全球区块链产业全景与趋势年度报告

（2018-2019 年度）

火币区块链研究院

2019.2

Huobi Research

【作者】
袁煜明、朱翊邦、肖晓、池温婷、刘洋、丁肇飞、李慧、胡智威、马天元、丁元、类承叁

http:// research.huobi.cn

全球区块链产业全景与趋势年度报告（2018-2019 年度）

摘要

2018 年系数字资产市场由狂热到理性的一年，二级市场各项数据均大幅下滑，并传导至一级市场。同年，**比特币链上活跃度亦大幅下跌。但算力、挖矿难度等核心指标依旧健康**，仅有年底受市场破位下跌带来部分矿工离场所导致的小幅下滑，整体全年仍呈波动上涨态势，熊市更多是“市场”层面而言。

2018 年也是数字资产市场转型年，五大转型正在发生：(1) 资产发行主体由民间扩大到国家；(2) 资产发行合规化，证券类通证发行目前领先 DAICO；(3) 交易市场类金融化，交易标的向衍生品、指数化产品拓展；(4) 清结算向稳定币方式转变；(5) 市场参与者主体机构化。

2018 年还是数字资产市场合规化元年，三种态势正形成：(1) **监管体系逐步明朗，“牌照+沙盒+行业自律”雏形初现**；(2) **“分类监管”正逐步让位“无差别监管”**；(3) **联合监管从以欧盟为首的区域经济体开始。**以合规交易所、合规托管、证券类数字资产、稳定币为支柱的**“合规基础设施”发展迅速。**

区块链产业板块：(1)硬件与基建层：新纳米矿机销售不理想，**矿场、矿池面临盈利压力，部分 PoW 币种算力下降威胁区块链安全**；(2)平台与基础层：**公链降温，市场对 TPS 追求回归理性**；(3)通用技术层：**公链生态推进带动开发者工具发展，其中 EOS 发展迅速**；(4)垂直应用层：“区块链+”逐步开展，并在**构建信任、数据自治与价值化及通证激励等场景加速落地**；(5)周边服务层：交易平台**社区化管理模式、云交易所开始出现，钱包交易所雏形显现。**

区块链技术层面：(1)2018 年系**扩展性解决方案大年**，形成了 **Layer0、Layer1 和 Layer2 的三层模型**；(2)隐私性解决方案方面，部分新的加密智能合约、密文数据计算项目出现，**基于 MimbleWimble 的匿名货币 Grin 和 Beam 大热**；(3)2018 年，跨链功能已成公链项目标配，**跨链资产互换也正向跨链资产转移发展，另外，主动型跨链、被动型跨链开始落地**；(4)以 DAG 为首的其他分布式账本技术领域，开始**积极探索融合智能合约等可编程功能的可能性。**

我们对 2018 年**十大重要事件**做了盘点：(1) EOS.IO 掀超级节点竞选热潮，**DPOS 机制受热捧**；(2)**“交易即挖矿”模式的兴与衰**；(3) **EOS Ram 启示**，人机交易/IBO 雏形，但 IBO 未如期爆发；(4) Fomo3D 引发**游戏 Dapp 思考**；(5) **传统巨头开始布局区块链**领域；(6) **区块链公司拥抱传统资本市场**；(7) USDT 面临信任危机，**合规稳定币出世，而算法稳定币出师不利**；(8) 监管不再限于纸面，**落地执行开始，并以美国为典型**；(9) 谁是真正的信仰者，从 **BCH 分叉看公链治理**；(10) 安全、黑客事件频发，**区块链安全机遇显现。**

我们亦对 2019 年做了**十大预测**：(1) 缺少造富效应，融资项目出清，**2019 年市场寻底后将宽幅震荡**；(2) **ETF 不会一帆风顺，**但个性化衍生品将持续涌现；(3)**公链改良循序渐进**，然性能已非痛点，有效场景才是；(4) 一站式区块链部署或成新宠，**跨链互通催生区块链落地多样性**；(5) **Web 3.0 到来**，5G 和基于 IPFS 的分布式存储成重要推动力；(6)**矿业金融化变革推动洗牌**，改弦更张者上位，抱残守缺者离场；(7) **传统应用掀 Dapp 化浪潮**，崭新流量世界将浮出水面；(8) **资产通证化案例涌现**，通证锚定权利逐渐丰富，但规模化仍存障碍；(9) 稳定币从交易转向应用和支付，**基于稳定币的“PayPal”将会出现**；(10) **主流国家监管持续优化，示范效应引多国效仿，**牌照、沙盒将普及。

火币区块链应用研究院简介

关于我们：

火币区块链应用研究院（简称“火币研究院”、“火币区块链研究院”）成立于 2016 年 4 月，于 2018 年 3 月起全面拓展区块链各领域的研究与探索，主要研究内容包括区块链领域的技术研究、行业分析、应用创新、模式探索等。我们希望搭建涵盖区块链完整产业链的研究平台，为区块链产业人士提供坚实的理论基础与趋势判断，推动整个区块链行业的发展。

联系我们：

咨询邮箱：	huobiresearch@huobi.com
简书账号：	火币区块链研究院
Website:	http:// research.huobi.cn
Twitter:	@Huobi_Research
	https://twitter.com/Huobi_Research
Medium:	Huobi Research
	https://medium.com/@huobiresearch
Facebook:	Huobi Research
	https://www.facebook.com/Huobi-Research-655657764773922

免责声明：

1. 火币区块链研究院与本报告中所涉及的数字资产或其他第三方不存在任何影响报告客观性、独立性、公正性的关联关系。
2. 本报告所引用的资料及数据均来自合规渠道，资料及数据的出处皆被火币区块链研究院认为可靠，且已对其真实性、准确性及完整性进行了必要的核查，但火币区块链研究院不对其真实性、准确性或完整性做出任何保证。
3. 报告的内容仅供参考，报告中的事实和观点不构成相关数字资产的任何投资建议。火币区块链研究院不对因使用本报告内容而导致的损失承担任何责任，除非法律法规有明确规定。读者不应仅依据本报告作出投资决策，也不应依据本报告丧失独立判断的能力。
4. 本报告所载资料、意见及推测仅反映研究人员于定稿本报告当日的判断，未来基于行业变化和数据信息的更新，存在观点与判断更新的可能性。
5. 本报告版权仅为火币区块链研究院所有，如需引用本报告内容，请注明出处。如需大幅引用请事先告知，并在允许的范围内使用。在任何情况下不得对本报告进行任何有悖原意的引用、删节和修改。

目录

一、数字资产市场回顾与展望

2018 年是数字资产市场从狂热到理性的一年，数字资产总数虽仍在增长，根据 Coin Marekt Cap 数据显示，目前全球已有超过 2,000 多种数字资产，较 2017 年末增长约 45%，然而数字资产总市值于 2018 年大幅缩水，市场交易量大幅下滑。而市场表现及信心的羸弱，亦逐步传导至一级市场，数字资产、区块链项目众筹完成度于 2018 年逐步降至冰点。但与此同时，数字资产市场的五个重要转型亦在悄然发生。

1.1 凛冬已至，数字资产市场持续降温

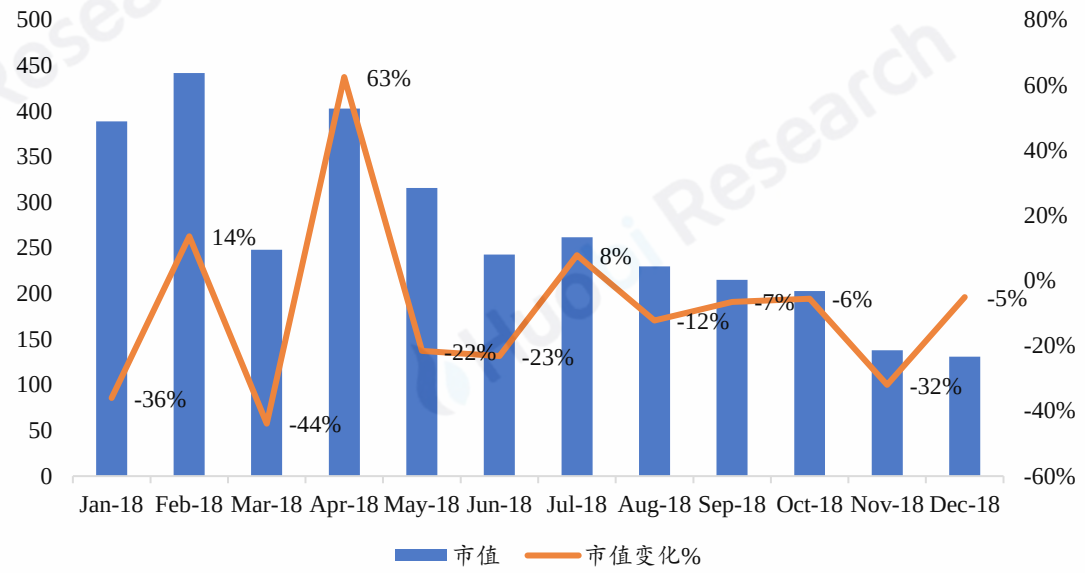
2017 年，数字资产市场经历了爆发式增长，总市值从年初的 177.4 亿美金暴涨至年末的 5,597.6 亿美金，增长 30 倍，超越了其他任何一类资产的回报。然而，**进入 2018 年后，数字资产市场掉转风向，价格剧烈回撤，截至 12 月 31 日，市场总市值约 1300 亿美金，今年整体市场缩水超 80%。**

图1：2018 年全球数字资产市值走势（单元：美金）

来源：Coin Market Cap、火币区块链研究院整理

除 **2 月，4 月和 7 月有明显上升外，2018 年其他月份数字资产市值都在持续下降**。其中 4 月主要是在多个采用 DPOS 共识机制的项目如 EOS、TRX 竞相开启超级节点竞选的刺激下，数字资产市场迎来了一波小行情，部分数字资产价格快速上涨。7 月，市场在交易挖矿以及 Fomo3D 为首的一系列 Dapp 应用兴起热点带动下，市场亦有明显的小行情出现。

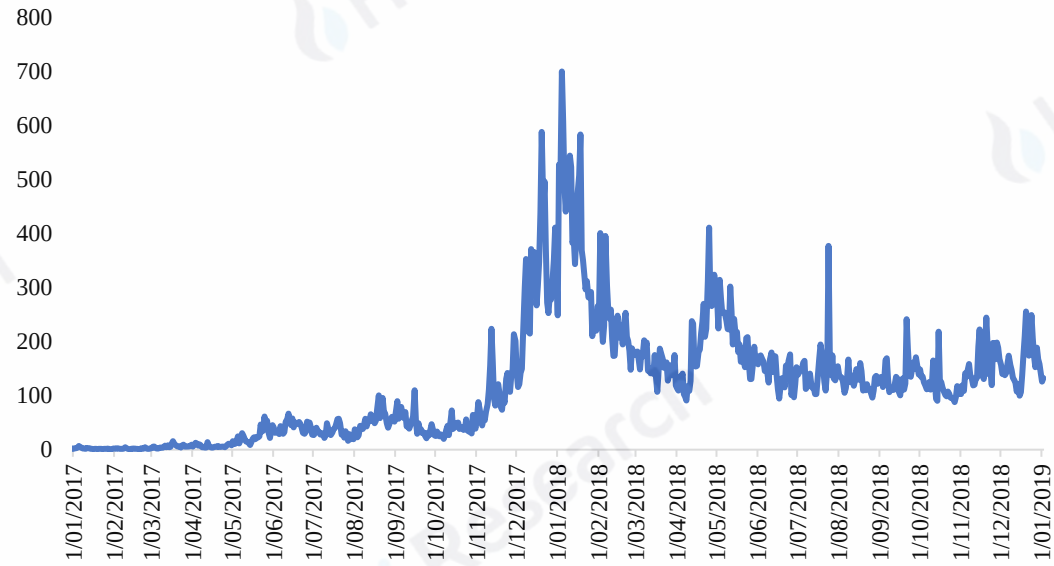
图2：2018 年全球数字资产月市值变化（单元：亿美金）



来源：CoinMarketcap、火币区块链研究院整理

2018 年，**全球数字资产 24H 交易量在 1 月 4 日达到最高峰（700.04 亿美金）**，随着数字资产市场行情转冷，**10 月 27 日达到 18 年来最低点 87.8 亿美金，较最高点下滑 87.6%**。目前 24H 交易量处于 100 亿-250 亿美金区间。

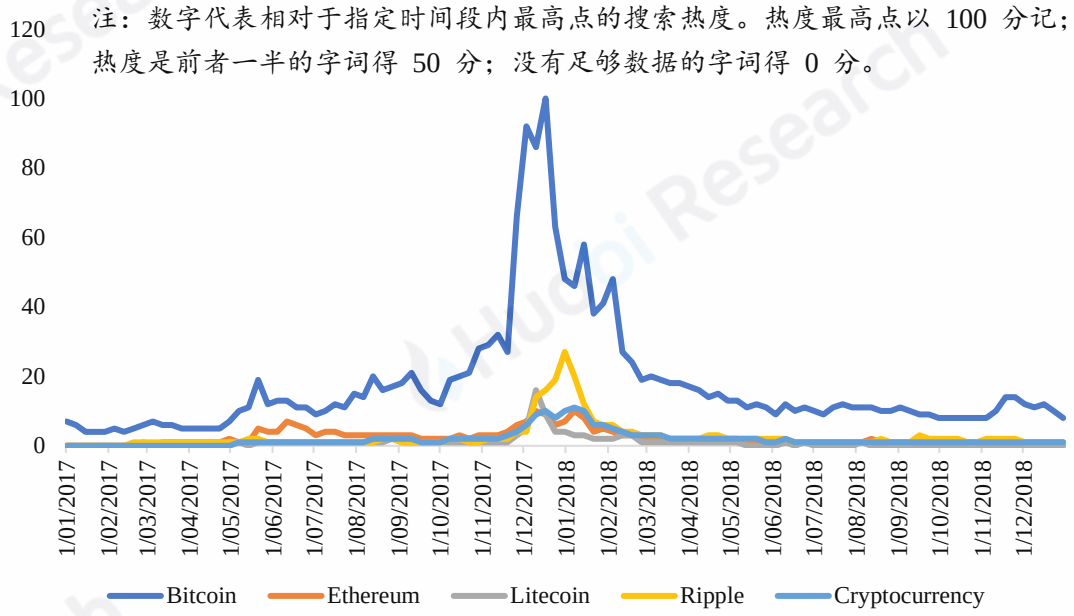
图3：全球数字资产 24H 交易量变化（单元：亿美金）



来源：CoinMarketcap、火币区块链研究院整理

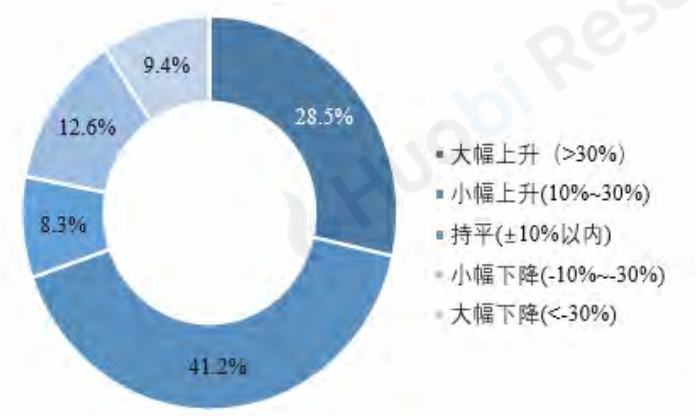
除交易量大幅下跌外，数字资产市场的活跃度也大幅下滑：

图4：数字资产相关搜索指数



来源：Google Trend，火币区块链研究院整理

图5：投资者市场期望-中期



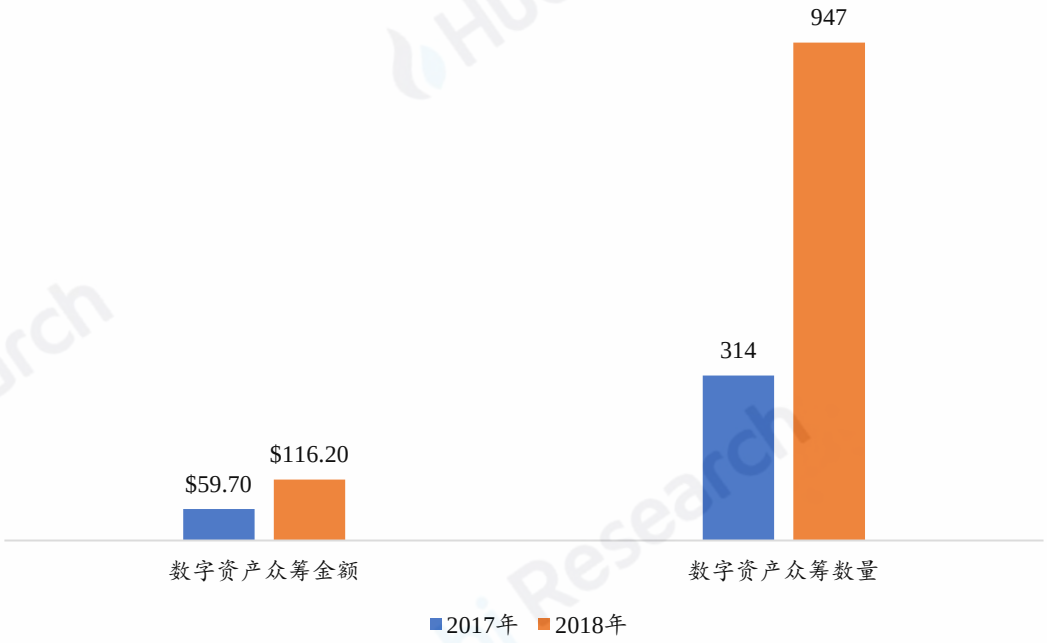
来源：火币区块链研究院市场情绪调查

不过，**从情绪面上来看，市场仍看多 2019 年上半年走势**。进入 2018 年后，数字资产市场整处于下跌趋势，但市场对 2019 年仍旧抱以希望。根据火币区块链研究院每月针对全球个人及机构投资者的情绪调查显示，市场对 2019 年上半年走势仍较为看好，认为将小幅上涨，其中，**78.0%的投票者认为未来半年的数字资产总市值会上升，其中 28.5%的投票者对市场很有信心，认为未来半年数字资产的市值会大幅上升 30%以上。**

1.2 凌寒料峭，区块链、数字资产融资断崖

2017 年新兴数字资产爆发，相关融资金额快速增长，2018 年再创新高。根据 ICO Rating 数据，2018 年一级市场共有 947 个项目完成众筹，合计融资金额超 116 亿美金，**项目数量同比增长 200%，融资金额同比增长 94%。**

图6：2017-2018 年数字资产众筹融资金额与数量（单元：亿美金）



来源：ICO Rating、火币区块链研究院整理

不过，2018 年数字资产众筹融资金额翻番，和上半年部分头部融资项目有很大联系。火币区块链研究院统计了排名前 10 的数字资产众筹项目，发现融资金额均超 1 亿美金。其中融资排名前三的分别是公有链项目“EOS”筹集 42.3 亿美金，通讯项目“Telegram Open Network”筹集 17 亿美金，以及游戏项目“Dragon Coins”筹集 3.2 亿美金等。若剔除 EOS 和 Telegram 的相关影响，2018 年数字资产众筹融资金额环比下降 4.7%。

