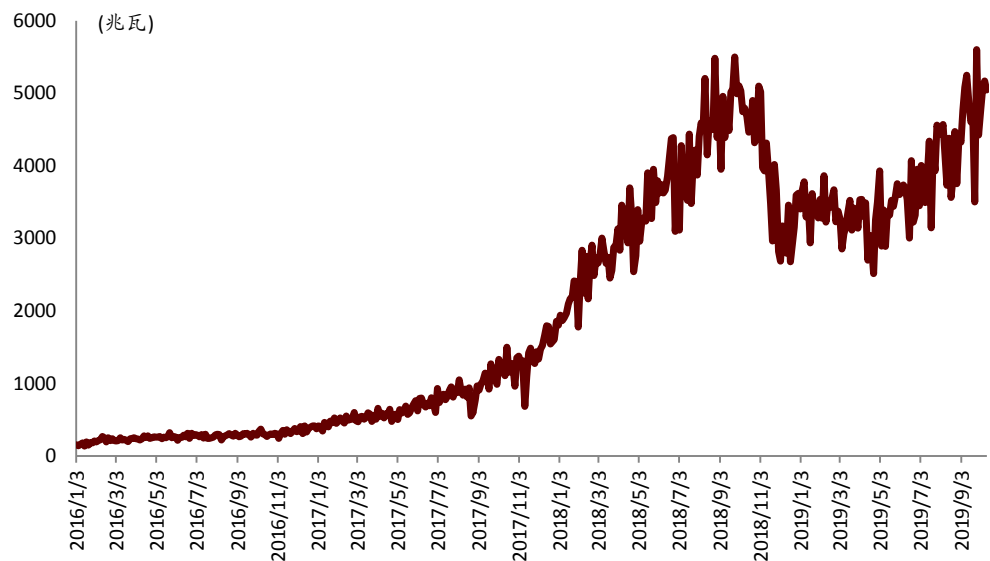
图表 73: 以太坊价格及在网算力



资料来源：etherscan.io, Coincodex，中金公司研究部



图表 74: 比特币挖矿全球能耗变化



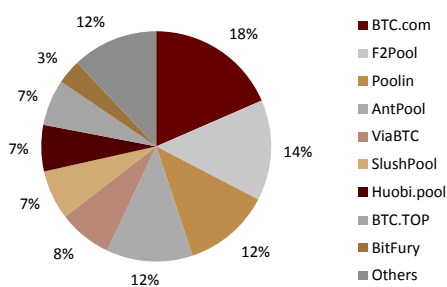
资料来源: bitcoin.com, 中金公司研究部; 注: 以在网算力和典型矿机能效比估算

#### 矿池算力集中度稳定

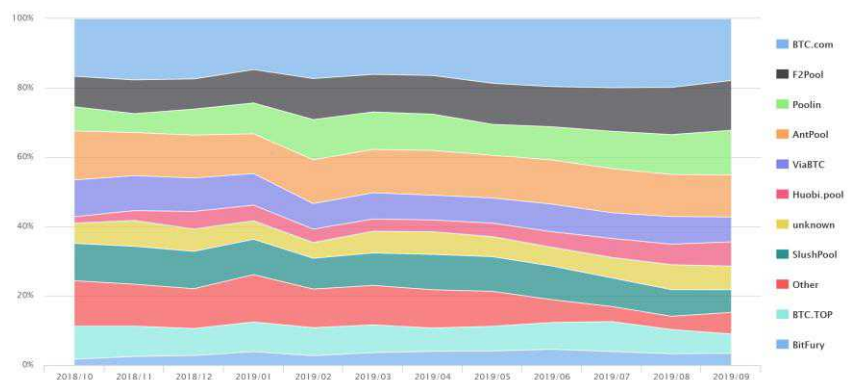
矿池的主要职能是协调大量矿工的算力共同挖矿, 矿池中的全部矿工共享奖励。通常情况下, 矿池会收取一定比例的费用。对矿工来说, 与单独个人挖矿相比, 加入矿池有两个优势: 一方面可以避免运行比特币全节点所需要的存储和带宽成本; 另一方面通过和其他矿工分享收益, 可以提高挖矿回报的稳定性。2018 年 12 月 3 日全网算力约 38.88EH/s, 一台蚂蚁 S9 算力为 13.5TH/s, 一天理论上可以挖到 0.063% 个比特币。

根据 BTC.com 统计, 以近 3 个月比特币出块数据计算, 目前前 6 大矿池垄断 71.5% 算力, 未加入矿池的独立算力不足总算力的 7%。过去一年, 94% 的比特币由矿池所属的地址挖到。我们注意到过去一年里, 矿池算力集中度较为稳定, CR6 基本保持在 70% 水平。

图表 75: 比特币矿池算力占比



图表 76: 比特币矿池市场份额变化



资料来源: btc.com, 中金公司研究部; 注: 以 2019/10/13 近 3 个月出块数据计算

资料来源: btc.com, 中金公司研究部





**交易所：提供衍生品交易服务成趋势，交易量真实性有待考证**

我们认为加密货币交易所可以分为两类，一类交易所重视合规，仅支持法币与加密资产兑换，如 Coinbase 和 Circle；另一类重在提高交易量，提升交易所活跃度，比如币安、火币等。相比仅提供现货交易的老牌交易所 Coinbase、BitMEX、火币、OKEx 等交易所通过提供高频的衍生品合约交易服务，使其交易量迅速提升。其中，提供百倍杠杆、相对低费率的 BitMEX 吸引了大量客户，交易量稳居前列。2019/10/14，BitMEX 近 30 天交易量达 706 亿美元。

2019 年 5 月，Bitwise 向美国 SEC 递交的一份白皮书认为，86% 的加密货币交易量可能是伪造的，且在其调查的 80 多交易所中，仅有 Binance、Bitfinex、Coinbase、Kraken、Bitstamp、BitFlyer、Gemini、itBit、Bittrex、Poloniex 等 10 家交易所的交易量是真实的。

**图表 77：主要交易所交易量排名（截止 2019/10/14）**

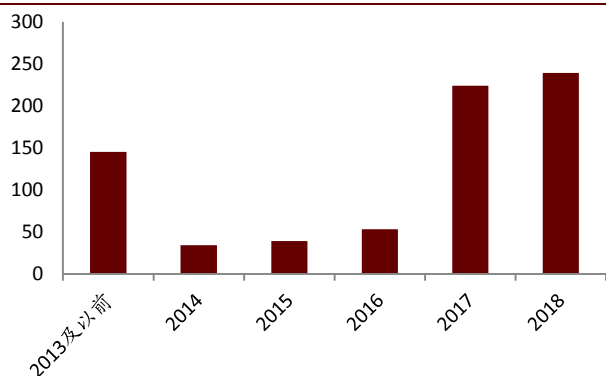
#	名称	近30天交易量	交易对数	成立时间	注册地
1	BitMEX	\$70,626,273,362	1	2014/1	塞舌尔
2	Fcoin	\$40,789,231,192	60	2018/5	新加坡
3	EXX	\$32,210,722,055	28	2018/7	马耳他
4	BKEX	\$31,241,863,623	80	2018/5	英属维尔京群岛
5	币安	\$28,387,753,612	556	2017/7	马耳他
6	MXC	\$26,716,334,536	171	2018/4	新加坡
7	胖比特	\$26,287,168,831	125	2017/12	美国
8	Coineal	\$25,852,137,124	37	2018/4	塞舌尔
9	Latoken	\$25,679,135,333	260	2017/9	爱沙尼亚
10	满币	\$25,096,135,712	215	2017/9	新加坡
11	OKEx	\$24,434,264,895	466	2014/1	马耳他

资料来源：CoinMarketCap, Crocosource, bt110, 中金公司研究部

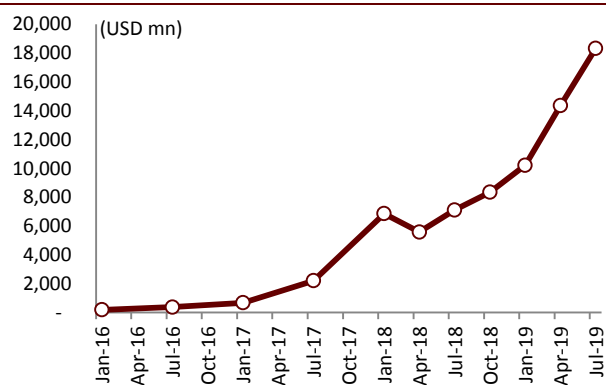
**加密货币基金：加密资产已成为一种新的另类投资资产**

加密资产已成为一种新的另类投资资产。据 CryptoFundResearch 统计，2017 年、2018 年新增加加密货币基金数量分别为 224 个、239 个；同时，目前加密货币基金管理规模 (AUM) 增长稳健，截至 2019 年 7 月，加密货币基金 AUM 已达到 183.2 亿美元。

2019/10/4，香港证监会（SFC）正式发布了针对加密资产基金管理人的监管条例。该条例适用于投资标的为虚拟资产的基金，以及有意向将 10% 及以上净值投资于虚拟资产的基金。这里的“虚拟资产”包括各类数字货币，以及其他虚拟商品或加密资产等。

**图表 78：新增加加密货币基金数量**

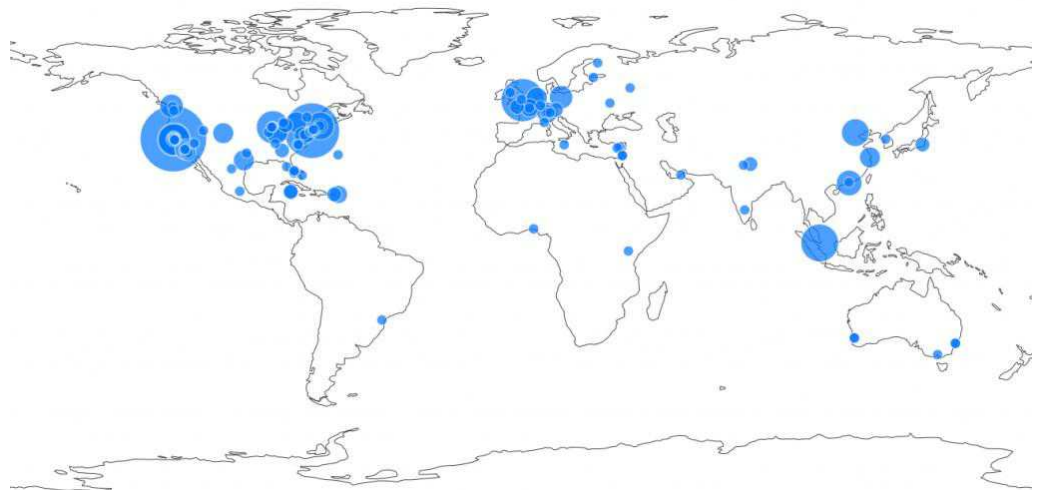
资料来源：CryptoFundResearch, 中金公司研究部

**图表 79：加密货币基金管理规模**

资料来源：CryptoFundResearch, 中金公司研究部



图表 80: 全球加密货币基金设立地点分布

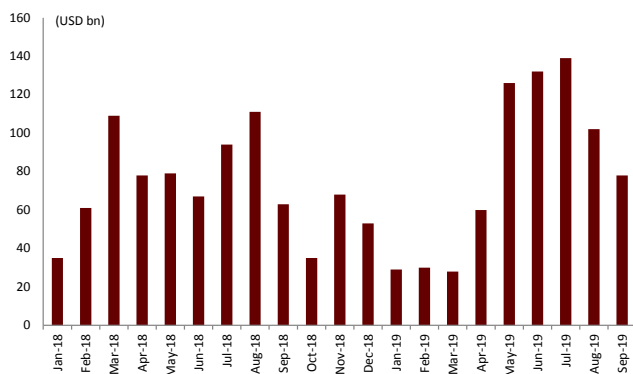


资料来源: CryptoFundResearch, 中金公司研究部

## 衍生品: 芝加哥商品交易所等开始上线比特币期货产品

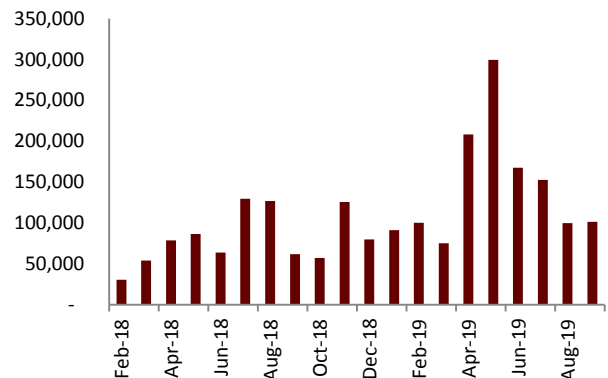
BitMEX 是全球最大的比特币期货交易平台, 据 CryptoCompare 数据, 全球 90% 以上的比特币期货交易是在 BitMEX 上完成的。从历史数据看, 比特币期货的交易量受加密货币市场行情影响较大, 历史交易量较为波动。2019/9, BitMEX 的比特币期货月交易量达到 780 亿美元。

图表 81: BitMEX 比特币期货月交易量



资料来源: BitMEX, 中金公司研究部

图表 82: CME 比特币期货合约数



资料来源: Bloomberg, 中金公司研究部

2017 年底, 芝加哥期权交易所 (CBOE) 和芝加哥商品交易所 (CME) 推出了比特币期货合约交易服务, 为未持有比特币的专业投资者提供了比特币期货的交易平台。CBOE 已经于 2019/5 停止了比特币期货合约的交易, CME 目前占据了比特币期货交易的大多数份额。受 CBOE 比特币期货停止的影响, 2019/5/13, CME 的比特币期货交易量首次超过 10 亿美元、交易合约数达 33,677 份。2019/9/20, CME 宣布计划于 2020 年第一季度推出比特币期权交易服务。

2019/9/22, 纽交所 (NYSE) 母公司洲际交易所 (ICE) 的子公司 Bakkt, 在获得美国商品期货交易委员会 (CFTC) 的监管牌照后, 正式推出了合规的实物交割比特币期货。我们认为, Bakkt 的意义在于, 一方面提供了加密货币实物提供了合规交易平台, 另一方面, 实物交割的比特币期货能防止市场操控, 有望成为长期的定价标准。



图表 83: Bakkt 与其他加密货币期货交易所对比

平台	交易品种	合约周期	合约类型	最大杠杆	最小合约价值	交易门槛	交易成本
BAKKT	BTC	定期（日/月）	双向	100x	1BTC	高	50美分/笔
BitMEX	XBT/ADA/BCH/ETH/LTC/TRX/XRP	永续/定期	反向/双向/线性	100x	1USD	较低	手续费
OKE	BTC/LTC/ETH/ETC/BCH/XRP/EOS/BTG	永续/定期	反向/双向/线性	20x	100USD	高	手续费
CBOE	XBT	定期（周/月/季度）	线性	2x	1BTC	高	合约价值的0.03%手续费
CME	BTC	定期（季度）	线性	3x	5BTC	极高	合约价值的0.03%手续费
HUOBI	BTC/ETH	定期	反向/双向/线性	10x	10USD	低	手续费
BBX	BTC/ETH/EOS/BCH	永续	正向/双向	100x	1USD	低	手续费
BTC Global	BTC/XRP/ETH/BCH/LTC/ADA/EOS/XLM	永续	线性	100x	4USD	较低	点差，隔夜利息无手续费

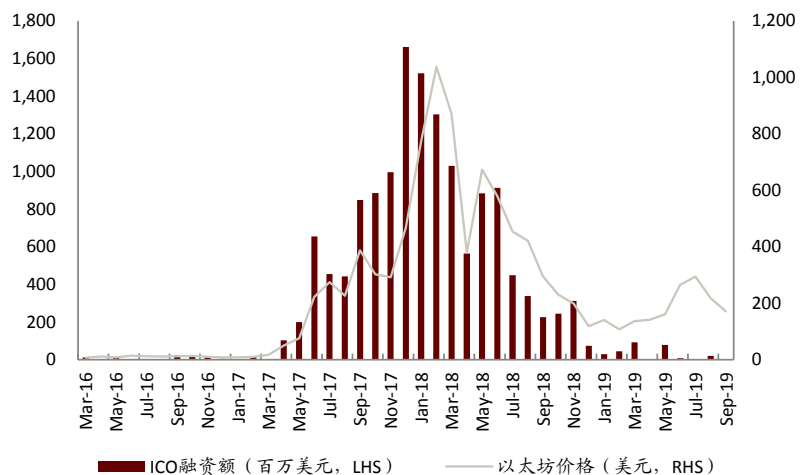
资料来源：星球日报，中金公司研究部

## ICO 基本失去融资能力，加密资产借贷业务开始兴起

以太坊 ICO（首次代币发行，Initial Coin Offering）是一种基于区块链智能合约的网上集资方式，ICO 发起人通过发行独创的加密资产以换取市场广泛使用的加密资产（如比特币、以太坊等），来发展公司的营运项目，投资者获得相关区块链项目的收益权。ICO 主要分为：资产支持加密电子货币（Asset-Backed Cryptocurrency）和效能代币（Utility Token），第一种有资产背书。目前 ICO，特别是没有资产背书的 Utility Token 存在诈骗等问题，有往 STO（Security Token Offering）发展趋势。STO 被称为证券化代币发行，其目标是在一个合法合规的监管框架下，实现代币的公开发售，以保证投资人利益。

伴随着比特币价格的上升，从 2017 年年初开始，ICO（Initial Coin Offer）融资额开始迅速上升，2017 年 12 月达到最高峰的单月融资额 16.6 亿美元。2018 年上半年 ICO 依然活跃，下半年受币价下跌以及各国强化监管的影响，市场迅速萎缩。根据 icodata 统计，全球 ICO 总募资额 2017 年 62.6 亿美元，2018 年为 78.6 亿美元。2017 年 ICO 总募资额相当于 Dealogic 统计的 2017 年全球 IPO 募资额（1992 亿美元）的 3%。

图表 84: ICO 融资额 vs. 以太坊价格



资料来源：icodata.io, CoinMarketCap, 中金公司研究部



截至 2018 年 12 月 31 日，ETH、EOS 等成功的 ICO 项目为投资人带来 38240%、158% 的高额回报。但参与 TTU、DRG、SRN 等项目的投资人几乎血本无归。主要原因包括：

- ▶ ICO 不是股权或者债权融资，目前仍没有完备的制度或法律，来监督被投资企业按照白皮书所写严格执行募资计划。和目前的 IPO 相比，ICO 流程无法保证资产上链时的准确性。
- ▶ 早期 ICO 主要被用作初创项目的融资，而项目本身就有较高的失败概率。一般而言，传统的初创项目融资应该由风险投资（VC）等专业机构执行。
- ▶ 甚至还出现了以欺骗投资人作为目的的空气币，这些项目并没有被按照白皮书执行，造成投资人对 ICO 整体失去信心。

图表 85：首例 ICO 以太币（ETH）及前十大 ICO 项目发行后价格表现

ICO 项目	代币	融资金额 (百万美元)	ICO 结束 日期	发行价 (美元)	2018/12/31 价格	2018 年底价格 较发行价涨跌幅
Ethereum	ETH	18	2014/09	0.36	136.91	38240%
EOS	EOS	4,200	2018/06	0.99	2.55	158%
Telegram	Gram	1,700	2018/03	1.10	-	-
TaTaTu	TTU	575	2018/06	0.25	0.02	-91%
Dragon	DRG	320	2018/03	3.03	0.05	-98%
Huobi	HT	300	2018/02	1.52	1.10	-28%
Filecoin	FIL	262	2017/09	5.00	2.92	-42%
Tezos	XTZ	232	2017/07	0.47	0.50	6%
SIRIN LABS	SRN	158	2017/12	1.53	0.04	-97%
Bancor	BNT	153	2017/06	3.86	0.64	-83%
Bankera	BNK	151	2018/03	0.02	0.00	-81%

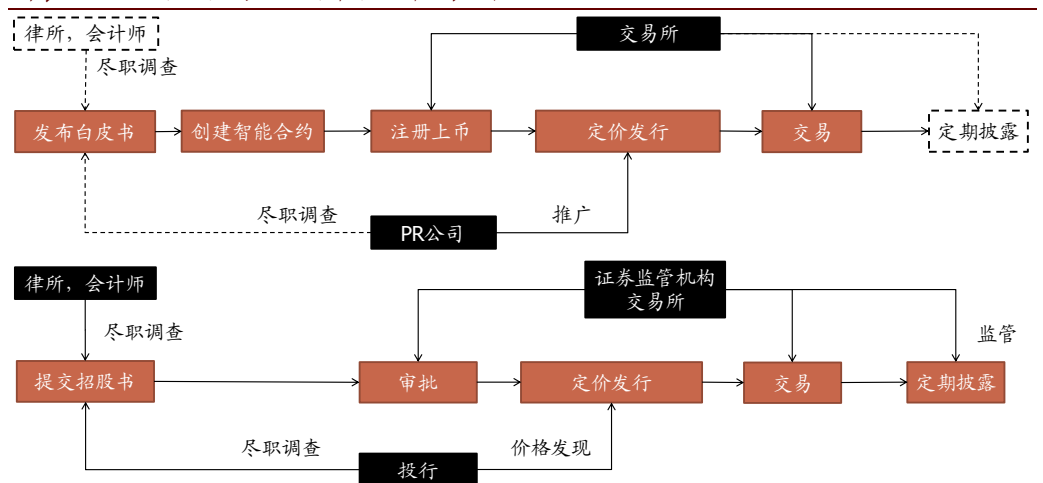
资料来源：CoinMarketCap, icodata.io, icodrops.com, icobench.com, 中金公司研究部；注：Gram 尚未在主网上线

图表 86：ICO、IPO、STO 与 ABS 的比较

	中文名	权益形式	交易场所	交易货币	投资人	法律监管	上市费用
IPO	首次公开发行	股权	股票交易所	法币	一般投资人	严格	高
ICO	首次通证发行	区块链内使用权	虚拟资产交易所	虚拟货币	所有公众	不明确	低
STO	证券通证发行	债权、股权、使用权等	虚拟资产交易所	虚拟货币	个案不同	一定监管	较低
ABS	资产证券化	债权	债券交易所	法币	专业投资人	一定监管	-
PE	私募股权	股权	无	法币	专业投资人	严格	-

资料来源：blockcircles, 中金公司研究部

图表 87：ICO（上）与 IPO（下）流程的比较



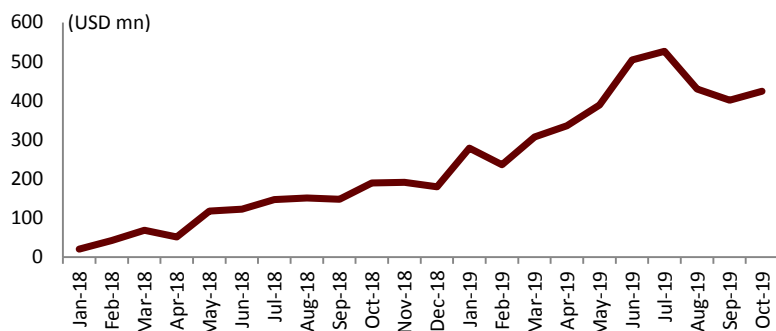
资料来源：翟晨曦等《区块链技术在金融领域的作用浅析》（2017），中金公司研究部



## 基于加密资产的借贷业务开始兴起

区块链行业的一个新趋势是基于加密资产的借贷业务开始兴起。基于以太坊的自动化抵押贷款平台 MakerDAO 于 2017 年底上线，是目前最知名、最有代表性的 DeFi 项目之一。根据 DeFi Pulse 统计数据，截至 2019/10/13，DeFi 项目总锁仓规模为 5.48 亿美元，其中 MakerDAO 占比达 53.16%；借贷类 DeFi 项目总锁仓规模为 4.42 亿美元，其中 MakerDAO 占比达 65.96%。

图表 88：借贷类 DeFi 项目总锁仓规模



资料来源：DeFi Pulse，中金公司研究部

图表 89：主要借贷类 DeFi 项目 (2019/10/16)

#	项目	区块链 技术	锁仓规模 (美元)	年化利率
1	Maker	以太坊	\$277.8M	10.5%
2	Compound	以太坊	\$111.6M	v1: 15.3% v2: 12.5%
3	InstaDApp	以太坊	\$31.6M	12.5%
4	dYdX	以太坊	\$25.9M	10.3%
5	Nuo Network	以太坊	\$10.7M	10.7%

资料来源：DeFi Pulse，loanscan.io，中金公司研究部

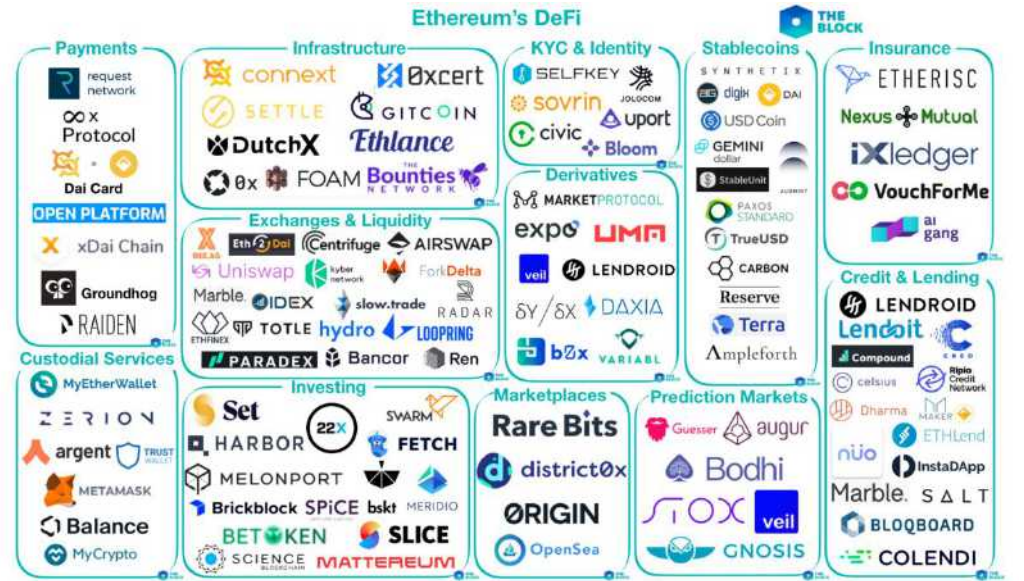
目前的传统金融服务是以中心化的金融机构提供的，具有繁杂的审核流程、区别化的服务、透明度低、手续费高、效率低等缺点。DeFi (Decentralized Finance, 去中心金融) 利用区块链技术，基于通证化资产，能够实现平等、高效、高透明、高可信的金融服务。得益于智能合约的应用，DeFi 的合约实现了自动执行，因此高度平等、可信；同时，DeFi 大幅缩减了中间环节，具有更高的效率、更低的手续费。DeFi 项目包括稳定币、借贷、衍生品、支付、去中心化交易所以及 KYC/AML 等类型，典型的项目有：