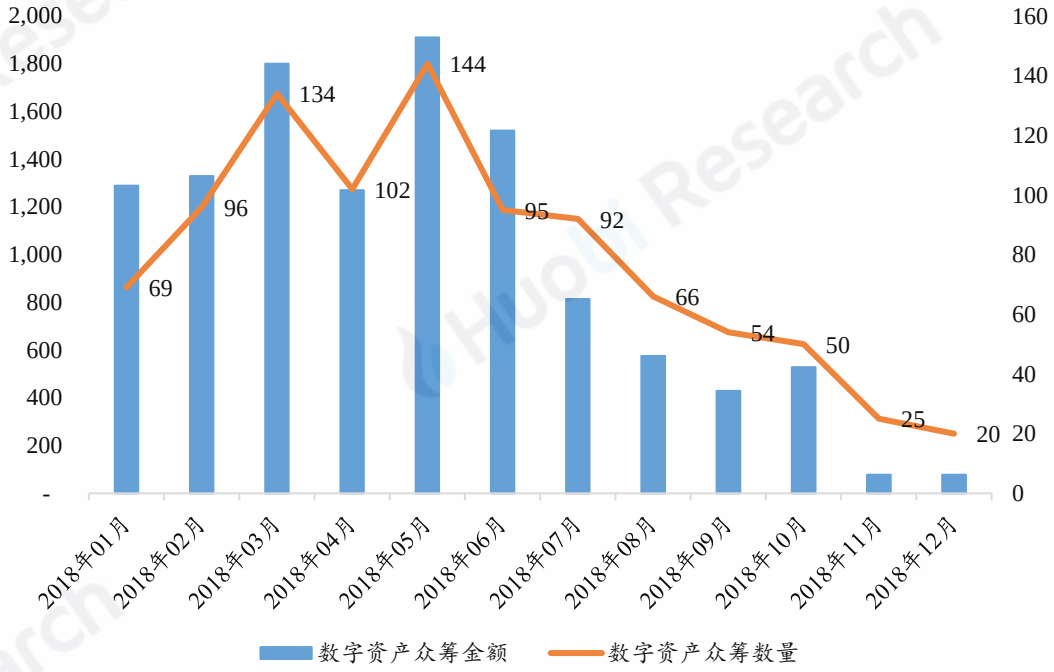
图7：2018 年融资金额前十大数字资产众筹项目

项目名称	项目类型	融资时间	融资金额
EOS	公有链	2018 年 6 月	$4,234,275,713
Telegram Open Network	通讯	2018 年 4 月	$1,700,000,000
Dragon Coins	游戏	2018 年 3 月	$320,000,000
DFinity	云存储	2018 年 2 月	$195,000,000
Bankera	金融服务	2018 年 2 月	$150,000,000
tZero	交易所	2018 年 8 月	$134,000,000
Basis	稳定币	2018 年 4 月	$125,000,000
Orbs	公有链	2018 年 5 月	$118,000,000
PumaPay	支付	2018 年 5 月	$117,019,041
Envion	智能移动挖矿	2018 年 1 月	$100,012,279
合计			$7,193,307,033

来源：火币区块链研究院整理

随着数字资产市场行情转冷，数字资产众筹金额和数量逐月递减，特别是在 2018 年下半年。2018 年 12 月，根据 ICO Rating 的收录只有 20 个项目成功完成众筹，创本年度新低；当月数字资产众筹金额仅为 7800 万美金，较最高峰 5 月减少 96%。**整体市场融资环比情况不容乐观。**

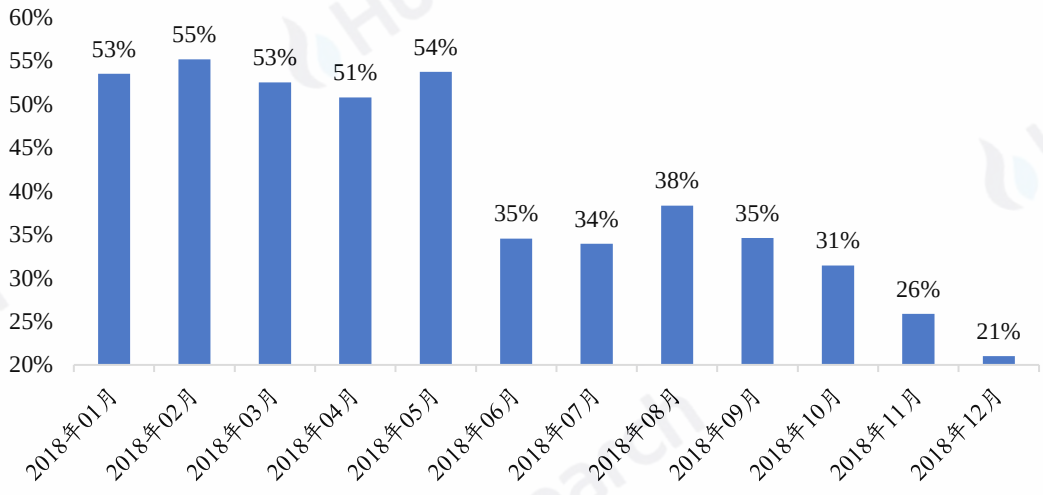
图8：2018 年至今数字资产众筹融资金额与数量（单元：百万美金）



来源：ICO Rating、火币区块链研究院整理

同时，数字资产项目众筹完成度逐渐下滑，大部分项目募集不满。

图9：2018 年至今月度数字资产众筹融资完成度

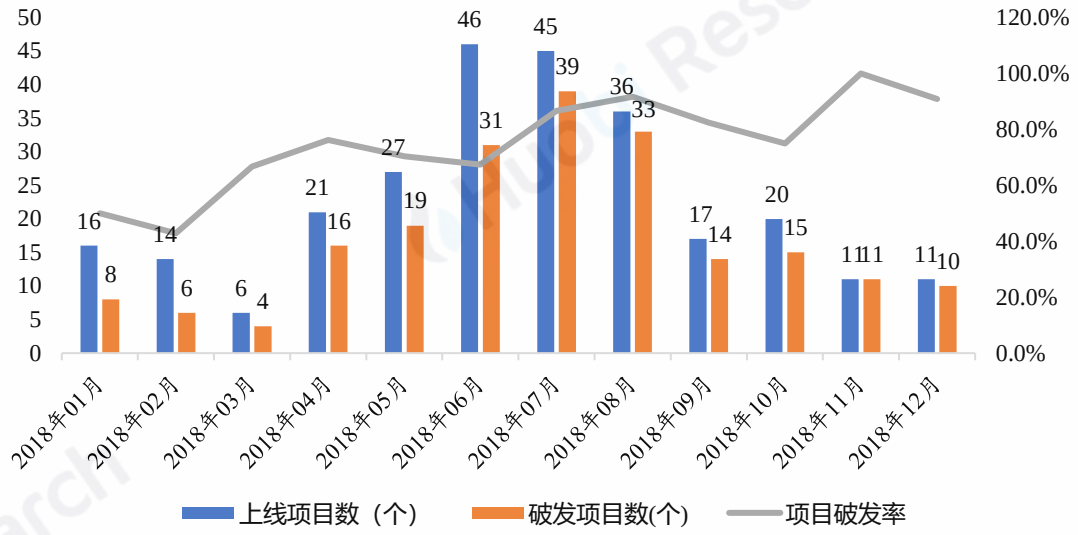


来源：ICO Rating、火币区块链研究院整理

2018 年数字资产众筹项目上线后破发率走高。随着全球监管机构对数字资产众筹欺诈的打击力度强化，同时，受过多项目带来资金分流，以及以太坊本身价格下跌的影响，大部分新增数字资产价格上线交易所即破发，部分项目因市场

环境而延迟上线。火币区块链研究院跟踪每月上线交易所的项目，对同时统计到众筹成本价和首次上线交易价格的项目计算破发率，**月平均破发率高达 75%。**

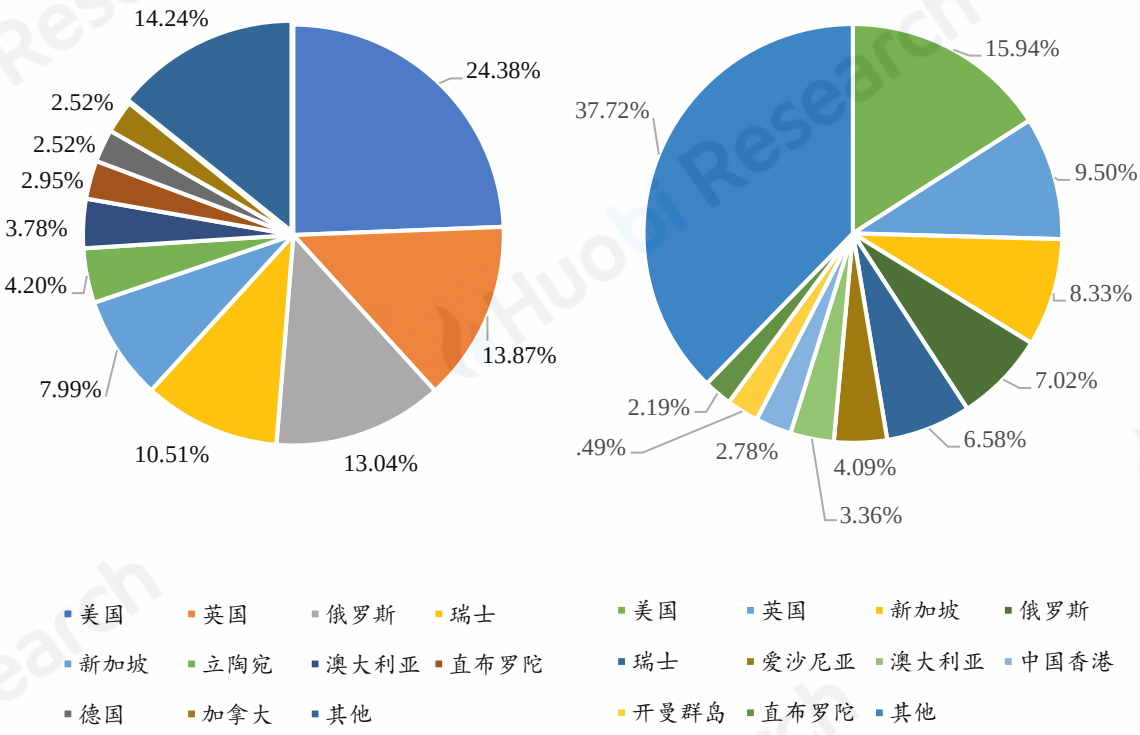
图10：2018 年数字资产项目破发情况



来源：ICOBench、Coinmarketcap、火币区块链研究院整理

根据 ICO Watchlist 数据，2018 年数字资产众筹项目主要分布在美国（15.9%），英国（9.5%），新加坡（8.3%），俄罗斯（7%），瑞士（6.6%）。**相比 2017 年，美国和瑞士的项目占比下降最为明显，主要因为明确的监管政策（纳入证券监管）导致部分项目选择在海外发展，剩下部分项目选择拥抱合规。新加坡的项目占比有所上升，主要因为政策相对完善并且较为宽松（如沙盒监管），项目发展相对自由。**具体数字资产众筹融资国家分布如下图所示：

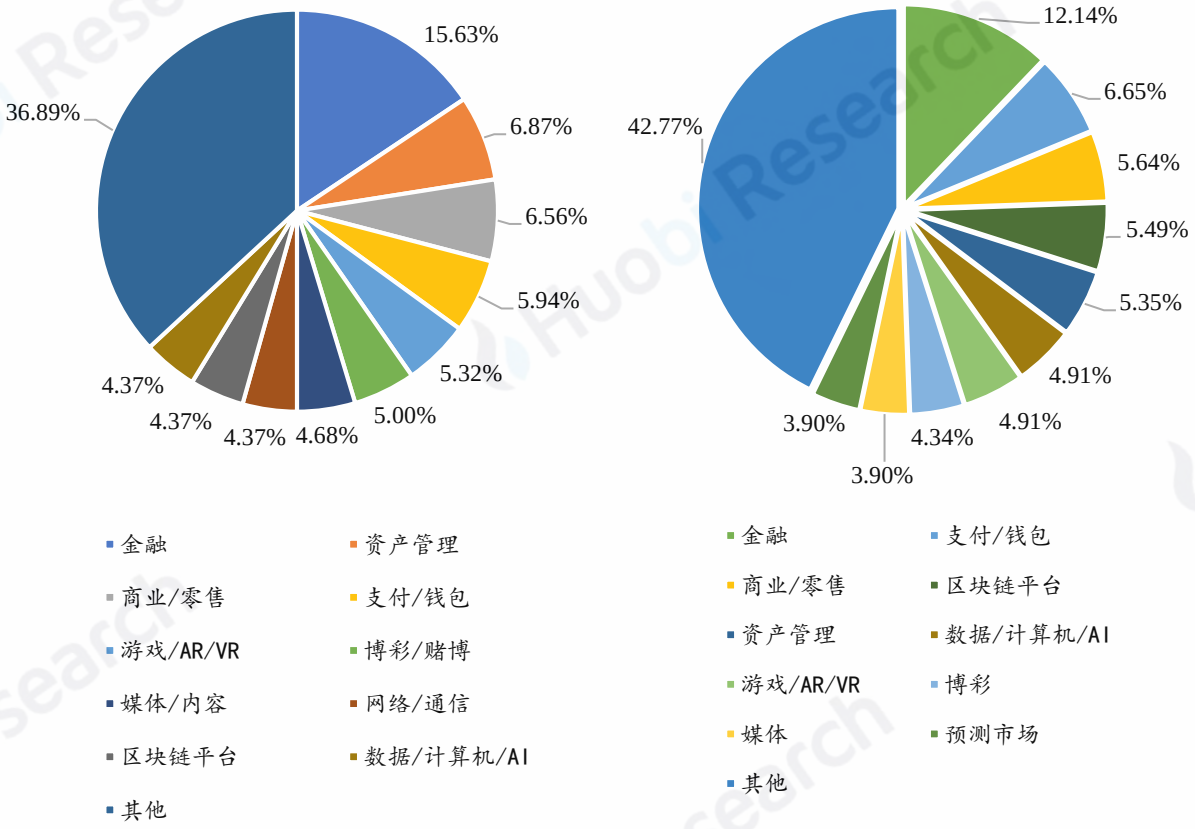
图11：2017 年数字资产众筹项目国家分布　　2018 年数字资产众筹项目国家分布



来源：ICO Watchlist、火币区块链研究院整理

另根据 ICO Watchlist 数据，2018 年数字资产众筹项目主要集中在应用领域，其中金融领域始终位居首位。排名前三的领域分别是金融（12.1%）、支付/钱包（6.7%）、商业/零售（5.6%）。相比 2017 年，资产管理类项目占比跌出前三，该类项目大都具备证券交易属性将面临监管等原因。具体的数字资产众筹融资应用领域分布情况如下图所示：

图12：2017 年数字资产众筹项目领域分布　　2018 年数字资产众筹项目领域分布



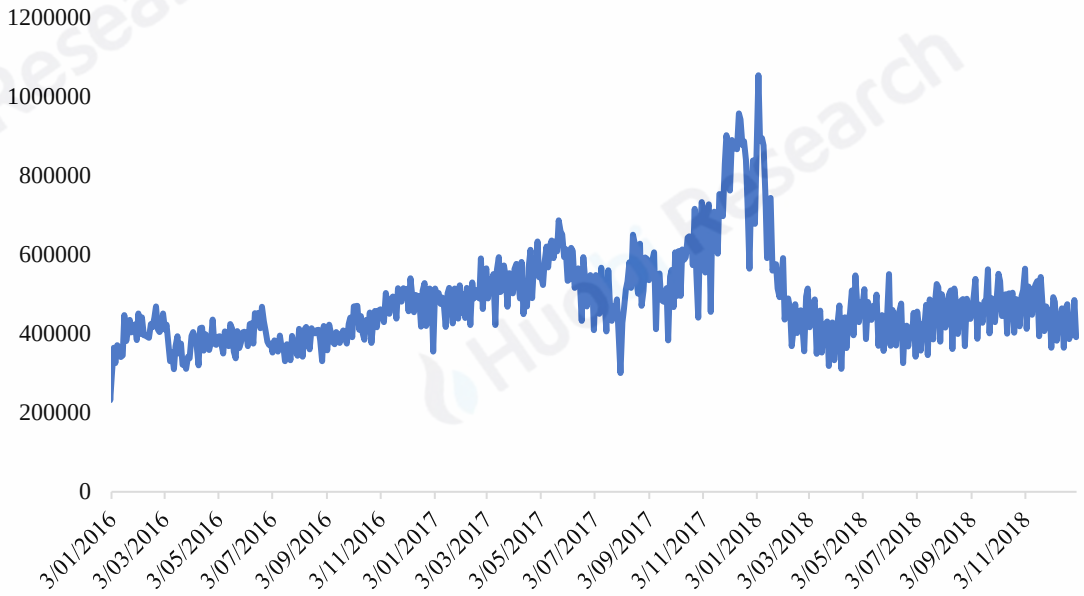
来源：ICO Watchlist、火币区块链研究院整理

1.3 链上活跃度遇瓶颈，但算力、挖矿难度等核心指标仍健康

1.3.1 链上活跃度数据增长停滞

2018 年 3 月后，比特活跃地址数增长停滞。2018 年 1 月 4 日，比特币日活跃地址数达最高点 105.5 万，随后一路暴跌至 31.1 万（2018/4/8），相比本年最高点下跌了 70.5%，可以说，**2018 年，是链上活跃数据一次持续较长时间的下跌。**目前，比特币日活跃地址数处于 30-60 万区间，已经基本与 2016 年的链上活跃度所持平。**由此可见，比特币活跃度与其市场价格表现仍有很强的正相关性，2017 年活跃度的大幅提升，和 2018 年活跃度的大幅下降，与市场价格上涨和下跌引发的投资、投机潮起潮落，有显著联系，比特币的投资、投机属性，仍旧占据了很大成分**，具体如下图所示：

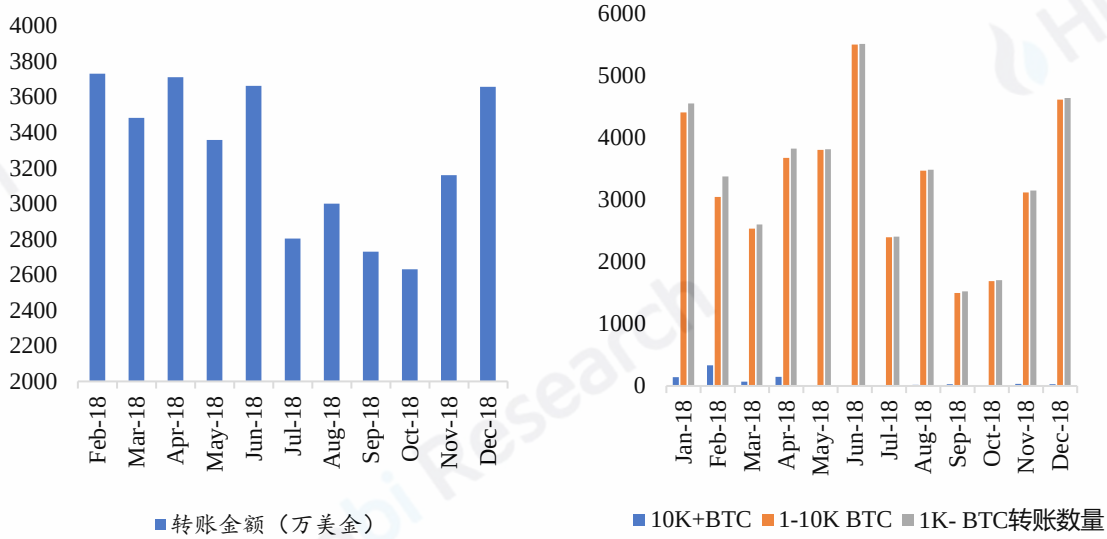
图13：比特币日活跃地址数（个）



来源：Blockchain.com，火币区块链研究院整理

除此之外，比特币链上转账金额同期亦呈现下降趋势，亦反映了链上活跃度的下降，**而 2018 年 12 月以后，比特币转账金额的增长，主要系 Coinbase 交易所正常的资产整理行为:**12 月初有大量的头部地址清空所有比特币（持币量排名 9-12 位，以及 30-31 位，45-54 位的地址等地址），被转出的比特币大部分最终转入 96 个新地址，每个地址包含 8000 个比特币。

图14：2018 年比特币转账金额及大额转账笔数

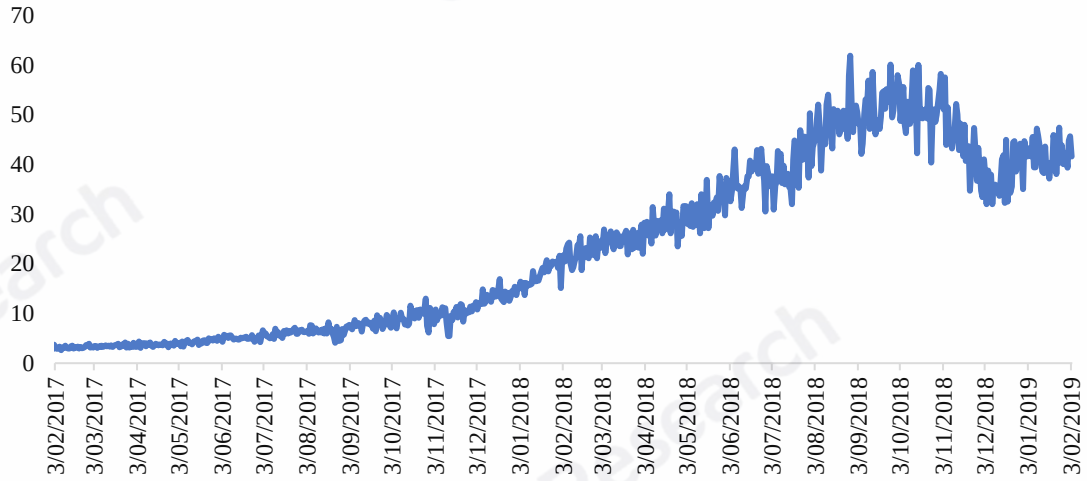


来源：Blockchain Node File、火币区块链研究院整理

1.3.2 哈希值（算力）、挖矿难度及节点数整体仍呈上涨态势

不过，与链上活跃度大幅下滑不同的是，以比特币为首的区块链网络的算力、挖矿难度等指标并未有同样剧烈的下跌：**比特币全网哈希值（算力）2018 年整体仍旧呈现上涨趋势，并在 9-11 月之间达到最高值**，约 50EH/s 至 60EH/s 之间，**12 月后全网算力出现了一定的下滑，主要系数字资产市场经历了 11 月的破位大跌，部分矿工离场所致**。目前，比特币全网哈希值（算力）仍在 40EH/s 左右。