- ▶ **稳定币：Dai。** 用户通过抵押加密资产（目前仅支持以太币）获得 Dai 货币，以智能合约为主体的超额抵押和强制清算机制维持了 Dai 对美元的稳定币价。发行 Dai 时，用户需要存入超过所获 Dai 价值 2~3 倍的其他加密资产，当抵押物价值下跌至 1.5 倍时，会触发强制清算，以折价激励向其他用户出售抵押物以收回 Dai，从而维持了已发行在外 Dai 总数量与抵押池总资产美元价值的平衡。相比于其他稳定币，这种稳定币不存在中心化发行机构，避免了审计不公开和超额发行的风险，此外使用加密资产而非美元抵押使得它具有更强的流动性。
- ▶ **借贷/衍生品：dYdX 平台。** dYdX 是一个建立在以太坊区块链上的去中心化金融协议，允许用户进行点对点的代币借贷与保证金交易，未来还将支持更多衍生品类别。通过一系列智能合约，实现抵押物仓位维护、交易执行、利率设置以及资产托管等功能。
- ▶ **支付：xDAI。** xDAI 是拥有专属侧链的稳定币，被用于建立单一代币的支付生态系统。通过建立全新侧链，使 xDAI 成为链上的原生代币，通过桥接机制，使得 xDAI 价值与稳定币 DAI 挂钩。不同于以太坊主链，新链的基础协议可以深度修改，通过建立半中心化的共识机制，解决了处理速度慢等链上货币用于支付的固有问题。
- ▶ **去中心化交易所：Loopring。** Loopring 是一种去中心化交易所的底层协议。通过嵌入在智能合约完成去中心化的交易匹配与指令执行，用户不再需要将加密资产托管在交易所。通过在交易匹配协议中引入环路撮合算法，可以实现跨币种的多边交易。
- ▶ **KYC/AML：Bloom。** Bloom 是基于以太坊的个人信用信息采集、加工、评分的区块链解决方案。Bloom 由三部分组成，身份系统允许用户创建自己在 Bloom 上唯一的身份信息；信用系统储存了用户的借贷历史记录；评分系统会根据用户的信用记录进行信用评级。通过与其他中心化或去中心化网络连接，可以在区块链分类账上自动化进行大量信用信息的记录、处理工作，提高信用信息的追溯性和安全性。





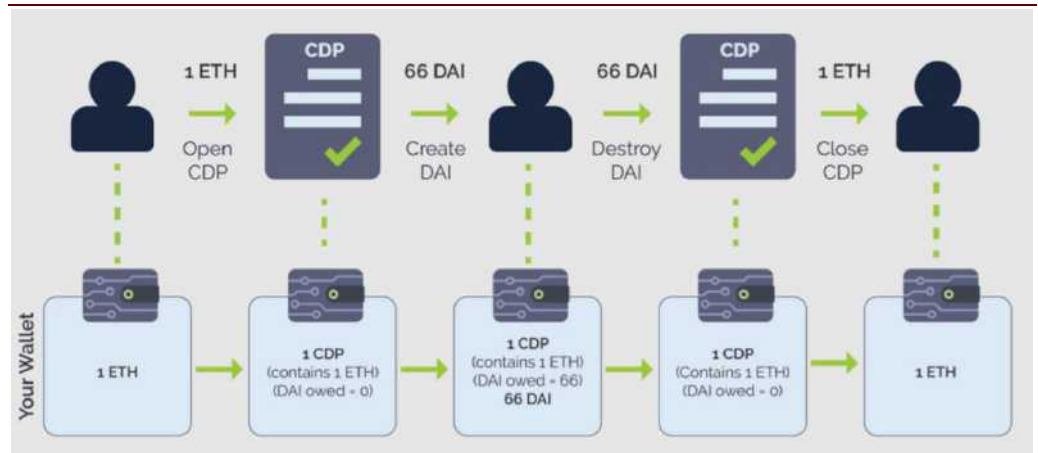
图表 90: 主要以太坊 DeFi 项目



资料来源: The Block, 中金公司研究部

MakerDAO 成立于 2014 年,是最早的去中心化的自治组织 (Decentralized Autonomous Organization, DAO) 之一。MakerDAO 推出的稳定币 Dai 于 2017/12 上线, Dai 通过超额抵押以太坊 (ETH), 实现了与美元 1:1 锚定。除稳定币 Dai 以外, MakerDAO 还发行了代币 MKR。MakerDAO 的借还款过程: 借款者以不小于 150% 的质押率将自己的 ETH 抵押给 MakerDAO 后, 获得 Dai; 当赎回抵押的 ETH 时, 需要支付 MKR。MakerDAO 的利息率是由 MKR 所有者投票决定的。借款者抵押 ETH、获得 Dai 的过程中, 需要将自己的 ETH 经过 WETH、PETH 等类 ETH 通证的中间转换环节, 采用智能合约技术的 CDP (Collateralized Debt Positions, 抵押债仓) 自动实现 Dai 的生成和回收。

图表 91: MakerDAO 借贷和还款运行机制



资料来源: Blockchain Whispers, 中金公司研究部



## 展望：区块链如何赋能传统金融

10 月 24 日，习近平总书记主持中央政治局第十八次集体学习，强调区块链技术的重要性，要把区块链作为自主创新的重要突破口，加大投入力度，推动产业创新发展<sup>23</sup>。经过过去几年发展，区块链技术已经被证明适合需要“多方共享”、“高频重复”、“交易链条长”的许多金融场景。我们认为，总书记的发言会大幅加速区块链技术在我国的落地速度，提升金融、政府等行业的运作效率。

**区块链如何赋能传统金融：**区块链的一个优势是通过数字签名等密码学技术，在保证数据唯一性和所有权不可篡改的前提下，实现多方之间的信息共享。这适合需要“多方共享”、“高频重复”、“交易链条长”的许多金融场景。过去几年，我们看到的主要应用案例包括：在跨境汇款领域，蚂蚁金服利用区块链技术为香港，以及菲律宾、巴基斯坦、马来西亚等一带一路沿线国家提供低费率、高速的跨境汇款服务。在清结算领域，港交所计划利用区块链结算系统简化互联互通下内地股票的北向交易流程，方便欧美投资人投资 A 股。在贸易融资领域，香港金管局和平安合作推出区块链贸易融资技术平台“贸易联动”，增加贸易参与者之间的信任，降低风险，提高贸易流程中获得融资的机会。

**中国金融企业积极拥抱联盟链：**金融企业在区块链方面的布局，一方面是投资区块链初创企业，另一方面是在开源架构或自建架构基础上的区块链业务实践。国内金融机构（中行、招行、平安、微众银行、蚂蚁金服、京东金融、港交所等）及国际金融机构（高盛、摩根士丹利、摩根大通、花旗、纳斯达克、澳交所等）在货币、跨境支付、清结算、贸易融资、ABS、风控等业务中，开始尝试运用区块链技术。此外，蚂蚁金服、平安科技等金融科技公司已经开始向外输出能力。

**中国科技企业在全球区块链行业占据重要地位：**区块链行业主要包括 1）以太坊、Hyperledger Fabric 等开源框架；2）蚂蚁区块链、平安、腾讯、万向等提供的区块链平台；以及 3）专注于行业应用的初创企业。目前大部分企业仍处于探索商业模式的阶段，主要的商业模式包括 1）提高集团自身现有业务效率，2）为政府及金融机构提供解决方案，3）向中小企业提供云服务等三条路径。根据 IPRdaily 和 incoPat 统计，2019 上半年全球企业区块链公开专利前 20 名中，中国企业占比 75%，其中蚂蚁金服、中国平安、腾讯、万向等企业在区块链平台技术上占据领先地位。此外，根据我们不完全整理，A/H/中概股中 66 家公司有区块链相关业务（参见图表 126）。其中市值较大的企业包括阿里巴巴、腾讯、平安、恒生电子、航天信息、众安在线等，未来如何受益有待进一步研究。

<sup>23</sup> [http://www.xinhuanet.com/politics/leaders/2019-10/25/c\\_1125153665.htm](http://www.xinhuanet.com/politics/leaders/2019-10/25/c_1125153665.htm)



### 习近平总书记明确区块链成为自主创新下一个重要突破口<sup>24</sup>

中共中央政治局 10 月 24 日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。

总书记指出，区块链技术应用已延伸到**数字金融、物联网、智能制造、供应链管理、数字资产交易**等多个领域。目前，全球主要国家都在加快布局区块链技术发展。我国在区块链领域拥有良好基础，要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展。

总书记强调，要强化**基础研究**，加强区块链**标准化研究**，加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合，发挥区块链在促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系等方面的作用。

习近平就以下几个具体领域对我国区块链发展做出重要指示：

**促进实体经济发展。**要推动区块链和实体经济深度融合，解决中小企业贷款融资难、银行风控难、部门监管难等问题。利用区块链技术探索数字经济模式创新，打造便捷高效、公平竞争、稳定透明的营商环境，推进供给侧结构性改革、实现各行业供需有效对接提供服务，加快新旧动能接续转换、推动经济高质量发展。

**保障和改善民生。**积极推动区块链技术在教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用。

**推进智慧城市建设。**探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理的智能化、精准化水平。要利用区块链技术促进城市间在信息、资金、人才、征信等方面更大规模的互联互通，保障生产要素在区域内有序高效流动。

**提升政务管理水平。**要探索利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，深化“最多跑一次”改革，为人民群众带来更好的政务服务体验。

此外，习近平总书记还特别提到了区块链技术风险防范。总书记指出，要加强对区块链安全风险的研究和分析，密切跟踪发展动态，探索建立适应区块链技术机制的安全保障体系，引导和推动区块链开发者、平台运营者加强行业自律、落实安全责任。要把依法治网落实到区块链管理中，推动区块链安全有序发展。

<sup>24</sup> [http://www.xinhuanet.com/politics/leaders/2019-10/25/c\\_1125153665.htm](http://www.xinhuanet.com/politics/leaders/2019-10/25/c_1125153665.htm)



### 金融企业如何拥抱区块链

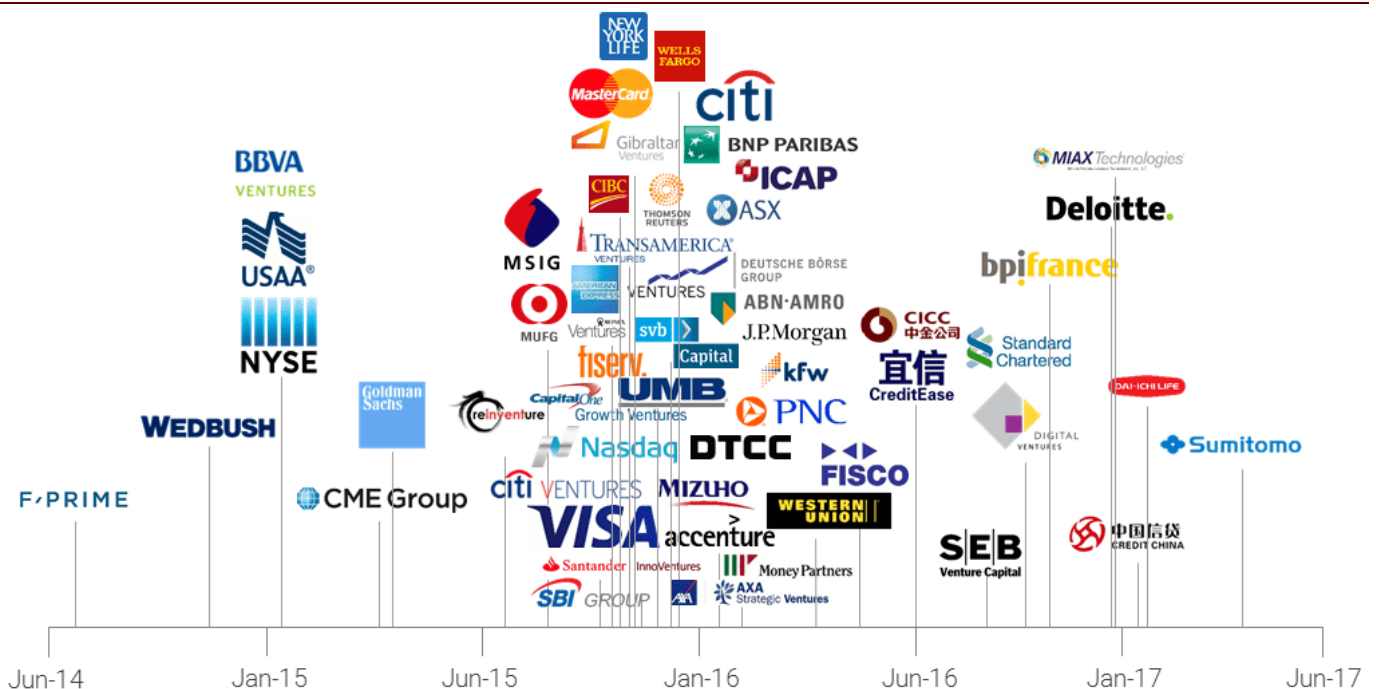
国际上金融企业在区块链方面的布局，一方面是投资区块链初创企业，2015 年起国际主流金融机构纷纷开始区块链相关的投资；另一方面是在开源架构或自建架构基础上的区块链业务实践。国内金融机构（中行、招行、平安、微众银行、蚂蚁金服、京东金融、港交所等）及国际金融机构（高盛、摩根士丹利、摩根大通、花旗、纳斯达克、澳交所等）在货币、跨境支付、清结算、贸易融资、ABS、风控等业务中，开始尝试运用区块链技术。

由于 1) 目前中国大部分金融机构的业务按照分业经营的原则设立而非“金融超市”式的混业经营（Universal Banking，即以商业银行为主要业务，但同时提供包括保险、投行等各类型的金融服务，例如花旗银行、汇丰银行在海外的布局）；2) 金融机构在非金融行业的股权投资受到严格监管，中资金融机构目前主要通过投入内部自研而非外包的方式进行区块链技术的储备和研究，并将重点放在解决现有业务的痛点。

就商业银行而言，目前区块链主要应用在跨境支付、清算结算、贸易融资和风控等领域。主要解决的痛点是原有业务交易确认和交割环节昂贵耗时、多参与主体交互认证效率低下、部分业务重复性强工作量大容易诱发操作风险等问题。但是，目前尚未有覆盖各主要商业银行的区块链技术协议或联盟，不同银行间开发的类似系统并不互认。

此外，中国的金融科技公司（Fintech）近年来发展快速，技术能力快速提高。头部金融科技公司的营收和利润规模在全球范围内都处于领先地位，保证了高强度的技术投入和迭代速度，并在部分领域（例如移动支付）达到全球领先水平。和金融行业头部公司基本为国有企业不同，头部金融科技公司大部分是民营企业，且其业务通过内生增长和股权投资已拓展到全球多个国家。由这些头部金融科技公司开发的基于区块链的部分技术和产品，已逐渐应用于大陆地区以外的部分市场（例如蚂蚁金服的全球汇款业务、基于平安金融科技技术的香港金管局贸易融资平台）。即使在中国大陆市场，由于金融科技公司和中小金融机构之间的合作关系大于竞争关系，我们判断其技术输出的速度也可能较快（例如目前微众银行的联合放贷技术）。

图表 92：金融服务机构首次区块链投资时间轴



资料来源：CB Insights，中金公司研究部





图表 93: 主要国内金融机构区块链实践

货币	跨境支付	清算结算	贸易融资	ABS	风控
 <b>中国银行</b> BANK OF CHINA	参与央行数字货币发行和基于区块链的数字票据交易平台研究工作				区块链抵押贷款估值系统
 <b>招商银行</b> CHINA MERCHANTS BANK	联手永隆银行、永隆深圳分行，成功实现区块链跨境人民币汇款	将区块链应用于跨境直联清算、全球账户统一视图以及跨境资金归集三大场景		牵头完成了以Pre-ABS功能为主的区块链平台	
 <b>中国平安</b> PING AN			中小企业金融服务云平台“壹企银”	金融壹账通ALFA智能ABS平台	
 <b>WeBank</b> 微众银行		与上海华瑞银行合作的“微粒贷”，用于两家银行间联合贷款的结算、清算业务			
 <b>蚂蚁金服</b> ANT FINANCIAL	AlipayHK与Gcash合作开发全球首个在跨境汇款全链路使用区块链的电子钱包				
 <b>京东金融</b> JD Finance				设立“京东金融-华泰资管19号京东白条应收账款债权资产支持专项计划”	与中国银联共建跨机构数据分布式存储及查询平台，接入双方风控数据
 <b>HONG KONG MONETARY AUTHORITY</b> 香港金融管理局			区块链贸易融资技术平台“贸易联动”		
 <b>HKEX</b> 香港交易所		区块链交易结算系统			

资料来源：SVInsight，36kr，中金公司研究部

图表 94: 主要国际金融机构区块链实践

货币	跨境支付	清算结算	贸易融资	ABS	风控
 <b>J.P. Morgan</b>	推出基于Quorum（自建区块链平台）的银行间信息网络平台IIN，解决跨境支付合规问题	在Quorum平台中整合Zcash的零知识证明安全层，以提供安全匿名的结算交易服务	与加拿大国家银行等合作使用区块链技术测试债券发行		
 <b>Citi</b>	Citicoin（已关闭）与Nasdaq合作，使用分布式账本实现到账自动化、自动处理跨境支付				参与 IBM LedgerConnect试运行（处理AML/KYC合规性以及贷款抵押品管理的平台）
 <b>Nasdaq</b>		私有股权交易平台 Linq			
 <b>Bank of America</b>					申请区块链相关专利达53件，涉及风险检测、交易验证、可疑用户警报等方面
 <b>ASX</b>		区块链交易结算系统			
 <b>Goldman Sachs</b>	SETLcoin	使用基于区块链的支付净额结算服务 CLSNet			使用BDS360区块链平台备份交易结算记录及其金融网络所管理下的资产转移
 <b>Morgan Stanley</b>		使用基于区块链的支付净额结算服务			

资料来源：SVInsight，36kr，中金公司研究部

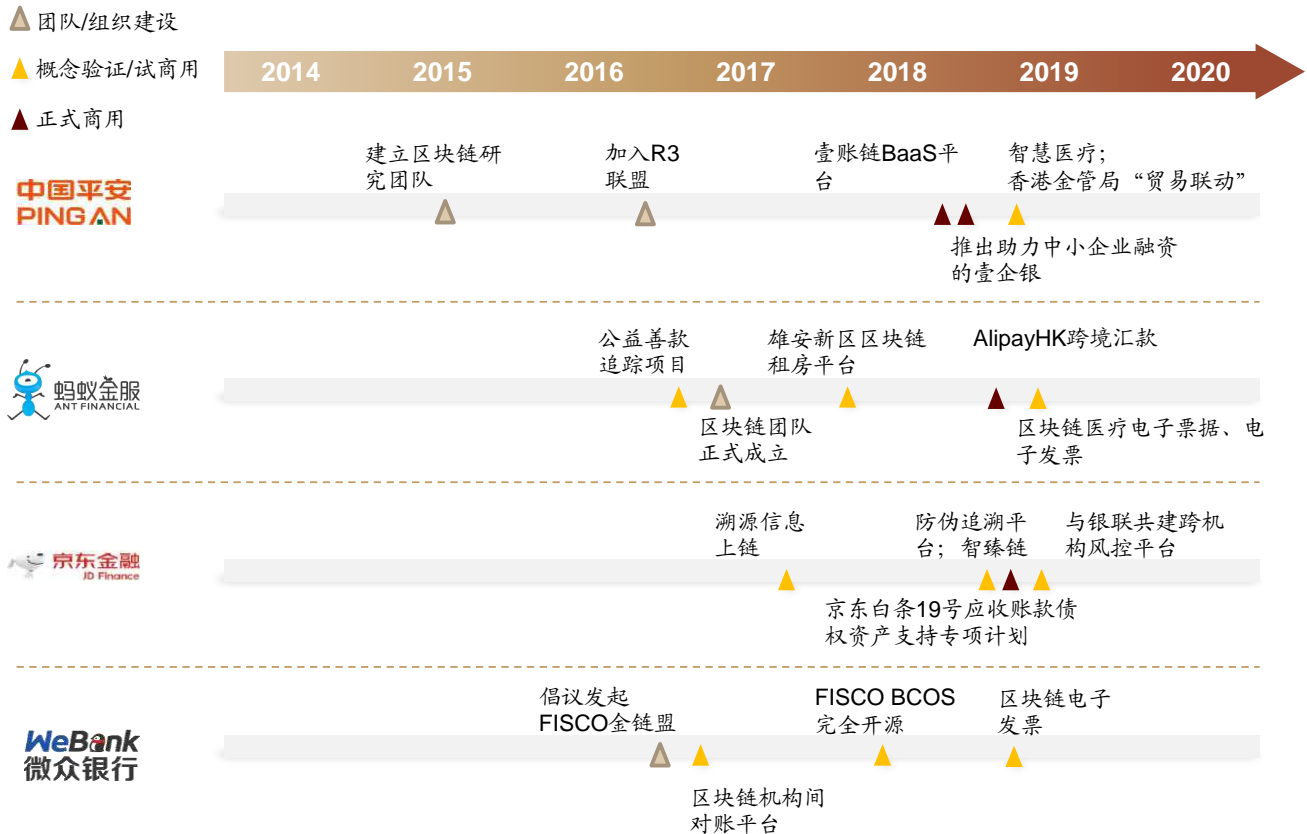




## 科技企业把握区块链发展机遇

过去几年，国内主要科技企业相继建立了自己的区块链团队。通过 1) 提高自身业务效率，2) 外部赋能，3) 云服务等三条路径在不断发展。

图表 95：国内主要区块链平台发展历程



资料来源：Hyperledger，R3，平安，蚂蚁金服，中金公司研究部

- **提高企业自身运营效率：**使用区块链优化业务流程，减少人力成本。例如京东全球购利用区块链技术实现供应链跨境全流程追溯；金融“京小租”信用租赁平台利用区块链解决租赁纠纷。
- **赋能政府与金融机构：**与政府、金融机构深度合作，定制大型解决方案。例如蚂蚁区块链可信公证平台赋能杭州互联网法院司法实践；深圳市税务局与腾讯合作建立区块链发票系统；平安区块链技术支撑香港金管局跨境贸易融资平台。
- **提供快速上链 BaaS 服务：**依托自身云服务的各类基础设施和功能组件，搭建面向中小企业的一站式区块链部署平台。例如华为云区块链服务，与华为云计算、数据库等传统云服务紧密结合，为互联网众筹保险提供全方位技术支持。

图表 96：主要科技企业开展区块链业务情况

企业	采用开源平台	区块链自主开发尝试	区块链服务	典型解决方案
蚂蚁金服	Hyperledger	蚂蚁开放联盟链	阿里云蚂蚁BaaS平台	跨境支付、供应链金融、电子票据
腾讯	Hyperledger, BCOS	TrustSQL	腾讯云TBaaS	供应链金融、电子票据
华为	Hyperledger, BCOS	国内唯一Hyperledger Maintainer，为Hyperledger贡献大量代码	华为云BCS服务	供应链溯源、众筹公证
万向	BCOS	PlatON	新链空间	供应链金融、物流监控
百度	Hyperledger	XuperChain	XuperEngine开放平台	版权追溯
京东	Hyperledger, BCOS	智臻链JD Chain	JD BaaS	物流追溯、信贷风控
平安	Hyperledger, R3 Corda	平安Fimax	平安金融壹账链	跨境贸易融资、资产证券化、物联网数据上链

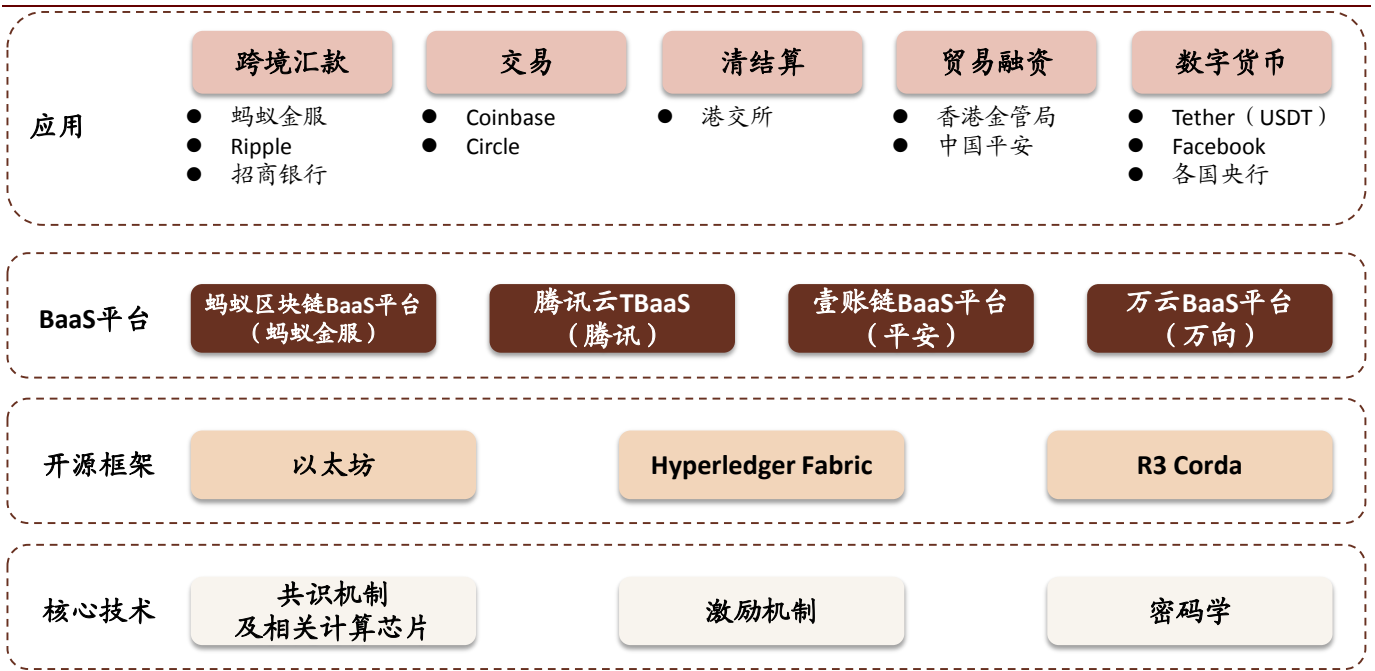
资料来源：蚂蚁金服，腾讯，华为，万向区块链，百度，京东，平安，中金公司研究部



我们将区块链产业分为基础层、服务层、应用层三个层次：

- **基础层**提供底层区块链或分布式账本技术框架，主要包括以太坊、Hyperledger Fabric、R3 Corda、FISCO BCOS 等；
- **服务层**是指 BaaS（Blockchain as a Service）平台，国内主要的 BaaS 平台有蚂蚁区块链 BaaS 平台、腾讯云 TBaaS、平安壹账链 BaaS 平台等；
- **应用层**是指区块链的终端使用者或服务供应商，现在区块链的主要应用场景有跨境支付、防伪溯源、供应链金融、贸易融资、电子票据、ABS 等。

图表 97：区块链产业地图



资料来源：中金公司研究部

**大型科技企业和金融机构区块链布局领先。**根据《福布斯》2019/4 最新发布的全球区块链 50 强（Blockchain 50）榜单，我们看到，谷歌、亚马逊、Facebook、微软、IBM、三星等大型科技企业，以及富达、花旗、摩根大通、Visa、MasterCard、安联保险、法国巴黎银行等金融机构，都在前 50 强之列。国内企业有蚂蚁金服、富士康、HTC 等。

图表 98：福布斯区块链 50 强（Blockchain 50）榜单

安联保险	亚马逊	百威英博	蚂蚁金服	BBVA	BITFURY	法国巴黎银行	BP PLC	BROADRIDGE	BUMBLE BEE FOODS
嘉吉	CIOX HEALTH	花旗集团	Coinbase	康卡斯特	CVS HEALTH	美国证券存托与清算公司	Facebook	富达	富士康
Golden State Foods	谷歌	HPE	HTC	IBM	ING	英特尔	摩根大通	马士基	万事达卡
大都会人寿	微软	纳斯达克	雀巢	Northern Trust	甲骨文	Overstock	PNC	Ripple	三星
Santander	SAP SE	Seagate Technology	西门子	Signature Bank	State Farm	瑞银	维萨	VMware	沃尔玛

资料来源：福布斯，中金公司研究部；注：以首字母顺序排序



**中国企业区块链技术专利储备领先。**根据 IPRdaily 和 incoPat 联合发布 2019 上半年全球企业区块链公开专利申请数排行榜。榜单前 20 名中，中国企业占比 75%；榜单前 100 名中，中国企业占比 67%，美国占 16%，反映出中国企业正积极加大区块链技术研发和专利储备。其中，专利数较为领先的国内企业包括阿里巴巴、中国平安等。

图表 99: 1H19 全球企业区块链专利申请数排行

#	公司	国家/地区	1H19 专利申请数
1	阿里巴巴（蚂蚁金服）	中国	322
2	中国平安	中国	274
3	nChain	安提瓜和巴布达	241
4	复杂美	中国	122
5	IBM	美国	104
6	众安科技	中国	99
7	百度	中国	90
8	元征科技	中国	86
9	中国联通	中国	81
10	MasterCard	美国	79
11	网心科技	中国	74
12	趣链科技	中国	66
13	腾讯	中国	66
14	京东	中国	59
15	Siemens	德国	55
16	中链科技	中国	52
17	点融	中国	51
18	全链通	中国	46
19	泰康	中国	41
20	Accenture	爱尔兰	37

资料来源：IPRdaily，incoPat，中金公司研究部



## 主要区块链框架介绍：Hyperledger、R3

大多数企业采用开源区块链框架为底层协议开发自己的区块链项目，目前主流的框架包括基于公有链的比特币（例如使用 Omni Layer 协议）、以太坊、以及基于联盟链的 Hyperledger Fabric 和 R3 Corda 等。

- ▶ 采用公有链开发的优点是协议公开，信息透明度高，所有数据都可以被公开访问；缺点是很难在满足去中心化和安全性的同时支持很高的交易量。
- ▶ 采用联盟链开发的优点是网络性能高、运作成本较低；缺点是透明性较公有链低。

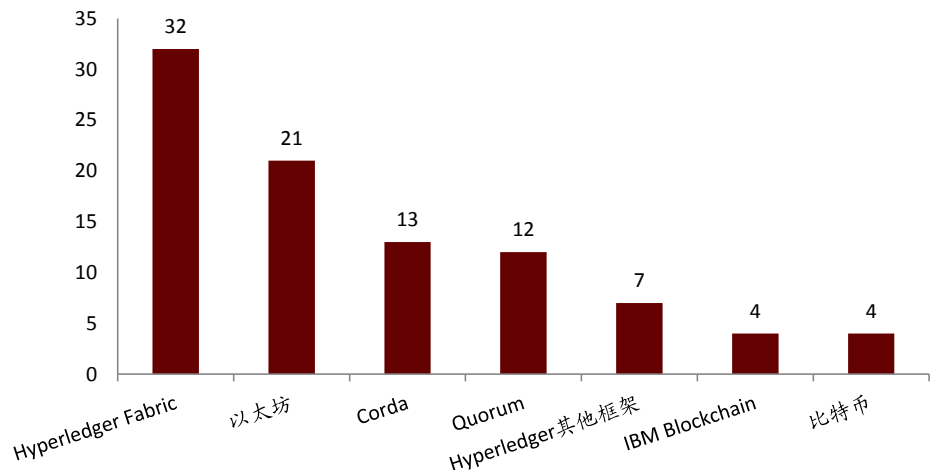
图表 100：主要公有链与开源联盟链开发框架比较

区块链	管理方	共识协议	单链基础TPS	智能合约	使用情况	设计
比特币区块链	公有链	PoW	7	无	比特币、USDT等基于Omni Layer的项目	单一区块链
以太坊	公有链	PoW	10~20	以太坊智能合约	各类加密资产和DeFi项目	引入智能合约功能
Hyperledger Fabric	Linux 基金会	最初采用PBFT，后转用 Kafka	1000	链码设计	覆盖各个行业	多个可交互的区块链网络
Corda	R3CEV	公证人变更共识	没有全局吞吐量	函数式设计	主要为金融企业测试项目	借鉴了区块链的一些机制的分布式账本，但并非区块链
金链盟BCOS	金链盟	并行计算 PBFT、RAFT	1000	EVM引擎智能合约	主要为国内金融机构	国内自主研发开源的企业级区块链底层平台
微软CoCo	微软	Paxos、Caesar	1600	依赖于底层协议	项目较少，如Mojix供应链 Dapp	基于其他底层区块链协议的联盟链
Quorum	企业以太坊联盟（包括芝交所、摩根大通等）	RAFT、Istanbul BFT	600	基于以太坊智能合约	项目较少，如摩根大通的跨行信息交互平台	基于以太坊的标准区块链设计，主要针对金融行业

资料来源：Hyperledger，R3，金链盟，微软，企业以太坊联盟，中金公司研究部

根据福布斯统计，Hyperledger Fabric 是主要企业开发区块链项目采用最广泛的框架。

图表 101：福布斯区块链 50 强（Blockchain 50）中采用不同区块链框架的公司数量



资料来源：福布斯，中金公司研究部；注：福布斯区块链 50 强中有 37 家企业采用了一种以上的区块链开发框架

## Hyperledger

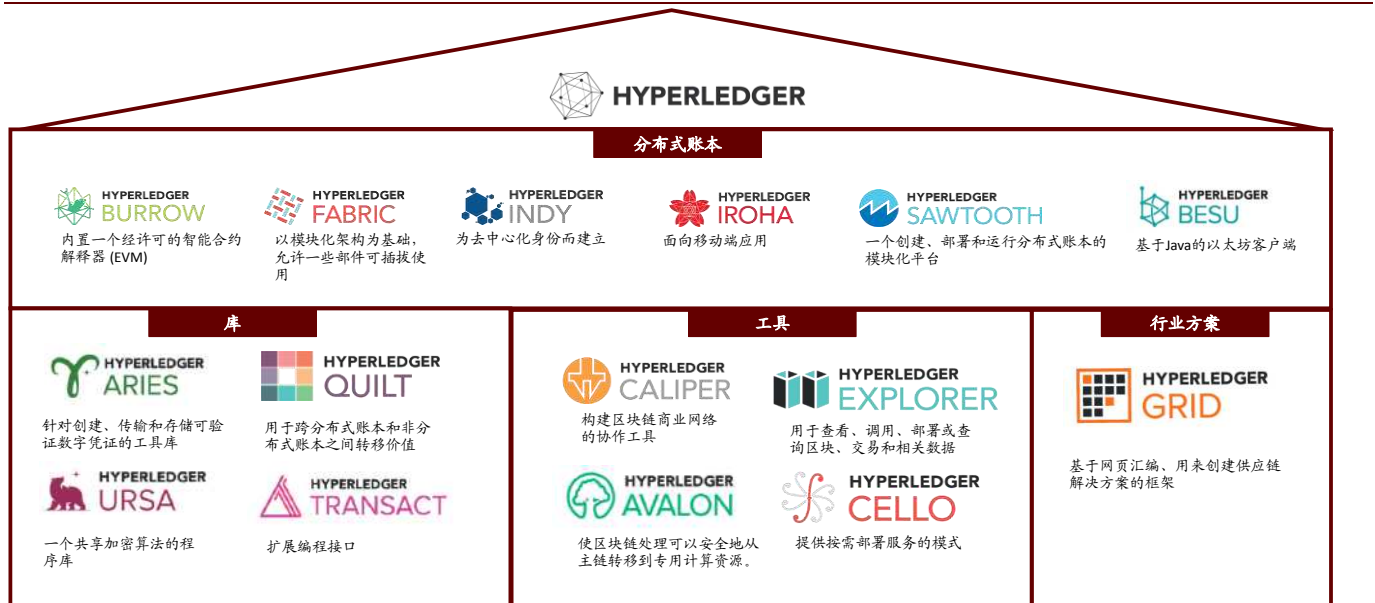
Hyperledger 是全球首个面向企业级应用场景的开源分布式账本平台，由 IBM 公司主导开发，于 2015 年底移交给 Linux 基金会并成为开源项目，目前已发展至 15 个子项目，其中子项目 Hyperledger Fabric 是应用最为广泛的开发框架。Fabric 的应用场景非常丰富，包括可信供应链、资产存管、商务合同、积分交换平台、商品身份溯源、食品安全等。Fabric 的特点：



- ▶ **联盟链框架：**Fabric 是联盟链开发框架，可以满足参与者管理交易的需求、具有一定的封闭性。与比特币、以太坊等公有链使用 PoW 共识机制不同，Fabric 的成员需经授权认证后加入，在一定程度上提高了效率、减少了资源消耗。
- ▶ **模块化结构：**Fabric 采用了模块化的架构，共识算法、密码算法、成员服务等均可根据业务场景需要进行替换、即插即用。

目前 Hyperledger 全球成员超过 275 个，其中中国企业超过 50 家，成员包括阿里云（云计算）、腾讯（云计算）、京东（物流）、华大基因（医疗健康）、民生银行（金融）、真相科技（司法）等多个领域领先企业。

图表 102: Hyperledger 现已发展至 15 个子项目



资料来源：Hyperledger，中金公司研究部

### R3 Corda

R3 Corda 是由 R3CEV 推出的面向金融机构的分布式账本系统，可以用来记录、管理和同步各机构间的协议。Corda 对于金融机构现有的业务系统具有良好的兼容性。Corda 采用类区块链模型，借鉴了比特币的 UTXO 模型以及以太坊的智能合约等特性。

R3CEV 是以银行为主的金融科技研究组织，参与者包括富国银行、美国银行、花旗银行、德意志银行、加拿大皇家银行等，我国的平安、招行等也是其成员。

R3 Corda 主要应用案例：1) 2017 年 6 月，德国商业银行、比利时联合银行、荷兰银行和荷兰商业银行联合开发的商业票据 (ECP) 系统；2) 2018 年 5 月，钢铁企业 Thyssenkrupp 和德国商业银行在 Corda 上进行了 50 万欧元的外汇交易；3) 2018 年 12 月，德国商业银行、法国外贸银行 (Natixis)、荷兰国际集团银行 (ING) 以及荷兰合作银行 (Rabobank) 完成了一笔基于 Corda 的商业票据交易。





## 主要区块链平台介绍：蚂蚁、腾讯、微众、平安、万向、华为、趣链

### 蚂蚁区块链

2018 年 8 月，阿里云宣布推出企业级区块链服务，以实现跨企业、跨区域的区块链应用。阿里云 BaaS 目前提供自研蚂蚁区块链、Hyperledger Fabric、企业以太坊 Quorum 三种区块链技术框架。阿里云与蚂蚁金服积极与政府、金融机构展开合作，目前已有包括跨境支付、电子票据、供应链金融、零售、司法、交通物流等领域在内的数十个项目落地。

蚂蚁开放联盟链是 2018 年 9 月发布的一个面向开发者的生态联盟链。该项目旨在面向全球中小开发者与机构客户提供低门槛一站式的 DAPP 开发平台与业务上链解决方案，提供多种共识机制、经济模型与激励治理方式，以及跨链共享的身份认证，构建全球性、开放性的区块链生态。

### 腾讯区块链

腾讯于 2015 年成立了区块链团队，2018 年 4 月，腾讯云推出区块链服务 TBaaS，为用户提供一键式区块链部署服务，并可提供业务通道管理、智能合约管理等多项功能，用户企业在腾讯云区块链网络中可以达到 1W TPS 的单通道性能。腾讯区块链已经在供应链金融、游戏资产、数字政务等多个场景实现落地。

### 微众银行 Fisco BCOS

微众银行联合万向区块链实验室与矩阵元联合研发 BCOS 企业级应用服务的区块链技术开源平台，于 2017 年 7 月完全开源。2017 年 12 月，微众银行所在的金链盟推出 BCOS 的金融分支版本 Fisco BCOS 平台。金链盟全称金融区块链合作联盟（Fisco），是以国内金融机构与金融科技为主要参与成员的区块链联盟，截止 2018 年底，已覆盖超过 32 个城市共 117 家企业。Fisco BCOS 平台，由博彦科技、华为、深证通、神州数码、四方精创、腾讯、微众银行、亦笔科技和越秀金科等金链盟成员开发维护，打造安全可控、产权自主、适用于金融领域的区块链底层平台。

Fisco BCOS 主要案例：微众银行的机构间对账平台、链动时代的不动产登记系统、仲裁链、四方精创的供应链金融、城商行旅游金融联盟的旅游金融、安妮股份的版权存证平台等。

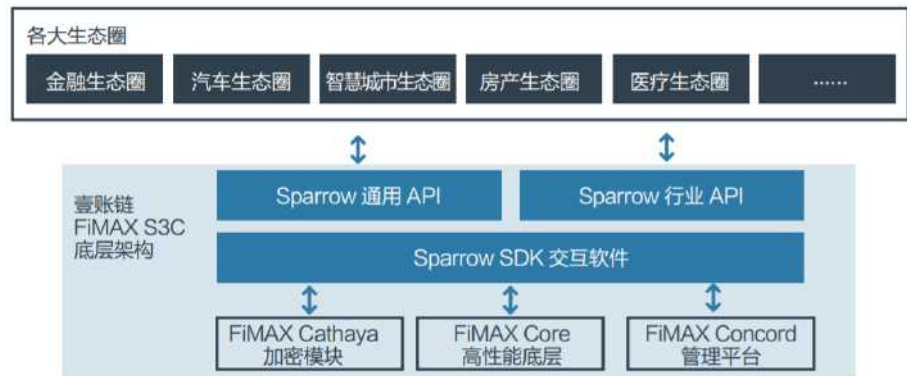
### 平安壹账链

平安集团旗下金融科技平台壹账通利用自研的 FiMAX S3C 区块链框架，已在贸易融资、ABS、供应链金融、再保险等领域部署了区块链项目。FiMAX 具有高吞吐量、准实时性和高效接入国密算法的特点。与传统 BaaS 上链服务不同的是，壹账链采用 BNaaS 多账户组网模式，可以由开发者拥有各自独立的账户体系、产生各自的网络节点，从而自主创建、设计、发布、营销联盟链网络。企业用户可以根据其需求选择适用的联盟链网络，并利用 FiMAX 通用化的底层技术迅速部署区块链节点。2018 年年报显示，平安集团通过金融壹账通打造全国最大的商业区块链平台，为国内外超过 200 家银行，20 万家企业及 500 家政府和其他商业机构提供服务。

平安区块链（金融壹账通）为香港金管局提供国际贸易融资网络的设计、开发及部署。凭借 3D 零知识证明技术、全球首创的可授权加解密技术、高吞吐量等优势，真正实现了订单的数字化，在保证信息共享的同时还兼顾了信息的安全性，大幅提升贸易金融行业的风控水平、效率、透明度和安全性。该网络在业务规模和先进技术应用领域均处于领先地位，这也是平安区块链技术的第一个海外合作项目。平安银行 SAS 平台立足大型核心企业，基于真实的贸易背景，为其产业链内供应商提供应收账款服务，从而盘活企业存量应收资产，使包括中小企业在内的各级供应商得到便利的应收账款金融服务。



图表 103：平安壹账链架构



资料来源：平安区块链研究院，中金公司研究部

### 万向 BCOS 与 PlatON

万向是国内较早开展区块链研究、部署与投资的企业。2017 年 7 月，万向与微众银行、矩阵元共同推出开源区块链基础设施平台 BCOS。基于 BCOS 的万向供应链金融服务平台已与包括江西银行在内的多家银行达成合作，为多家中小微企业实现融资，截至 2019 年 9 月，平台上发生的总融资金额已超过 1 亿元。

2018 年，万向推出 PlatON 网络，旨在建立跨行业的数据交换与协同计算基础设施，为数据资源、算力资源的资产化、可交易化创造条件，适用于区块链、分布式计算等各类去中心化系统。通过加密算法，和对算力等分布式经济中的新型价值的度量与交易结算，使人工智能和科学计算等大型复杂的计算工程在保证数据安全与隐私性的同时也能通过 PlatON 获取算力。

万向于 2019 年 9 月在第五届区块链全球峰会正式发布《分布式经济白皮书》。白皮书指出，去中心化经济（DeCo）分为四个阶段，行业目前正处于 DeCo 3.0 开放金融阶段，区块链去中心化价值网络特点开始体现，通证化、稳定币开始出现；万向预计在去中心化经济下一阶段——DeCo 4.0 分布式经济生态系统阶段，去中心化信任网络将开始应用到各种经济场景。

图表 104：去中心化经济（DeCo）四阶段



资料来源：云栖大会，中金公司研究部



### 华为 BCS

2018 年 4 月，华为推出了基于 Hyperledger Fabric 平台的区块链服务 Blockchain Service (Huawei BCS)，帮助企业在华为云上快速高效、低成本地搭建企业级区块链应用场景。华为区块链平台与华为云服务其他基础技术紧密结合，保证了可靠性与扩展性，2019 年 9 月，华为区块链已经支持华为鲲鹏计算集群。华为在 BCS 架构中，提供了基于国密算法的证书签名机制。用户可以选择使用国密算法作为区块链平台的加密算法。目前华为云区块链服务主要聚焦于数据、IoT、金融、运营商、供应链、政务等方向。

### 趣链

杭州趣链科技有限公司成立于 2016 年，主要区块链产品有：（1）自研区块链底层平台 Hyperchain，该平台是国内第一批通过工信部标准院与信通院区块链标准测试并符合国家战略安全规划的区块链核心技术平台；（2）分布式数据协作网络 BitXMesh，为企业提供数据存储、数据共享和分布计算环境（3）一站式 BaaS 平台飞洛 FiLoop，提供区块链部署、监控、运维等服务，帮助用户实现业务快速上链。

主要应用案例：中国农业银行联合太平养老保险股份有限公司的国内首条养老金联盟链；浙商银行区块链企业应收款链平台，2018 年累计业务规模达 1400 亿；中国银联、光大银行、浦发银行的分布式 POS 电子签购单系统；杭州互联网公证处的可信司法联盟“印刻链”。

### 其他区块链相关企业介绍：恒生电子、航天信息、众安在线

#### 恒生电子

恒生电子是国内领先的金融软件和网络服务供应商。早在 2016 年 5 月，恒生电子便参与发起金链盟（金融区块链合作联盟，FISCO），致力于开发基于联盟链的数字票据系统，并于 2016 年 10 月加入 Hyperledger。目前，恒生电子的区块链业务的基础平台包括基于 Hyperledger Fabric 的恒生金融级联盟许可链技术平台 HSL（Hundsun Shared Ledger），主要用于贸易金融、供应链等场景，以及面向合同链、私募股权链场景的 FTCU 范太链（FinTech Block Chain Union）。恒生电子已经帮助天津金融资产交易所、海南省知识产权局等将区块链技术运用到实际业务中。

#### 航天信息

航天信息对区块链技术的研究和筹备最早追溯到 2016 年。2018 年 11 月，航天信息正式组建区块链技术研发团队，主要面向金税、金融和物联网三个业务场景，并推出了面向企业级应用的区块链技术开发平台。公司目前的主要区块链应用是电子发票，目前基于联盟链的电子发票已经在湖北、山东、北京、内蒙和宁夏 5 个地区试点，有效解决了传统发票“共享难、流转难、归集难、查验难”的问题。此外，航天信息还推出了基于区块链的粮食流通质量追溯系统，保证粮食从生产到销售的各个环节全程可追踪溯源。

#### 众安在线

众安在线是国内首家互联网保险公司，由蚂蚁金服、腾讯、平安等于 2013 年共同发起成立。众安在线积极运用区块链技术提升保险业务的质量和效率，开发出基于保险产品的区块链资产协议（蚂蚁区块链 BaaS 平台保险通证，PBT），探索保险资产通证化。与此同时，众安也推出电子签约、数字身份、分布式加密存储、防伪溯源、存证、供应链金融等基于众安链的行业解决方案，并推出了安链云 BaaS 云服务平台。







### 联盟链的主要应用场景

联盟链技术企业主要利用区块链的**分布式记账（DLT）、智能合约**等技术，帮助金融行业提升服务的效率和透明性。目前，区块链在需要“多方共享”、“高频重复”、“交易链条长”的场景下最为适合：

- ▶ **多方共享。**区块链的一个优势是通过数字签名等密码学技术，在保证数据唯一性和所有权不可篡改的前提下，实现多方之间的信息共享。这解决了不改变数据所有权的条件下，多方如何实现信息共享的问题。在调研中，我们看到，**跨境支付、跨境贸易融资、供应链金融、资产证券化（ABS）、电子发票**等应用场景，多需要相互独立金融机构之间互相协作，区块链能够明显降低各方的沟通成本。
- ▶ **高频重复。**基于区块链的智能合约，能够通过实现业务自动化，取代简单的人工。对于**交易后清算、监管风控**等高频重复业务上取代人工非常适合，但对于**IPO、兼并收购**等低频、定制程度高的业务不是很适合。
- ▶ **资产上链是难点。**区块链的一个理想状态是所有的交易要素都在链上实现，这要求货币、资产、法律条文等都区块链技术来实现。但在实践中，如何保证这些资产要素上链时候数据的准确性，以及链上信息与链下资产之间的 1-1 绑定关系，在法律和技术上都是重要挑战。我们认为这也是 ICO 失败的主要原因之一。

图表 105：区块链在金融业务中的应用场景

分类	应用	现有解决方案	区块链解决方案	
 货币	数字货币	各国法币	比特币/稳定币	央行数字货币 →
	跨境汇款	SWIFT	Ripple	蚂蚁区块链 →
 清算交易	交易后清算	CCASS（港交所）		港交所区块链平台 →
	交易	上交所	Coinbase	→
	电子票据	税务发票系统	区块链发票	→
 融资	融资	IPO	ICO	STO →
	贸易融资	各银行独立进行		香港贸易联动平台 →
	ABS	各银行独立进行		招行/京东ABS →
 风控	征信系统	S&P/中诚信	公信宝	→
	KYC/AML	World-Check		中行质押贷款系统 →
			IT公司推动	金融机构推动

资料来源：中金公司研究部





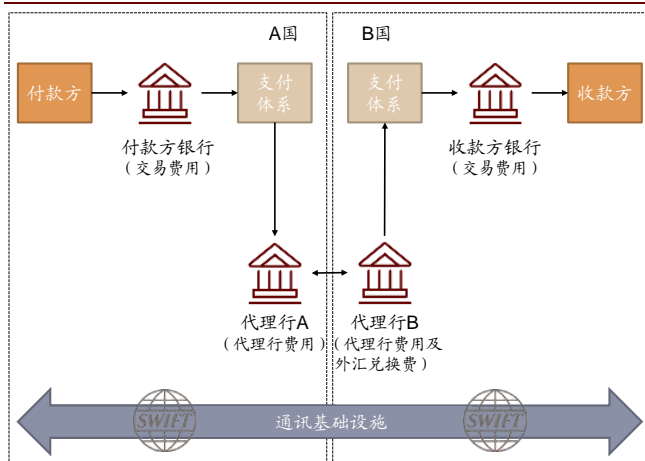
**应用场景#1: 跨境支付: 当菲佣遇到区块链**

目前主要国家都实现了高效的境内银行间支付清算，例如，中国人民银行自主开发的中国现代化支付系统（CNAPS，China National Automatic Payment System）能够高效、安全、快捷地处理银行的各种支付业务。但是跨境支付业务目前还存在耗时（2-3 工作日）、费用高（平均 30-40 美元/笔）等问题。

目前全球跨境支付主要通过 SWIFT（Society for Worldwide Interbank Financial Telecommunication，环球银行金融电信协会）进行。SWIFT 成立于 1973 年 5 月，是一家国际银行同业合作组织，2018 年 SWIFT 全球支付报文数达 78 亿，日均报文处理 3130 万次，同比上涨 11.3%。SWIFT 采取代理银行（Correspondent Bank）制度，在 200 多个国家和地区设有代理银行，代理银行之间在对方银行互相开户。汇款的时候，付款方通过付款方银行-付款国代理银行-收款国代理银行-收款方银行，实现向收款方汇款。这个制度解决了付款行和收款行之间没有直接商业关系的问题，但中间环节多导致汇款时间长、手续费高昂。

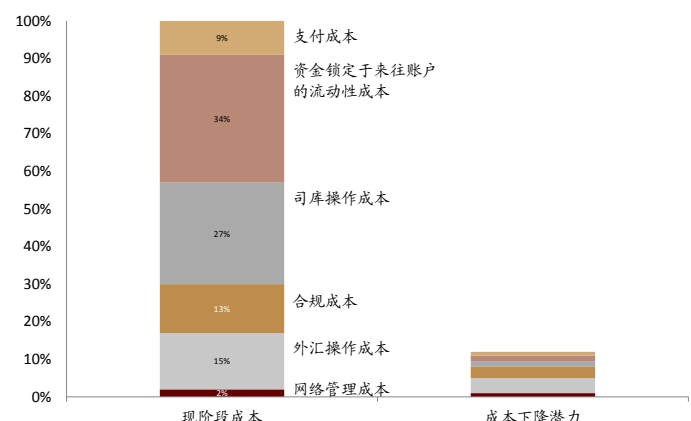
据埃森哲统计，全球每年通过银行进行的跨境支付规模达 25 万亿-30 万亿美元，全年总交易次数 100 亿-150 亿笔，每笔交易需缴纳费用 30-40 美元。IBM 预计，2020 年全球跨境支付市场规模将达 2 万亿美元。根据麦肯锡 2016 年和万向区块链首席经济学家邹传伟的研究，跨境支付的主要成本来自代理银行账户的流动性成本（34%，这些资金可以用于收益更高的地方）、司库操作（27%）、外汇操作（15%）和合规（13%）。通过区块链技术，理论上可以大幅压缩 90-95% 的成本。