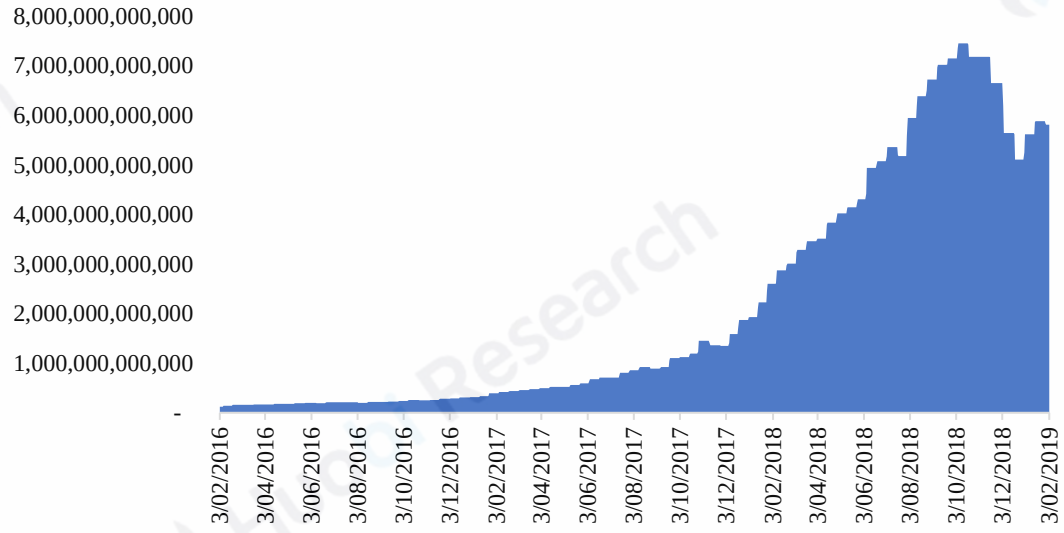
图15：比特币全网算力变化图（EH/s）



来源：Quandl、火币区块链研究院整理

另外，比特币挖矿难度亦呈现类似的增长态势，并于 9-11 月达到最高峰，12 月随着部分矿工离场，算力下降，难度随之下调。

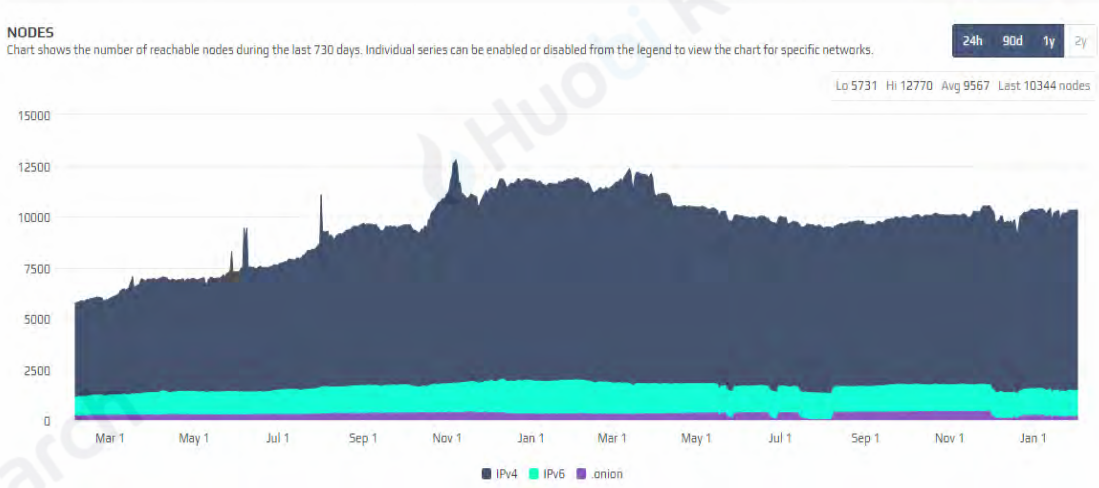
图16：比特币挖矿难度变化图



来源：Quandl、火币区块链研究院整理

而比特币验证节点数量基本稳定，仅有小幅下滑，亦说明了维持整个区块链网络运转的矿工群体仍相对稳定，**2018 年熊市带来的影响更多是市场层面的，而非安全、底层技术层面的：**

图17：比特币网络验证节点数变化图（个）



来源：Bitnodes、火币区块链研究院整理

1.4 数字资产市场正经历的五个转型与过渡

1.4.1 资产发行主体由民间扩大到国家

2018 年，数字资产不再仅仅局限于民间，众多国家政府机构也相继加入，法定数字货币开始出现：

2018 年 1 月，委内瑞拉政府发布了人类历史上第一个法定数字货币“石油币 PTR”（petro cryptocurrency），它以奥里诺科重油带阿亚库乔区块 1 号油田的50亿桶石油储量作为发行石油币的物质基础,每个石油币与1桶石油等价。石油币是委内瑞拉政府试图拯救国内经济而催生的产物。2014 年至今，委内瑞拉货币四年内贬值超 99%,国民对法定货币玻利瓦尔失去信心,在这样的混乱中，国民一方面开始回归到以物易物的生活方式，比如以面包换取药品；一方面开始大量涌向比特币等数字资产，从 2014 年 8 月到 2016 年 11 月，委内瑞拉比特币用户数量从 450 人上涨到 8.5 万人。**为了防止国民最终抛弃以政府信用为背书的法币玻利瓦尔，政府决定推出“石油币”，并于 2018 年 11 月，最终宣布确认石油**

币成为该国法定货币，将玻利瓦尔价格与石油币挂钩。目前，石油币可以使用人民币、美元等法定货币和比特币、以太币等数字资产购买。目前委内瑞拉国内采购石油的交易都需使用石油币进行支付，比如各航空公司的飞机在委内瑞拉当地补充燃料时也需支付石油币。12 月，政府又开始以石油币支付居民养老金。

除委内瑞拉外，又先后有多个国家宣布有意推出法定数字货币。此外，据国际货币基金组织（IMF）的最新报告，有 15 家中央银行认真参与了法定数字货币的研究，数字资产正逐步走入国家队时代。

新加坡

新加坡是较早宣布探索法定数字货币的国家，其法定数字货币项目名为“Ubin 项目”，计划通过三个阶段的努力，实现全球各国央行通过区块链技术实时处理汇款交易功能。2018 年，“Ubin 项目”已进入第三阶段，开始与加拿大银行合作，使用两家中央银行发行的加密通证测试和开发跨境解决方案。

土耳其

2018 年初土耳其副总理表示，土耳其政府将寻求发起全国性加密货币，而之前土耳其前工业部长兼民主主义行动党副主席 Ahmet Kenan Tanrikulu 撰写了一份有关发行国有加密货币的详细报告，并在报告中将其命名为 " 土耳其币 "（Turkcoin）。

瑞典

2018 年 4 月，瑞典央行透露将与 IOTA 合作，在两年内推出国家数字货币 E-Krona，可以用于消费者、企业和政府机构之间的小额交易。具体操作上，瑞典央行透露，资金将会被存储在数据库中，可以通过应用程序或银行卡获取。此外，反洗钱、KYC 规则，安全和匿名性也必须予以重点考虑。

印度

2018 年 4 月，印度储备银行 RBI（印度央行)发布声明表示正考虑发行央行数字货币(Central Bank Digital Currency, 简称 CBDC)，且已成立了一个跨部门工作小组，调查 CBDC 的潜在优势和可行性。

泰国

2018 年 8 月，泰国中央银行 (BOT) 对外宣布了名为 Inthanon 的中央银行数字货币 (CBDC) 项目，有关各方将会在 R3 的 Corda 平台上，通过大规模发行其数字货币 CBDC，来共同设计和开发各银行间资金转账系统的原型。

来源：火币区块链研究院整理

1.4.2 资产发行合规化，证券类通证发行目前领先 DAICO

2017 年中到 2018 年上半年，数字资产众筹经历了从萌芽到爆发的过程，但随之而来的也是资产发行无序，市场上各类项目良莠不齐，大部分的功能型通证并无实际使用价值。进入 2018 年，数字资产市场出现了合规化资产发行模式：

2018 年年初，以太坊创始人 Vitalik 提出 DAICO 模式，希望在数字资产众筹中引入社区监管，对项目方予以约束。DAICO 在传统的数字资产众筹模式基础上融合了去中心化自治组织 DAO 的一些特点，赋予了通证持有者以投票权，可通过投票的方式来监管募集资金，并由智能合约实现资金释放，除此之外，通证持有者也有机会要求退回资金。**DAICO 概念提出后市场激动一时，但该模式自年初至今并没有看到爆发态势，自全球第一个 DAICO 募资项目 The Abyss 之后，只有少数跟随者，如 Tokedo：**

项目名称	项目类型	融资时间	融资金额
The Abyss	区块链游戏分发平台	2018.5	1,438 万美金
Tokedo	区块链通证化平台	2018.11	1,687 万美元

来源：火币区块链研究院整理

主要原因，我们认为是 DAICO 模式目前还存在一定的问题，包括：

- 社区民主并不一定对项目本身的发展是有利的，大部分的通证持有者关心的只是通证价格，并一定会站在长远的角度为项目本身考虑；
- 其次 DAICO 本质上仍旧是一种众筹融资行为，仍需遵循各国的监管条例，其和传统的数字资产众筹面临一样的潜在监管约束；

- 最后，通证购买参与者并未因为 DAICO 增加了对项目方的约束而提升参与热情，通证购买参与者在 2018 年熊市环境下，转而重点关注的底层资产质量本身，并不是 DAICO 模式所能解决的。

证券类通证发行，则是另一种通证发行的探索，专指在确定的监管框架下，按照法律法规、行政规章的要求，进行合法的通证发行。相比传统的数字资产众筹，**证券类通证发行系将通证的属性明确为证券，而非原先的功能型通证，并在发行、流通易等方面均受到较大限制：**

- 发行端遵循证券发行流程，美国的通证融资只能通过 Reg A+、Reg D、Reg CF、Reg S 或直接 IPO 渠道完成；
- 流通端必须在有限的持牌交易所交易，并对投资人设置壁垒和一定的限售期，如美国的 Reg D 要求募资只能针对合格投资人开放，Reg A+和 Reg S 对投资人数量上限也有要求，另外，Reg D、Reg CF、Reg S 融资都有 12 个月禁售期，即只有具备风险承受能力的投资者才可参与。

从监管的角度看，**与 DAICO 相比，证券类通证发行背书更强**，也更容易被项目方和投资人，尤其是传统的机构投资者所接受。**截至 2018 年 10 月底，美国 SEC 已经审核通过了 39 个证券类通证发行项目，包括 Tzero，Filecoin，Telgeram 等明星项目均走了合规的证券发行。**

1.4.3 交易市场类金融化，交易标的向衍生品、指数化产品拓展

数字资产现货市场的普遍下跌，催生了市场对衍生品，尤其是风险对冲工具的需求，促使数字资产交易所推出各类衍生品来吸引用户：

根据 Visual Capitalist 的数据，在传统金融世界中，全球股票市值约为 73 万亿美元，全球政府债务、企业债务、家庭及个人债务总和达到 215 万亿美元，全球发达国家房地产市值约达到 217 万亿美元，现金总量约为 7.6 万亿美元，黄金现货市值约为 7.7 万亿美元，白银市值 170 亿美元。而全球基于各种现货的金融衍生产品市值约为 544-1200 万亿美元，比全球股票市值高出一个数量级。**对应到数字资产市场，截止到 2018 年 12 月 31 日，全球数字资产总市值达到 1316 亿美元，以 10 倍估算，数字资产衍生品市场规模应该可以达到万亿美元的水平。**

图18：各类资产市值规模（单位：万亿美元）

来源：Visual Capitalist，火币区块链研究院整理

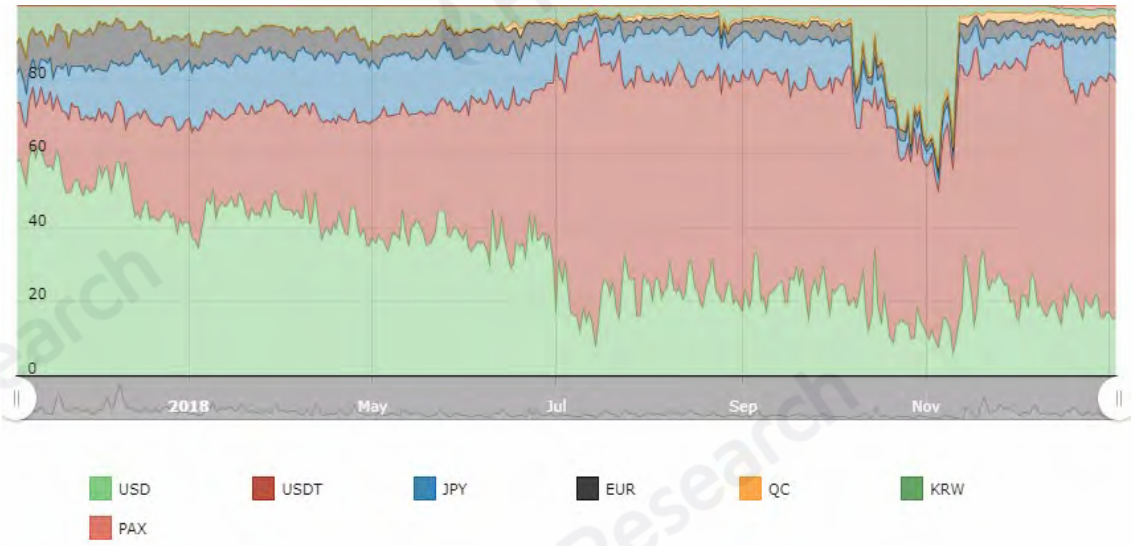
- **目前头部数字资产交易所正在积极向衍生品市场扩张。**目前，BitMex、OKEx 等交易所均有合约交易板块。
- **另外，传统交易所也正往数字资产衍生品市场渗透。**2017 年 12 月，CBOE 和 CME 相继推出市场期待已久的比特币期货，正式承认了比特币衍生品的合法地位。纽约证券交易所（NYSE）的母公司洲际交易所（ICE）也在 2018 年 8 月成立了比特币期货交易平台 Bakkt，并为推出以实物结算的比特币每日期货合约而努力。而美国 CFTC 下辖 Swap Execution Facility 牌照的持有者 LedgerX 也上线了比特币期权。
- **而除了期货、期权等产品，指数化产品亦是一个重要的探索方向，**以方便机构和大资金用户进行大类资产配置，例如彭博联合了 Galaxy Digital（GD）推出加密货币基准指数 Bloomberg Galaxy Crypto Index (BGCI)。

不过我们也需要看到，衍生品、指数化产品市场的发展必须要有成熟的现货市场为依托，然目前数字资产市场尚处在初级阶段，**还没有找到真正合理的估值方法，市场流动性、深度等各方面均有不足，投资者风险承受能力较弱**等等，这一些均是未来，衍生品、指数化产品市场进一步拓展需要跨越的障碍。

1.4.4 清结算向稳定币方式转变

2018 年初，比特币交易对中美金的交易规模占据了 57.97%，而稳定币 USDT 交易仅占据了 15.66%。**2018 年，随着稳定币 USDT 进一步发展，以及 TUSD、USDC、PAX、GUSD 等新的稳定币诞生，可以明显看到比特币交易中稳定币的占比升高。稳定币在数字资产交易、结算中作用正不断增加：**

图19：2018 年比特币各货币对交易量占比变化

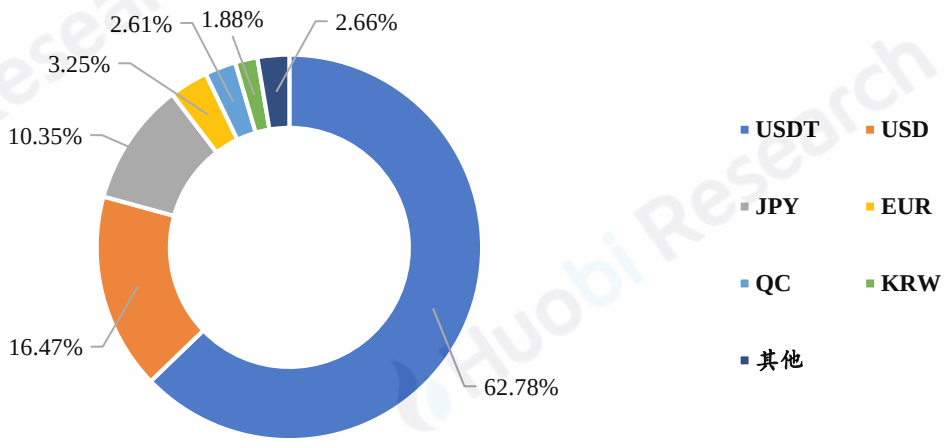


来源：Crypto Compare，火币区块链研究院整理

在稳定币还没有出现的时代，用户需要交易数字资产，往往需要先去例如 Coinbase 这样的法币交易所，或者类似 CoinCola 一类的 OTC 平台购买比特币、以太坊等主流数字货币，然后再去币币交易平台用主流数字货币交易其他币种；另外，若用户在市场波动大时想出售数字资产避险，也需要反向经过同样的步骤。

这样一来，数字资产世界出入金步骤繁琐，中间成本较高，形成了新用户进入数字资产世界的障碍，同时，Dapp 等数字资产世界的应用，与法币体系是不通的，用户无法直接通过法定货币参与使用。**而稳定币的诞生打通了数字资产世界和现实世界的隔阂，为数字资产世界提供了方便的入金渠道和避险途径。也正因为稳定币的便利性，数字资产的交易和结算越来越多的使用稳定币，成为数字资产交易领域新的基础交易对。**以 2018 年 12 月 31 日为例，就比特币来说，USDT 交易占比已经上升至 62.78%，而法币中交易占比最高的美金仅占到 16.47%，就是一个非常明显的证明，具体如下：

图20：2018 年 12 月 31 日比特币各货币对交易量及占比（单位：BTC）

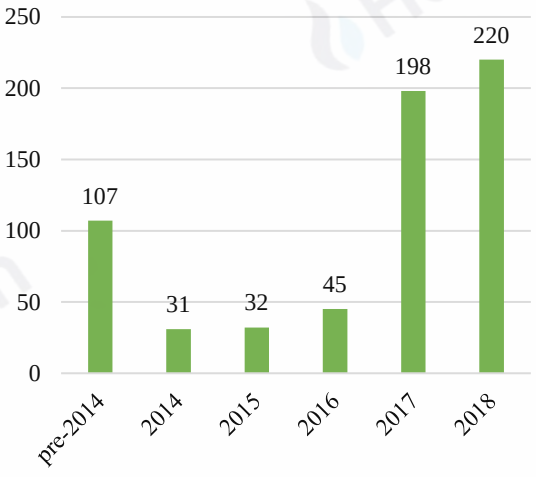


来源：Crypto Compare，火币区块链研究院整理

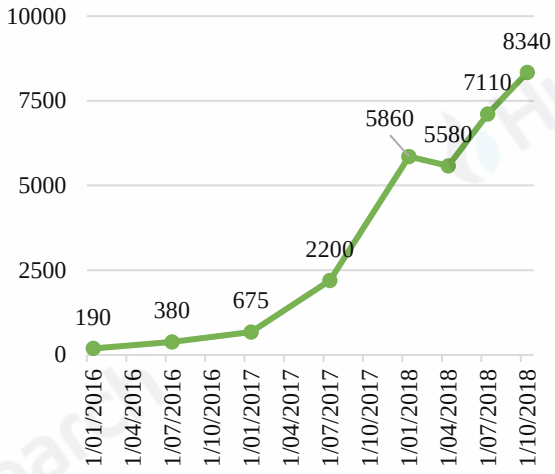
1.4.5 市场参与者主体机构化

2018 年，数字资产市场的机构投资者明显增多。2018 年全年约新增 220 家数字资产基金，**目前全球约有 632 个数字资产基金，其中对冲基金 311 家，风险投资基金 302 家。**截至 2018 年 10 月底全球**数字资产基金总管理规模约为 83.4 亿美元，在 2018 年数字资产市值大幅下跌的环境下仍较年初增长 42.3%。**