图表 106: SWIFT 汇款模式



资料来源：Aite Group，中金公司研究部

图表 107: 跨境支付成本分析（2013-2015 平均）



资料来源：麦肯锡，万向，中金公司研究部

我们认为，基于区块链的跨境汇款技术长期可能挑战目前 SWIFT 在此领域的垄断地位。通过利用分布式账簿技术，解决金融机构之间的互信问题，在满足各地监管要求的前提下，区块链有望大幅降低交易成本，实现几乎实时的跨境支付。目前，Ripple、蚂蚁金服等均已较为成熟的区块链跨境支付解决方案，SWIFT 也在积极试验区块链跨境支付网络。2017 年 4 月，SWIFT 与多家银行合作利用 Hyperledger Fabric 1.0 测试了分布式跨境支付系统，2019 年 1 月，SWIFT 宣布了另一项测试计划，允许区块链软件公司 R3 接入 SWIFT 全球支付创新服务（GPI）。

**案例#1: Ripple（瑞波）公司推出多种基于区块链的跨境支付解决方案**

Ripple（瑞波）公司通过基于区块链技术的 RippleNet，为银行、支付服务提供商、企业和交易平台提供快捷、低费用的跨境支付服务。目前，RippleNet 已接入来自六大洲 40 多个国家的 100 多家金融机构。RippleNet 包括 xCurrent、xRapid 及 xVia 三种解决方案

1) xCurrent 主要针对银行间跨境支付；Ripple 当前主要业务是与银行合作，帮助他们利用 xCurrent 简化跨境支付，其客户包括渣打银行和美国十大银行之一的 PNC 等。xCurrent



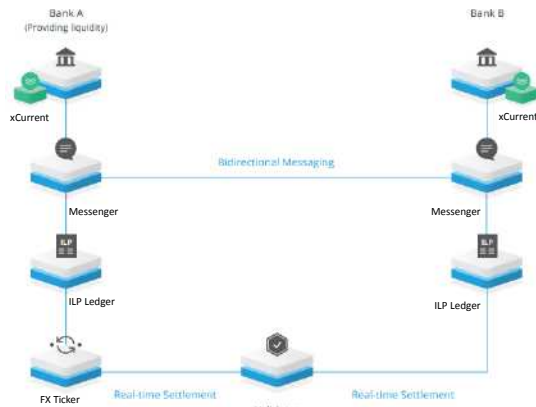


不需借助瑞波币，其可以为包括法币和加密货币在内的任意货币提供互操作性，且 Ripple 认为有望使银行间国际支付成本降低 33%；

2) xRapid 在交易中引入了瑞波币 (XRP) 进行货币转换，使用该服务的支付提供商无需在各市场预存当地货币，从而获得更低的流动性成本；

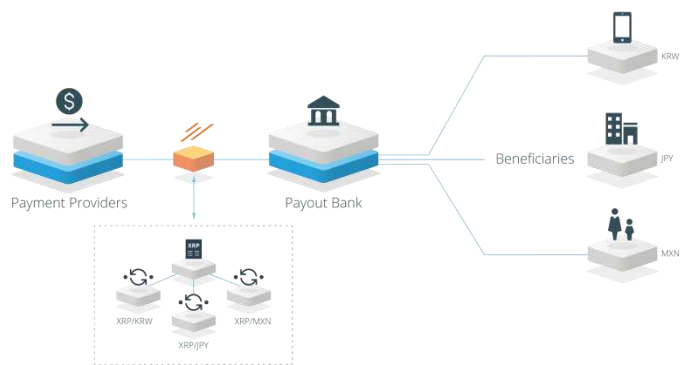
3) xVia 则为普通企业接入 RippleNet 提供了更加标准和快捷的入口。

图表 108: Ripple xCurrent 支付架构



资料来源：Ripple，中金公司研究部

图表 109: Ripple xRapid 架构



资料来源：Ripple，中金公司研究部

### 案例#2: 蚂蚁金服的跨境汇款方案

Ripple 目前提供的跨境支付解决方案主要是面向机构，而蚂蚁金服于 2018 年 6 月在香港推出了全球首个基于区块链的电子钱包跨境汇款服务。AlipayHK、菲律宾电子钱包 Gcash 和渣打银行（香港/新加坡）共用分布式账本，由渣打银行进行清算和兑汇。

我们于 2019/1/29 在香港第一次尝试了基于区块链的跨境汇款服务，利用 AlipayHK 向 Gcash 进行跨境转账，向组内成员家菲佣支付了部分本月工资。我们发现利用 AlipayHK 转账能够提供相比其他跨境汇款方式更优惠的汇率，并无需转账服务费，且整个转账过程只需花费数秒，体现了区块链技术在跨境支付的良好应用前景。

- ▶ **AlipayHK 提供了更加优惠的汇率，每年可为在港菲佣群体共节约 1 亿港币。**通过对比菲佣在香港常用的几大跨境汇款方式，包括 WesternUnion、Worldremit、TNG，我们发现 AlipayHK 有着明显的汇率优势。再加上每笔汇款节约的手续费（15 港币/笔），我们估测通过 AlipayHK 每年每位菲佣可节约 500 港币。而对于整个在港菲佣群体（目前共有 201,090 人），如全部转用 AlipayHK，每年可共节约大约 1 亿港币。此外，到账时间缩短至 3 秒，且实现了 7x24 小时服务。相比传统汇款方式，不管是时间还是成本上均具有较大的比较优势。



图表 110: 利用 AlipayHK 进行跨境汇款



资料来源: AlipayHK, 中金公司研究部

图表 111: WesternUnion 汇款网点



资料来源: 中金公司研究部拍摄

图表 112: 香港汇菲律宾各跨境汇款方式对比 (注: 汇率为 2019/1/29 汇率)

汇款机构	WesternUnion	Worldremit	TNG	AlipayHK
汇款方式	在线或网点汇款	在线汇款	在线汇款	在线汇款
每笔服务费	15港币	15港币	19港币	暂时免费
汇率	6.6848	6.64319	6.6600	6.7234
单日汇款上限 (港币)	7,999	40,000	7,999 (尊贵会员) 100,000 (至尊会员)	5,000
到账时间	几分钟内 (到指定机构提现) 1个工作日内 (银行账户)	实时到账 (需有BDO账户) 一小时内 (指定机构提现)	15分钟内	数秒内到账 (需有Gcash钱包)

资料来源: WesternUnion, Worldremit, TNG, AlipayHK, 中金公司研究部

图表 113: 菲佣跨境汇款市场规模预测

	WesternUnion	AlipayHK
菲佣人数	201,090	
每月最低工资 (港币)	4,500	
菲佣跨境汇款市场总规模 (港币)	109亿	
汇率	6.68	6.72
每人每年工资可兑比索数量	360,720	362,880
每笔手续费 (港币)	15	0
每人每年手续费支出 (港币)	180	0

资料来源: WesternUnion, AlipayHK, 中金公司研究部; 注: 时间截至 2019/1

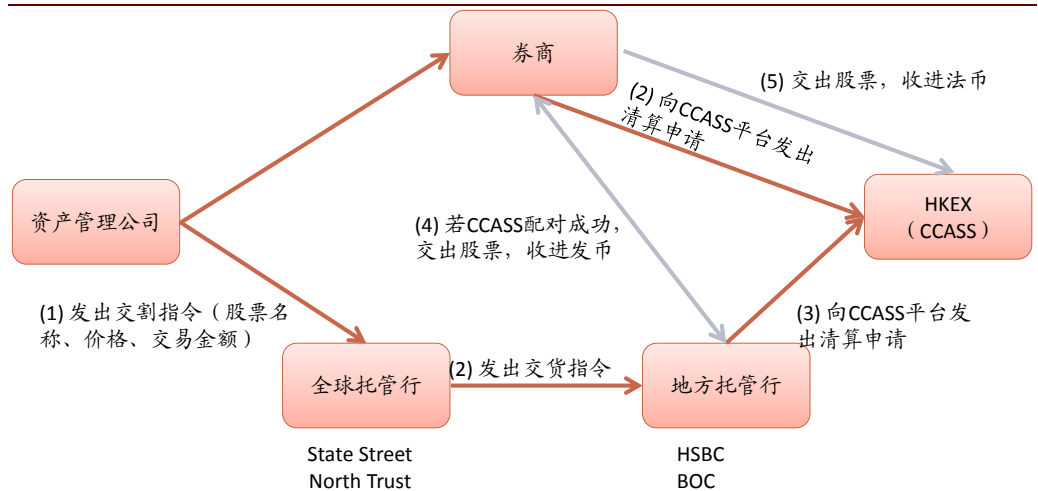


## 应用场景#2：交易后清算：区块链增加透明度、缩短清算时间

如下图所示，全球主要股票交易市场的清算流程涉及基金公司、证券公司、交易所、本地托管行、全球托管行等可能来自不同国家的主体。各个交易参与方所处时区不同，需要满足的监管要求也不同，造成整个清算流程复杂，交易成本高昂。

以香港为例，证券交易日和交割日需要2天时间。清算过程一旦出现错误，需要人工干预，在高频及大量交易时，人工效率较低，且人为操作失误可能会造成严重影响。中心化的系统容易遭受攻击，对安全性投入要求非常高。国际咨询公司 Oliver Wyman 估计清算环节每年为市场增加了 650~800 亿美元的成本。

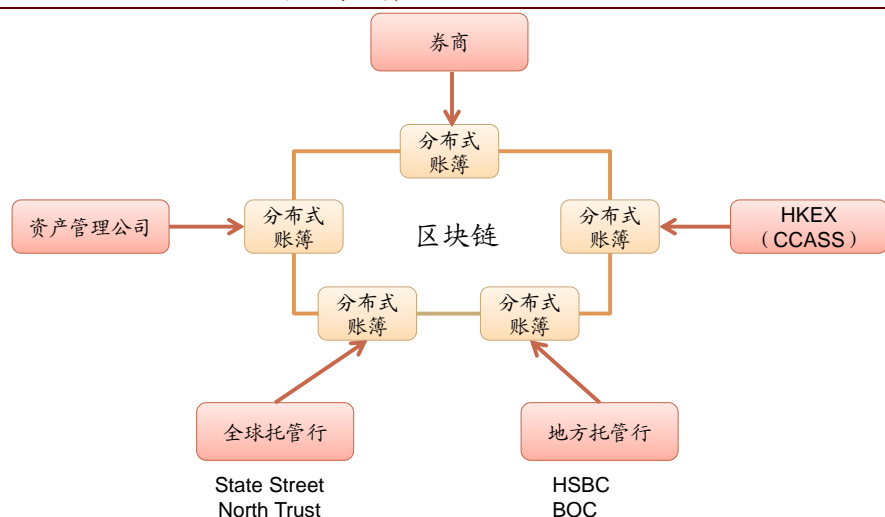
图表 114：传统证券交易结算流程十分繁冗



资料来源：港交所《金融科技的运用和监管框架》（2018），中金公司研究部

中国的清结算体系，采用客户直接在中证登开户，各家券商代理客户直接与中证登进行清/结算的集中化结算形式，大幅简化了交易流程，缩短交易指令配对时间，做到账户全面穿透，交易结算时间实现当日结算（T+0）。

图表 115：区块链重塑传统证券交易结算流程



资料来源：港交所《金融科技的运用和监管框架》（2018），中金公司研究部

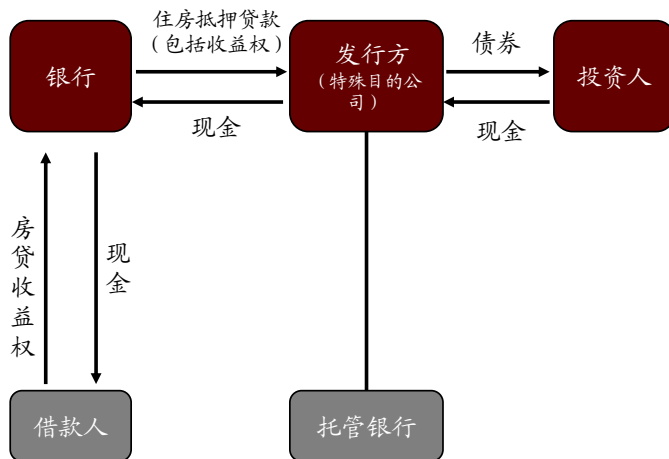
参与沪深股通的国际投资者不论处在哪个时区，也需要满足当日完成清算的要求。这对券商、交易所、清算机构都提出巨大挑战。2018年3月，港交所宣布与 Digital Asset 公司展开区块链领域合作，建立新的区块链结算系统，该平台将简化互联互通下内地股票的北向交易流程，实现 T+0 结算。



**应用场景#3：资产证券化（ABS）：解决“看不清”、“管不住”的问题**

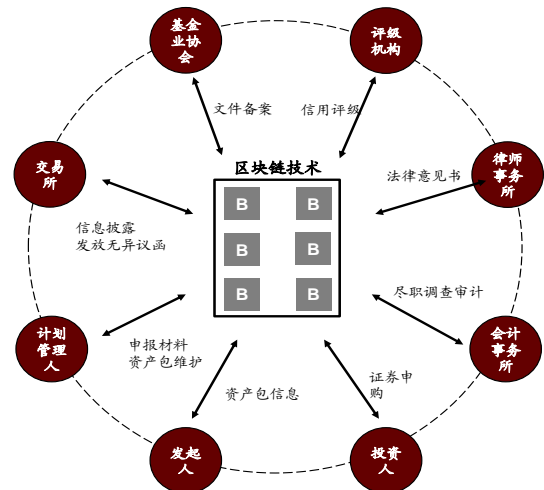
资产证券化是指将流动性较差、但有预期稳定现金流的资产，通过结构化设计进行信用增级，以发行证券的方式出售，获得融资并提高资产流动性的过程。资产证券化服务机构需对市场上资产提供风控、定价、产品设计、发行、存续期管理等多项服务。

图表 116：目前 ABS 场景（以房贷为例）



资料来源：zuehlke，中金公司研究部

图表 117：区块链对 ABS 的改变



资料来源：goodaudience，中金公司研究部

**痛点：**ABS 存在“看不清”、“管不住”等问题：1）无法确保标的资产真实性；2）若中介机构出现问题，账款偿还的后续问题无人处理；3）ABS 产品复杂度不断加强，参与主体数量较多，数据流和现金流分配过程繁复，风险逐步累积。

**解决方案：**智能合约实现 ABS 底层资产实时监控，并简化管理流程。1）可对底层资产动态实施实时监控，若触发加速清偿或违约事件，合约条款将被自动强制执行，解决“管不住”的问题；2）加速清偿或违约事件会及时通知各方，使底层资产实现透明化管理；3）实现智能化管理，如自动对账等，简化投后管理工作，缩减管理成本。

- ▶ **京东白条 ABS：**2018 年 6 月，“京东金融-华泰资管 19 号京东白条应收账款债权资产支持专项计划”设立，并在深交所挂牌转让。京东金融将 ABS 云平台开放给各方技术团队一同对区块链底层技术进行完善，与华泰资管和兴业银行共同建立了多方独立部署的联盟链，在基础资产上实现数据保真和实时共享，实现了信息的高效透明传输，降低了信用风险，并且在专项计划层面将逐步加入自动化管理流程，提高管理效率，最终实现 ABS 产品全链条上的技术升级。
- ▶ **招商银行 ABS 区块链平台：**招行目前牵头完成了以 Pre-ABS 功能为主的区块链平台，目前平台的主要功能是共享底层资产包数据并进行各类分析，完成各类 ABS 券发行前的各类报告等。后续招行计划创建一个在参与机构间实现 ABS（乃至同类产品比如 MBS，CDO，CLO，ABN 等）分层券的认购、转让、资金清算、存续期管理等功能的全方位区块链平台，实现 ABS 全生命周期管理。
- ▶ **港交所前海联合交易中心（QME）：**针对动产难以被标准化计量为有效抵押品的问题，QME 利用物联网和区块链技术，解决货物真实性，货权清晰性，处置流动性和公允价格确定等问题：利用智能识别等物联网技术，对生产、交易、物流、仓储全流程进行监控，将仓库提货凭证、实物资产的物流信息等相关信息转化为数字数据，有效解决虚假仓单、重复质押等问题；利用联盟链技术，将全流程信息上链，不再由仓库单方面提供凭证，而是由包括物流企业、经销商、监管者如检疫机构在内的所有参与方共同维护，可追踪、可溯源，从而实现中小企业经营资产的标准化和数字化，为企业融资提供信用支持。





#### 应用场景#4：电子票据：实现异地看病报销

税务发票和以医疗收费票据为代表的财政票据，可以利用区块链不可篡改、可追溯的特性，实现电子票据的防篡改、交易溯源、多方可信协作。传统电子票据存在以下问题：

- ▶ **收票信任问题。**受限于开票主体和收票主体之间各自独立，收票方无法直接获取与开票有关的交易细节。1) 当电子发票重复打印使用或篡改信息时，对于收票方而言难以识别真伪，存在多报、虚报问题；2) 申报人员取得电子票据后，需要打印出来形成纸质凭证，结合其他必要文件提交，还需要经过复杂的验证环节，流程繁琐。
- ▶ **监管效率问题。**现阶段税务部门等监管主体并不能完全掌握开票主体的交易行为，开票行为与真实交易行为并不一定对应，虚开虚抵、偷税漏税的问题并未完全解决。同时发票领用、抄税上传等手续繁杂，降低了企业的经营效率。

区块链电子票据与传统电子票据的区别在于其具有分布式存放、可追溯的优势。每一个相关方都将接入分布式账本，税局、开票方、报销方多方参与共同记账。从领票、开票到流转、入账、报销、全环节流转状态完整可追溯，解决了各主体间的信任问题。区块链票据系统由主节点和轻节点组成，只有税务机关、社保部门等主节点才有全量数据，其他节点只能查看与自身有关的信息。

- ▶ **对于开票方，**通过数据实时上链和智能合约实现的发票自动配额，免除了发票领用、抄税上传等手续，实现按需开票，避免了周期性申领票据造成的高峰期排队现象。
- ▶ **对于收票方，**采购过程中的订单、物流、资金流等信息被写入区块链，收票方可随时在本地节点查询支付行为并知悉相关交易细节，来检验发票真伪，提高了财务运行效率。
- ▶ **对于税务局等监管部门，**通过对发票的开具、流通、报销等环节的实时监控和相关交易信息的掌握，保证了发票的真实性，杜绝了偷漏税问题；通过智能合约，实现限额调整等功能的自动化，让税务局对发票的监管更加精细。

阿里和腾讯在过去一年分别发布了各自的区块链发票解决方案：

图表 118：微信支付的区块链电子发票功能



资料来源：腾讯科技，中金公司研究部

图表 119：浙江省使用区块链实现医保零星费用网上报销和异地报销



资料来源：云栖大会，中金公司研究部

- ▶ **腾讯的税务发票区块链。**2018 年 8 月，由腾讯提供技术支持，深圳市税务局区块链电子发票系统开出全国首张区块链电子发票。截止 2019 年 8 月，深圳市已开出超 600 万张区块链电子发票，累计开票金额达 39 亿元。针对在全国范围内开展部署，腾讯提出了“主链+侧链”的分布式架构方案：全国分为几大区域，由主链进行勾联，进行全国数据的共识、共享；区域内的各省市可以自主搭建侧链，负责本地数据管理；国家税务总局作为一个主链的超级监管节点，负责对区块链电子发票系统的全局管理。各省市的发票数据信息可互查互访，节点的运维工作下放





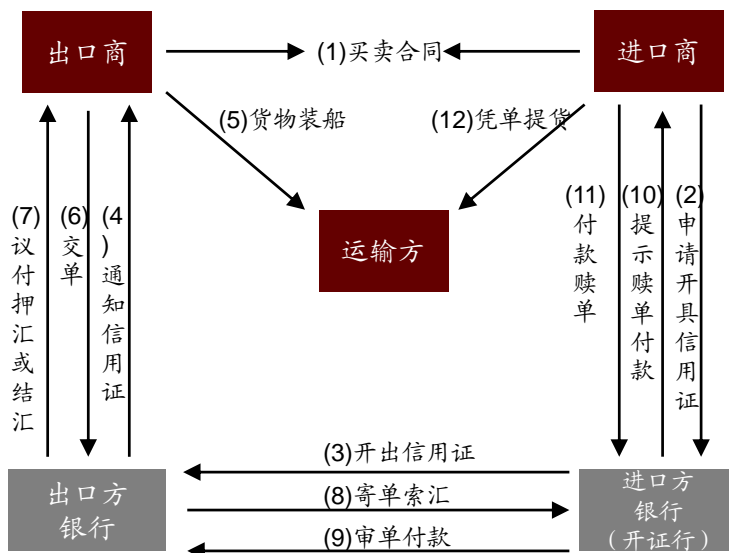
至各省市，相较于传统的全国统一数据中心更易于管理。

- **阿里的医疗收费票据区块链。**浙江省财政厅和蚂蚁区块链合作，2018 年 8 月上线的电子票据平台目前已经接入近 100 家医疗机构，并已实现医保零星费用网上报销和异地报销；据蚂蚁区块链数据，该电子票据平台将原先 170 分钟的人均就诊时间降为 75 分钟，原先半个月的保险理赔时间降至几分钟。此外，广州市国税局和蚂蚁区块链于 2018 年 6 月合作推出了“税链”平台，可有效解决开票难、成本高等问题，目前该平台已经开票超 2 亿张、接入企业超 200 万家。

#### 应用场景#4：贸易融资：减少交易处理时间及造假风险

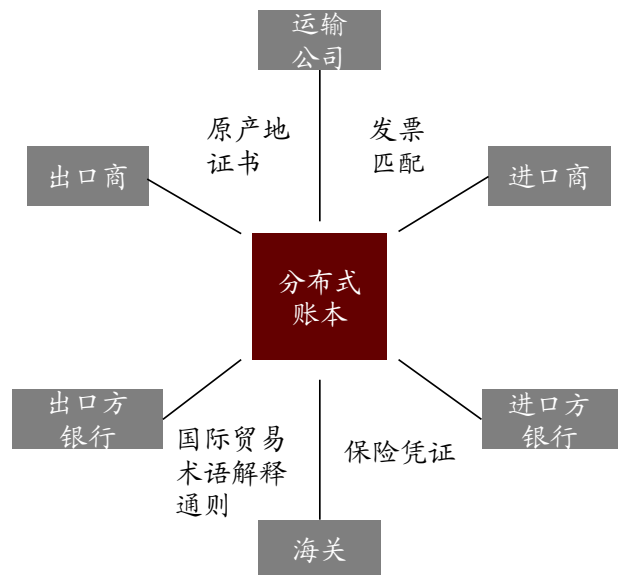
贸易融资是银行对公主要业务之一，银行运用短期融资工具，为商品交易中的存货、预付款等资产进行融资。每一笔交易都要有严格的凭据，并执行客户资信背景、市场、运输、储存等情况的调查。贸易融资存在投入产出比低、贸易造假风险：贸易融资单笔金额一般较小，笔数较多，涉及多个部门和环节来进行资料收集、审核等，流程繁琐，单笔交易往往需要花费 7 到 10 天时间，特别是跨境贸易时，存在丢件和贸易单据造假风险，处理时间有时长达 1 个月。

图表 120：目前贸易融资的流程



资料来源：zuehlke，中金公司研究部

图表 121：区块链对贸易融资的改变



资料来源：goodaudience，中金公司研究部

区块链的智能合约技术，可实现贸易环节全流程掌控。利用智能合约，跨境贸易各环节都可被接入区块链平台，1) 可以很好地解决贷前调查、贷中审查、贷后管理实时监控，保证预设条件触发后强制及自动执行相关流程；2) 减少人力投入，提升投入产出比；3) 信息集中上链，利于银行准确进行信息验证和对比，减少造假风险。

以国际信用证交易为例，进出口商、双方银行、物流企业等可在智能合约上定制详细的交易规则，满足特定条件即自动判定达成交易，降低交易对手风险。同时，各参与方可通过自己的私钥对交易进行签名认可，减少了不同主体之间的沟通成本。

- **中银香港：**2017 年 5 月，中银香港成功利用区块链技术完成首宗本地贸易融资服务，区块链助力验证交易的真实性，减少融资时长及纸张和人力资源使用，提高效率。该服务初期只跟买家和供应商合作，并以本地发票融资交易作试点，为扩大区块链的应用，中银香港表示计划邀请更多买家、供应商及其他相关业务参与者如航运公司及速运公司参加，并研究扩大应用范围至其他贸易产品。
- **香港金管局：**区块链贸易融资技术平台“贸易联动”。2018 年 10 月香港金管局推出区块链贸易融资技术平台“贸易联动”，以提高交易效率及准确性，提高融资透



明度，避免融资诈骗。该平台主要包含三方面功能：1）数字化贸易文件，帮助贸易参与方在该平台有效及时传送和查看文件；2）加密技术，确保仅有贸易参与方能共享贸易资料，并依此向银行申请融资；3）利用智能合约，保证发货收据、采购单、收据对账单等流程自动化。

- ▶ **粤港澳大湾区贸易金融区块链平台：**人民银行数字货币研究所与中国人民银行深圳市中心支行共建粤港澳大湾区贸易金融区块链平台，该平台支持应收账款、贸易融资等多种融资活动，也方便监管机构进行动态实时监测。成员单位包括中国银行、建设银行、招商银行、平安银行、渣打银行及比亚迪公司等，目前已开始第一期试运行阶段。

#### 应用场景#5：供应链金融：实现核心企业信用的多级穿透

供应链金融是中小企业获得融资的主要方式之一。供应链上的核心企业通过担保、回购等方式提供信用，上下游企业通过提供交易记录并抵押应收、预付、存货等动产来从金融机构获得融资。

当前供应链金融存在诸多问题亟待解决：1）供应链末端企业仍存在融资难问题。核心企业的一级经销商、一级供应商的应收账款或预付账款与核心企业自身业务联系紧密直观，但是核心企业信用资质难以向供应链下一级传递；2）银行确定企业信用成本较高。银行需要严格核实融资发放对象的交易信息、质权可靠性与回款控制能力，需要与对手方企业相关信息对账，还要识别信息造假，如伪造仓单骗贷，对银行来说存在收益与成本不匹配的问题；3）难以从供应链管理角度发掘更多价值。传统供应链金融服务将主要精力投入相关企业财务信息的核查和融资风险与收益的计量，较少参与至核心企业自身的供应链优化管理。

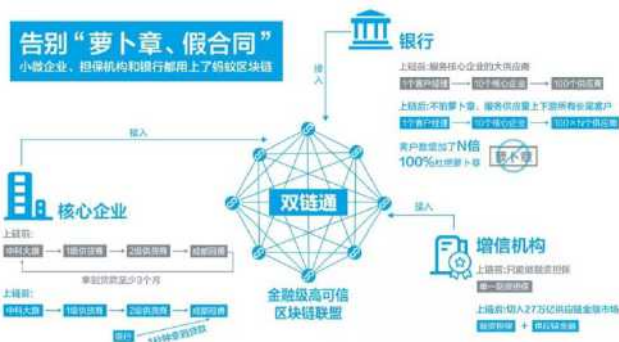
#### 基于区块链的解决方案（案例：蚂蚁区块链）

供应链上各级供应商、经销商、物流企业、银行、增信机构都可接入区块链平台，通过使用分布式的共享账本，从而 1）推动资金流转。通过对核心企业相关交易的多级追溯，将全供应链的应收、预付、存货等资产的确认、流转、清分等操作流程上链，实现清晰的资产确权，同时资金可实现多级分配和流转，有效解决末端企业融资难问题；2）降低金融风险与操作成本。金融机构能够清晰获知各相关企业的风险与经营状况的真实信息，降低贷款不良率，减少调查成本，提升投入产出比；3）增加全供应链协同性。通过分布式账本实现全供应链数据的实时同步与对账，降低了各实体间的协作成本与信用风险，此外，各企业信息流的有效整合，有利于发现协同效应，增强供应链黏性，提高全产业链整体竞争力。

由蚂蚁区块链于 2019 年 1 月推出的“双链通”供应链存证平台，以应付账款作为信用凭证，通过区块链使中小企业的信用信息在各级银行、担保机构、各级链公司之间透明流转，有效降低供应链金融风险。蚂蚁区块链已经为全国 7,800 万家中小微企业提供秒级融资服务。

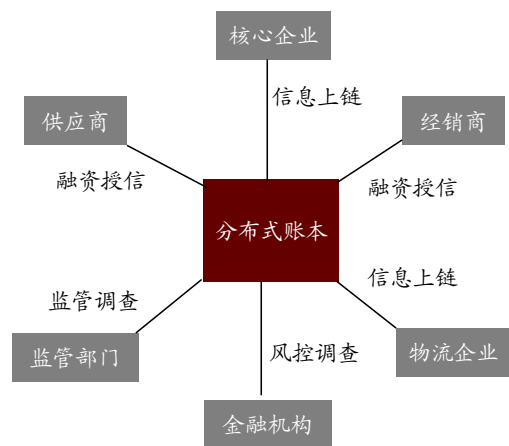


图表 122: 蚂蚁区块链“双链通”



资料来源：云栖大会，中金公司研究部

图表 123: 上链后的供应链金融

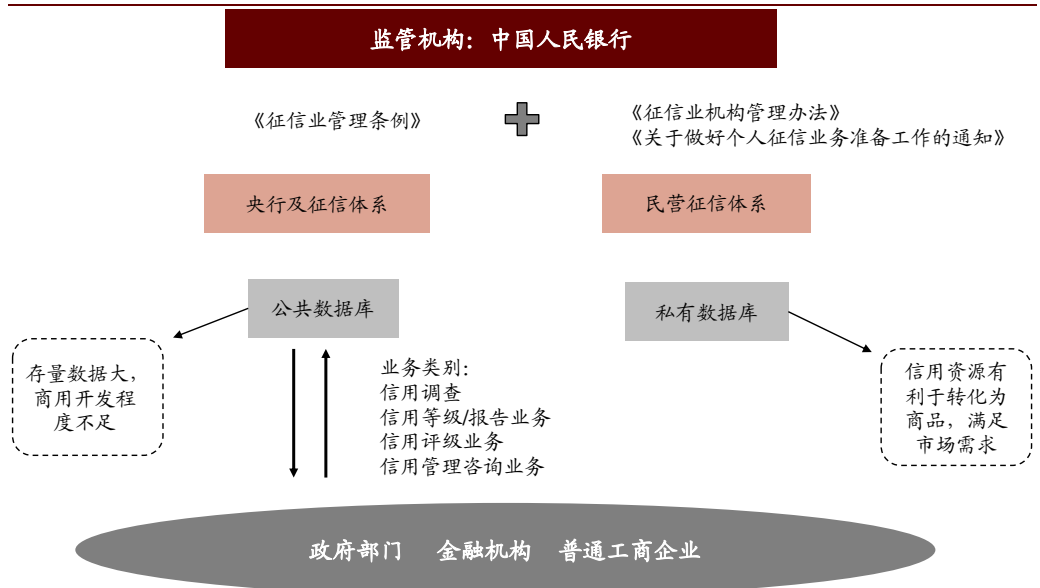


资料来源：蚂蚁区块链，平安区块链，中金公司研究部

#### 应用场景#6: 监管科技: 共享数据, 消除信息孤岛

征信系统对个人或企业在信用活动中产生数据做出及时、准确、全面的记录。征信和金融风控有着紧密联系, 包括贷前防控、反欺诈服务、信用决策、贷后行为预警等。

图表 124: 中国征信框架



资料来源：中国人民银行，中金公司研究部

**痛点:** 征信业信息孤岛问题严重。1) 出于隐私保护的顾虑及传统技术架构的局限性, 各机构没有积极进行数据交换共享; 2) 金融业内信贷机构、消费金融公司、电商金融公司等机构的海量信用数据尚未发挥其应有价值, 金融业内信用信息割裂在法院、政府部门、电信运营商等机构手中。

**解决方案:** 搭建征信数据共享交易平台, 加速信用数据的存储、转让和交易, 促进参与交易方最小化风险和成本。平台主要的共享交易模式有两种: 一是征信机构与征信机构共享部分用户信用数据, 二是征信机构从其他机构获取用户信用数据, 并形成相应信用产品。



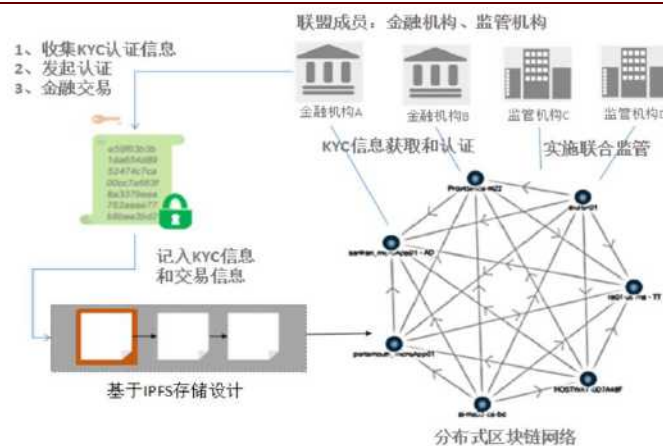
### KYC 及 AML：信息可追溯和可验证（案例：R3 Corda 的 KYC 试点项目）

KYC 是对客户背景信息的调查，分为个人 KYC 和公司 KYC。个人 KYC 要求客户提供姓名、地址、财产情况等个人信息；公司 KYC 要求更为复杂，其内容还包括各种复杂的所有权结构、营业范围、上下游企业等。AML 即反洗钱合规性程序，是银行重要的合规流程，包括多个项验证流程，所需时间长，过程繁琐。

**痛点：**KYC/AML 缺乏统一标准。各国银行、金融机构以及其他受监管机构目前所处的监管环境复杂，缺乏统一的标准，各机构进行 KYC/AML 的时间成本和经济成本越来越高。根据 LexisNexis Risk 的数据，2018 年美国银行业反洗钱支出达到 250 亿美元。

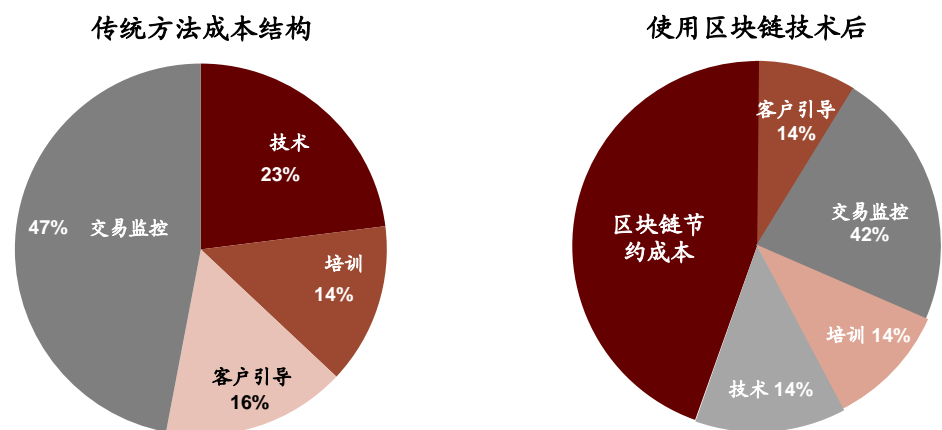
**解决方案：**区块链可以确保 KYC 信息从采集到每次变更可追溯、可验证，并有机构的签名确认；金融机构发起的金融交易会实时同步到监管机构节点，监管机构可以对交易属性进行事中监管或者事后监管；存储在区块链网络中的 KYC 认证信息可被联盟链上的节点共享使用，减少客户审核上的重复性劳动。

图表 125: KYC 区块链技术总框架



资料来源：信通院《金融区块链研究报告》（2018），中金公司研究部

图表 126: 区块链技术将有助于节约大量 AML 支出



资料来源：Celent，中金公司研究部

- ▶ **案例#1: Shyft 推出基于区块链的 KYC 网络 Shyft Network。** Shyft 于 2018 年 2 月 9 日推出基于区块链的革命性 KYC 网络 Shyft Network 以帮助金融机构缩减传统合规系统所需的繁琐流程和高昂成本。在 Shyft 所搭建的生态系统中，已经执行过 KYC 流程的银行等机构可作为信任锚（Trust Anchors）加入，把他们已有的用户信息与用户的加密签名联系起来，并记录在相应的二级分类账中，用以证明用户的个人信用。第三方应用程序可以利用加密渠道检索到用户的个人信用信息，根据监管机构的需要提供信息，在没有真正透露身份信息的情况下实现名誉审查。这样的



流程大大提高了 KYC 的效率，也缩减了金融机构在 KYC 流程中所需投入的高额人力成本。除此之外，由于区块链的分布式记账特性，用户的个人信息也得到了保护。

- ▶ **案例#2: R3 Corda 区块链平台推出 KYC 程序试点项目。** R3 Corda 平台和咨询公司 Synechron 合作推出基于区块链技术的全新 KYC 试点程序,包括 BNP、德意志银行、法兴银行以及来自中国的工商银行和招商银行在内的 39 家银行加入了此次测试中。相比于传统的 KYC 流程,新 KYC 程序可使客户管理和实时更新个人信息并授权给多个银行进行查阅,从而减少各家金融机构进行重复性的 KYC 过程,以达到提升效率、节约成本的目的。





**附录：主要区块链相关企业**
**图表 127：主要区块链相关企业及其相关业务**

Ticker	公司	市值（十亿元人民币）	主要区块链业务				
区块链框架							
未上市	Hyperledger	-	开发框架Hyperledger Fabric				
区块链平台							
BABA.N	阿里巴巴	3,211	阿里云区块链服务、蚂蚁区块链BaaS平台				
0700.HK	腾讯控股	2,730	TBaaS区块链服务平台、金联盟开源平台				
2318.HK	中国平安	1,564	平安壹账链FiMAX				
未上市	华为	-	Huawei BCS				
JD.O	京东	322	区块链ABS平台 Jdch、京东云区块链数据服务BDs				
BIDU.O	百度	256	莱茨狗、百度区块链引擎BBE、超级链、图腾				
未上市	万向	-	区块链基础设施平台BCOS、PlatON网络				
未上市	趣链科技	-	底层平台Hyperchain、分布式数据协作网络BitXMesh、飞洛FiLoop BaaS平台				
Ticker	公司	市值（十亿元人民币）	主要区块链业务	Ticker	公司	市值（十亿元人民币）	主要区块链业务
区块链应用				区块链应用			
0762.HK	中国联通	220.4		300525.SZ	博思软件	8.1	
TAL.N	好未来	180.5	未来学迹链	002530.SZ	金财互联	7.7	
601360.SH	三六零	152.4		002610.SZ	爱康科技	7.3	
300059.SZ	东方财富	101.3	SRC证书链	600756.SH	浪潮软件	6.7	
IQ.O	爱奇艺	89.3	百度超级链超级节点	002117.SZ	东港股份	6.4	电子票据区块链、TK BaaS平台、电子发票区块链、电子证照区块链
600588.SH	用友网络	76.1		603636.SH	南威软件	5.9	证照链
600570.SH	恒生电子	60.2	恒生共享账本HSL	002104.SZ	恒宝股份	5.8	
300033.SZ	同花顺	53.8	保单信息存证平台	300386.SZ	飞天诚信	5.6	
002153.SZ	石基信息	40.6		002235.SZ	安妮股份	5.2	版权区块链
600271.SH	航天信息	38.0	航天信息区块链平台	002400.SZ	省广集团	5.1	
6060.HK	众安在线	34.5	BaaS平台、积线、品牌溯源、钛平台、步步鸡	002447.SZ	晨鑫科技	5.1	竞斗云
000977.SZ	浪潮信息	32.0		300468.SZ	四方精创	4.8	
002439.SZ	启明星辰	29.8		002177.SZ	御银股份	4.7	
0268.HK	金蝶国际	25.1	金蝶信心链	002369.SZ	卓翼科技	4.5	
603000.SH	人民网	23.2		600571.SH	信雅达	4.4	
3888.HK	金山软件	22.8	KBaaS	300465.SZ	高伟达	4.4	
002268.SZ	卫士通	21.6		000606.SZ	顺利办	4.3	
002152.SZ	广电运通	20.0	运通链	300542.SZ	新晨科技	4.1	信用证传输系统、交易撮合平台
300271.SZ	华宇软件	17.5		603106.SH	恒银金融	4.0	
600446.SH	金证股份	17.5		002587.SZ	奥拓电子	3.8	
000021.SZ	深科技	15.7		300541.SZ	先进数通	3.5	
600093.SH	易见股份	14.4	可信数据池、易见区块	300469.SZ	信息发展	3.4	供应链管理、追溯存证、存证应用
300339.SZ	润和软件	11.0	贸易金融区块链联盟	002103.SZ	广博股份	2.5	
002537.SZ	海联金汇	10.0	供应链金融	300688.SZ	创业黑马	2.3	
300379.SZ	东方通	10.0		XNET.O	迅雷	2.3	迅雷链开放平台、迅雷链
600797.SH	浙大网新	9.4		300431.SZ	暴风集团	1.7	节点基础设施服务
300170.SZ	汉得信息	9.0	BaaS平台	2488.HK	元征科技	1.4	
300377.SZ	赢时胜	8.9		0863.HK	BC科技集团	1.3	加密货币的保险托管服务
300663.SZ	科蓝软件	8.8		未上市	复杂美	-	
002063.SZ	远光软件	8.5	商品溯源、供应链金融、企业应用服务	未上市	中链科技	-	
2098.HK	卓尔智联	8.5	卓链联盟	未上市	点融	-	
300130.SZ	新国都	8.4		未上市	全链通	-	
300458.SZ	全志科技	8.2					

资料来源：万得资讯，网信办，中金公司研究部；市值数据截至 2019/10/25



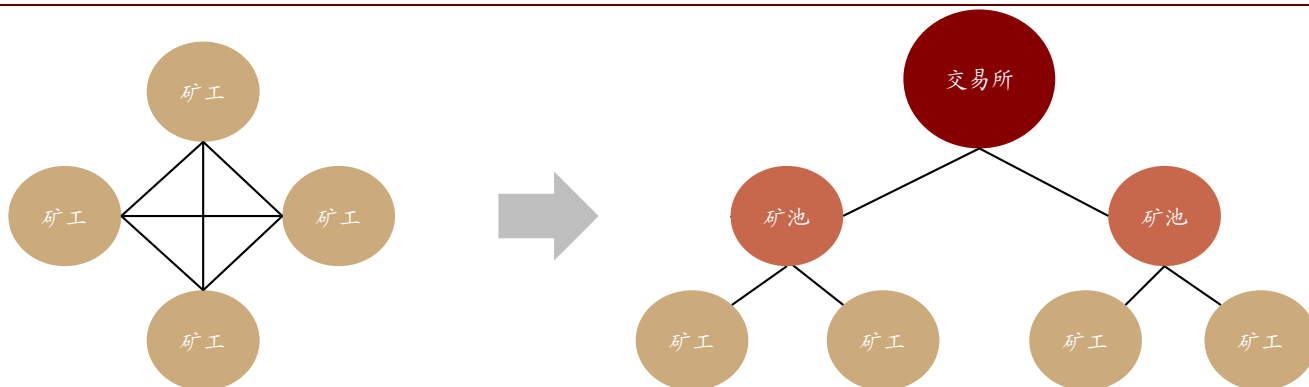
## 回溯：加密资产技术及产业链全景

区块链是一种不可篡改的分布式记账技术，其四大核心技术包括：

- ▶ **分布式账本**：账本被分散保存在所有成员节点，数据的添加不需要通过任何中心化主体；
- ▶ **密码学**：保障资产安全和进行 PoW 哈希运算的作用；
- ▶ **共识机制**：解决如何在分布式环境下竞争记账的问题；
- ▶ **激励机制**：通过发行和分配加密资产给参与共识机制的网络节点（矿工），来维护系统良性发展。

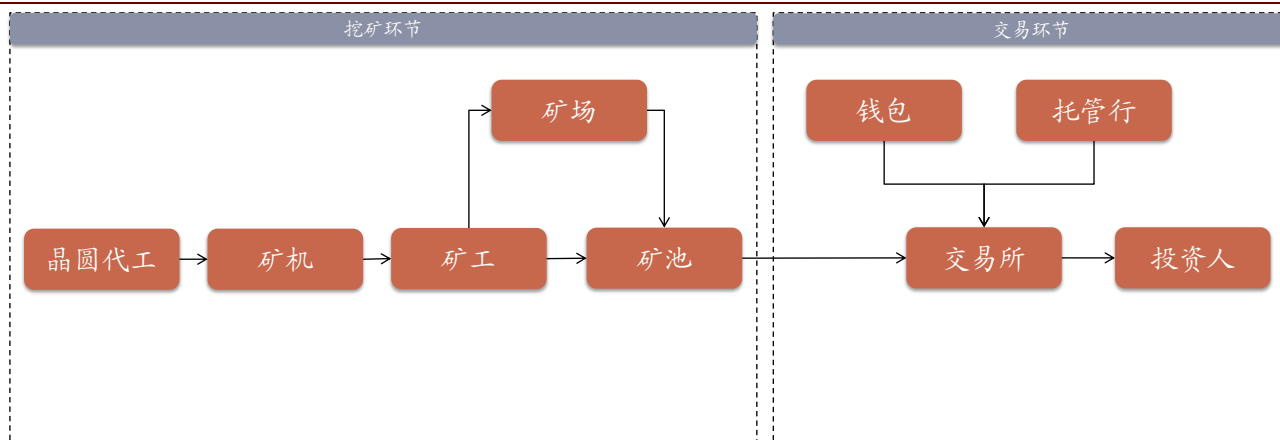
比特币最初的设计理念是基于密码学的去中心化网络。相互独立的矿工通过进行工作量证明计算形成共识，维持网络的运行并获得收益。但币价上升带来的收益提升，在比特币生产环节，带动专用挖矿设备（矿机），共同挖矿服务（矿池）等商业模式的出现。在交易环节，由于比特币网络交易速度过慢等问题，出现基于第三方信任的交易所、托管行等提供类似于目前金融行业功能的组织，整个网络向中心化演化。

图表 128：比特币网络逐渐向中心化演进



资料来源：巴比特，链世界，区块链，中金公司研究部

图表 129：加密货币产业链



资料来源：巴比特，链世界，区块链，中金公司研究部

- ▶ **矿机**是专门用于挖矿（工作量证明计算）的计算机，矿机的特点是通过采用大量专用挖矿芯片进行并行计算，实现远远优于 CPU/GPU 等传统通用芯片的能耗比和计算设备硬件的性价比。



- ▶ **比特币矿工**通过参与竞争记账，获得比特币网络的奖励和交易发起方支付的交易手续费。目前矿工一般加入某个矿池，参与共同挖矿，矿工一定时间能够获得的收益与矿机成本、电力成本、全网算力、自身贡献算力、币价等因素有关。
- ▶ **矿池**的主要职能是通过专用挖矿协议，协调大量的矿工一起挖矿。成功出矿的奖励先支付给矿池，矿池再根据各个矿工的贡献分配收益。矿池从中收取一定比例的费用。加入矿池，比特币用户一方面可以避免运行全节点；另一方面也可以减少挖矿回报的方差。根据 BTC.com 统计，目前前 6 大矿池垄断 71.5%算力，不参加任何矿池的独立算力不到总算力的 7%。
- ▶ **矿场**是为矿机提供托管服务的专用数据中心。矿场的作用在于将矿机物理集中在电价较低的区域，利用低电力成本获取更大收益。在中国来看，一般会选择内蒙古、四川、云贵高原、新疆等电力资源丰富且电价便宜的地方。根据 blockchain.info 的统计，2018 年中国矿场占全球比例约 58%。
- ▶ **交易所**提供加密资产链下交易平台。由于比特币区块链区块大小设计的限制，每秒只能处理 7 笔交易，无法支撑快速上升的交易需求，交易所由此应运而生。交易所主要提供：1) 法币-加密资产之间的兑换服务；2) 不同加密资产之间的兑换服务；3) 杠杆交易等融资服务。

### 主要加密资产#1：比特币：第一个得到广泛使用的加密资产

比特币是世界上第一个得到广泛使用的加密资产。目前仍然是市值和交易量最大的加密资产。2008 年，署名为“中本聪”的匿名人士发表论文《比特币：对等网络电子现金系统》。

图表 130：比特币币价波动分析及大事记



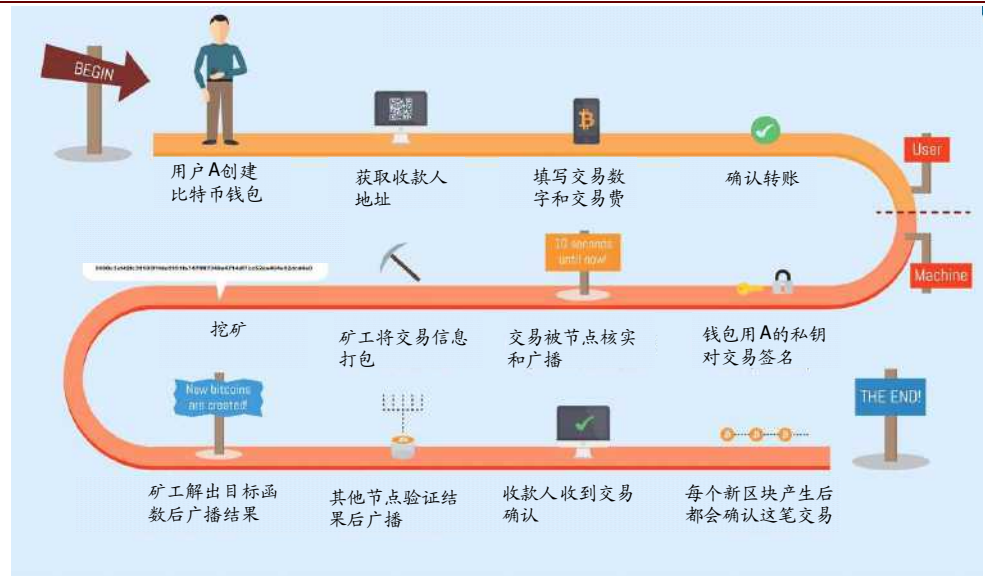
资料来源：bitcoin.com，中金公司研究部

**网络架构：**比特币采用完全的去中心化网络（Peer-to-Peer）。

**共识机制：**基于工作量证明（PoW）的竞争记账。每一笔交易包含付款方地址、付款方交易确认信息、付款人的资金来源信息、收款方地址和交易时间数额等信息，通过比特币网络广播发送交易信息给矿工（节点），矿工根据未确认交易池中的交易，进行工作量证明后，把交易信息打包生成一个区块，广播到网络里。约每 10 分钟生成一个区块，目前每个比特币区块容量为 1M，一笔交易的大小是 250Bytes，所以一个区块最多可以保存 4000 笔交易，但考虑到记账时间成本，平均为 1000-2000 笔。



图表 131: 比特币记账机制



资料来源：ISPI Montreal，中金公司研究部

**激励机制：**比特币网络对打包成功的矿工支付费用。矿工的收益包括 1) 来自交易发起方的交易佣金以及 2) 比特币网络新生产的比特币补偿。目前成功打包一个交易的奖励是 12.5 个比特币。来自比特币网络的奖励（新发行的比特币）每四年减半，下一次减半是 2020 年 5 月左右。这个机制保证到约 2140 年比特币挖完为止，全网比特币总量将达到设计上限——约 2100 万个。

**账本结构：**比特币没有通常意义上的账户余额或资产负债表，而是采用类似流水账的 UTXO（Unspent Transaction Output）数据结构。这一模型下，系统记录每一笔交易，通过计算地址未花费的交易额得到实际余额。若想获取某个账户的余额，则需要汇总所有的交易，得到 UTXO 集：一台电脑接入到比特币网络，从邻近节点获取 UTXO 集并读取交易记录计算余额。

### 比特币的分叉

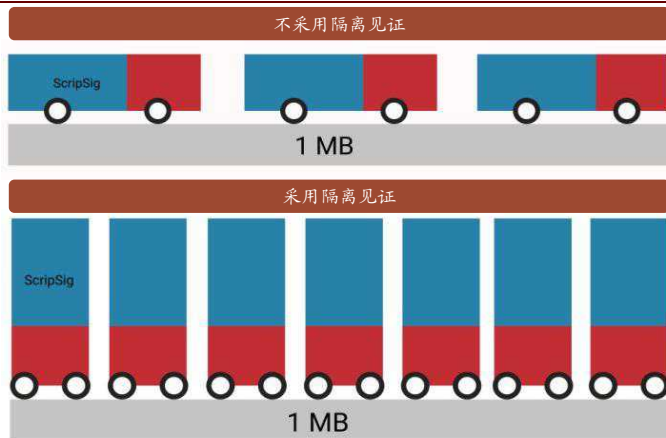
一般来说，加密资产分叉主要因为加密资产功能无法应对市场需求。以比特币为例，分叉主要是因为其无法满足交易量需求，进而社区要求比特币扩容。比特币历史上发生过数十次分叉，出现的币种包括比特币现金（BCH）、比特黄金（BTG）、比特钻石（BCD）和比特无限（BTX）等。比特币现金是 2017 年 8 月由原比特币区块链上，通过硬分叉产生的一条新链。BCH 总量同样是约 2100 万个，加密算法与比特币相同。