图21：每年新增数字资产基金数量



数字资产基金管理规模 单位：百万美元

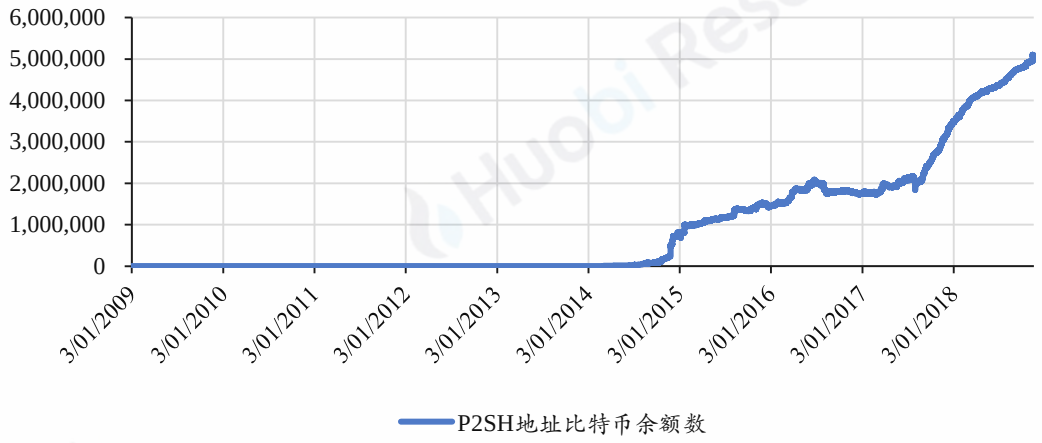


来源：Crypto Fund Research，火币区块链研究院整理

而另一个能反映数字资产市场参与者主体机构化的例证是**多重签名的应用提升以及相应地址余额的增加。**标准化的多重签名的实现最早源于比特币改进协议 BIP11，但真正普及并被大量钱包使用在于 Pay-To-Script-Hash（P2SH）交易

类型的产生，其大大简化了多重签名的执行流程。火币区块链研究院统计了比特币网络基于 P2SH 样式的地址的相关比特币余额数据，

图 22：比特币多重签名地址（P2SH 样式的地址）资产余额变化图



来源：火币区块链研究院整理

可以看到：**P2SH 样式地址的资产余额共经历了两次快速增长，第一次系 2014 年底至 2015 年初，系 P2SH 脚本出现之后被社区认可，P2SH 样式地址中比特币余额增长至 100 万个，第二次系 2017 年下半年起，真正反映了机构用户的上升，截止目前，P2SH 样式地址中比特币余额已增长至逾 500 万个。**由于多重签名优势在于安全性，防止私钥单点沦陷带来的风险，适合机构用户，因而我们认为，上述多重签名钱包数据的增长，实际从侧面反映了数字资产市场中机构参与者数量的增加，并正通过多重签名方式管理其资产。

我们认为，机构参与者的大幅增加，本身是对数字资产市场、区块链行业前景的一种认可，而为机构化创造外部条件的，亦有 3 个原因：一是各国监管开始加速干预数字资产市场，合规性日趋完善，一定程度上降低了监管不确定性；二是托管的出现为机构资金提供了资产保管的解决方案，大大降低了资金入场的门槛和风险；三是数字资产衍生品的出现为机构投资人对冲市场波动提供了便利。

二、数字资产合规与监管动态解读

2.1 全球区块链、数字资产监管最新动态及趋势

我们认为，2018 年系数字资产市场合规化的元年，全球市场进入加速合规阶段。一方面，2017 年数字资产市场因达成智能合约的共识而经历前所未有的爆发式增长，加上数字资产与区块链行业机会与风险并存的特点，引发了各国监管的重视和快速介入。另一方面，一些在合规方面走在前列的国家推出的监管政策对整个行业产生了示范效应，进一步加速了合规化的进程。火币区块链研究院回顾 2018 年的政策动态，总结以下几个主要趋势和方向：

（1）监管体系逐步明朗，“牌照+沙盒计划+行业自律”雏形初现

数字资产还处在早期阶段，具备较高的专业性和技术性，变化亦较快，因而**对数字资产的监管本身理应是个动态的过程，且需要整个行业与监管机构的共同努力，单纯的集中式监管难以满足行业发展需求。**而好的一点在于，我们确实看到整个监管体系正不断明朗，且变得**越来越包容，在牌照门槛外纳入行业自律和沙盒计划等有效补充，形成了“牌照+沙盒计划+行业自律”三轮驱动的局面。**例如，除新加坡金融管理局（MAS）本身于 2017 年下半年提出沙盒监管，韩国主要采用自律组织监管外，美国 SEC 亦于今年设立了“创新和金融技术新战略中心”—Finhub，以构建市场和 SEC 之间就创新理念和技术发展的沟通桥梁，另外香港证监会于今年发布《有关针对数字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》，在宣布对数字资产进行全面监管，并需获取牌照的同时，亦提出了沙盒计划，希望与行业内的领先企业进行合作。

（2）“分类监管”正逐步让位“无差别监管”

分类监管主要系对“证券类数字资产”和“非证券类数字资产”在监管上进行差别化对待，即严格监管“证券类数字资产”，而不对“非证券类数字资产”予以限制。2017 年至 2018 年初，各国对数字资产（尤其是数字资产发行）的监管便大多采用了这种方式，最典型的当属新加坡，将通证分为证券型通证（资本市场产品）和功能型通证两类，而资本市场的监管框架只适用于证券型通证；瑞

士金融市场监督管理局（FINMA）也将通证分为支付类通证、功能类通证、资产类通证（即证券）三大类，仅针对资产类通证进行证券框架内的强监管。

然而即便属于“非证券类数字资产”，**其仍具备很强的投机性、价格波动性。进入 2018 年后，越来越多的国家、地区正逐步走向“无差别监管”，即无论是否符合“证券”定义，均一视同仁，且有如下两种监管思路：**

- **香港是典型采用完全证券化监管思路的地区。**2018 年 11 月 1 日，香港证监会发布《有关针对数字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》，取消了之前相对模糊的“证券类数字资产”和“非证券类数字资产”分类监管的思路，宣告进入全面的“证券监管”时代，即：无论数字资产是否构成《证券及期货条例》(第 571 章)中所界定的“证券”及“期货合约”，出于投资者保护考虑，均被纳入同等监管框架，均参照《证券及期货条例》(第 571 章)。
- **除了证券化监管，部分国家和地区则是采用数字资产相关业务全面管辖的思路。**以新加坡为例， 2019 年 1 月 14 日，新加坡金融管理局向议会提交的《支付服务法案》得到正式通过，任何从业者提供任何涉及支付型通证的、或者运营平台交易任何支付型通证的必须获得相应的牌照，与传统的支付服务公司遵循相同的政策监管，即，非资本市场商品的通证亦会被监管。而美国实际上亦是归属该类全面管辖思路的典型，若涉及证券，则受 SEC 管辖，而若不属于证券，亦会被包括金融犯罪执法网络（FinCEN）、商品期货交易委员会（CFTC）、货币监理署（OCC）和州金融管理局（DFS）等在内的机构所约束。

无差异化监管其实是基于各国现有的法律框架，如证券法、公司法、银行法、民法等等，对数字资产市场进行监管，可以说是相对简单有效的监管方式。一方面，**各国现有的法律框架经过历史的迭代已经相对完善，可以作为数字资产市场合规的基础和起点。**另一方面，近年来随着稳定币等基础设施、以及数字资产衍生品等金融工具的诞生和普及，**数字资产市场的金融属性也越来越明显**，也较过去更加适用于传统金融市场的监管体系。

（3）联合监管从区域经济体开始，欧盟将率先落地，并向外渗透

数字资产本身具有跨区域性，链上交易实际是无国界的，这对单一国家监管带来了很大挑战。事实上，当今技术的发展速度，已经超越了单一国家政策的应对能力，联合监管呼之欲出。然而，由于目前各国对数字资产的态度和利益仍存在一定的分歧，针对数字资产市场打造全球性的监管框架还有着很大的困难。不过，**对于本身就是高度融合、利益相对一致的区域经济体来说，难度便小了很多。对此我们认为，联合监管将率先从欧盟这样的区域经济体落地。**而虽然欧洲证券和市场管理局（ESMA）目前未明确将数字资产的性质进行说明并纳入监管，我们有理由认为，未来，对数字资产，尤其是发行和交易，仍将会参照传统的金融监管框架，并依据**最新于 2018 年 1 月 3 日生效的《金融工具市场指导 II》(MiFID II)进行规管。**目前，已有相关市场参与者积极寻求符合 MiFID II，包括位于列支敦士登的数字资产交易所 Blocktrade 以及列支敦士登数字资产交易所 LCX。

2.2 世界主要国家和地区监管动态梳理

火币区块链研究院持续对世界主要国家和地区的监管政策进行跟踪，并不断优化评估体系，对监管特点进行考察。目前，我们主要审视如下四个维度：

- **是否对数字资产性质进行明确**
- **是否对数字资产的交易和流通进行监管**
- **是否限制数字资产的发行和销售**
- **是否对数字资产其他相关行为进行约束**

同时，由于 2018 年尤其是下半年，全球数字资产合规化进程快速推进，大部分主流国家和地区均或多或少推出了相关政策或指导意见，为了能更好反映全球数字资产和区块链监管的发展情况，和方便市场参与者和创业者进行决策参考，**我们将不再采用上半年报告中使用的监管严格指数，而是引入监管完善指数，综合上述四个维度，对各国家和地区对区块链、数字资产的监管按照成熟度进行评分：从一颗星到四颗星，星数越多，代表该国家和地区监管体系越完善。**我们挑选了监管较为完善和典型的几个国家和地区，进行了梳理：

2.2.1 美国：多头监管，体系完善，践行较早，成熟度 ★★★★

美国在全球数字资产监管领域一直处于重要地位，2018 年美国将数字资产明确定性，并推出了一系列的政策，形成较为完善的监管框架，对整个市场监管具有指导性的意义。目前，美国是全球少数实行多头监管的国家，监管主体包括证券交易委员会（SEC）、金融犯罪执法网络（FinCEN）、商品期货交易委员会（CFTC）、货币监理署（OCC）和州金融管理局（DFS）等。

是否对数字资产性质进行明确

美国对数字资产定性主要有三种，涵盖了**证券属性**、**商品属性**和**货币属性**：

（1）证券属性

主要受 SEC 监管，2017 年，SEC 曾发布“DAO Report”，奠定了只要数字资产涉及证券（参照“豪威测试”），便受监管，而发行主体是否为去中心化组织、是否以法定货币或数字资产形式提供服务均不影响监管效力。2018 年，SEC 主席 Clayton 表示数字资产发行销售过程中涉及的通证，是用来筹资的，具有证券性质，需收到监管。

（2）商品属性

主要受 CFTC 监管，涉及美国的期货和期权市场，早在 2015 年 CFTC 就将数字资产视为商品，相比于 SEC，CFTC 对数字资产的监管显得相对开放，主要监管期货、期权等场内的合规衍生品。

（3）货币属性

主要受 FinCEN 和 DFS 监管，主要打击金融及数字货币交易中洗钱、恐怖融资和其他金融犯罪，它对数字资产的监管更偏向货币属性，因而侧重其流转层面，2013 年，其就已明确数字资产交易所及其管理者是货币转移服务商，需注册成为 MSB (Money Service Business)，另外，每个州亦有各自货币转移方面的规定，需获取相应州的货币转移许可 MTL（Money Transmitting License）。

是否对数字资产的交易和流通进行监管

数字资产的交易和流通，在美国主要受 SEC、CFTC 和 FinCEN 及 DFS 监管：

（1）FinCEN 及 DFS

早在 2013 年，FinCEN 就已经明确虚拟货币（Virtual Currency）交易所及其管理者系货币服务商（Money Services Business, MSB），货币服务提供者及货币转移服务商（Money Transmitter）都需遵守《银行保密法（BSA）》及其实施条例，并在 FinCEN 注册为 MSB，遵守反洗钱和反恐怖主义融资（AML/CFT）规定。另外，每个州实际亦有各自的货币转移规定，需向 DFS 获取相应州的货币转移许可 MTL（Money Transmitting License），方可向该州居民提供服务，其中，纽约州还为数字资产业务引入了一个独立的牌照，称为 Bitlicense。

（2）SEC

2018 年 3 年 7 日，美国 SEC 发布公开声明，要求交易符合证券定义的数字资产的平台必须在 SEC 注册为国家性证券交易所（National Securities Exchange）或得到豁免。国家性证券交易所为美国证券交易法（Exchange Act Rule 3a1-1(a)）定义的证券交易平台，如 New York Stock Exchange LLC、The Nasdaq Stock Market LLC、Chicago Stock Exchange, Inc.等，也包括部分衍生品交易平台，如 Chicago Stock Exchange, Inc.、Chicago Board of Trade 等。

而在获得证券交易法（Exchange Act Rule 3a1-1(a)）豁免的情况下，交易平台无需注册为国家性交易所，可注册成为 ATS（Alternative Trading Systems），并遵守相关另类交易系统规则（Rules 300-303 of Regulation ATS）。截至 2018 年 6 月底，被批准的 ATS 共有 91 家。2018 年 7 月 18 日 SEC 又发出公告，接受 ATS 监管修正法规，提高 ATS 交易所运营透明度和监管力度。自此，ATS 牌照的发放开始收紧，截至 2018 年 11 月底，被批准的 ATS 数量变为 88 家。

（3）CFTC

数字资产衍生品交易方面，美国 CFTC 一直持有较为开放和鼓励的态度。2017 年 7 月向纽约的比特币期权交易所 LedgerX 发放许可，允许其交易和结算比特币的衍生品合约，这是 CFTC 首次向数字资产衍生品交易发放许可。2017 年 12 月 CBOE 及 CME 经 CFTC 批准，相继推出了比特币期货合约。2018 年 5 月 21 日，CFTC 市场监管部门和清算及风险部门针对数字资产衍生品交易所合规发布了一项新的指导文件，建议交易所必须有能力监控供应其定价数据的基础现货市场的完整性，并及时与 CFTC 工作人员相互协调。不过，该文件不被视为最终的“合规检查清单”，但它确实表达了 CFTC 的态度，希望帮助清算所和交易所跟上数字资产市场的变化。

是否限制数字资产的发行和销售

随着美国 SEC 将融资目的的数字资产全部视为证券，数字资产的发行和销售也有了明确的政策限制。美国任何证券的发行和销售只能通过两种途径：1）依照 1933 年证券法第 5 条在 SEC 进行证券登记注册；2）满足一定豁免条件而无须在 SEC 登记注册，但仍需接受 SEC 监管。美国 JOBS 法案（Jumpstart Our Business Startups Act，也叫“创业企业扶助法”）下的“Reg A+”、“Reg D”、“Reg CF”、“Reg S”等就是上述第二种豁免注册的发行通道。在针对数字资产融资的专项法规出台之前，美国项目或面向美国公民融资的海外项目将主要通过这些通道进行合规的证券型通证融资，且此类证券型通证未来只能上国家性证券交易所。

是否对数字资产其他相关行为进行约束

除了数字资产发行、销售、交易方面，美国 SEC 还对数字资产有关的投资、咨询提出了相应的要求：

（1）投资

根据“投资公司法案—1940 年”（Investment Company Act of 1940），SEC 认定证券投资公司为主要业务系“证券”投资、交易，并且管理的投资组合 40%

以上投资于证券的非政府主体。包括：（1）基金管理公司；（2）单位信托基金；（3）面额证券公司；（4）新兴的 ETF 等。根据法规，证券投资公司需向 SEC 注册，而其基金或权益份额的销售，亦属于证券发行，需满足证券发行、销售法律法规。

（2）咨询

根据“投资顾问法案—1940 年”（Investment Advisers Act of 1940），证券投资顾问系任何符合下述三个条件的个人或公司主体：（1）有偿服务，但不一定直接来自客户；（2）为主要或唯一业务；（3）涉及提供投资建议、投资咨询、研究报告发布、证券分析，无论直接，还是通过对外公布的形式，让用户认为相关主体正提供相关服务。证券投资顾问需向 SEC 进行注册，并满足相应的监管要求。

2.2.2 瑞士—分类明确，监管风格偏重实质重于形式，成熟度 ★★★

瑞士系对区块链及数字资产相对友好和支持的国度，其监管主体主要为瑞士金融市场监督管理局（FINMA），其在 2018 年 2 月 16 日发布的《ICO 指引》中明确了金融市场的法律和法规并不适用于所有数字资产融资案例，奠**定了其监管风格偏重实质而非形式**，2018 年 12 月 7 日，FINMA 发布了《瑞士分布式账本技术及区块链的法律框架》（下称“法律框架”），更细致地描述了其监管逻辑：

是否对数字资产性质进行明确

FINMA 在《ICO 指引》和“法律框架”中，根据通证的用途，明确地将通证分为三个类别：支付型通证（Payment token）、功能型通证（Utility token）及资产型通证（Asset token）

（1）支付型通证

与比特币等数字资产类似（包括比特币现金、比特币黄金等分叉币以及莱特币等变体等），仅作为支付工具使用的通证，通常使用方和接收方不构成合约关系。另外，如果通证是作为各个区块链项目系统内的购买商品或服务的支付方式、或系统内的价值转移方式，且不涉及合约的权利义务关系，也属于支付类通证。功能类通证和资产类通证也有可能带有支付属性，这种情况下可称其为“混合类通证”（Hybrid Tokens）。

（2）功能型通证

持有人可以访问某个区块链平台或某项应用，并享受其提供的服务及便利。它们与代金券或筹码一样，可根据设定的规则来兑现所欠服务。功能类通证在一些场景下可能被用作该区块链系统中的支付手段，此时它也具有支付类通证的性质，在监管上需与支付类通证一致。另外，需要注意的是，如果通证的发行是为了融资来进行平台开发，且在平台上线之前无法提供服务的，在发行时该

通证不属于功能类通证，而是资产类通证，因为通证发行方本质上是在融资，而通证购买方是在投资，监管上的处理方式与资产类通证一致。

（3）资产型通证

是一种资产凭证，例如代表着对实物、公司、收益、参与分红或利息支付的权利等。它是标准化的，可被用于大规模的标准化交易。在经济功能上，它类似于股票、债券或衍生品，其投资性质涉及到区块链之外的现实资产。除了基于通证的性质为其分类，FINMA 还基于《金融市场基础设施法案》（Financial Market Infrastructure Act, FMIA）给出了各类通证是否属于“证券”的判断：**FMIA 定义下的“证券”只包括标准化的、认证或非认证的证券、衍生品和间接持有证券**四种类别，且需要与资本市场有关联。其中“标准化”体现为该证券以相同的结构和面额发行、可供大众公开交易；“非认证证券”（Uncertificated Securities）包括大批量生成且相互无差异、可替换的权利，发行方仅关心数量和面额，对持有人没有特殊要求，通常没有公开交易。

是否对数字资产的交易和流通进行监管

对于符合 FINMA 定义的“证券”类数字资产的交易所，属于金融市场基础设施，需要获得 FINMA 的授权；除此之外，如果所交易的通证属于 FinSA 法案下定义的“金融工具”，即权益证券、债券、衍生品、结构化金融产品、期末价值或利息收益与市场风险相关的存款产品（除利息与标准化的利率指数挂钩的产品），交易所还需遵守 FinSA 法案规定，包括尽职披露、文件说明等，确保交易的通证是可信的，而本身 FinSA 定义的“金融工具”范围就包涵了 FINMA 法案定义的“证券”范围。

而对于非“证券”类数字资产的交易所，则目前还无需获得 FINMA 的授权，但需要满足瑞士的反洗钱，反恐融资等要求，具体合规方式，一是成为受 FINMA 认可的自律组织（Self-Regulatory Organization，简称 SRO）成员，二是直接向 FINMA 注册，成为直接隶属的金融中介（Directly subordinated financial intermediaries，简称 DSFI）。

是否限制数字资产的发行和销售

FINMA 的《ICO 指引》将数字资产的发行分为 2 种情况，并予以不同的监管：

（1）融资时已有主网

融资时已经有主网，通证已经是可以流通使用的状态，针对这种情况，FINMA 将根据该通证的三大类别进行个案分析，最终予以确定监管对策。

（2）预售/预融资（Pre-Sale/Pre-financing）

融资时项目还处在开发阶段，所购买的通证将在未来发放，属于预售/预融资行为，FINMA 将这种情况的通证全部视为资产类通证，属于 FIMA 法案定义的“证券”，适用于 FMIA、FinSA 及全套证券监管框架。