进行硬分叉的起因是为了提高比特币的扩展性而进行的“BIP91 方案”分叉尝试，提出在 2017 年 7 月之后 6 个月内进行隔离见证（SegWit）的同时，将底层区块大小升级为 4M（1M 主区块和 3M 见证区块）。然而，2017 年 8 月 1 日，比特大陆旗下矿池 ViaBTC 算力介入，推出了自己基于比特币原链硬分叉体系的“比特币现金”，并稳定出块。

► **隔离见证（SegWit）是为了解决交易拥堵问题而提出的手段之一。**其将数字签名（scriptSig）从区块的基本结构抽离出来隔离验证，不占用区块 1M 的大小，进而使每个区块可以容纳更多交易。比特大陆则倾向增大区块容量，并认为隔离见证不能从根本上解决交易拥堵问题。另外，见证隔离的代码中有中心化和管控的倾向，违背了比特币（或中本聪）的初衷。比特币现金将原先区块内存 1M 提高到了 8M（2018 年 5 月再次升级为 32M），并且拒绝采用隔离见证。正是由于对解决交易提速的手段出现分歧，BTC 自此发生硬分叉，产生新币 BCH。



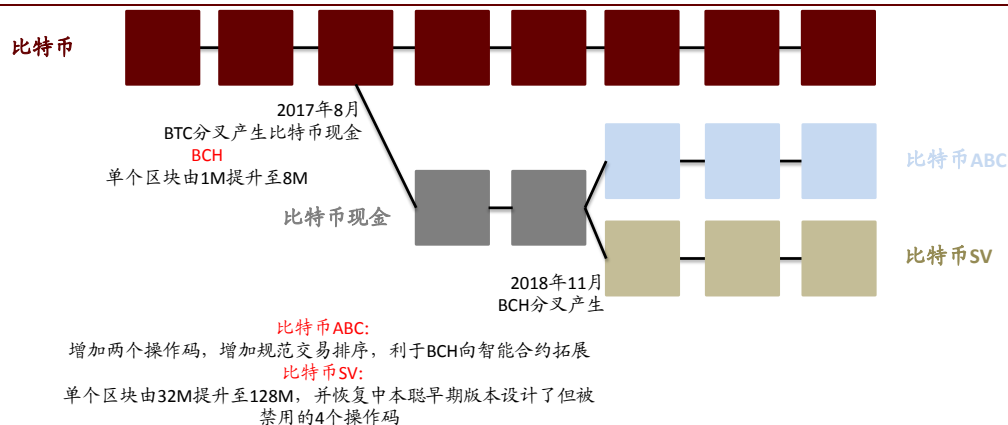
图表 132: 非隔离见证 VS 隔离见证



资料来源：知乎，中金公司研究部

- **比特币现金：**为解决比特币交易速度太慢、提高每秒交易笔数，由比特币硬分叉形成。在分叉点前，BCH 和 BTC 所有数据都是兼容的，而后的 BCH 链条上，BCH 将比特币原先的区块容量由 1M 提高到了 8M，因此一个区块上可以记录更多交易，理论上每秒处理交易量可以提升到约 56 笔。比特币现金在 2018 年 11 月 15 日又进行了一次分叉。分叉原因是 BitcoinABC 提出 Bitcoin ABC 0.18.0 (支持智能合约)，而 nChain 提出 Bitcoin SV (区块扩容至 128M)，且意见未达成一致。

图表 133: 比特币及比特币现金分叉历程



资料来源：巴比特，链世界，区块链，中金公司研究部

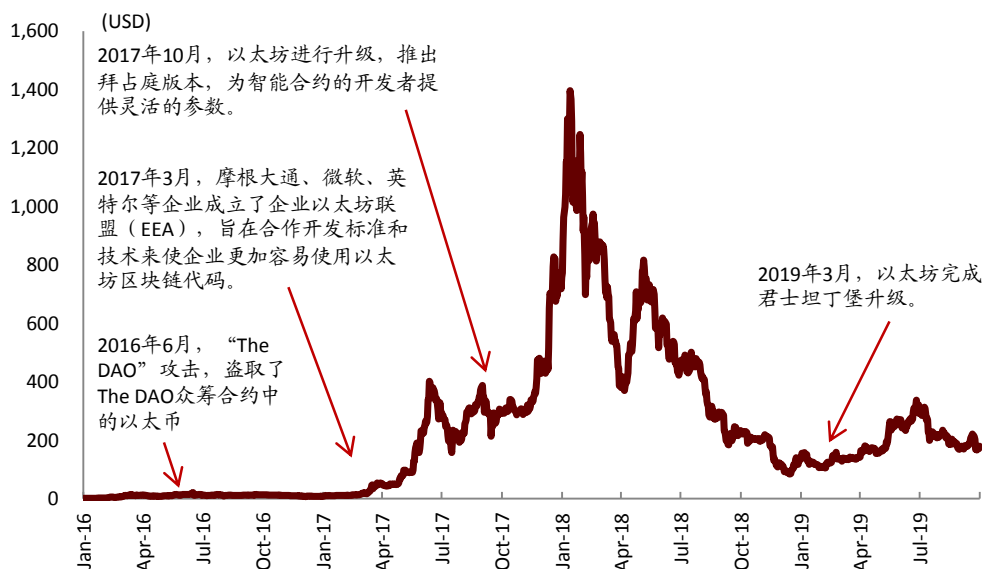




## 主要加密资产#2：以太坊：具有智能合约功能的区块链平台

2013年，Vitalik Buterin（V神）受到比特币启发，首先提出以太坊网络以改善比特币对智能合约支持不足等问题。最初的以太坊由 Ethereum Switzerland 公司开发，现在已转至以非营利机构以太坊基金会运作。截至 2019/10/13，以太币市值是仅次于比特币的第二大电子加密资产，达 199 亿美元，占加密货币总市值的 8.8%。

图表 134：以太币币价波动分析与以太坊年表



资料来源：CoinMarketCap，中金公司研究部

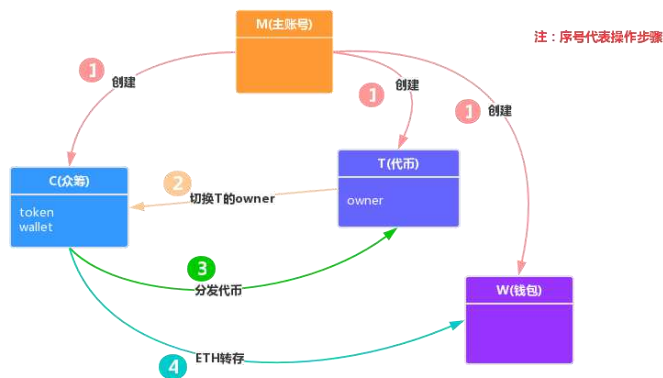
和比特币最大的不同是，以太坊开发者可以利用以太坊的区块链技术上的智能合约技术，采取类似于 IPO 融资的方式，通过 ICO（Initial Coin Offering）的方式发行 DAPP 项目专属 token 来筹集以太币（类似 IPO 中筹集现金）。Token 持有者将可以使用 token 换取此 DAPP 项目提供的服务，或宣示持有者对此项目的所有权。简单来说，由于开发者需要利用以太坊的智能合约技术记录项目中的合约内容，而记录和更新合约需要提供以太币作为补偿。

**以太坊 ICO：**目前基于以太坊的 ICO 一般采用 ERC20 协议。考虑到整个 ICO 过程的可控性、安全性、以及监管等要求，ICO 过程会涉及到三个合约：众筹合约、Token 标准合约、钱包合约，以及用于创建这三个合约的主账号。以 C 代表众筹合约，用 T 代表 Token 标准合约，用 W 代表钱包合约，用 M 代表主账号。

- ▶ 流程说明：1）创建合约：通过主账号 M 分别创建三个合约 C、T、W，此时 3 个合约的所有者 owner 均为主账号 M；2）切换 T 的 owner：为了让众筹合约能够分发代币，需要将代币合约 T 的 owner 换成众筹合约 C；3）分发代币：C 收到 ETH 后将代币按约定自动发送给认购用户；4）ETH 转存：分发代币的同时，C 会将用户转入的以太币转存到事先设置好的钱包合约 W 中。
- ▶ 智能合约：是一个被代码控制的账户，其私钥掌握在合约部署者的手里。这段代码（智能合约）被部署在分享的、复制的账本上，它可以维持自己的状态，控制自己的资产并且对外界的信息进行回应。智能合约如同计算机编程语言中的 if-then 语句，一旦预先定义的条件被触发，合约就会智能的执行，对数字财产进行交换。其主要分为构建、分布存储、执行三部分。

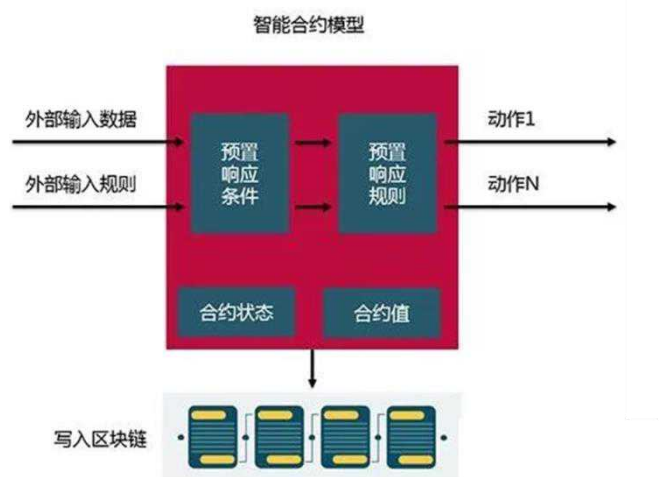


图表 135: 以太坊 ICO 机制说明



资料来源：CSDN，中金公司研究部

图表 136: 以太坊智能合约机制说明



资料来源：动脉网，中金公司研究部

**网络架构：**以太坊采用的完全的去中心化网络（Peer-to-Peer）。

**共识机制：**以太坊最初采用和比特币类似的基于工作量证明（PoW）的竞争记账，未来将向 PoS 方式转换。以太坊的发展分为四个阶段，分别是 Frontier（前沿）、Homestead（家园）、Metropolis（大都会）和 Serenity（宁静），每一阶段均采用硬分叉的方式完成升级。前三个阶段的共识机制为 PoW，最后的 Serenity 阶段采用 PoS。目前，以太坊处于从 PoW 向 PoS 过渡的 Metropolis 阶段，该阶段又分为 Byzantium（拜占庭）硬分叉和 Constantinople（君士坦丁堡）硬分叉，已经分别于 2017/10 和 2019/3 完成升级。

**激励机制：**以太坊除了发行类似于比特币的以太币（ETH）奖励成功更新区块的矿工以外，还引入“Gas”机制，以支持智能合约的顺利运行。以太坊中运行智能合约，都需要消耗 Gas（而不是 ETH）。交易发起者需要设置 Gas 价格（Gas price）和 Gas 上限（Gas limit）。Gas 价格类似于执行一步操作需要消耗的 Gas，而 Gas 上限则表示最多愿意付出多少 Gas（如果 Gas 值不足导致交易失败，交易发起者的状态将回滚且已消耗的 Gas 值不退回）。Gas 可以使用以太币购买。每一个合约包含 Gas，Gas 就像汽油，合约执行时会“燃烧”掉，虚拟机操作时需要 Gas 才能执行，每一笔交易都有消耗的 Gas 的最大数量。当 Gas 消耗完以后，如果当前执行没有完成，就会回滚到交易最初的状态，所以必须把足够的 Gas 充进去，才能够保证交易正常进行。

**账本结构：**以太坊余额模型 Ethereum 其实就是一个巨大的状态机，其中的状态都是由多个账户组成的，在以太坊中有两种类型的账户，一种是被私钥控制的账户，它没有任何的代码，与比特币地址基本有完全相同的功能，能够向网络中发送已签名的交易；另一种是被合约代码控制的账户，能够在每一次收到消息时，执行保存在 contract\_code 中的代码，所有的合约在网络中都能够响应其他账户的请求和消息并提供一些服务。

### 以太坊 2.0

以太坊 1.0 采用的 PoW 机制具有 TPS 低、资源消耗大等问题。为了解决这两个问题，以太坊 2.0（即 Serenity 阶段）将转为 PoS 共识机制，并引入分片。PoS 机制无需挖矿，将大幅降低以太坊运行的资源消耗，同时分片可以大幅提高以太坊的吞吐量。2018/12/10，Vitalik 称，采用基于 PoS 的分片技术的区块链“效率将提高数千倍”。

以太坊 2.0 的主要结构包括 Beacon Chain（信标链）、Shard Chains（分片链）和 VMs（虚拟机层）。其中，信标链是以太坊 2.0 的中枢，负责 PoS 共识机制的执行，以及连接分片、实现分片通信。以太坊基金会预计，以太坊 2.0 的启动预计需要花费 2 年时间，在其实现完整功能之前，其并不具备账户、交易、智能合约等功能。这段时间内，以太坊 2.0 将与以太坊 1.0 同时独立运行，以太坊基金会预计 2021 年以太坊 1.0 的实际运行权将交给以太坊 2.0。由于在以太坊 1.0 的 PoW 链上引入了“难度炸弹”，在“难度炸弹”爆炸

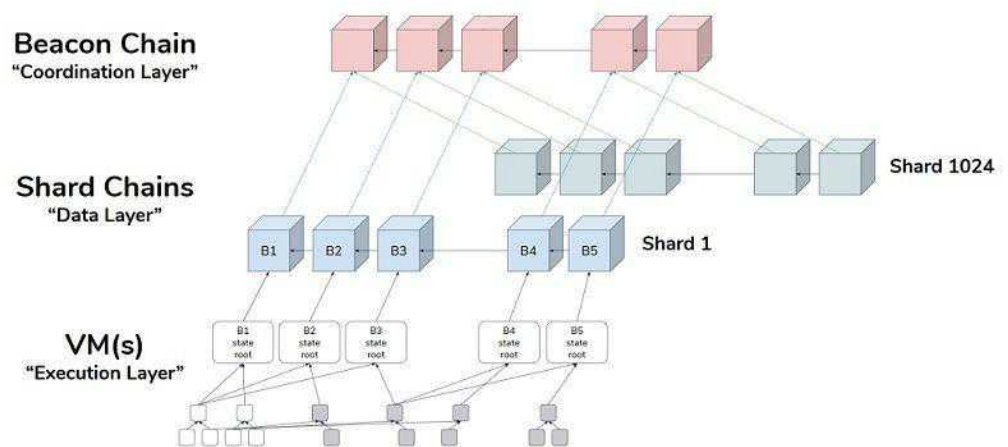


后，挖矿难度大幅上升，1.0 链将会出块困难、挖矿收益极低，最终被完全冻结，进入“冰川时代”（Ice Age）。

在 2021 年以太坊实现完成功能前，将经历三个阶段：

- ▶ 2019 年阶段 0，启动 Beacon Chain（信标链）：该阶段的信标链没有实际功能，主要用于导入验证者，用户在链上存入 32 个 BETH（Beacon ETH）即可成为验证者。
- ▶ 2020 年阶段 1，启动 Shard Chains（分片链）：在信标链的基础上引入分片链，该阶段的分片链同样没有实际功能，主要用于试运行分片结构。
- ▶ 2021 年阶段 2，启动 VMs（虚拟机层）：引入虚拟机 eWASM，从而实现了完整的以太坊 2.0 结构，账户、智能合约在该阶段被引入系统。在阶段 2 后，以太坊将正式进入 2.0 时代。

图表 137：以太坊 2.0 结构示意



资料来源：以太坊，中金公司研究部

**PoS 机制将有助于解决以太币的通货膨胀问题。**与比特币不同，以太币并未设计发行数量的上限，并且其发行量增长率高于比特币，通货膨胀是以太坊社区需要解决重要问题。目前，比特币发行量年增长率为 4% 左右，我们预计 2020/5 完成第三次产量减半后增长率将降至 2%；而以太币的发行量年增长率 2017-2018 年为 7%，2019/3/1 完成君士坦丁堡硬分叉升级后为 4%（挖矿奖励由每块 3 ETH 降低为 2 ETH）。当以太坊转为 PoS 机制后，以太币增发速度可以大幅下降而不影响区块链的安全性，这将有效解决通货膨胀问题。



## 主要加密资产#3：稳定币：价值相对稳定的加密资产

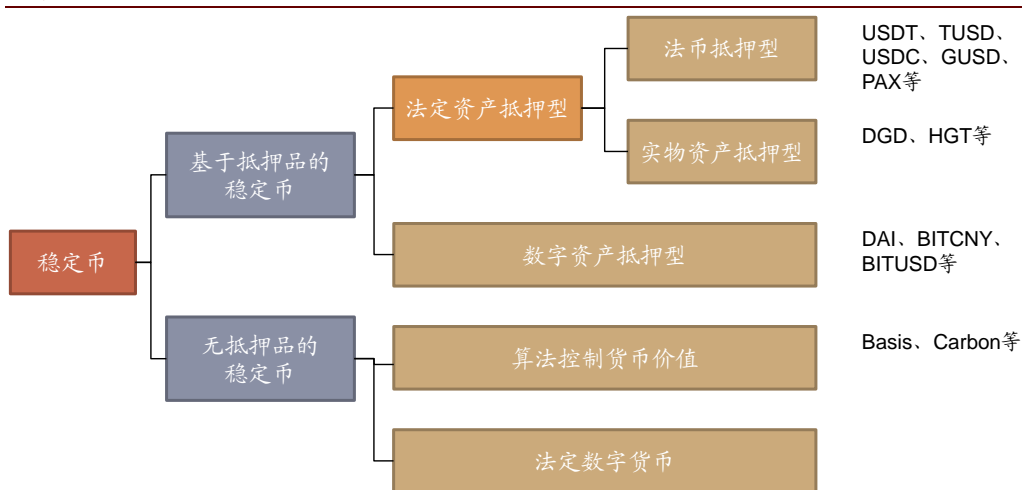
为了解决普通加密货币价格波动过于剧烈的问题,各种形式的稳定数字货币(Stable Coin)陆续进入市场。稳定币不仅部分解决了比特币价格大幅波动带来的问题,还成为连接法币与其他加密货币的重要资产。稳定币存在的好处:

- 规避整体下跌风险。币币交易中,若发生剧烈的币价下跌亏损,可以迅速将币换成USDT,进行资产保值。
- 拥有其他加密资产的好处,比如透明、快捷、隐私保护、成本低。用户可以利用稳定币进行贸易往来,用户不必担心投机性风险。

稳定币可以按有无抵押品分类:

- 基于抵押品的稳定币又可按照其抵押品类型,分为法定资产抵押型(法币、或黄金等实物资产)和数字资产抵押型。
- 无抵押品的稳定币中,一类通过算法控制货币价值,另一类则是由央行发行的法定数字货币。

图表 138: 稳定币分类



资料来源:王同益《稳定币的影响及其发展趋势研究》(2018),链得得,中金公司研究部

图表 139: 主要稳定币对比

	USDT	USDC	TUSD	PAX	DAI
发行时间	2014	2018	2018	2018	2017
底层协议	比特币Omni/以太坊ERC20/TRON TRC20	Stablecoin neutral	以太坊	Nano-Fork	以太坊
备抵资产	美元、欧元	法币	美元	美元	ETH
锚定价格	1:1美元	1:1美元	1:1美元	1:1美元	1:1美元
透明度	低	较高	中	高	高
市值 (百万美元)	4,110	466	188	258	83
主要合作伙伴 或关联方	BitFinex	Circle, Coinbase	-	-	DigixDAO, Maker

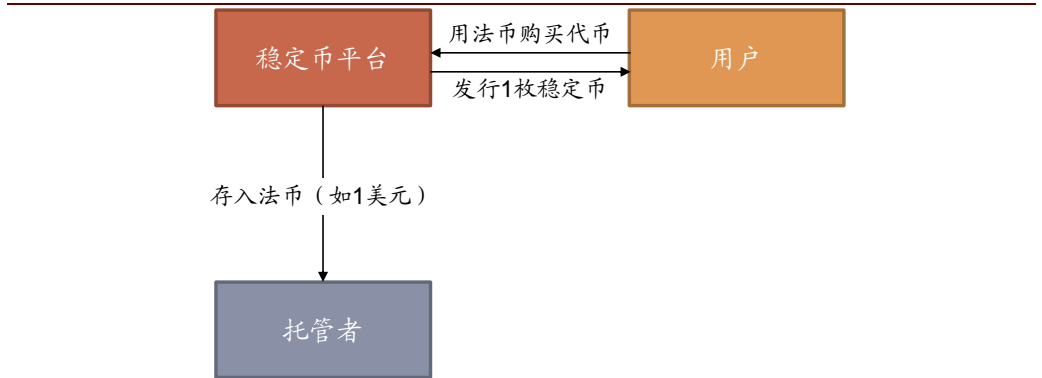
资料来源:火星财经, 55coin, 中金公司研究部; 注: 市值数据截至2019/10/19



## 法定资产抵押型

发行机构发行法定资产抵押型稳定币的同时，将法币或黄金等资产抵押，确保稳定币持有者可以固定的比率兑换回相应资产。在法定资产抵押型稳定币运行过程中，用户每购买一个稳定币，需要支付相应价值的法定资产给稳定币平台，稳定币平台会将该法定资产存放在托管平台。主要的法定资产抵押型稳定币包括：锚定美元的 USD Tether (USDT)、TrueUSD (TUSD)、USD Coin (USDC)，锚定欧元的 EURS，抵押黄金的 DigixDAO (DGD)、HelloGold (HGT) 等。

图表 140: 法币抵押型稳定币工作原理



资料来源：哈希派，中金公司研究部

USDT (USD Tether, 泰达币) 是 Tether 公司发行的 1:1 锚定美元的稳定币。USDT 最初通过 Omni Layer 协议在比特币区块链上以代币形式发行，目前部分资产在以太坊上发行。USDT 的发行机制如下：公司每发行 1 USDT，将有 1 美元存储在香港 Tether 公司。用户可以通过 SWIFT 电汇美元至 Tether 公司提供的银行账户，或通过交易所换取 USDT；反向操作可用 USDT 赎回美元。

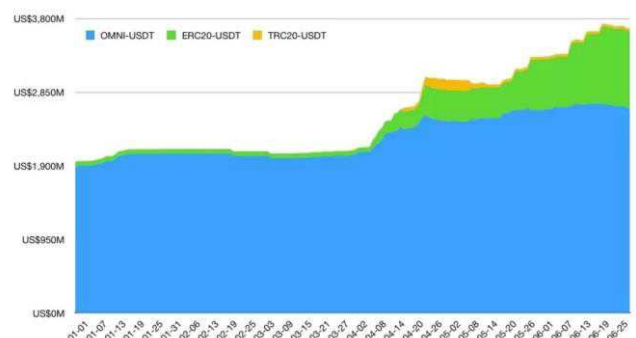
除了最开始基于比特币 Omni 协议的 Omni-USDT，2018/1 Tether 公司推出了基于以太坊 ERC20 协议的 ERC20-USDT，2019/4 新增了基于 TRON 网络 TRC20 协议的 TRC20-USDT，2019/7 后又新增了基于 EOS 网络和 Liquid 网络的 USDT。目前，Omni-USDT、ERC20-USDT、TRC20-USDT 分别占大约 48%、46%、6% 的发行量份额，基于 EOS 网络和 Liquid 网络的 USDT 目前发行量还很小。根据各类 USDT 使用的区块链网络的 TPS 不同，其转账速度也有较大差距，Omni-USDT 转账需要 0.6~2 小时，ERC20-USDT 需要 10 分钟左右，TRC20-USDT 仅需几秒至几分钟。当发起链上转账时，Omni-USDT 和 ERC20-USDT 分别和比特币转账、以太坊转账一致，需要花费少量的比特币和 Gas，TRC20-USDT 不收取手续费。

图表 141: 三种协议 USDT 技术对比

USDT协议	OMNI	ERC20	TRC20
区块链网络	比特币网络	以太坊网络	波场网络
转账速度	半小时至两小时	几分钟至数十分钟	几秒钟到几分钟
手续费	最高 (4~10个 USDT)	一般 (2~5个 USDT)	无
安全性	最高	高	低于前两者
吞吐量 (TPS)	7	30	1,000

资料来源：HELLOBTC，星球日报，中金公司研究部

图表 142: 2019 年上半年三种协议 USDT 发行量分布



资料来源：DAppTotal，中金公司研究部

主要法定资产抵押型稳定币透明度对比：

- USDT 是目前交易量最大的稳定币，但由于其没有定期的外部审计，备抵资产的银行





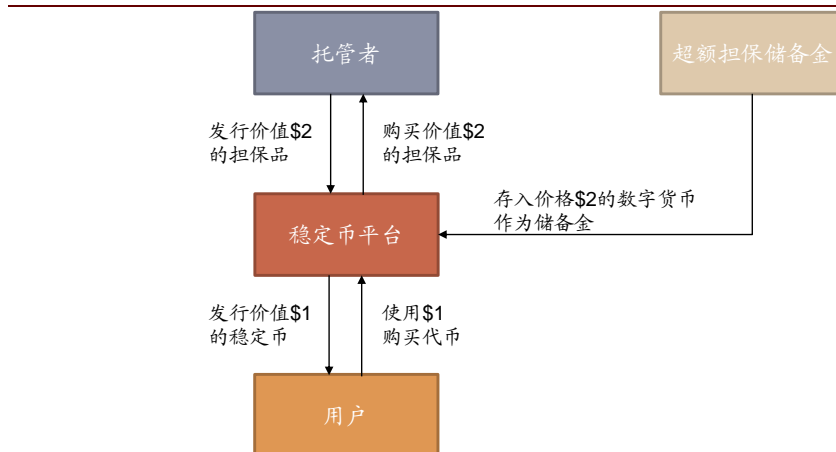
账户不透明，同时涉嫌超额滥发、联合兄弟公司 Bitfinex 交易所等问题，其透明度一直受到市场的质疑。

- ▶ TUSD 有定期的第三方审计，因而其透明度相对 USDT 高很多。
- ▶ USDC 不仅有定期的第三方审计，同时其发行方 Circle 和 Coinbase 监管牌照较为齐全，因而有较好的信用背书。
- ▶ 2018 年 9 月，锚定美元的 Gemini Dollar (GUSD) 和 Paxos Standard (PAX) 获得纽约金融服务部 (NYDFS) 批准发行，受政府监管、每月由注册会计师事务所对其账户资金进行审计，因此拥有很高的透明度和可信度。

### 数字资产抵押型

发行机构将持有的加密货币资产进行抵押，且在抵押资产价值下降时，补充抵押资产以维持币价稳定。相比法定资产，加密货币资产具有高透明度的优势。主要的数字资产抵押型稳定币有 Dai、bitCNY、bitUSD 等。

图表 143: 数字资产抵押型稳定币工作原理



资料来源：哈希派，链得得，中金公司研究部

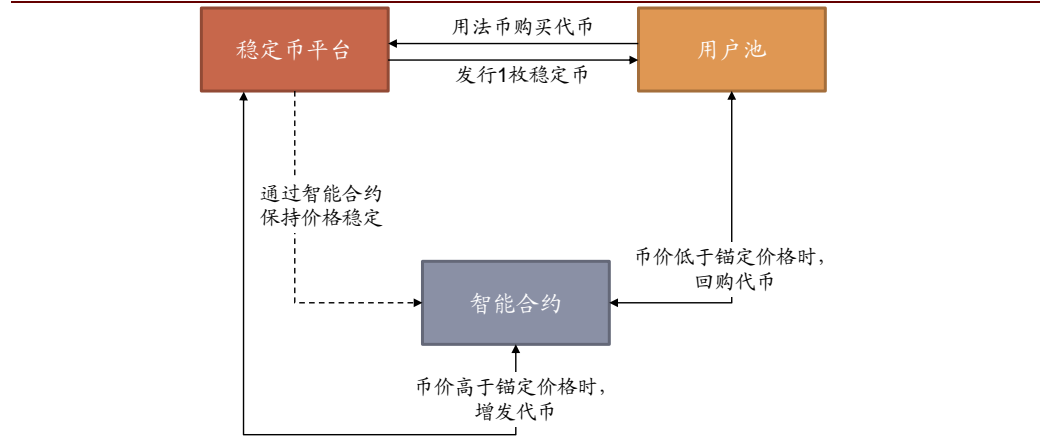
Dai 是将以太币作为抵押资产、并 1:1 锚定美元的稳定币。用户通过抵押自有的以太币获得 Dai 货币，以智能合约为主体的超额抵押和强制清算机制维持了 Dai 对美元的稳定币价。发行 Dai 时，用户需要存入超过所获 Dai 价值 2~3 倍的其他加密资产，当抵押物价值下跌至 1.5 倍时，会触发强制清算，以折价激励向其他用户出售抵押物以收回 Dai，从而维持了已发行在外 Dai 总数量与抵押池总资产美元价值的平衡。相比于其他稳定币，这种稳定币不存在中心化发行机构，避免了审计不公开和超额发行的风险，此外使用加密资产而非美元抵押使得它具有更强的流动性。

### 算法控制型

基于智能合约，利用算法自动增加或缩紧货币供给，调节供需以保持币价稳定。主要的算法控制型稳定币包括 Basis、Carbon 等。



图表 144: 算法控制型稳定币工作原理



资料来源：哈希派，链得得，中金公司研究部



**产业链#1: 矿机、矿工、矿池**

共识机制是区块链技术的重要组成部分之一。其目的是使分散于各处且互相平行的网络节点之间达成一致。主要的共识机制包括 PoW (ASIC), PoS (GPU) 为了实现高效的网络运转, 一般会采用专用芯片加速网路运算。

比特币及以太坊等主要加密资产采用哈希运算等工作量证明 (Proof of Works) 的形式进行竞争记账。作为成功记账的奖励, 参与记账的节点 (矿工) 获得 1) 交易发起方支付的手续费; 2) 比特币网络新生成的区块奖励 (比特币)。矿工主要成本包括 1) 进行哈希运算消耗的电费; 2) 矿机的初始成本以及折旧。

2008 年“中本聪”提出比特币是基于密码学的去中心化网络。相互独立的矿工在自己家里利用 PC 通过工作量证明形成共识, 维持网络的运行, 并获得收益。用户通过钱包实现点对点的支付, 整个交易不需要通过银行等可信赖第三方机构的支持。比特币矿机专门用于挖矿 (工作量证明计算) 的计算机, 矿机的特点是通过采用大量专用挖矿芯片进行并行计算, 实现远远优于 CPU/GPU 等传统通用芯片的能耗比和计算设备的性价比。

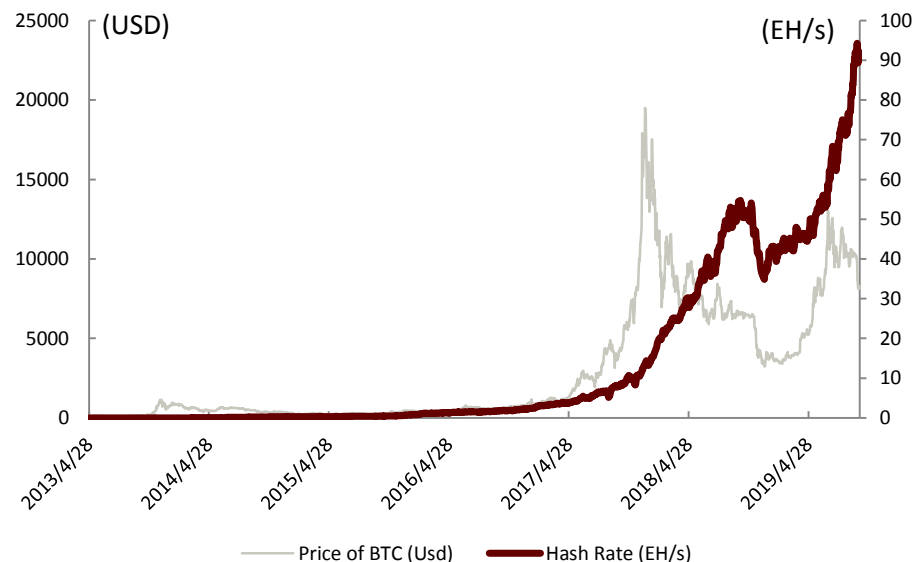
图表 145: 主要共识机制及其对应芯片解决方案

	PoW		PoS	DPoS	PBFT
区块链应用	BTC/BCH	ETH	NXT	EOS	Hyperledger Fabric
芯片解决方案	ASIC	CPU/GPU	CPU/GPU	CPU/GPU	CPU/GPU
主要厂商	嘉楠耘智、亿邦国际	英特尔、英伟达、AMD	英特尔、英伟达、AMD	英特尔、英伟达、AMD	英特尔、英伟达、AMD
2017年市场规模	30亿美元	很小	很小	很小	未知

资料来源: AMD, 英伟达, 英特尔, 嘉楠耘智, 亿邦国际, 中金公司研究部

**币价、在网算力、矿机销售量之间的关系:** 我们注意到比特币价格和网算力之间存在动态平衡的关系。在网算力直接影响矿机的销售。

图表 146: 在网算力和币价之间关系

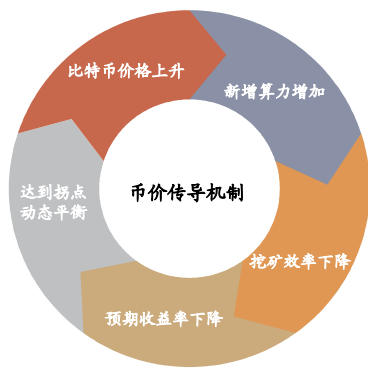


资料来源: btc.com, 中金公司研究部

- ▶ **当比特币价格处于上升通道:** 市场较为火爆时, 预期挖币收益提高, 回本周期缩短, 带动矿机售价及销量走高, 新增算力持续增加; 直至某个节点, 新增矿机预期回本周期不具备吸引力, 则会有矿机退出, 达到动态平衡状态。
- ▶ **当比特币价格处于下行阶段:** 市场较萎靡时, 预期挖币收益降低, 回本周期拉长, 拉低矿机售价及销量, 算力增速降低, 有矿工持续退出; 直至某个节点, 单台矿机经济效益达到上升拐点, 再次吸引矿工加入, 达到动态平衡状态。

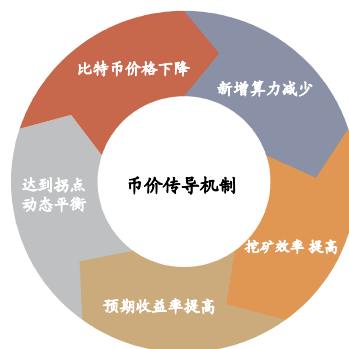


图表 147: 币价上升时全网算力变化趋势



资料来源：巴比特，星球日报，中金公司研究部

图表 148: 币价下降时全网算力变化趋势



资料来源：巴比特，星球日报，中金公司研究部

### 比特币矿工

**比特币矿工**通过参与竞争记账，获得比特币网络的奖励和交易发起方支付的交易手续费。目前矿工一般加入某个矿池，参与共同挖矿，矿工一定时间能够获得的收益与矿机成本、电力成本、全网算力、自身贡献算力、币价等因素有关。一个简化的收益公式如下。

$$\text{总收益}(T) = -\text{矿机买入价} + \sum_{t=0}^T \left( \text{区块奖励} \times \text{币价}(t) \times \frac{\text{自身算力}}{\text{全网总算力}(t)} - \text{电力成本} \right)$$

- ▶ **矿机成本**：矿工可以通过选择不同的矿机来控制矿机成本，但这个也会同时影响矿机算力。一般新一代矿机成本较高，但算力贡献也大。
- ▶ **电力成本**：矿工可以选择到电费低的地方挖矿，或者通过加入电费较低的**矿场**来降低电力成本。
- ▶ **全网总算力**：矿工无法控制，长期来看，取决于币价走势。币价上涨会导致总算力增加，然后最终达到均衡。
- ▶ **自身贡献算力**：取决于矿机的算力。但由于现在全网算力很大，单台矿机几乎无法取得收益，因此几乎所有矿工选择加入矿池，提高节点算力和挖到比特币的几率，之后通过矿池分成模式获得对应收益。
- ▶ **币价**：矿工无法控制，取决于比特币市场行情。

图表 149: 影响矿工收益的各个因素

	矿机成本	电力成本	全网算力	自身贡献算力	币价
相关性	-	-	-	+	+
矿工能够控制	可以	可以	不可以	可以	不可以

资料来源：巴比特，星球日报，中金公司研究部

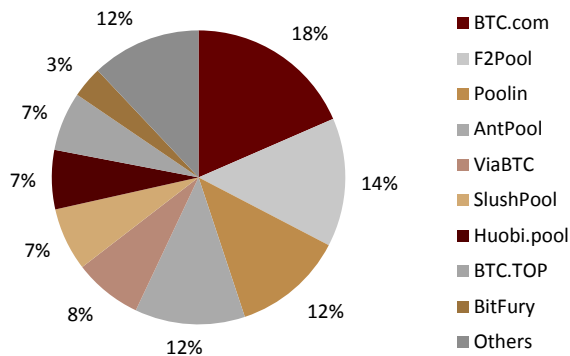
### 矿池

矿池的主要职能是通过专用挖矿协议，协调大量的矿工一起挖矿。连接到矿池里的矿工，在挖矿时与矿池服务器保持连接，和其他矿工同步工作。矿池中的矿工共享奖励。成功出矿的奖励支付到矿池的比特币地址，而不是单个矿工。一旦奖励达到一个特定的阈值，矿池服务器便会支付奖励到矿工的比特币地址。通常情况下，矿池服务器会提供矿池服务收取一定比例的费用。



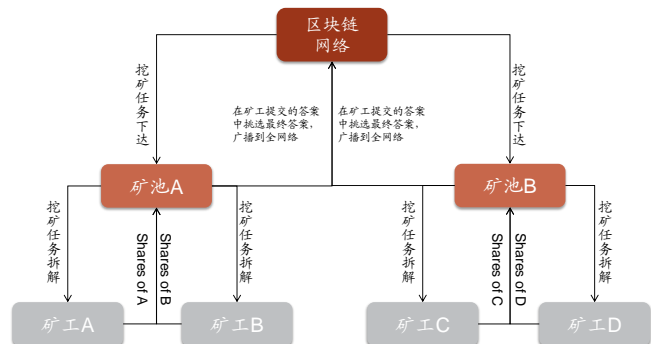
对矿工来说，和个人挖矿相比，加入矿池有两个好处。一方面可以避免运行比特币全节点所需要的存储和带宽成本；另一方面通过和其他矿工分享收益，可以提高挖矿回报的稳定性。2018 年 12 月 3 日全网算力约 38.88EH/s，一台蚂蚁 S9 算力为 13.5TH/s，一天理论上可以挖到 0.063% 个比特币。

图表 150: 比特币矿池算力占比



资料来源: btc.com, 中金公司研究部; 注: 以 2019/10/13 近 3 个月出块数据计算

图表 151: 矿池的工作原理



资料来源: 火星财经, 链世界, 中金公司研究部

矿池的商业模式和收益: 成功挖矿的关键在于最先找到全网难度的随机数。矿池在接收到下一个区块难度时，会将区块难度分成很多难度更小的任务下发给矿工计算，矿工完成一个任务后将结果提交给矿池，这个过程算矿工提交一个 share。假设全网难度要求 n 的值为 100，即前 100 个比特币为 0，矿池可能会给矿工分配一个任务，要求前 30 位为 0，然后再从所有提交的任务中，寻找有没有凑巧前 100 位为 0 的目标值。

不同矿机算力的大小不同，矿池会根据算力大小分配不同难度的任务。比如 A 矿机的额定算力 5T，B 矿机的额定算力为 10T，那么矿池给 A 矿机分配任务要求计算哈希难度的前 5 个比特币为 0，B 矿机的任务可能会是哈希难度的前 10 个比特币为 0。找到前 10 个比特币为 0 的难度要远大于找到前 5 个比特币为 0，而前 10 个比特币为 0 成为符合条件目标值的概率也大于前 5 个比特币为 0 的概率。所以从概率上来讲，B 矿机可能贡献正确答案的概率要大于 A 矿机。

由于是聚集很多矿机的算力挖矿，在挖到比特币之后，要给矿工计算收益。矿池和矿工之间主要采取以下两种结算模式：

- **PPLNS (Play Per Last N Shares):** 收益结果和每个人贡献的 shares 相关。假设 A 提交了 3 个可能正确的 shares，B 提交了 5 个可能正确的 shares，那么无论最后的答案是 A 提供的还是 B 提供的，A 都将获得这次收益的 3/8，而 B 将获得 5/8。
- **PPS (Play Per Share):** 完全根据算力贡献按比例分享收益。假设全网总算力为 100T，整个矿池算力 20T，A 矿机算力 5T，A 矿机算力占全网 5%，那么 A 矿机理论上每天可以获得 90 个比特币。无论矿池收益如何，A 矿池的收益不变。如果矿池当天的收益多于理论值，那么多余的收益归属矿池；如果矿池当天的收益小于理论值，那么矿池自行承担亏损。

我们可以很容易看出，PPS 相较于 PPLNS 模式收益稳定，而且矿池自负盈亏，自担风险。因此，PPS 模式的矿池费相较 PPLNS 会高一些，大约 8%，而 PPLNS 的矿池费大约为 4-5%。

### 矿场

矿场是为矿机提供托管 (Hosting) 服务的数据中心。矿场的作用在于将矿机物理集中在电价较低的区域，利用低电力成本获取更大收益。在中国来看，一般会选择内蒙古、四川、云贵高原、新疆等电力资源丰富且电价便宜的地方。





图表 152: 比特币矿场



资料来源: btc.com, 中金公司研究部

图表 153: 主要国家电费比较 (2018 年)

国家	电价 (Usd/KWh)
澳大利亚	0.21
日本	0.2
美国	0.17
巴西	0.17
英国	0.15
加拿大	0.14
中国	0.14
俄罗斯	0.1
阿尔及利亚	0.02

资料来源: Electricity Tariffs, Power Outages and Firm Performance, 中金公司研究部

根据 blockchain.info 的统计, 2017 年全球比特币耗电量达到 227 亿度, 其中中国矿场约占全球 70%。2017 年 9 月 4 日, 央行限制比特币交易所在中国的运营; 11 月互联网金融整治办开会讨论引导矿场退出问题, 央行要求各地政府从电力供应入手, 逐步削减比特币矿场规模。在政策不利的情况下, 很多矿场开始向海外转移。

由于矿场选址的两个条件: 1) 电价低; 2) 温度低, 加拿大、俄罗斯、冰岛等地区逐渐成为挖矿首选地区。莱比特和微比特两个中国较大矿场已经在加拿大、冰岛和美国设立分部。

矿场经营的另一个压力来自比特币价格的不断下跌。2018 年 12 月 4 日比特币价格为 3859 美元, 和年初最高点相比已经下跌 70%, 这意味着挖矿获得的收益已经不足以支付电费、管理费等挖矿成本, 很多中小型矿场迫于成本压力将会选择退出市场。

## 产业链#2: 交易所和托管行

交易所交易包括币币交易及法币与加密资产的交易, 主要有两种获利方式: 交易费和上市费。1) 交易费: 概念类比证券交易所, 收取千分之一到千分之四的交易费不等, 根据交易实际情况而定; 2) 上市费: 数字资产若想登录交易所, 需要支付百万至千万人民币的申请费。

我们认为交易所可以分为两类, 一类交易所重视合规, 仅支持法币与加密资产兑换, 如 Coinbase 和 Circle; 另一类重在提高交易量, 提升交易所活跃度, 比如币安、火币等。我们认为, 未来合规化是大方向, 交易所将努力拿到更多的国家牌照来拓展业务。

图表 154: 主要交易所交易量排名 (截止 2019/10/14)

#	名称	近30天交易量	交易对数	成立时间	注册地
1	BitMEX	\$70,626,273,362	1	2014/1	塞舌尔
2	Fcoin	\$40,789,231,192	60	2018/5	新加坡
3	EXX	\$32,210,722,055	28	2018/7	马耳他
4	BKEX	\$31,241,863,623	80	2018/5	英属维尔京群岛
5	币安	\$28,387,753,612	556	2017/7	马耳他
6	MXC	\$26,716,334,536	171	2018/4	新加坡
7	胖比特	\$26,287,168,831	125	2017/12	美国
8	Coineal	\$25,852,137,124	37	2018/4	塞舌尔
9	Latoken	\$25,679,135,333	260	2017/9	爱沙尼亚
10	满币	\$25,096,135,712	215	2017/9	新加坡
11	OKEx	\$24,434,264,895	466	2014/1	马耳他

资料来源: CoinMarketCap, Crocosource, bt110, 中金公司研究部



图表 155: 主要交易所及所运营的国家或地区

	美国	中国	日本	韩国	中国香港	新加坡
币安	✓			计划进入	✓	✓
OKEx	✓		✓	✓	✓	✓
火币	✓		✓	✓	✓	✓
Coinbase	✓					✓

资料来源: CrocoSource, Odaily, 中金公司研究部

阻碍加密资产普及的一个主要问题是其被盗问题。和黄金等有形资产不同，加密资产是一种特殊的无形资产，私钥是其唯一的资产凭证。在线存储时容易受到黑客攻击，离线存储流动性较弱。

为了解决交易所被盗时的法律问题，在 Coinbase 等主要交易所的推动下，加密资产行业正逐步建立托管制度，托管行是指负责保管、持有基金管理公司等投资机构从客户处募集到的资金，并对基金管理人使用这笔资金进行监管和对外披露信息的机构。针对法币的托管行，通常由商业银行来担当。2018 年 10 月，纽约金融服务部（NYDFS）批准了 Coinbase 成立托管信托公司的申请（<https://www.dfs.ny.gov/about/press/pr1810231.htm>），允许 Coinbase 为用户提供 BTC、BCH、ETH、ETC、LTC 以及 XRP 等币种的托管服务。

图表 156: 主要比特币被盗事件

时间	受影响交易所	损失币种及金额	后续处理
2011.06	Mt.Gox	约2609枚比特币	-
2014.02	Mt.Gox	约80万个比特币	Mt.Gox宣告破产，CEO入狱
2014.03	Poloniex	约97个比特币	Poloniex称所有受到影响都用户收到了补偿
2014.08	BTER	约5000万个NXT币，价值约1000万人民币；110个比特币赎金	加强安全措施，冷钱包存币；交易所将会承担所有损失，将分批次陆续偿还给用户
2015.01	LocalBitcoins	约17个比特币	公司补偿被盗用户，完善安全漏洞
2015.01	Bitstamp	约19000个比特币	冷钱包存储交由专门机构存储
2016.08	Bitfinex	约119756个比特币	每位用户的账户平均损失36%
2017.04	Youbit	约4000个比特币	公司申请破产
2017.06	Bithumb	各种电子加密资产共约350亿韩元	加强安全措施
2018.01	Coincheck	约5.26亿个NEM	交易所以每个新币88.55日元的价格赔偿26万名受损失的客户
2018.03	Binance	API交易机器人大量买入VIA币，控制币价	损失由用户自行承担
2018.06	Coinrail	价值1950万美元的NPXS代币；价值1380亿美元的Aston X；价值580万美元Dent代币；价值超过110万美元的Tron波场币	将使用冷钱包存币
2018.09	Zaif	包括BTC、BCH和MonaCoin在内的加密资产总价值约67亿日元	公司将全数归还用户损失，管理层引咎辞职
2019.01	Cryptopia	300448枚ETH	-
2019.03	DragonEX	146万枚USDT，20.5万枚EOS在内价值超过602万美元的数字资产	用户自行承担损失
2019.05	Binance	被盗7000枚比特币，损失约3亿元人民币	将会使用用户安全资产基金全额支付用户损失
2019.06	Bittrue	价值约430万美元的XRP和ADA代币	-
2019.07	Bitpoint Japan	包括XRP在内的价值35亿日元加密货币	-

 资料来源: cryptochainchart.info, <http://www.btcbricks.com>, 中金公司研究部

据彭博报道<sup>25</sup>，高盛等众多传统金融机构，已经开始考虑提供数字资产托管业务。

<sup>25</sup> <https://www.bloomberg.com/news/articles/2018-08-06/goldman-is-said-to-consider-custody-offering-for-crypto-funds>



图表 157: 推出加密资产托管的主要金融机构

公司名	推出托管服务时间	国家
新韩银行	2017.11	韩国
Grayscale Investment	2018.03	美国
北方信托	2018.03	美国
Komainu	2018.05	日本
BitGo	2018.05	美国
kindom Trust	2018.05	美国
Coinbase	2018.07	美国
DACC	2018.08	美国
Vontobel银行	2019.01	瑞士
Fidelity	2019.03	美国

资料来源: [cryptochainchart.info](https://cryptochainchart.info), 中金公司研究部

## 主要企业介绍: Coinbase、Circle

## Coinbase: 估值最高的交易所, 向合规方向发展

Coinbase 是美国知名的加密资产交易平台, 成立于 2012 年, 总部在美国旧金山, 目前有来自 33 个国家的 2,500 万注册用户, 月活用户达到 60 万。Coinbase 从成立开始已经完成 7 轮融资, 总计 5.25 亿美元, 最新估值 80 亿美元, 投资方包括著名基金 Tiger Global Management, Union Square Ventures, Andreessen Horowitz, IDG Ventures 等。另外, 还有老牌金融机构纽约证券交易所 NYSE, 美国大牌金融机构 USAA, 日本东京银行 Bank of Tokyo, 日本三菱金融集团 MUFG 等知名传统金融机构。

图表 158: Coinbase 融资情况

时间	轮次	投资方个数	融资金额 (百万美元)	领投方及部分投资者
2012/9/12	种子轮	7	0.6	Y Combinator, FundersClub, Alexis Ohanian, Hard Yaka, Garry Tan, Harjeet Taggar, Invenmax
2013/5/7	A轮	8	6.1	SV Angel, FundersClub, Union Square Ventures
2013/12/12	B轮	5	25	Andreessen Horowitz, Union Square Ventures, QueensBridge Venture Partners
2015/1/20	C轮	14	75	DFJ, Andreessen Horowitz, Union Square Ventures, Boost VC
2016/6/7	风险轮	3	10.5	Bank of Tokyo-Mitsubishi UFJ, Sozo Ventures
2017/8/10	D轮	12	108.1	Institutional Venture Partners, Greylock Partners, Batley Ventures, Spark Capital
2018/10/30	E轮	5	300	Tiger Global Management, Y Combinator, Andreessen Horowitz, Wellington Management

资料来源: 链得得, 中金公司研究部

Coinbase 是注重合规的典型代表, 在美国和全球几乎拥有所有合规的牌照。

图表 159: Coinbase 牌照类别

范围	类别	获取途径
地域范围	美国各州	取得50个州的转账交易牌照 (Money Transmitter License)
	纽约州	取得数字货币交易所办法的BitLicense, 和取得数字托管牌照
	美国联邦	正在申请国家银行特殊牌照 (Special National Bank Charter)
	全球	取得33个国家合法经营许可, 以及英国和欧盟的E-Money牌照
上下游产业链	支付	自营Coinbase Commerce, 并收购2家支付公司获得支付牌照
	储蓄	通过Coinbase Ventures收购Compound公司获得储蓄经营许可
	贷款	通过Coinbase旗下关联公司投资Dharma公司获得贷款经营许可
	金融衍生品交易	通过Coinbase旗下关联公司投资dYdX公司获得衍生品交易资格
	另类资产交易	收购Venovate Marketplace公司拥有另类资产交易资格
	券商交易	收购Keystone Capital公司拥有券商交易资格牌照
	投资顾问牌照	收购Digital Wealth公司拥有投资顾问牌照

资料来源: Coinbase 官网, 中金公司研究部

Coinbase 依托合规的牌照, 在全球开展加密资产全生态链和全球化的布局:



图表 160: Coinbase 全产业链布局

类别	名称
普通客户交易平台	Coinbase Consumer
专业客户交易平台	Coinbase Pro
机构客户交易平台	Coinbase Prime
数字货币存管	Coinbase Custody Trust Company
钱包	Coinbase Wallet
支付	Coinbase Commerce, Celo, Spacemesh
储蓄	Compound
指数基金	Coinbase Asset Management
金融衍生品交易	dYdX
稳定币	USDC (Co-Founder), Reserve
合规和反洗钱	Distributed Systems, Abacus
贷款	Dharma
另类资产交易平台	Venovate Marketplace
券商交易	Keystone Capital, Paradex
投资顾问牌照	Digital Wealth
比特币应用	earn.com

资料来源: Coinbase 官网, 中金公司研究部

Circle: 致力于建立加密资产生态

Circle 成立于 2013 年, 是一家提供加密资产交易平台以及加密资产储存的创业公司。创始人是 Macromedia 前科技总监 Jeremy Allaire 及 Sean Neville。目前旗下业务包含 Circle Trade 场外交易服务、Poloniex 交易平台、Circle Invest 以及 Circle Pay 等。