是否对数字资产其他相关行为进行约束

除了数字资产发行、销售、交易，瑞士还在数字资产托管等方面有相应的规定，即若属于纯安全保管目的而产生的托管行为，不需要持有银行牌照，但需满足反洗钱要求，而若涉及运用募集的资金进行投资、资产管理等行为，托管平台方或数字资产众筹中的募资方都需要持有银行牌照（除非满足豁免条件）。

2.2.3 香港—从差异化监管到无差异监管典型，成熟度 ★★★

香港早期对数字资产奉行差异化监管策略，若不涉及“证券”，则无需获得授权和牌照资质，而若涉及“证券”，则会受香港证监会体系监管。2018 年 11 月 1 日，香港证监会发布《有关针对数字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》（简称“新规”），实际宣告香港踏上对数字资产进行全面监管的道路，确立了证监会对数字资产的监管地位，并走向牌照制，告别之前对“证券类数字资产”和“非证券类数字资产”分类监管的思路：

是否对数字资产性质进行明确

香港对数字资产性质有明确的定义，2017 年 9 月，香港证监会发布声明称数字资产发行可能属于证券，综合来看，只要符合《证券及期货条例》(第 571 章)中所界定的“证券”及“期货合约”，便被认定为“证券类通证”，而不符合的，则属于“非证券类通证”。

是否对数字资产的交易和流通进行监管

根据香港新规，“非证券类通证”交易平台和“证券类通证”交易平台均被纳入监管，且共同参照《证券及期货条例》(第 571 章)条例规定，需获取第 1 类（证券交易）及第 7 类（提供自动化交易服务）牌照。另外，新规还指出，证监会将结合交易所的运营操作特性施加某些特殊的监管标准，具体施加的特殊监管标准将会在沙盒阶段，由交易平台与证监会沟通确定，可能包括：数字资产交易在同一法律主体下进行；（2）只向专业投资者提供服务；（3）首次通证发行的通证至少 12 个月或项目产生利润后才可上线；（4）不可为客户提供融资、期货衍生品交易服务。另外，新规提出了去中心化交易所可能在现有的监管体系内不适宜进行，或暂不对上述类型交易平台予以批准的观点。

是否限制数字资产的发行和销售

根据香港监管规定，数字资产发行可能涉及三种身份：如果数字通证代表一家公司的股权或拥有权权益，则有可能被视为“股份”，如果用途是订立或确认由发行人借取的债务或债项，便有可能被视为“债权证”，如果数字资产收益源于发行者集体管理并投资于不同项目，便有可能被视为“集体投资计划”，具体来说，若属于“证券类通证”，须获香港证监会发牌或向证监会注册。

是否对数字资产其他相关行为进行约束

除发行销售、交易流通外，香港还对涉足数字资产业务的基金管理人，涉足数字资产业务基金的份额分销商等有相应的约束要求：

（1）涉足数字资产业务的基金管理人

根据新规，已明确投资目标为数字资产（无论是否属于“证券类通证”），或有意向将投资组合中 10%或以上（不达 10%可以豁免）的总资产投资于数字资产的基金管理人，需持有第 9 类受规管活动的相应牌照，并需要满足一定应对数字资产风险而衍生的特殊监管标准，包括：（1）只向合格投资者募集资金，并披露所有相关风险；（2）选择合适的资产托管方案，无论是自托管、第三方托管或存放于交易所，均需站在客户利益最大化角度进行评估；（3）审慎、小心地对投资组合进行估值，对估值原则、方法、模式及政策作出合理适当的选择，并妥善向投资者进行披露；（4）设立良好的风险管理及控制体系；（5）聘请会计师对管理基金进行外部独立审计；（6）保留合适的流动资金。

（2）涉足数字资产业务基金的份额分销商

任何人如在香港进行或向香港公众分销投资于数字资产的基金，无论数字资产是否构成证券或期货合约，除非获得豁免，否则便须就第 1 类受规管活动（证券交易）获发牌或注册。

2.2.4 日本—数字资产合法化早期践行者，成熟度★★★

日本是全球最早为数字资产提供法律保障的国家。2016 年 5 月 25 日，日本内阁签署《资金结算法》修正案，并将数字货币纳入法律规制体系之内。该法案于 2017 年 4 月 1 日开始实施，在全球数字资产监管方面有着重要意义。

是否对数字资产性质进行明确

日本于 2016 年通过的《资金结算法》承认数字资产为一种合法的支付手段，并不是商品或证券。这种态度与日本的国情也有一定关系。日本央行金融科技中心负责人河合祐子曾对外表示，由于日本人对个人信息泄漏极度敏感，对现金的依赖非常高，所以日本数字化进程很慢，远没进入无现金社会时代。而数字资产的出现为日本实体经济发展带来新机遇。

是否对数字资产的交易和流通进行监管

《资金结算法》规定日本数字资产交易所及相关服务商需在日本金融厅完成登记。该登记制度所覆盖的业务范围包括：数字资产的买卖或与其他虚拟货币的兑换、针对此类买卖和兑换的中介和代理服务、以及对用户的法币及数字资产管理服务。该制度同样适用于设立在日本境外的交易所，也就是说，未在日本登记的海外数字资产交易所，不得对日本国内人员进行数字资产交易的劝诱活动。同时，数字资产交易所的义务包括：1）信息安全管理；2）向投资者提供信息；3）投资者的财产管理；4）与指定虚拟货币交换业务纠纷解决机构签订合同义务；5）提交业务报告；6）备案义务。此外，数字资产兑换服务商所经

营的全部种类的数字资产，以及此后新增的数字资产种类都必须告知金融厅。2017 年 9 月，日本金融厅首次正式批复了 11 家数字货币交易所。

2018 年 3 月，由于此前 1 月的 CoinCheck 交易所发生 NEM 被盗事件，日本金融厅对国内数字资产交易所强化审查。此次采取更严厉的监管主要是在《资金结算法》的基础上对客户 KYC 等规定的进一步趋严。

是否限制数字资产的发行和销售

《资金结算法》要求数字资产的发行方向金融管理局进行“数字资产兑换服务商”的登记，或通过已登记的数字资产兑换业者发行。因为若以法币进行数字资产的融资发行，则属于上述“数字货币的买卖”；若以与比特币等其他数字货币的兑换进行融资发行，则属于“与其他数字资产的兑换”。所以数字资产发行一旦涉及融资，该发行方就会被定义为“数字资产兑换服务商”。

是否对数字资产其他相关行为进行约束

由于日本一直以来都是数字资产交易和使用的大国，税务也是监管的重头。日本国家税务机构(NTA) 于 2018 年 11 月 30 日发布《关于数字货币相关税务问题 FAQ》文件，对于日本现在的数字货币的交易中的税务相关问题进行了详细解答，并公布了详细的计算细则和计算方法。从 2018 年 1 月至 2018 年 12 月的这段时间内，通过数字货币产生的相关收入超过 20 万日元(约 1780 美元)的人需要缴纳各类不同的税项。

2.2.5 新加坡—持续迭代，全面监管，成熟度 ★★★★

2017 年 11 月，新加坡金融管理局 MAS 发布了《数字通证发行指南》（A Guide to Digital Token Offerings），该《指南》被视为 MAS 对数字资产融资监管的澄清性文件，MAS 也在其中对监管过程和范围给出了更清晰的说明。时隔一年，2018 年的 11 月 30 日，MAS 又在 2017 年《数字通证发行指南》的基础上，针对市场中出现的新情况和新模式，如不断涌现的通证交易平台和证券型通证融资，推出了更新版的《指南》。另外，2019 年 1 月 14 日，MAS 向议会提交的《支付服务法案》（Payment Services Bill, "PSB"）正式通过，该项法案扩大了受监管的范围，更多业务将被纳入“牌照制监管”的行列。

是否对数字资产性质进行明确

在 2017 年发布的《指南》中，MAS 将数字资产分为“资本市场产品”和“功能型通证”两大类。2018 年《新指南》在之前基础上又稍加扩大了定义的范围：

（1）“资本市场产品”（Capital Market Product）

如 2017 年的《指南》中提到的股票、债券、集合投资计划单位基金、以及 MAS 特别指定的金融产品；2018 年的《新指南》在其基础之上增加了另外两个类别：单位商业信托，代表了对该商业信托基金的所有权；以及基于证券的衍生品合约，包括任何基于股票、债券或单位商业信托的衍生品合约。此类通证在新加坡被视为证券。另外，如果加密货币项目被定义为证券，也可申请进入 MAS 的监管沙盒，进行试验性运营，MAS 会按具体情况放松监管要求。

（2）功能型通证（Utility Token）

其余不属于以上“资本市场产品“定义的为功能型通证。

是否对数字资产的交易和流通进行监管

所有辅助通证发行的主体都将受到 MAS 的监管，并需要按规定持有资本市场服务许可证。包括可为项目方提供“基础数字通证发行”的平台、“数字通证交易平台”的运营方等。MAS 还规定，作为中介，就任何数字通证提供财务建议的任何人均须获得财务顾问的牌照。

是否限制数字资产的发行和销售

MAS 规定，若通证属于“资本市场产品”，则必须遵守新加坡证券期货法（Securities and Futures Act, SFA），且现有的新加坡资本市场的其他法律将直接适用。相关要求包括需要提供一份像招股书一样正式的通证发行说明书（prospectus），而不是仅仅发布一份白皮书。但证券型通证的发行也可以享有以下一些例外性的豁免情况：1）小额发行（12 个月内不超过 5 百万新币）；2）私募（12 个月内向最多 50 个投资人发行）；3）仅向机构投资者发行；4）仅向合格投资者发行。

2018 年 11 月 20 日，新加坡证券交易所（SGX）为计划进行数字资产发行的上市公司制定了指导方针，并提出在进行数字资产发行之前，上市公司应该与新交所的监管部门（SGXRegCo）保持沟通，以便让投资者做出明智的决定。新交所认为，根据新加坡的 SFA，数字资产发行中通证属于“证券或资本市场产品”，因此必须满足证券发行招股说明书的注册要求以及新加坡证监会规定的证券交易商的注册要求。另外，此类发行需要通过子公司来进行。

该项指导方针提到了通证发行方必须提供给投资者的信息包括：1）基本原理和风险；2）资金的用途以及利用这些资金能够实现的关键性进展；3）用于解除洗钱和恐怖主义融资风险的 KYC 检查；4）账务和估值处理；5）发行方资金在通证发行过程中的用途；6）发行通证对发行方造成的财务上的影响以及结算条款带来的影响；7）对现有投资者权益造成的影响；8）以及其他 SGXRegCo 认为有必要提供的信息。除此之外，发行方（上市公司）还必须取得法定审计的认可，以确保财务状况良好，资金的使用状况也不存在异常。

是否对数字资产其他相关行为进行约束

依据最新通过的《支付服务法案》（Payment Services Bill, "PSB"），从事提供任何数字支付通证交易服务或任何促进数字支付通证交换服务的人必须获得牌照，需要制定反洗钱/反恐怖主义的风险规避措施，并在这方面受 PSB 监管。

2.2.6 马耳他—积极拥抱，通过立法明确监管，成熟度 ★★★★

2018 年 7 月 4 日， 马耳他议会正式通过了 3 项法案，建立了分布式账本技术（DLT）和加密货币的监管框架，这也是世界上首个区块链、加密货币和分布式账本技术领域的国家级法律。

第一部法案是《马耳他数字创新管理局法案》（Malta Digital Innovation Authority Bill，简称 MDIA 法案），建立了马耳他数字创新管理局，并明确了管理局在相关数字创新公司运营资质认证、监管、以及执法等方面的职责以及权力。

第二项法案称为《创新技术处理和服务法案》（Innovative Technology Arrangement and Services Act，简称 ITAS 法案），提出所有 DLT、智能合约、DAO 相关的创新公司或组织在经营前需要经过管理局认证，并颁发相应证书，认证公司仅可在认证的范围内经营，并需要遵守 MDIA 法案。申请认证过程中，DLT 服务商需要尽可能详细地提供业务相关信息以及书面材料。加密资产交易所以及去中心化应用平台都包括在其中。

第三项法案是《虚拟金融资产法案》（Virtual Financial Assets Bill，简称 VFA 法案），明确了数字资产发行、交易、钱包提供商等方面的全套监管制度，也是全球首个专门针对数字资产设计的监管法案。

是否对数字资产性质进行明确

MFSA 将与分布式账本相关的资产都称为“DLT 资产”，并按照资产的属性，将其分为虚拟通证、虚拟金融资产、电子货币、金融工具四大类。其特点在于，没有套用传统的证券或货币监管体系将数字资产视为货币，而是提出了“虚拟通证“、”虚拟金融资产“的新概念，并建立了针对这类新型资产的新法规。

（1）“虚拟通证”（Virtual Token）

是指在 DLT 平台之外没有效用、价值或应用的数字媒介记录形式，并且只能通过此类 DLT 资产的发行人直接兑换此类平台上的资金，而不能上市流通。此类资产仅需符合 DLT 创新公司的法规，在公司运营之前认证经营资质。

（2）“虚拟金融资产“（VFA）

是指用作价值交换媒介、账户单位或价值存储的一切数字资产，可上市流通。此类资产需要遵循 VFA 法案的监管。

（3）“电子货币“（Electronic Money）

是指数字化后的货币。此类资产暂时不受数字资产相关法规监管，仅需遵循反洗钱等基本条例。

（4）“金融工具“（Financial Instrument）

是指证券、衍生品等传统金融世界的金融产品，与数字资产没有很大的关系。

是否对数字资产的交易和流通进行监管

根据新规，任何提供 VFA 或被归类为 VFA 服务提供商的实体都需要通过注册过的 VFA 代理商从 MFSA 处获取经营牌照，且 MFSA 视其经营情况有权随时收回该经营牌照。获得牌照之后，经营者也需要定期向 MFSA 提交审计报告。

在各类 VFA 的交易过程中，MFSA 将持续监管其发行主体的经营情况，如有任何有悖 VFA 法案的行为，MFSA 有权随时对该 VFA 处以短期暂停交易或永久暂停交易的惩罚。

是否限制数字资产的发行和销售

VFA 法案从白皮书、营销广告、项目运营等各方面对马耳他境内以及面向马耳他居民公开发行虚拟金融资产（VFA）的实体提出了全面的要求，比如营销和广告信息需要准确无误导性。值得一提的是，VFA 法案是全球首个将白皮书要求法律化的法案，对白皮书提出了 16 项基本原则，如白皮书需要用规定格式撰写、非技术语言表述的项目综述，以便投资人在类似项目之间做比较，需注明完成日期，需注明白皮书撰写人的名字、职能、以及声明其撰写的内容全部真实，发行方的行政管理团队需要在白皮书中声明该白皮书符合 VFA 法案要求，整个白皮书必须有英文版等等。其中对白皮书需要包含的内容做了详细的列举：该 VFA 发行的目的，项目背后相关技术详细描述，项目可持续性以及规模化的详细分析，项目面临的挑战和风险以及对应的解决方案，该 VFA 的特性和用途详细介绍，发行方、发行服务方（代理商等）、开发团队、顾问、以及其他所有与项目落地相关的团队的详细介绍， 发行方钱包地址披露，安全控制流程以及风险规避方案详述，过往项目里程碑和融资情况以及未来的规划列举等，共 38 项信息。

另外，VFA 法案还规定每一个准备上虚拟金融资产交易所（VFA exchange）的项目都必须找到在 MFSA 处注册过的 VFA 代理商来为其辅导及保荐。

是否对数字资产其他相关行为进行约束

除了这三项法案覆盖的范围，马耳他暂时未对其他数字资产相关的领域做出要求。这些法案旨在使马耳他成为在区块链及加密资产领域开设公司最理想的地

点之一。由于这些法案现已纳入法律体系，马耳他也因此会成为经济创新的先驱。反过来，也将通过创造一个新的经济利基来加强该国的经济。

2.3 合规基础设施：合规交易所、合规托管、证券类数字资产、稳定币

数字资产市场的合规化已是难以逆转的趋势，其结果是可以建立一个传统资金可以介入的机制和桥梁，并让传统世界的资金、资源注入和迁移。**而在合规化进程中起到重要作用的，是我们称之为“合规基础设施”的四大支柱：合规交易平台、合规托管、证券类数字资产、稳定币，分别对应了交易、托管、标的资产、清算方式。**2018 年，上述四个赛道发展迅速：

（1）合规交易平台

托管、证券类数字资产和稳定币本质上都是为价值的流转、交互服务的，若没有交易平台（无论是中心化还是去中心化），以数字资产为载体的现实、虚拟价值便无法得到最大化和流通。目前，推动交易平台合规化的主要有两种力量，一个是传统金融力量，另一个是区块链企业主动寻求合规化。

- **传统金融力量**

主要源自美国和欧洲部分重要国家的推动。纽交所母公司 ICE 集团发起的 Bakkt 交易所系美国 CFTC 批准的期货交易所，而近期期货交易所 ErisX 得到纳斯达克注资，两者均正大力推进比特币期货事宜，**并为传统投资者提供全套的持牌“资产托管+交易+清结算”解决方案。**7 月 6 日，瑞士证券交易所 SIX 宣布将于 2019 年上半年推出数字资产交易平台，并受瑞士金融监管局 FINMA 监管，12 月 12 日，德国第二大证券交易所斯图加特宣布计划在 2019 年第二季度推出数字资产交易。**足以看到最核心的传统金融势力正逐步渗透。**

综合来看，传统金融力量在数字资产领域的布局主要有如下核心的特征：**1）更多是基于数字资产的投资属性，并按照传统金融体系的模式，围绕市场基础设施去进行布局，主要涉及搭建合规的交易平台、合规的清结算提供商以及合规的托管商；2）推出的交易标的以数字资产衍生品为主，以期货为典型，现货数字**

资产为辅；3）清结算仍主要采用传统证券交易的模式，运用法定货币进行清结算，即以“法定货币-数字资产”交易为主。

- **区块链企业主动寻求合规化**

合规化趋势下，区块链企业也正主动拥抱合规和监管，提供受规管的数字资产交易流转服务，位于纽约州的 Gemini 和 itBit 早在多年前便已经获得了纽约州金融管理局发放的信托牌照，而 Coinbase 亦是纽约州数字资产牌照 Bitlicense 的持有者，可向用户提供合规服务。**2018 年，寻求合规化的主力军主要系火币、币安和 OK：**火币集团通过设立独立本地站的形式在日本、韩国等地落地了合规交易服务，其中日本的经营资质系通过收购拥有合法牌照的 BitTrade 交易所获取，另外，火币通过与战略合作伙伴 HBUS 合作的形式进入美国市场，除此之外，火币还自主申请了欧洲直布罗陀的 DLT 牌照，可在欧洲合规开展区块链资产交易业务；币安则是全力推进全球各地的合规法币交易所落地，目前已上线币安乌干达、币安泽西岛，前者支持乌干达先令，后者支持欧元、英镑；OK 集团则是与马耳他证券交易所签署了备忘录，推动全新的证券类通证平台落地，除此之外，其美国主体 OKCoin 取得了货币服务商 MSB 牌照，拥有开展数字资产交易资质。

（2）合规托管

在传统金融体系中，第三方资产托管系常见安排，基金的投资资产需在合格托管人处托管。**那么参照传统金融市场体系，合规化趋势下，数字资产的第三方托管便有其重要意义，并将成为引入传统投资者的重要设施。**然而与传统资产不同的是，数字资产依赖“私钥”，私钥即所有权，这使得数字资产的托管实际与过去的不记名纸质证券有类似之处，**包含了“私钥保护+合规资质”两个层面。**目前，数字资产托管市场主要分成了“To C 消费级市场”和“To B 企业级市场”，**而合规托管，主要是侧重后者“To B 企业级市场”，目前该领域参与者众，2018 年，该赛道发展迅速，形成了如下的综合竞争格局：**

- **专业的托管服务商，**例如瑞士的 Xapo，香港的 Invault，美国的 DACC，欧洲的 Swiss Crypto Vault 和 Koine Finance 等；
- **企业钱包服务商转型，**例如拿下南达科他州信托牌照的 Bitgo 以及中国的数字资产钱包服务商 Cobo Wallet；

- **持牌数字资产交易所衍生业务，**例如纽约州信托公司 Gemini 和 itBit 提供的托管服务，以及 Coinbase 与美国证券经纪商 ETC 合作的托管服务；
- **传统金融机构衍生业务，**例如 Kingdom Trust、Prime Trust 和 Bank Frick 等在内已在运作的，和高盛、野村、纽约梅陇银行已宣布要提供服务的。

我们认为，托管除了引导传统资金入场的功能外，自身亦本就包含了巨大的影响这个市场的能量，体现在：**1）各类资产必须在持牌托管人处托管，意味着其会成为 ETF 等金融衍生品在数字资产市场落地的关键；2）对目前数字资产交易模式形成重大影响，由于资产必须托管在合格托管人处，目前充值至交易所再行交易的模式存在缺陷，合规化进程下，或将倒逼交易平台获取托管牌照，或独立托管人直接承担经纪职能，为客户提供撮合交易，并逐步演变为交易柜台。**

（3）证券类数字资产

目前数字资产市场中的**大部分资产发行，并没有成熟的框架予以约束，实际未纳入监管，缺乏发行背书，同时，大部分的数字资产发行亦无现实资产的支撑，难以吸引真正的主流机构投资者入场参与。**而证券类数字资产，即合规数字资产发行则是解决上述症结的重要方式，市场需要一种合规的通道对区块链资产的发行进行约束和筛选，以协助重塑市场信用，加大投资者参与的信心。**而除了在资产发行层面，证券类数字资产也是传统证券实现资产上链的重要典型，让传统证券在链上进行流转，可提升流动性和流转效率。即证券类数字资产，理论上应该包含数字资产的证券化，以及证券的数字资产化两个层面。**2018 年系证券类数字资产共识元年，围绕证券类数字资产，已经慢慢上形成了一整个生态格局，

- **发行平台：**证券类数字资产实际是将传统证券市场中的合规准则通过代码的形式通过智能合约内嵌至数字资产中，因而需要特殊的发行平台予以协助，包括 Polymath、Swarm、Harbor、Securitize 以及 Securrency 等；
- **交易平台：**证券类数字资产，本质即为“证券”，只是以数字资产的形式存在，其交易需在合规的持牌交易平台进行，包括持有美国 ATS 牌照的 Open Finance Network, Tzero, Sharespost 以及 Coinbase，也包括本身系传统证券交易所的伦敦证券交易所、纳斯达克、瑞士证券交易所等；

- **周边服务商：**除了发行平台和交易平台外，还有包括分销平台、投行服务、法律服务、流动性服务、信息平台、托管服务商等在内的各类机构，亦是整个生态中重要的组成部分。

（4）稳定币

由于法定货币流转受限于传统的银行体系，**为了进一步促进法定货币的流转，去到法定货币无法触及的时空，产生了价值 1:1 锚定法定货币的稳定币，可在 365/24/7 的背景下进行自由流转和低成本交易。**稳定币最早起源于泰达公司发行的 TetherUSD，属于法币抵押稳定币。然而由于法币抵押稳定币具备入金属性，因而以 TetherUSD 为首的稳定币一直占据着市场主要地位，但 TetherUSD 目前仍未得到监管背书，其潜在的不透明性常被市场所担忧。

2018 年，稳定币市场一家独大的局面开始转变为群雄逐鹿局面。定位于“合规稳定币”的 TUSD、USDC、GUSD、PAX 分别在：1）合规性，前两者采用了“Licensed Money Transmitter”模式，分别由资产上链平台 TrustToken 和金融科技公司 Circle Fintech 和 Coinbase 发起的 Centre 联盟扶持，后两者采用了“Licensed Trust Company”模式，分别由纽约州信托公司 Gemini Trust Company 和 Paxos Trust Company 发起；**2）透明性**，引入了独立会计师事务所对美元储备金进行审计和披露；**3）美金储备安全性**，美元储备含保险，受美国联邦存款保险公司保护。这三个层面对 USDT 进行了改良并得到了市场认可。

法币抵押模式稳定币的蓬勃发展，与目前数字资产市场所处的阶段是密不可分的：**即目前市场规模仍较小，大部分的资产、资源、业务仍未从链下转移到链上，大部分的人亦未持有数字资产，迫切需要通过合规的通道将传统资产转移为数字资产，提供入金的方式，推进“资产上链”运动，这就给了法币抵押稳定币重要的发展驱动力。**而价值稳定、可随时赎回成法定货币的合规稳定币，将成为这一波浪潮中，传统机构参与链上数字资产交易和流转，以及进出这个市场重要的关键所在。**未来，我们很可能看到托管服务商（也会是经纪商、交易柜台和银行）与稳定币的购赎 API 相连，实现客户的快速法币入金、交易及退出，而这一切的实现，也只能由合规的稳定币来实现，即对于合规稳定币来说，相当于为交易场景提供了“Fiat Gateway as a Service”的服务。**

三、区块链产业发展现状解读

区块链作为一种革命性技术，在赋能各类产业的同时，也催生出了一个完整的产业，火币区块链研究院将整个区块链产业链分成五大板块：

- **硬件与基建层：**为各种区块链提供、整合底层算力和硬件支持；
- **平台与基础层：**为各种区块链应用提供底层架构、开发平台和生态；
- **通用技术层：**让区块链应用更方便部署和被应用，为开发者和用户服务；
- **垂直应用层：**将区块链应用于各个行业及场景，服务最终用户；
- **周边服务层：**帮助资金、信息等流动，为产业链参与者提供专业服务。

3.1 硬件与基建：低纳米矿机市场表现不佳，矿场、矿池面临诸多考验

矿业，也被称为区块链世界中的基础设施，起到整合底层算力与硬件支持的作用，是区块链原生的产业。其因比特币而诞生，后随着区块链技术逐渐发展，成为一条成熟的矿业产业链。2018 年，随着整个数字资产市场的持续降温，矿业也面临了诸多考验，亟待破局者出现：

（1）低纳米矿机因市场环境因素而占有率不足，性能提升红利逐渐缩小

各大矿机芯片设计厂商，今年均有高性能的新产品问世，虽然在功耗比方面更具有优势，但是因市场下挫，销量都不甚理想。

比特大陆系矿机界的佼佼者，然从 2016 年开始，其芯片研发进度有所放缓，直到 2018 年中旬的蚂蚁 S9 Hydro，仍然使用的是 16nm 芯片。11 月份，另一矿机厂商嘉楠耘智率先发布 7nm 矿机阿瓦隆 A9，之后比特大陆同为 7nm 的 S15 矿机发布。新锐矿机生产商神马和芯动于今年异军突起，凭借单矿机高算力和功耗比的优势在市场中杀出一条血路，整个低纳米矿机市场竞争激烈。

然而 7nm 矿机对于矿工来说，最大的问题并不在设计与性能，而在产量与价格。除了投产需要较长的周期外，其产量严重不足，受到台积电与三星生产线产能制约，其芯片或与手机芯片制造产生产能冲突，进而不利成品矿机产量。除此之外，7nm 芯片价格不菲，其设计、流片、制造等一系列成本会转嫁到矿工身上，**那么在熊市中，价格高企的高性能矿机是否是矿工的首选，就是个问号。**

从长期来看，未来竞争核心的确将逐渐变为 7nm 芯片的矿机，**但从芯片领域发展历史来看，每次升级所带来的边际收益正逐渐递减。**从 28nm 到 16nm 的时候还可以带来 40%左右的性能提升，但是从 16nm 到 10nm 或 7nm，却未能带来性能大幅度的提升。而且 7nm 基本已是目前芯片领域技术极限，在可预见的未来很难再有大幅度的工艺升级。**因此，矿机升级所带来的性能提升红利还能持续多久，亦是一个问号。**

（2）矿场大干快上掉头难，矿池业务纵深盈利难，反过来影响算力稳定

对于矿工来说，币价、算力、电费、矿机成本、维护成本是影响其收益的关键要素。**但矿场却无需关心这么多，其本质上是“收租子”（电价差及托管费）的传统房地产生意，关键是能够找到便宜的电和地。**以中国为例，丰水期的云贵川小水电，新疆、内蒙许多便宜的电力一般均能够吸引到矿场投资者。

但“租房”市场也不会永远兴隆，**在数字资产价格不见明显回升的时候，“经济萧条”，矿工交不起“房租”，那么诸多小型、高电费矿场也面临倒闭，在熊市出清产能，而这也是 2018 年很大一批矿场所面临的尴尬境地。**另一方面，数字资产监管层面的不确定性，也影响着矿场的生存和发展。

矿池在市场中的作用在于整合散户矿工和部分中小型矿场，通过收取管理费和服务费盈利，不直接负担矿机成本。表面上看，这一特点使其在这个寒冬生存的并不那么艰难，但由于矿池之间竞争的存在，如果仅仅做矿池一项业务，而从未涉及矿场、挖矿或其他产业链衍生业务，也会面临竞争力不足的局面。然而虽然背靠完整产业链的矿池具有更强的优势，**但受市场因素影响，“矿工”、“算力”离场，盈利也越发困难，面临着不同程度的危机，而这正反过来在影响算力的稳定，对区块链网络的安全性造成了很大的影响。**根据 Crypto51 数据，目前，

部分区块链网络（以采用 PoW 共识机制的次主流币为主，比特币等大币种相对仍健康），发动 1 小时 51%算力攻击的成本已低至一万美金以下：

图 23：发动 51%算力攻击成本汇总

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$63.95 B	SHA-256	35,751 PH/s	*$232,163*	0%
Ethereum	ETH	$13.05 B	Ethash	166 TH/s	*$93,086*	6%
Bitcoin Cash	BCH	$2.31 B	SHA-256	1,364 PH/s	*$8,861*	2%
Litecoin	LTC	$1.95 B	Scrypt	191 TH/s	*$20,195*	7%
Monero	XMR	$755.36 M	CryptoNightV8	544 MH/s	*$5,229*	4%
Dash	DASH	$627.17 M	X11	2 PH/s	*$4,332*	35%
Ethereum Classic	ETC	$476.33 M	Ethash	11 TH/s	*$6,357*	84%
Zcash	ZEC	$316.20 M	Equihash	2 GH/s	*$13,593*	7%
Bitcoin Gold	BTG	$213.27 M	Zhash	3 MH/s	*$1,071*	14%
Bytecoin	BCN	$118.23 M	CryptoNight	343 MH/s	*$215*	65%
Siacoin	SC	$96.34 M	Sia	1 PH/s	*$0*	0%

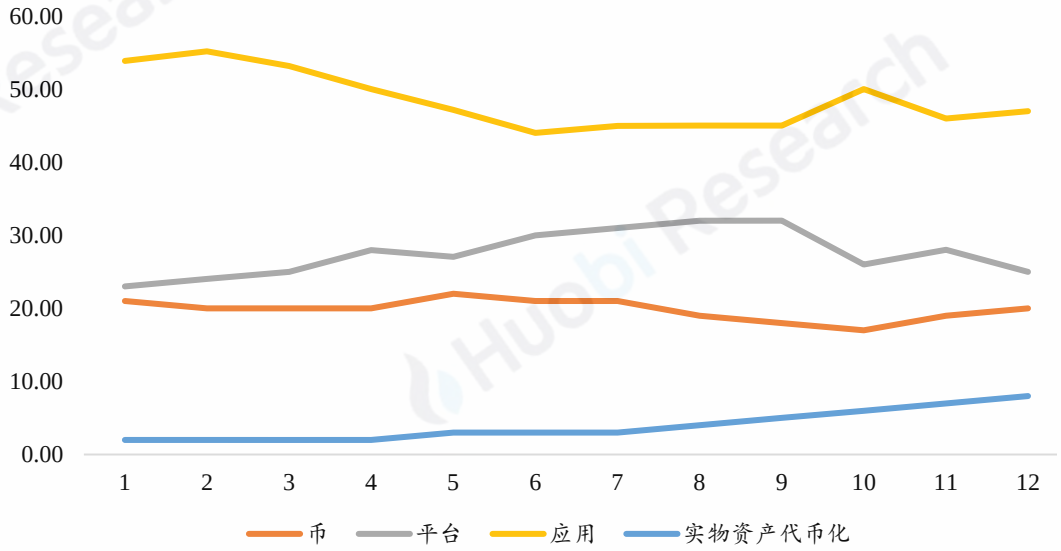
来源：Crypto51，火币区块链研究院整理

3.2 平台与基础：公链降温，回归理性，“欲速则不达”

一直以来，火币区块链研究院根据数字资产代表权益属性的不同将其分为“币”、“平台”“应用”和“资产通证化”四类。

通过对目前市值排名前 100 的数字资产进行分类，我们发现，**全年应用项目个数是遥遥领先的，但同时也看到，自 2018 年上半年起应用项目数目下滑趋势明显**，这也和市场真实感觉一致：2018 年初简单的应用项目就能获得较好估值，大量应用项目涌现市场，它们基本上是利用公链平台去落地行业应用；然而随着大众对区块链技术越来越了解，并逐渐意识到主流公链平台的可扩展性不强，应**用项目纷纷不甘“寄人篱下”，掀起了自己开发公链平台潮，公链项目数量在二、三季度增长迅速**，如下图所示：

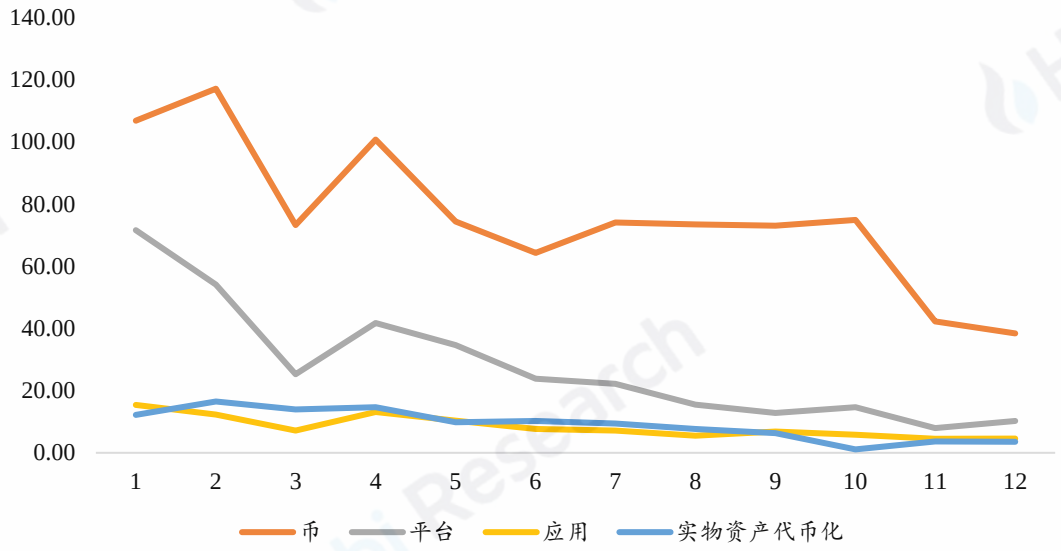
图 24：2018 年市值前 100 数字资产市值类型分布



来源：Coin Market Cap，火币区块链研究院整理

然而随着二、三季度公链平台潮爆发后，市场又出现了部分公链平台无人使用的情况，花了大力气开发出来的公链平台除了应用项目自己使用外，无法拓展其他生态，于是到了 2018 年下半年公链平台潮热度也开始下滑，**市场回归理性。Top100 的公链平台和应用项目市值基本上归一到了同一个级别，而实物资产通证化项目市值，反倒是随着合规稳定币的兴起，需求的增加，而不断上涨：**

图 25：2018 年市值前 100 数字资产平均市值趋势



来源：Coin Market Cap，火币区块链研究院整理

综上，整个 2018 年，区块链项目尤其是公链项目经历了以下几个阶段：

- **第一季度应用项目热潮转向第二、三季度的公链平台潮；**
- **第四季度公链平台潮的褪去，而实物资产通证化出现上涨；**
- **公链项目和应用类项目市值回归同一个量级。**

从技术层面上看，2018 年新出来的公链项目基本都采用“Fork +改编”路线，很多 Fork 出来的公链均以高 TPS 为主打旗帜，TPS 也以过万、过十万甚至过百万著称，似乎速度已经成为了公链唯一的追求。**然而我们对比一些支付服务商数据就能知道，即便是采用中心化的解决方案，达到数十万甚至百万，也是困难重重，而达到那么高 TPS 的是否存在必要，亦是一个疑问：**

项目	是否区块链	TPS
BTC	是	5～7
ETH	是	20～30
EOS	是	3996
Visa	否	56,000
Paypal	否	100,000
支付宝双 11	否	491,000

来源：火币区块链研究院整理，基于 2018 年 12 月底数据

除此之外，我们也整理了 2018 年有一定知名度的 25 条公链上主网情况，发现公链的开发落地也并不是一番风顺，如下表所示：

项目名称	计划主网上线日期	实际主网上线日期	预计
Cardano	2018 年 Q2	延迟，发布过 KEVM, IELE, Byron, Plutus, Marlowe 五个公开测试网，1 个 Treasury 内部测试网	2019 年 Q1
Aeternity	2018 年 6 月 21 日	延迟，第一批主网通证转换登记已于 11 月 25 日结束	2019 年 Q1
Aelf	2018 年 6 月 30 日	延迟	2019 年 Q1
Aion	2018 年 5 月初	2018 年 4 月 25 日	
Bytom	2018 年 4 月 30 日	2018 年 4 月 24 日	
Credits	2018 年 6 月 30 日	2018 年 6 月 30 日	
CyberMiles	2018 年 10 月 15 日	2018 年 10 月 15 日	
EOS	2018 年 6 月 2 日	2018 年 6 月 2 日	

Everitoken	2018 年 7 月 31 日	2018 年 7 月 31 日	
Fusion	2018 年 6 月 30 日	延迟，主网测试阶段	
Hashgraph	2018 年 Q2	延迟，主网测试（12 月 19 日开通申请）	2019 年 3 月份
Internet of Services	2018 年 6 月 30 日	延迟	2019 年 2 月 25 日
Nebulas	2018 年 Q1	2018 年 3 月 30 日	
NULS	2018 年 5 月 31 日	2018 年 7 月 11 日	
Ontology	2018 年 6 月 30 日	2018 年 6 月 30 日	
Rchain	2018 年 12 月	延迟	2019 年
SmartMesh	2018 年 4 月 30 日	2018 年 4 月 30 日	
Tezos	2018 年 Q3	2018 年 9 月 17 日	
Theta	2018 年 Q4	延迟	2019 年 3 月 15 日
TomoChain	2018 年 Q2	2018 年 12 月 14 日	
Tron	2018 年 5 月 31 日	2018 年 5 月 31 日	
Vechain	2018 年 6 月 30 日	2018 年 6 月 30 日	
WaykiChain	2018 年 5 月中旬	2018 年 5 月 13 日	
Zilliqa	2018 年 Q3	延迟	2019 年 1 月 31 日
Filecoin	2018 Q1	延迟	2019 年 Q3

来源：火币区块链研究院整理

从上表可以得到以下几个结论，2018 年既定主网上线的公链项目中，有：

- 近一半的项目主网上线滞后；
- 至少三分之一的项目滞后严重，推迟到了 2019 年；
- 在 EOS 主网上线期间出现了公链主网扎堆上线、抢先上线的情况；
- 扎堆主网上线的项目容易出现年内迅速迭代升级的情况，上线的主网只有基础功能并未覆盖白皮书全部功能甚至优势功能的情况；
- 头牌明星项目的愿景和开发难度在项目成立之初往往被忽视，如 ADA，ZIL、Filecoin 等，纷纷滞后严重。

纵观 2018 年公链项目，活跃度相对更高的主要是 EOS 和 TRON，他们将 TPS 提升到了千级，并带动了 Dapp 的发展。但另一方面，以高 TPS 著称的 EOS 和 TRON 也碰到了上链数据大量来自于简单游戏、数据量暴增和资源制约问题，

引发了数据价值问题以及公链价值的思索。**也许对区块链技术的使用，我们目前仍然没有想得很清楚，单纯提升扩展性，或求快速构建一条完美的公链，都是不切实际的，而这，也不禁让人想起了“欲速则不达”的道理。**

3.3 通用技术层：公链生态推进带动开发者工具发展

公有链之间的竞争有两个层面，向下要争取到更多的用户，向上则要争取到更多的开发者。不论公有链的底层技术如何，任何一条公有链的繁荣都不可能一蹴而就。2015-2017 年，公有链都在紧锣密鼓地开发中，诸多公链只能在概念上一较高下。但是 2018 年，多条知名的公有链主网上线，公有链之间开始争夺社区支持，尤其是开发者的支持，**而提供通用技术模块组件，降低开发者的开发成本，让开发者可以快速、简易的开发和部署应用，便成为了重中之重。**