图表 161: Circle 主营业务

表格	功能	备注
Poloniex	加密资产交易平台	2018年2月Circle收购Poloniex, 将与Circle Trade、Circle Pay等服务对接, 实现多种法币币种的交易
Circle Trade	加密资产场外交易服务	在收购Poloniex之前, 主要靠OTC业务服务加密资产交易
Circle Invest	加密资产投资服务	
Circle Pay	加密资产交易服务	

资料来源: Circle 官网, 中金公司研究部

Circle 的主要投资人包括高盛、IDG 资本、Pantera、中金公司、光大、百度等。2018 年 5 月 Circle 完成 1.1 亿美金的 E 轮融资, 投后估值 30 亿美金。

与 Coinbase 一样, Circle 的优势也在于齐全的合规牌照。

图表 162: Circle 牌照类别

范围	类别	获取途径
地域范围	美国各州	取得49个州的转账交易牌照 (Money Transmitter License)
	纽约州	取得数字货币交易所办法的BitLicense
	美国联邦	正在申请国家银行特殊牌照 (Special National Bank Charter)
	全球	获得英国金融市场行为监管局颁发的E-Money牌照
上下游产业链	支付	自营Circle Pay, 并收购Poloniex获得交易所执照
	投资	自营Circle Invest

资料来源: Circle 官网, 中金公司研究部



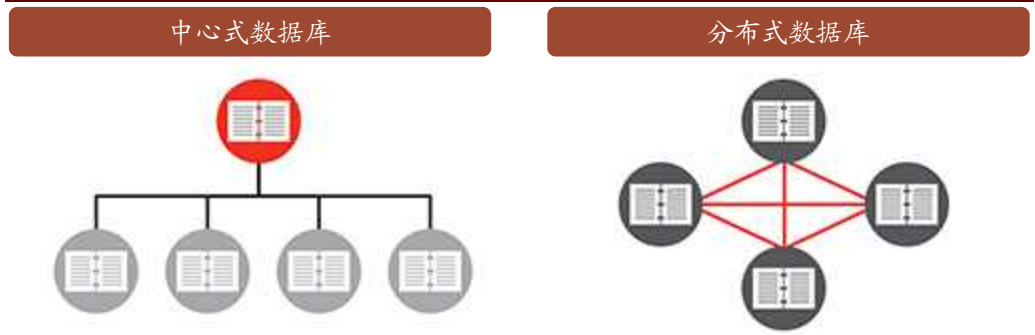
## 区块链的核心技术及未来技术演进

区块链是一种不可篡改的分布式记账技术，其四大核心技术包括：1) 分布式账本；2) 密码学；3) 共识机制；4) 激励机制。

### 分布式账本

“**分布式账本**”是指账本被分散保存在所有成员节点，数据的添加、删除、修改等不需要通过任何中心化主体。节点之间相互沟通，确保对交易准确、及时的记录。

图表 163: 传统中心式数据库和分布式数据库比较



资料来源：CCN，中金公司研究部

### 数据结构：通过哈希密码算法链接的区块的顺序链

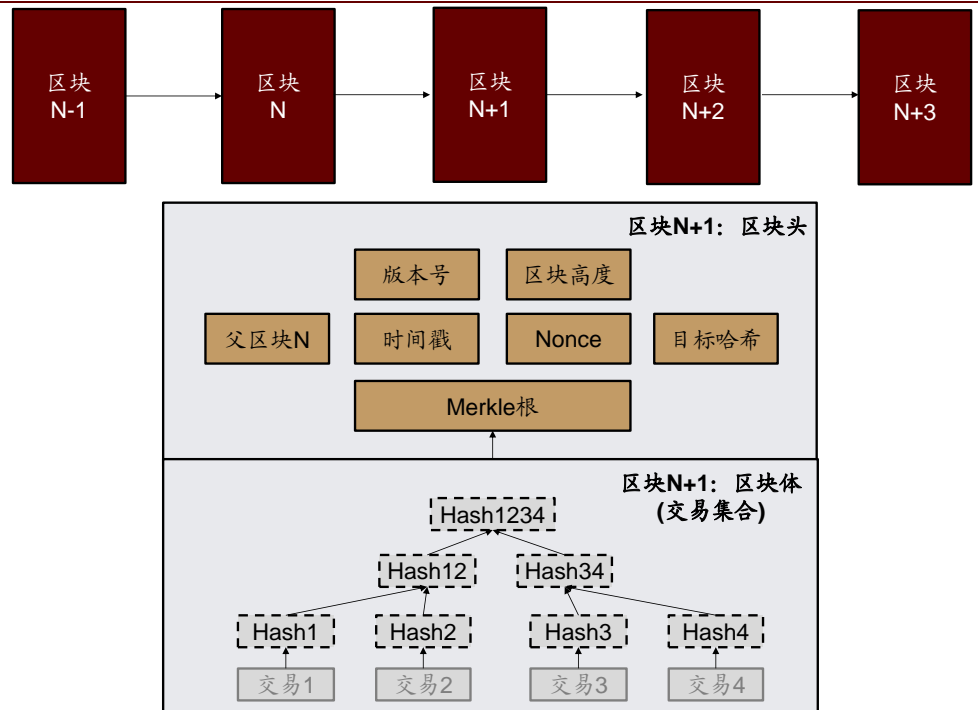
区块链是“通过哈希密码算法链接的区块的顺序链”的数据结构，保证数据一旦被保存以后，不可被篡改。哈希函数的特点是可以将任意长的消息压缩为一个固定长度（例如 256bit）的摘要。哈希函数的一个重要特性是给定任意哈希值，很难从中恢复原消息或者找到另外一个具有同一哈希值的消息。区块的签名中用到非对称加密技术，即公钥、私钥加密机制，用于数字签名。

每个区块包括区块头和区块体。区块头封装了版本号、父区块哈希值、目标哈希、当前区块 PoW 算出的随机数（Nonce）等。区块体包含经过当前区块认证、区块创建过程中生成的全部交易记录，这些记录通过 Merkle 树的哈希过程生成唯一的 Merkle 根，并被封装进区块头。





图表 164: 区块链的数据结构






资料来源: Learnblockchai, 中金公司研究部

## 共识机制: 工作量证明 (PoW) 权益证明 (PoS)、股份授权证明 (DPoS)

区块链通过引入“共识机制”解决如何在分布式环境下竞争记账的问题。目前主流共识机制有工作量证明 (PoW)、权益证明 (PoS)、股份授权证明 (DPoS)。PoW 应用较为广泛, 完全去中心化, 但共识达成周期长且消耗大量能源; POS 目前尚无广泛应用, 根据每个节点所占加密资产的比例及时间, 等比例降低挖矿难度; EOS 采用 21 个超级节点的 DPoS 代理人机制, 提高交易处理速度, 但中心化程度加强。

图表 165: 工作量证明 (PoW)、权益证明 (PoS)、股份授权证明 (DPoS) 比较

	PoW	PoS	DPoS
定义	一种由算力大小决定记账权的共识机制: 拥有的算力越大, 挖出下一区块的概率越大	一种由权益大小决定记账权的共识机制: 拥有的权益越大, 挖出下一区块的概率越大	由节点选出的若干代理人验证和记账
优点	<ul style="list-style-type: none"> <li>✓ 规则简单、透明、有效、可靠</li> <li>✓ 完全去中心化</li> </ul>	<ul style="list-style-type: none"> <li>✓ 缩短了共识达成周期</li> <li>✓ 减少了能源消耗</li> </ul>	<ul style="list-style-type: none"> <li>✓ 共识达成周期短、效率高</li> </ul>
缺点	<ul style="list-style-type: none"> <li>× 造成大量能源消耗</li> <li>× 共识达成周期长</li> </ul>	<ul style="list-style-type: none"> <li>× 规则复杂, 且完备的、难以攻击的规则较难制定</li> <li>× 非完全去中心化</li> </ul>	<ul style="list-style-type: none"> <li>× 去中心化程度低</li> </ul>
典型币种	<ul style="list-style-type: none"> <li>● 比特币BTC</li> <li>● 以太坊前三个阶段 (Frontier前沿、Homestead家园、Metropolis大都会)</li> </ul>	<ul style="list-style-type: none"> <li>● 以太坊第四阶段 (Serenity宁静)</li> <li>● 未来币NXT</li> <li>● 量子链QTUM</li> </ul>	<ul style="list-style-type: none"> <li>● EOS</li> </ul>
			

资料来源: 比特币白皮书, 以太坊白皮书, EOS 白皮书, 中金公司研究部

## 激励机制 (挖矿)



区块链通过发行和分配加密资产给参与共识机制的网络节点（矿工），来维护系统良性发展。以比特币为例，网络节点（矿工）付出计算资源和电能参与工作量证明记账，作为成功记账的回报获得相应的比特币。以太坊将 GAS 作为运行智能合约的费用，地位与比特币系统中的交易手续费相当，并采用 ETHASH 方式挖矿，防止 ASIC 矿机垄断。EOS 每年增发 5%，1% 用于超级节点和候选节点的补偿，4% 用于 EOS 平台建设，EOS 补偿不是根据节点算力大小而通常是 EOS 币的数量决定，所以不存在大型矿厂或高算力 ASIC 矿机。私有链中则不一定需要进行激励，因为往往记账是基于链外的特定，强制力实施。

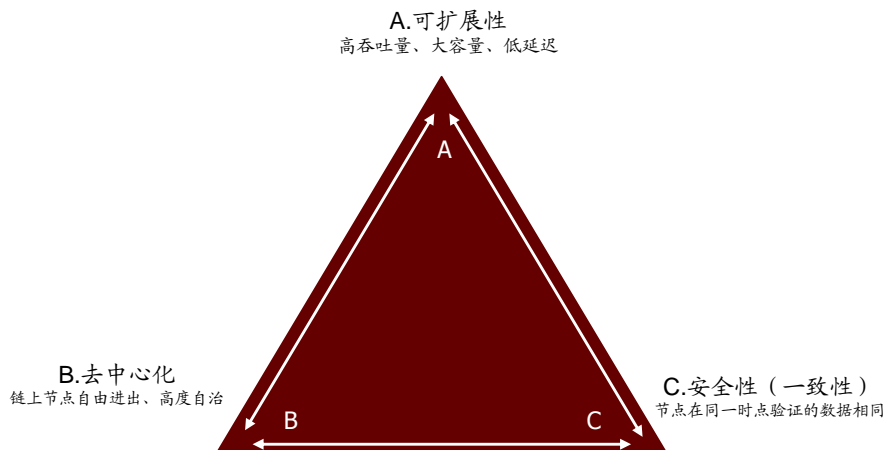
区块链通过发行和分配激励用户成为节点参与社区运作。比特币从 2009 年开始可以挖矿，最开始的四年每个区块出 50 个币，四年减半一次（目前是 BTC12.5/块），预计 2140 年比特币将被挖完，总量将在 2.1 千万左右；以太币 2014 年 7 月众筹了约 7200 万以太币，每年产量上限 1800 万，暂时未设置上限；EOS 在 2017 年 6 月开始通过以太币众筹出售，2018 年 6 月结束众筹，总共放出 10 亿个 EOS 币，而后每年增发上限为 5%。

### 不可能三角：去中心化，吞吐量，安全性的悖论

比特币网络的最大问题是其吞吐量。比特币网络目前每秒最多只能处理 7 笔交易。这限制了比特币作为交易手段的应用场景。为了解决这个问题，各个加密资产社区分别提出了各自的解决方案。

- ▶ 比特币现金：将区块扩容 8 倍至 8M，但依旧无法做到高吞吐量，在支付场景仍受限。
- ▶ 以太坊：追求可扩展性和中心化，但牺牲了安全性，如发生了“The DAO”事件。
- ▶ EOS：采用超级节点的模式，以部分牺牲去中心化的特点，实现每秒百万笔的处理能力。

图表 166：区块链的不可能三角——去中心化，速度，安全



资料来源：壹零财经，中金公司研究部

### 分布式自治组织（DAO）：全新的机构形态，不受中心化控制，有着明确目标，自我发展

DAO 为分布式自治组织（Distributed Autonomous Organization）的缩写，这是一种基于区块链的组织形式，它通过一系列公开公正的规则，可以在无人干预和管理的情况下自主运行。这些规则常以开源形式存在，可以通过购买该组织的股份权益，或者提供服务的形式来成为该组织的参与者。

当初始程序设定完成后，它会按照既定的规则开始运作，并在运作的过程中，根据实际情况不断的自我维护和升级，来适合周围环境。DAO 的形态非常广泛，它可能是某种加密资产，也可能是一个系统或者机构，甚至可能是无人驾驶汽车，它们都为客户提供有价值的服务。DAO 不受任何中心化控制，且有着明确目标，可以自我发展进化。



图表 167: DAO 形态广泛，包含加密资产和无人驾驶汽车等



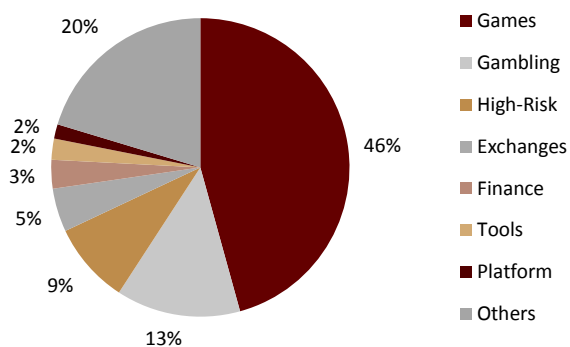
资料来源: Ethereum-Kaufen.de, 中金公司研究部

## 分布式应用 (DAPP)

DAPP 与 DAO 的最大区别在于自动化程度不同。DAPP 在设立之后，每一个 DAPP 用户作为 DAPP 社区的一员，可以对 DAPP 的更新方向进行投票，而 DAO 只能根据预先设定好的程序运行，规则无法修改。

DAppTotal 数据显示，以太坊上所有 DAPP 的总日活人数在 5 万人左右，纳入 DAppTotal 统计的以太坊 DAPP 一共 2,329 个，其中活跃应用 238 个，日活人数在 500 以上的应用有 7 个。在所有以太坊应用中，游戏类 DAPP 占比 46% 排名第一，博彩类 13%，被标注“高风险”（即存在高欺诈风险）的 DAPP 占到了 9%。交易量前 10 的 DAPP 中，交易所 5 个，金融类 3 个，游戏类、博彩类各 1 个。

图表 168: 以太坊各类型 DAPP 占比 (日活大于 10)



资料来源: DAppTotal, 中金公司研究部; 截至 2019.10.22

图表 169: 以太坊 7 日交易量前十的 DAPP

#	Name	Category	Balance (€)	Users 24h (€)	Volume 24h (€)	TX 24h (€)	Users 7d (€)	Volume 7d (€)
1	CDP Portal	Exchanges	1.89M	396 +12.78%	2.23K +119.02%	601 +15.11%	2.91K +4.62%	20.32K +1.39%
2	Maker	Finance	1.89M	490 +13.22%	2.23K +119.02%	650 +19.55%	2.93K +4.02%	20.31K +1.21%
3	dice2win	Games	458.1	73 +15.87%	3.73K +56.89%	5.68K +3.09%	220 +17.32%	15.09K +7.70%
4	dYdX	Exchanges	0	126 +53.60%	1.84K +76.87%	512 +74.74%	392 +3.77%	14.76K +0.30%
5	Kyber	Finance	1.74K	315 +6.79%	1.96K +296.64%	697 +33.02%	1.55K +12.22%	11.75K +30.40%
6	SingularX	Exchanges	3.9K	124 +0.81%	589.62 +0.96%	412 +17.60%	475 +1.29%	7.51K +14.24%
7	Tokenion	Exchanges	0	169 +29.01%	860.37 +0.64%	371 +32.02%	789 +16.39%	7.02K +42.37%
8	Uniswap	Finance	40.6K	294 +21.49%	1.71K +155.11%	948 +17.47%	1.16K +6.24%	7.01K +37.68%
9	X2BETWIN	Gambling	12.56	580 +3.39%	731.28 +17.70%	626 +3.81%	801 +0.75%	6.42K +58.11%
10	exexiDEX	Exchanges	41.72K	305 +16.90%	582.27 +15.96%	3.68K +29.07%	1.52K +0.60%	5.17K +13.62%

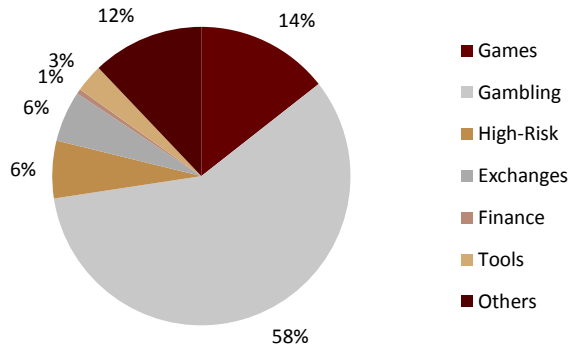
资料来源: DAppTotal, 中金公司研究部; 截至 2019.10.23

DAppTotal 数据显示，截至 2019 年 10 月 23 日，EOS 上所有 DAPP 的总日活人数在 10 万人左右，纳入统计的 DAPP 一共 618 个，其中活跃应用 180 个，日活在 500 人以上的应



用有 27 个。在所有 EOS 应用中，博彩类 DAPP 数量占比 58%左右，排名第一，游戏类 DAPP 占比 14%左右，排名第二。交易量前 10 的 DAPP 中博彩类 7 个，交易所 1 个，金融类 1 个，“高风险”1 个。

图表 170: EOS 各类型 DAPP 占比（日活大于 10）



资料来源：DAppTotal，中金公司研究部；截至 2019.10.22

图表 171: EOS 7 日交易量前十的 DAPP

#	Name	Category	Balance	Users 24h	Volume 24h	TX 24h	Users 7d	Volume 7d
1	Newdex	Exchanges	166.98K	1.59K	8.04M	429.05K	4.6K	52.31M
2	BigGame	Gambling	1.03M	604	319.48K	201.72K	1.32K	3.18M
3	EosBlue	Gambling	62.05K	276	324.32K	551.45K	626	2.42M
4	Dice	Gambling	122.24K	11.61K	415.17K	755.77K	24.48K	2.32M
5	EOS REX	Finance	105.69M	392	216.85K	1.12K	1.66K	1.81M
6	Gato Binary	High-Risk	5.32K	785	344.92K	546.83K	1.07K	1.44M
7	Spinach	Gambling	42.78K	133	145.87K	24.81K	253	665.61K
8	EOSBet	Gambling	121.04K	305	65.02K	52.42K	911	537.4K
9	EOSPLAY	Gambling	366.4K	19	35.98K	26.93K	67	856.68K
10	BATDAPP	Gambling	7	1	66.51K	2.22K	3	458.4K

资料来源：DAppTotal，中金公司研究部；截至 2018.10.23

金融方面：人们希望探索区块链在金融其他领域更多的可能性，可以把区块链作为可编程分布式信用基础设施，用来支撑智能合同等应用。智能合约包含三个要素：要约、承诺和价值交换，这帮助区块链将应用范围从货币扩展至具有合约功能的其他领域，比如保险合同、知识产权等。

生活方面：更多区块链应用会扩展到生活的其他方面，比如工业、科学、文化等。它可以提供一种全球通用的解决方案，不再依赖第三方的监督或信用保证，从而提高社会整体资源的运营效率。区块链将连接所有的人员及设备，全球形成统一的网络，可以实时推动价值及资源在全球范围的流动。



---

## 法律声明

---

### 一般声明

本报告由中国国际金融股份有限公司（已具备中国证监会批复的证券投资咨询业务资格）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，但中国国际金融股份有限公司及其关联机构（以下统称“中金公司”）对这些信息的准确性及完整性不作任何保证。本报告中的信息、意见等均仅供投资者参考之用，不构成对买卖任何证券或其他金融工具的出价或征价或提供任何投资决策建议的服务。该等信息、意见并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对任何人的个人推荐或投资操作性建议。投资者应当对本报告中的信息和意见进行独立评估，自主审慎做出决策并自行承担风险。投资者在依据本报告涉及的内容进行任何决策前，应同时考量各自的投资目的、财务状况和特定需求，并就相关决策咨询专业顾问的意见对依据或者使用本报告所造成的一切后果，中金公司及/或其关联人员均不承担任何责任。

本报告所载的意见、评估及预测仅为本报告出具日的观点和判断，相关证券或金融工具的价格、价值及收益亦可能会波动。该等意见、评估及预测无需通知即可随时更改。在不同时期，中金公司可能会发出与本报告所载意见、评估及预测不一致的研究报告。

本报告署名分析师可能会不时与中金公司的客户、销售交易人员、其他业务人员或在本报告中针对可能对本报告所涉及的标的证券或其他金融工具的市场价格产生短期影响的催化剂或事件进行交易策略的讨论。这种短期影响的分析可能与分析师已发布的关于相关证券或其他金融工具的目标价、评级、估值、预测等观点相反或不一致，相关的交易策略不同于且也不影响分析师关于其所研究标的证券或其他金融工具的基本面评级或评分。

中金公司的销售人员、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。中金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。中金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不一致的投资决策。

除非另行说明，本报告中所引用的关于业绩的数据代表过往表现。过往的业绩表现亦不应作为日后回报的预示。我们不承诺也不保证，任何所预示的回报会得以实现。分析中所做的预测可能是基于相应的假设。任何假设的变化可能会显著地影响所预测的回报。

本报告提供给某接收人是基于该接收人被认为有能力独立评估投资风险并就投资决策能行使独立判断。投资的独立判断是指，投资决策是投资者自身基于对潜在投资的目标、需求、机会、风险、市场因素及其他投资考虑而独立做出的。

本报告由受香港证券和期货委员会监管的中国国际金融香港证券有限公司（“中金香港”）于香港提供。香港的投资者若有任何关于中金公司研究报告的问题请直接联系中金香港的销售交易代表。本报告作者所持香港证监会牌照的牌照编号已披露在报告首页的作者姓名旁。

本报告由受新加坡金融管理局监管的中国国际金融（新加坡）有限公司（“中金新加坡”）于新加坡向符合新加坡《证券期货法》定义下的认可投资者及/或机构投资者提供。提供本报告于此类投资者，有关财务顾问将无需根据新加坡之《财务顾问法》第 36 条就任何利益及/或其代表就任何证券利益进行披露。有关本报告之任何查询，在新加坡获得本报告的人员可联系中金新加坡销售交易代表。

本报告由受金融服务监管局监管的中国国际金融（英国）有限公司（“中金英国”）于英国提供。本报告有关的投资和服务仅向符合《2000 年金融服务和市场法 2005 年（金融推介）令》第 19（5）条、38 条、47 条以及 49 条规定的人士提供。本报告并未打算提供给零售客户使用。在其他欧洲经济区国家，本报告向被其本国认定为专业投资者（或相当性质）的人士提供。

本报告将依据其他国家或地区的法律法规和监管要求于该国家或地区提供。





**特别声明**

在法律许可的情况下，中金公司可能与本报告中提及公司正在建立或争取建立业务关系或服务关系。因此，投资者应当考虑到中金公司及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突。

与本报告所含具体公司相关的披露信息请访问 [http://research.cicc.com/disclosure\\_cn](http://research.cicc.com/disclosure_cn)，亦可参见近期已发布的相关个股报告。

与本报告所含具体公司相关的披露信息请访问 <https://research.cicc.com/footer/disclosures>，亦可参见近期已发布的关于该等公司的具体研究报告。

**中金研究基本评级体系说明：**

分析师采用相对评级体系，股票评级分为跑赢行业、中性、跑输行业（定义见下文）。

除了股票评级外，中金公司对覆盖行业的未来市场表现提供行业评级观点，行业评级分为超配、标配、低配（定义见下文）。

我们在此提醒您，中金公司对研究覆盖的股票不提供买入、卖出评级。跑赢行业、跑输行业不等同于买入、卖出。投资者应仔细阅读中金公司研究报告中的所有评级定义。请投资者仔细阅读研究报告全文，以获取比较完整的观点与信息，不应仅仅依靠评级来推断结论。在任何情形下，评级（或研究观点）都不应被视为或作为投资建议。投资者买卖证券或其他金融产品的决定应基于自身实际具体情况（比如当前的持仓结构）及其他需要考虑的因素。

**股票评级定义：**

- 跑赢行业（OUTPERFORM）：未来 6~12 个月，分析师预计个股表现超过同期其所属的中金行业指数；
- 中性（NEUTRAL）：未来 6~12 个月，分析师预计个股表现与同期其所属的中金行业指数相比持平；
- 跑输行业（UNDERPERFORM）：未来 6~12 个月，分析师预计个股表现不及同期其所属的中金行业指数。

**行业评级定义：**

- 超配（OVERWEIGHT）：未来 6~12 个月，分析师预计某行业会跑赢大盘 10%以上；
- 标配（EQUAL-WEIGHT）：未来 6~12 个月，分析师预计某行业表现与大盘的关系在-10%与 10%之间；
- 低配（UNDERWEIGHT）：未来 6~12 个月，分析师预计某行业会跑输大盘 10%以上。

研究报告评级分布可从<https://research.cicc.com/footer/disclosures> 获悉。

本报告的版权仅为中金公司所有，未经书面许可任何机构和个人不得以任何形式转发、翻版、复制、刊登、发表或引用。

V190624  
编辑：樊荣



## 中国国际金融股份有限公司

中国北京建国门外大街1号国贸写字楼2座28层 | 邮编: 100004

电话: (+86-10) 6505 1166

传真: (+86-10) 6505 1156

### 美国

**CICC US Securities, Inc**

32<sup>th</sup> Floor, 280 Park Avenue

New York, NY 10017, USA

Tel: (+1-646) 7948 800

Fax: (+1-646) 7948 801

### 英国

**China International Capital Corporation (UK) Limited**

25<sup>th</sup> Floor, 125 Old Broad Street

London EC2N 1AR, United Kingdom

Tel: (+44-20) 7367 5718

Fax: (+44-20) 7367 5719

### 新加坡

**China International Capital Corporation (Singapore) Pte. Limited**

6 Battery Road, #33-01

Singapore 049909

Tel: (+65) 6572 1999

Fax: (+65) 6327 1278

### 香港

**中国国际金融（香港）有限公司**

香港中环港景街1号

国际金融中心第一期29楼

电话: (852) 2872-2000

传真: (852) 2872-2100

### 上海

**中国国际金融股份有限公司上海分公司**

上海市浦东新区陆家嘴环路1233号

汇亚大厦32层

邮编: 200120

电话: (86-21) 5879-6226

传真: (86-21) 5888-8976

### 深圳

**中国国际金融股份有限公司深圳分公司**

深圳市福田区益田路5033号

平安金融中心72层

邮编: 518048

电话: (86-755) 8319-5000

传真: (86-755) 8319-9229