其中表现最突出的新兴公有链之一就是 EOS.IO。相比于 PoW 系公有链，如以太坊中的矿工节点而言，EOS 社区的 BP 节点会更愿意去推动免费的开发者工具。典型的社区的开发工具包括：CPU 租赁、区块链浏览器、测试网、投票工具、快照工具、公投工具、通用库、开源构架、术语和词汇表、合约开发工具、API 工具、侧链、安全监测工具、Chrome 插件、评级工具、协议等：

工具类型	工具举例
CPU 租赁	Chintai、CPU 租赁、CPU 自助租赁、CPU 急救等
区块链浏览器	Bloks.io、eosflare、EOSPark、EOS Tracker 等
测试网	Jungle Testnet、CryptoKylin Testnet 等
Chrome 插件	Scatter 等
合约开发工具	EOSEasyContract、EOSFactory、EOS Guardian、Dev4eos 等
公投工具	eosio.forum、EOSPark 等
API 工具	EOS API Proxy、dfuse 等
综合工具	EOS Ecosystem 等
快照工具	Block Matrix 等

来源：火币区块链研究院整理

这是因为 BP 的候选人是有潜在收益的。BP 义务为社区制作开发工具，一方面可方便自身的开发团队使用，另一方面则可以吸引社区更多选民选票支持。

获取更多的投票意味着 BP 更可能进入前 21 名并获取更多的 EOS 收入。**而且竞选越激烈，社区工具迭代更新就会越快。**

同时，**如果某款工具既能服务社区内的开发者，又能获得直接收益，这类工具发展速度则会更快。**比如 EOS 目前已有不小于 10 款 CPU 资源租赁的工具，既有 B2C 盈利性质的，也有 C2C 撮合性质的，还有 B2C 公益性质的，一应俱全。资源租赁这个现象在 2017 年是没有的，因为在过去没有对区块链网络资源的需求。但如今，由于 EOS.IO 网络特殊的设计，以及 DApp 的逐步发展，开发团队非常需要足够的廉价的资源来维持 DApp 的运转，因此 CPU 租赁工具等也同样快速发展。我们可以预计到的是，伴随着 REX（Block.one 开发）等工具的上线，在 2019 年开始，资源租赁的规模将会随着 DApp 不断壮大。**假如 DApp 进一步繁荣，甚至可能会出现基于资源租赁的多种金融衍生品。**

而与新兴的公有链如 EOS.IO 目前的通用技术工具还相对基础，侧重资源型，且较为分散不同的是，**以太坊为首的老牌公有链，由于时间积淀更长，其通用技术工具更为模块化和成熟，并有一系列集合式的解决方案项目出现**，例如数字资产流通解决方案 0x 推出了 0x Launch Kit，让使用者快速部署去中心化交易平台，又例如区块链游戏、侧链解决方案 Loom Network 集成了让开发者自行架设以太坊侧链和部署 Dapp 的模块组件包等等。

3.4 垂直应用层：“区块链+”逐步开展，商业模式赋能及强化成破局关键

2018 年的区块链应用与 2017 年的基于区块链发行资产不同，市场不再为通证的价格炒作买单，也不仅仅满足于区块链在价值交换方面的应用，而是把关注点放在了商业模式上，于是，“区块链+”模式的应用开始逐步开展。

在纯粹的区块链项目中，需要从零开始基于区块链建立社区，可能需要经历漫长的开发、用户获取、社区运营、商家获取等过程才能实现商业化。**而“区块链+”中的“+”体现在，盈利模式或者应用场景原本即存在，区块链技术更多是在此基础上赋予更多价值，具体包括：构建信任（利用区块链分布式账本特性），**

数据自治及价值化（利用区块链价值传输网络特性），行为激励（利用区块链通证激励特性）三大核心应用层面[1]，具体如下：

（1）构建信任（利用区块链分布式账本特性）

分布式账本与传统第三方中介方式相比，在构建信任方面有着较大优势，背后的思想与传统社会使用的复式记账的思路一脉相承，也类似于订立合同时一式多份的做法，是希望通过在多个业务主体间共同保有多个备份来尽可能避免对记录内容的篡改，但在**实现方式上，是予以电子化，一旦达成共识，该信息会在网络上予以同步，以此降低信用成本，增强可信度。**

在信任重构方面，显著降低时间及信任成本的应用系存证。2018 年 6 月 28 日，中国杭州互联网法院对一起侵害作品信息网络传播权纠纷案进行了公开宣判，首次对采用区块链技术存证的电子数据的法律效力予以确认。该案中的原告华泰一媒在诉讼阶段通过第三方存证平台保全网提交了一系列证据，保全网通过开源程序自动收集了网页源码和截图等原始信息并打包压缩，将哈希值等相关信息上传至 Factom 和比特币区块链平台上，确保不可篡改，免去了第三方公证。在此之后，2018 年 9 月 7 日，中国最高人民法院公布《最高人民法院关于互联网审理案件若干问题的规定》，即日起施行，并明确了区块链存证的法律效力。

我国在增强可信度方面还有一些应用案例：2017 年，微众银行联合广州仲裁委、杭州亦笔科技三方基于 FISCO BCOS 区块链底层平台打造“仲裁链”；2018 年 2 月，广州仲裁委基于“仲裁链”出具了业内首份裁决书。通过“仲裁链”，仲裁机构能够从证据产生初期就参与到存证业务的过程中，参与多方共识进行实时见证，当发生纠纷时，经核实签名的存证数据即可被视为直接证据。

（2）数据自治及价值化（利用区块链价值传输网络特性）

区块链可以实现将微小的行为数据化，再通过通证的形式将其价值化，而这一切将通过私钥的形式由用户本身保留有数据的所有权和自治权，并借助区块链价值传输网络的特性，予以在数据需求者和数据提供者之间有偿流转。具体来说，基于区块链和公钥/私钥对，用户可以实现对颗粒化个人数据的控制，以及实

[1] 详细介绍请参考《火币区块链产业专题报告-区块链四层应用模型的构建与解析》

现对任何一项细分数据的访问授权，只有在用户授权同意的前提下，智能合约才可以被执行。2018 年，在用户数据自治方面的区块链尝试，源于互联网巨头 Facebook，5 月，其宣布了增设了专门的区块链部门，重点在于解决用户隐私问题，而就在此之前，被成为“史上最严格隐私规范”的欧洲《通用数据保护法案》(General Data Protection Regulation, GDPR)也正式生效，使得 Facebook 等互联网公司面临更大的压力，用户数据自治和价值化将是未来重要的方向之一。

（3）行为激励（利用区块链通证激励特性）

而基于真实业务场景，引入以区块链通证为价值载体而建立的通证激励体系，以此突破业务的瓶颈，带来增量，则是“区块链+”的另一大杀器。换个角度理解，这一种模式，**可以认为是一种升级版的会员积分计划，具备两大特性：**

- **独立社会化传播：**与传统模式不同，通证激励体系，其记录、流通、交换、交易等环节均在链上完成，单中心控制变成社会化传播；
- **可编程的实体经济赋能：**成为“区块链+”通证经济的重要基础，为实体经济赋能提供新的技术和商业解决思路，实现业务逻辑逻辑的智能化。

借助上述特性，通证激励体系将会**充分调动各个关联方的贡献，即打破积分孤岛困局，充分激励利益相关方，**同时，亦可**借助可编程的组织治理机制，优化市场资源配置**，人们的行为贡献都能通过算法规则和通证机制实现分布式账本的确权，并通过赋予通证多维度的高阶权益，提升组织内和组织间的资源配置效率。

日本 LINE 公司于 2018 年 8 月 31 日宣布即将开展区块链项目 Link Chain 便是非常典型的案例，在 LINE 的设想里，一切用户行为都可以算作挖矿，因为这些用户行为其实都在为生态系统贡献用户行为数据，所以都应该获得通证奖励。而用户拿到这些 LINK 积分之后，可以在多种渠道使用，包括在各个 Dapp 中进行支付，实现跨场景流通，亦包括在积分交易市场上进行流通。而通过这种方式，用户会更有激励去进行知识板块的问答、答题板块的竞猜、美食签到等板块的分享等等行为，自发地为整个生态的扩张贡献力量。

2018 年 2 月上线的网易星球，亦是我们所提的借助通证激励体系思维的一款产品。星球会给予用户原力（相当于动态的积分会员等级）和区块链积分“黑

钻”，原力值越高，可搜集到的黑钻越多，黑钻可用于兑换产品，而原力值则由用户通过完成各种行为任务（比如签到、分享、发现原创音乐、阅读资讯等）获得。进一步地，当更丰富多样的行为在网易星球上产生，用户在旅行、健康、教育程度、社交信用、娱乐、购物等偏好信息的数据价值就会沉淀在黑钻上。

3.5 周边服务层：交易生态变化，推动交易平台、钱包转型

区块链产业链上的周边业务目前主要包括数字资产交易所、媒体及社区、行情及资讯终端、数字资产钱包等，该部分周边业务属于行业的信息、资讯端口以及交易、资金汇集中心。**2018 年，这一领域最大的变化便是交易生态正逐步发生变化，并推动着交易平台、钱包、行情/资讯终端转型。**

（1）交易平台的去中心化、分散化

- **社区化管理模式的探索**

交易所当前形态为股份制，通过公司组织结构，实现有效分工，取得了规模效应和竞争效率，但仍受制于股份制弊端，面临潜在的用户、平台、供应商利益不一致等情形。而区块链世界的核心是社区，是共享，是充分调动参与者的积极性，实现多方利益的统一。**在这一浪潮中，交易所也在不断进行社区化探索，对社区有益的行为，将会得到社区奖赏；对社区有害的行为，将会受到惩罚。**目前来看，交易所的社区化管理模式改造，还主要在于资产端，即通过投票的形式筛选上线交易的资产：

资产端社区化管理典例

BINANCE **Binance**	最早由币安 Slack 社区爱好者建议，币安于 2017 年 9 月初开启每月的投票上币机制，每期筛选出 5 个通证品种参与投票上币活动，第一名可上线币安交易所。参与投票的用户每投一个通证品种需消耗 0.1BNB (可以选择多个币种，但有且仅有 1 次投票机会），另外，用户对每个通证品种的投票量依据用户的 BNB 持仓量而定，每个账户最高 500 票。

Huobi Next	Huobi Next 系原火币子品牌 Hadax 的升级，为火币交易平台业务社区化管理的 2.0 尝试，在资产端引入了投票上币机制。围绕 Huobi Next 形成了自助上币平台、区块链项目展示中心、推荐机构、合格投票者以及投资者共赢基金的生态，公开投票环节超出预先设置的达标投票数量的项目将获上币资格。
Etherfinex	Etherfinex 是 Bitfinex 专注以太坊生态的社区自治型交易所子品牌，项目在平台上建立与社区的沟通平台，社区用户在讨论区域对项目进行结构化分析和讨论。同时，Etherfinex 引入平台通证 Nectar，对在平台上交易的用户进行发放，而只有拥有 Nectar 的用户才可参与投票上币，决定上线的通证种类。

深度社区化管理典例

FCoin	Fcoin 从一开始就定位社区交易所，与上述主要在资产端进行社区化管理尝试不同的是，Fcoin 的社区化管理延伸到了更广泛的事宜，成立了社区委员会，社区委员会成员由 FT 持有者构成，包括平台方、投资机构、项目方、生态合作方以及个人投资者等，社区委员会有权草拟各类提案，并由社区公投。

来源：火币区块链研究院整理

不过综合来看，社区治理场景仍较为复杂，一蹴而就并不现实，我们可能会面临：（1）治理权之争：是谁带来更多的流动性，更有发言权，还是持有更多的 token 更有发言权，仍存争议，而这更像 PoW 和 PoS 之间的争论；（2）51%攻击：当恶意一方持有了 51%的 token，以社区 token 投票进行治理，是否还具有意义；（3）公地悲剧：如何调动 token 持有者投票积极性。

因此，为了避免社区治理陷于混乱，在社区化治理还并不成熟的情况下，**我们认为应当采用渐进式的社区治理模式，即“中心化+社区化治理”，再到“完全社区化治理”模式，以交易所场景中的资产端社区化管理为例，可采用：**

第一阶段：社区拥有否决权和决定权，由交易所初步筛选出项目，再由平台积分者持有者进行公投。最后，获得社区共识的项目通过；

第二阶段：社区民主阶段，弱化内部审核机制，交易所内部机构只负责协调，上币权移交给社区，由社区提交项目提案，社区投票决定。

- **共享深度的数字资产交易联盟出现**

与传统证券市场之中，某一资产仅在单一交易所交易不同的是，数字资产市场中，流动性是分散的，单一资产可在各个不同的交易所同时交易。虽然一定程度上，各地涌现的数字资产交易所，可以为当地的用户提供数字资产的购买、交易服务，但**不同的交易所之间，事实上也分割了流动性和深度，一个全球的、互通的交易池因而呼之欲出。**

2018 年 6 月后，全球三大主流交易所币安、火币、OKEx 均开始推出自己的“连锁加盟机制”，方便具备用户、资金但缺少研发、技术、安全等实力的团队实现“一站式开设交易所”，称之为“EaaS”(Exchange as a service)；另外，新兴数字资产交易所 BHEX，以及美国 SharesPost 推出的全球流动性和结算系统网络 GLASS 设计机制之中，亦有云交易所的身影：

OKEx 数字资产交易所 开放共赢计划	2018 年 6 月 19 日，OKEx 官网宣布正式启动数字资产交易所开放共赢计划，首期开放 100 个名额，锁定 50 万枚 OKB 的团队可报名，参与该计划成员有机会成为“OK 伙伴”。OKEx 将通过开放在数字资产交易领域积累的经验和技术给到“OK 伙伴”，进而打造一批自治的、高效的、透明的数字资产交易所。而任何想要创立数字资产交易所的团队，只需提供自己的域名、LOGO 以及运营主体，聚焦于交易所的管理和运营推广上，复杂的研发、运维等工作将由 OKEx 全球技术团队来提供全流程解决方案。同时，“OK 伙伴”之间将共享深度。
币安 数字资产交易所 开放联盟计划	2018 年 6 月 21 日，币安宣布，将在全球局部地区试点启动“数字资产交易所开放联盟计划”。 参与联盟的成员将获得币安在数字资产交易领域积累的撮合系统、管理系统、冷钱包系统、热钱包系统、资金清算系统、全球多语言的客服支持，首期 1000 家将采用平台通证的运作模式，需锁仓 10 万 BNB。
火币云	7 月 20 日，火币集团"火币云"业务正式上线，通过技术服务允许用户在火币现有平台上构建数字资产交易所，第一期采取 5/5 分佣合作模式，前 1000 个合作伙伴 0 费用，0 押金，免费培训，需要质押 50 万 HT。与 OKEx 数字资产交易所开放共赢计划、Binance 数字资产交易所开放联盟计划不同之处在于，火币云提供的是围绕数字资产交易的一整套生态系统服务，将提供 OTC、币币交易、运营和生态四大解决方案。

来源：火币区块链研究院整理

公有云交易所模式是一种底层基础的共享服务，先共享庞大的基础设施，然后再共享交易深度。从新生数字资产交易所角度来看，初期面临的最大问题都是

交易深度和流量问题，没有一个强大的信用背书和激励方式很难吸引大量的用户群体，加上技术门槛和安全防护以及用户体验的影响，初生的数字交易所存活率并不高，**且做一个交易所其实是需要巨大投入的。**

不过，交易系统、安全机制等基础设施方面的投入是具有共通性的，实际可以进行共享和输出，这就构成了云交易所以及“EaaS”(Exchange as a service)服务的基础，可大大节省新团队的投入成本，而共享的交易深度，则是解决了初期的交易深度和流量，保证启动顺利。虽然某种程度上也存在交易所技术服务商可提供同类服务的可能性，但由于无法解决交易深度和流量，在提供的价值规模上，仍略逊于交易所的“EaaS”。

（2）钱包交易所雏形：Dapp 与通证的高频交互场景

2018 年，随着 Dapp 应用落地推进，数字资产的作用正慢慢从纯交易走向应用，而流量入口也正慢慢从交易所转移至钱包，其不仅能快速接入各类 Dapp，也能实现 Token 兑换，**原本只是用于数字资产存储的钱包，正变为钱包交易所。**

目前，根据钱包提供的交易相关类服务的轻重程度，主要包括如下五类：（1）行情资讯服务；（2）资产聚合类服务；（3）交易及兑换类服务；（4）理财、借贷服务；（5）POS 挖矿服务。

- **行情资讯服务**

钱包内置丰富的新闻资讯、行情快报、项目简介、K 线图、大额资金流动监控、代码活跃度等数字资产市场行情信息。

区块链项目的资讯和行情信息是通证持有者与市场保持同步的需求，也是集聚用户流量的大入口，钱包产品若能很好地集成资讯行情服务不仅能对现有用户产生足够的黏性，还可以带入更多的增量用户。不过资讯行情服务需要投入一定的人力财力，会较大地增加产品的运营成本。目前大部分钱包集成的新闻资讯服务并不是很完善，主要以提供行情信息为主。

- **资产聚合类服务**

此类钱包可为用户提供资金聚合服务，通过 API 接口将用户在多个钱包和交易所的通证持有情况进行汇总聚合，对于 API 接口服务支持度不佳的平台也可以采用手动维护进行初始输入。

这主要是由于，目前各大交易所以及钱包平台种类较多，每个交易所以及钱包支持的数字资产品种都不一样，因此用户的资金通常会分散到不同的平台，不利于集中管理和查询，因此聚合类服务能较好地满足用户查询的需求。这类钱包需要配合众多交易所、钱包等进行 API 接口开发，存在一定的开发和维护成本。

- **交易及兑换类服务**

钱包内置数字资产交易功能，有接入中心化交易所平台的钱包，如 BitPie；也有接入去中心化交易平台的钱包，如 Imtoken；还有接入 Bancor 机制自动化交易平台的钱包，如 Tokenpocket。有的钱包推出“闪兑”功能，即不同 Token 之间按照一定“汇率”进行互换，其后台通常也是用了去中心化交易模式进行货币的兑换。

钱包用户天然拥有交易需求，若 Token 不用提出钱包就可以实现交易，不但减少了用户提币转币的操作步骤，减少了犯错的概率，也增强了用户黏性，为钱包项目的后续转型提供了很好的发展方向和资金沉淀。不过内置交易所极大地增加了系统的复杂度，为本身对安全性要求较高的钱包类产品引入了更大的风险，用户资金安全性将受到一定程度挑战。

- **理财、借贷服务**

钱包内置理财模块，理财类型包括长期固定收益型，余币宝短期灵活型，数字资产 P2P 融资借贷型，抵押贷款型。目前这些理财模块有的是接入第三方服务，本身不参与提供理财服务；有的是为本身平台的发展提供廉价资金而开发的理财产品，由平台收益来支付用户收益；有的则是将平台募集的数字资产再投入一级或二级市场交易以此来获取超额收益并支付用户收益；还有的则是提供点对点的数字资产借贷交易服务，为资产需求方和提供方提供撮合服务。

对于长期持有的用户来说，数字资产理财服务切中刚需，持有也能获得收益，目前各类钱包提供的理财产品年收益率在 4%~20%不等。不过区块链行业发展迅速，数字资产市场波动性较大，流动性不佳的理财产品将面临更大的风险。且目

前数字资产理财市场并不成熟，还未出现行业标杆性龙头企业，风险控制经验和能力以及兑付能力还待市场考验。

- **POS 挖矿服务**

对于支持 POS 共识算法的区块链项目，一些钱包提供锁仓加入 POS 挖矿服务，挖矿收益将定期发送给用户。

通常由钱包项目方提供 POS 挖矿的主节点，符合一定资金要求的数字资产可参与 POS 挖矿，有固定锁定时间挖矿，也有支持随时可赎回的挖矿模式，钱包项目方将从挖矿收益中按比例抽取分成，钱包项目方和用户都能有较为稳定的额外收益。目前支持 POS 挖矿较多的币种有：达世币 DASH，莱特币 LiteBitcoin，小零币 ZCoin，量子链 Qtum 以及超级现金 Hcash。

基于以上提供的各类偏交易类的服务，目前钱包的盈利模式如下表所示：

类型	盈利模式	概述
热钱包	交易手续费	对于内置交易所的钱包，交易手续费将成为收入的主要来源，无论中心化或是去中心化交易方式，钱包项目方都可从中获得收益。
	资产管理费	钱包可提供资金托管或理财服务，并从中收取管理服务费。如 COBO 提供 POS 挖矿资产托管服务，并收取一定的资产管理费用。
	法币通道手续费	在允许法币直接购买数字资产的国家，服务商通常会收取一定的数字资产转换服务费。如 Coinbase 会根据国家/地区收取 1.5-4%的转换费。
	第三方服务费	对外提供 SDK 接口收取第三方服务手续费。如提供支付接口，并收取手续费。
	广告费	对于内置的广告或者 DAPP 收取一定的推广费用。
冷钱包	设备销售收入	与热钱包不同，冷钱包收入来源主要为硬件钱包销售收入。如 Trezor 的主要收入来源为冷钱包设备销售收入。

来源：火币区块链研究院整理

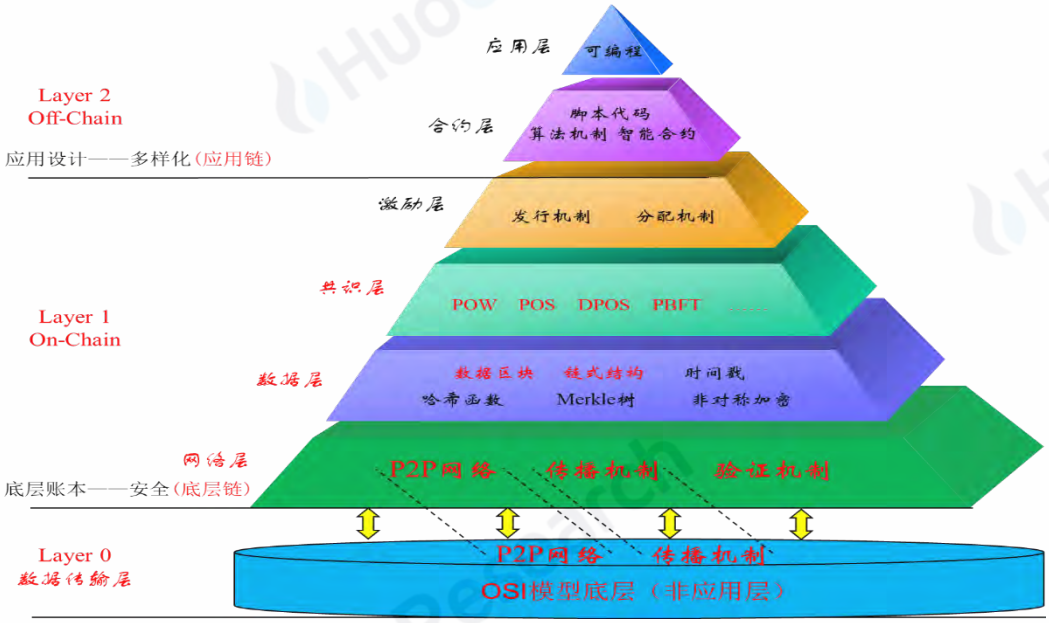
四、区块链技术发展解读

4.1 可扩展性解决方案动态梳理

2018 年系对第三代区块链技术探索的一年。当前，以太坊为代表的区块链底层可扩展性有限，难以支撑大规模的应用落地。而可扩展性最直接的表征一般采用 TPS（Transactions Per Second）来间接描述，代表了系统每秒能够处理的业务量，是衡量系统吞吐量的核心指标。于是，众多项目在对标以太坊图灵完备智能合约的第二代技术上不断提升 TPS。典型代表就是 6 月份上线主网的 EOS.IO。

我们借鉴计算机网络分层管理、各层标准化设计思想，将区块链与传统互联网 OSI 模型结合，建立了目前区块链技术可扩展方案的分层模型[2]，包含了**三个一级层级：Layer 0 层数据传输层，Layer 1 层 On-Chain 公链自身（底层账本）层和 Layer 2 层 Off-Chain 扩展性（应用扩展）层。**在此基础上，结合区块链架构又可以进一步分解成**七个二级层级**来梳理可扩展性的解决方向：

图 26：区块链扩展性分层解决方案



来源：火币区块链研究院整理

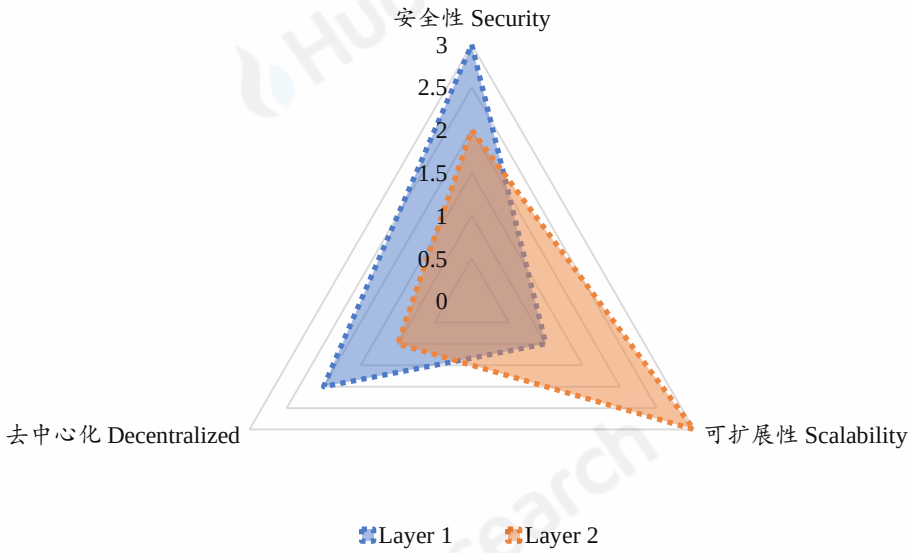
- **Layer 0 层数据传输层与传统 OSI 七层模型对应，负责优化区块链与传**

[2] 详细介绍请参考《火币区块链产业专题报告-区块链技术可扩展方案分层模型》

统网络的结合问题。区块链是整个互联网协议层中的最上层，本身还是要依赖于底层的协议为它工作，虽然在比特币 P2P 网络设计的时候已经考虑了节点之间的发现、节点连接的握手协议、节点间地址广播和数据通信等，鉴于已经有部分项目开始探索 P2P 网络与传统 OSI 模型的结合，甚至将改进延伸到数据链路层，本报告倾向将 P2P 网络和传播机制并入到 Layer 0 层和传统 OSI 模型一起作为一类可扩展方案进行归类；

- **Layer 1 层解决底层账本问题**，负责安全，妥协性能，注重于记账功能。结合区块链架构，Layer 1 层可以分解成四个二级层级，从网络层的验证机制上使用诸如分片技术去优化，从数据层的数据区块使用诸如隔离见证和链式结构上使用 DAG 等技术去优化，从共识层的共识机制去优化；
- **Layer 2 层解决广义应用问题**，主要负责性能，妥协去中心化，注重于计算功能。结合区块链架构，Layer 2 层可以有两个二级层级，通过跨链、状态通道、Plasma、TrueBit 等多链并行、链上链下结合甚至是中心化的方式来满足性能需求，借助 Layer 1 层来保证安全。

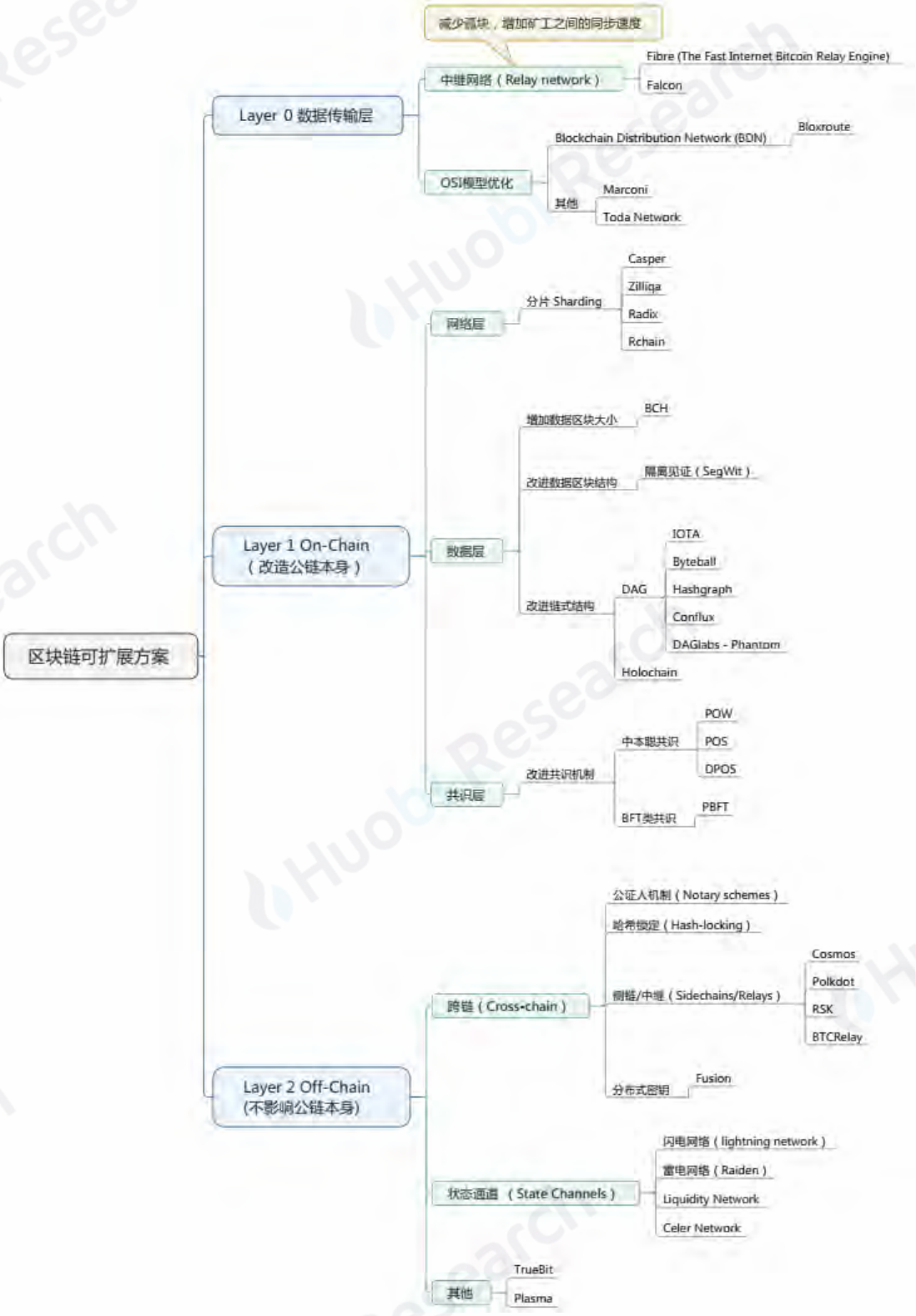
图 27：Layer1 与 Layer2 三角性能展示图



来源：火币区块链研究院整理

目前，涉及不同层级的区块链扩展性解决方案的典型项目众多，汇总如下：

图 28：区块链扩展性解决方案项目汇总



来源：火币区块链研究院整理

不过，就目前来看，我们认为区块链扩展性的提升，并不是独立依靠某一种解决方案所能实现的，而是更适合采用分层的思路，并拓展至公链体系本身的设

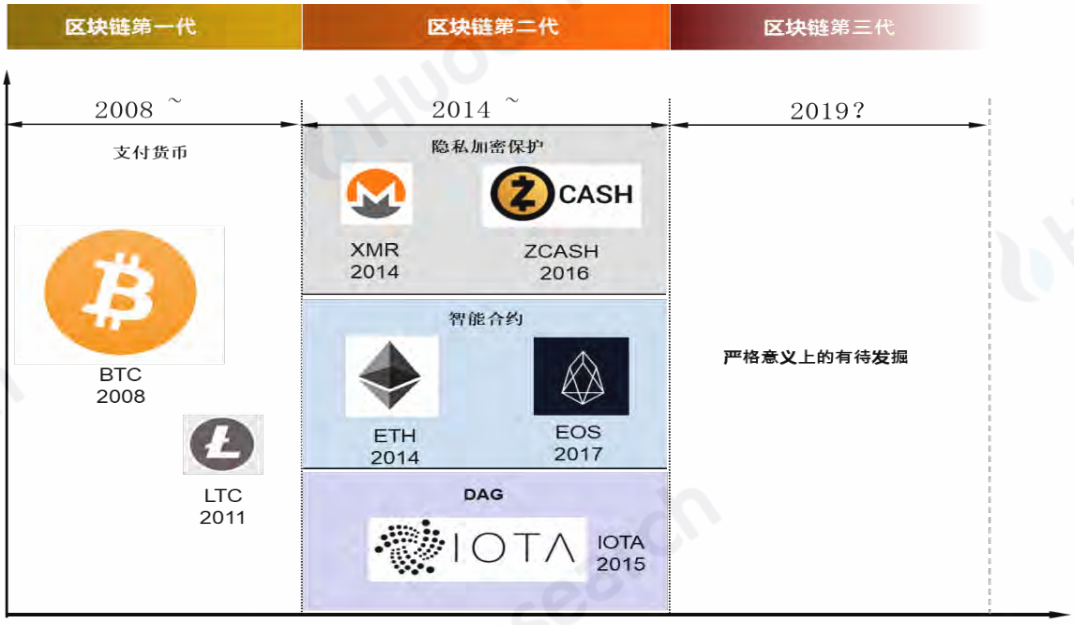
计之中。而从分层的角度去设计一个区块链项目，可以有效的规避区块链的三元悖论问题：**Layer 1 层主要负责安全，妥协性能，注重于记账功能；Layer 2 层主要负责性能，妥协去中心化，注重于计算功能，Layer 1 层底层设计时就充分考虑好 Layer 2 层的交互问题。**

实践证明，以太坊社区的 ETH 2.0 也是朝着这个思路进行的，通过分层处理，各取所需，达到动态平衡。而 Loom Network 做为以太坊上 Layer 2 层扩展技术 Plasma 的典型代表，也将自身定位成跑在以太坊上的 EOS，可见**不仅仅是技术上的分层，包括公链的应用也出现了分层、分场景、分垂直行业的细分苗头。**

4.2 隐私性解决方案的升级迭代

我们一直认为，如今，从区块链技术的发展上看，普遍公认的主要有两个阶段：一是以比特币（BTC），莱特币（LTC）等为代表的作为支付货币的第一代区块链；在第一代的基础上，第二代区块链包括智能合约、隐私保护和 DAG：

图 29：区块链三个阶段发展历程



来源：火币区块链研究院整理

（1）隐私保护技术动态进展及分析

隐私加密保护技术也一直是个热门的方向和刚需，根据区块链技术的特点，**目前隐私保护机制主要针对两个方向：传输网络的隐私保护和交易/内容的隐私保护，其中交易/内容的隐私保护就包含了大家常提到的匿名币功能：**

传输网络的隐私保护主要通过阻止攻击者依据发现网络拓扑而获得身份隐私信息，将区块链运行在具有隐私保护特性的网络上：

- 例如洋葱网络（Tor，The Onion Network），通信数据首先被多层加密然后再由若干个被称为洋葱路由器组成的通信线路上传播，每个 Tor 节点只知道最少相关信息，传输时，逐个节点类似剥洋葱皮一样逐层解密，只有最后一层节点会相对脆弱，直接暴露容易受到关注，但是发送者的真实 IP 等到了很好的保护；
- 除了 Tor 之外，门罗币采用了另一种替代 Tor 的匿名通信协议 I2P，相对于 Tor 协议使用同一条网络链路实现数据的发送和接收，I2P 使用多条链路发送数据和接受数据，能够更好的隐藏 IP。

交易/内容的隐私保护则主要有混币、环签名、零知识证明、同态加密和安全多方计算等：

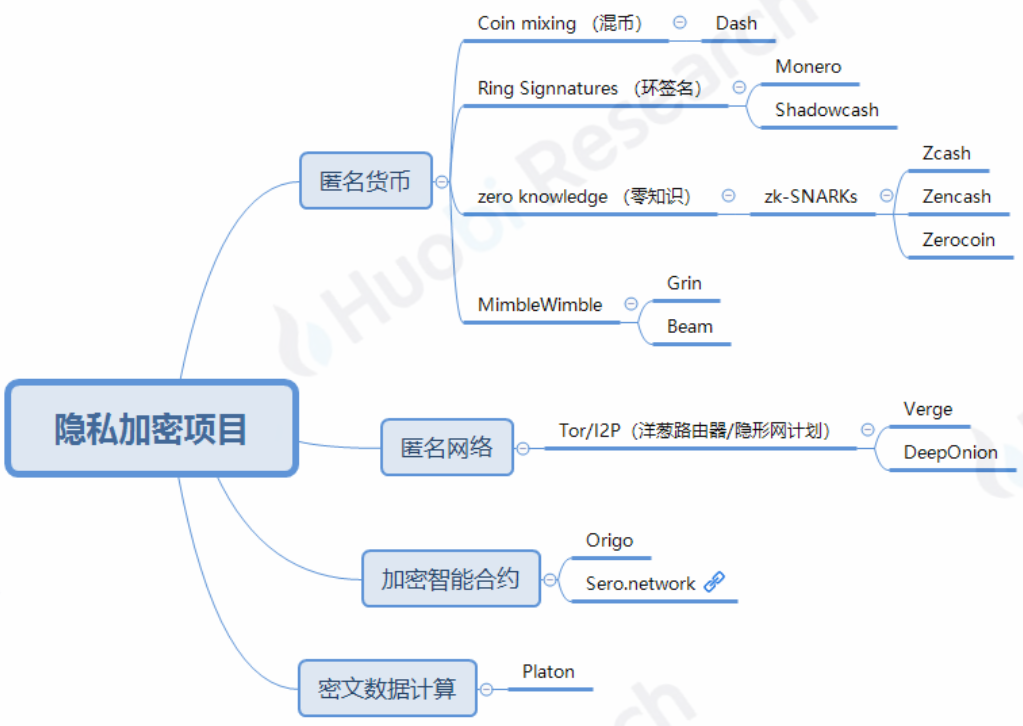
- 混币主要是打乱输入输出之间的关联性，将大量的输入和输出全部混淆在一起，这样就很难发现一一对应关系，但它的本质并不是基于密码技术，更像是物理反应；发展初期会基于可信中介，然后逐渐演变成去可信中介的机制 CoinShuffle、TumbleBit 等，典型代表就是 Dash 项目；
- 环签名是环中一名成员利用自己的私钥和其他成员的公钥进行签名，整个过程不需要征得其他成员的允许，验证者只知道签名来自这个环，但不知道谁是真正的签名者，特性可以简称为“拉你入环、与你何干”。它解决了对签名者完全匿名的问题，允许一个成员代表一组人进行签名而不泄漏签名者的信息，典型代表就是 Monero 项目；
- 零知识证明属于密码学技术，可在不泄露数据本身情况下证明某些数据运算真实性，它允许两方（证明者和验证者）来证明某个提议是真实的，而且无需泄露除了它是真实的之外的任何信息，典型代表 ZCash 项目；

- 同态加密是一种无需对加密数据进行提前解密就可以执行计算的方法，应用场景多为安全外包计算；
- 安全多方计算是解决一组互不信任的参与方之间保护隐私的协同计算问题，它要确保输入的独立性，计算的正确性，同时不泄露各输入值给参与计算的其他成员。应用场景如电子选举、电子投票、电子拍卖、秘密共享、门限签名等。

（2）基于隐私保护技术的区块链应用动态与分析

上述经典的传输网络的隐私保护和交易/内容的隐私保护技术在应用场景上有衍生出了**匿名网络，匿名货币，加密智能合约，密文数据计算等应用，2018 年，相关项目体系逐步成熟：**

图 30：区块链隐私加密项目汇总



来源：火币区块链研究院整理

而上述项目之中，**2018 年最为引人注目的便是基于 MimbleWimble 的匿名货币 Beam 和 Grin。**MimbleWimble 技术于 2016 年就已出现，系**基于混币和同态加密的全同态（加法和数乘操作）思路**，并结合 UTXO 来对比特币交易的隐私性予以改进的隐私技术，最终精髓落在了 Pedersen 承诺（C = r*G + v*H）上。

2016 年 7 月 19 日，Tom Elvis Jedusor 将 MimbleWimble 白皮书放入比特币研究频道并消失；后来 Ignotus Peverell 启动了一个名为 Grin 的 Github 项目，并致力于将 Mimblewimble 论文落地；Blockstream 的 Andrew Poelstra 在 2017 年斯坦福 BPASE 大会上展示了这项工作，之后 Grin 开始受到很多主流关注，Grin 在 2019 年 1 月 15 日主网上线；同时在 2018 年 4 月又出现了另一个 Mimblewimble 项目 Beam，它是 C++从头开始写，并于北京时间 2019 年 1 月 3 日 22：00 上线。

4.3 互通性、跨链技术进展解读

随着越来越多的公链涌现，单一的链已难以支撑起人们日益多样化的区块链应用需求，跨链势在必行。**目前的区块链世界就好比互联网时期的单机时代，链与链之间高度异构化，彼此难以互通，所有的数据和服务都局限于孤岛式的区块链中**。未来，或许各个区块链系统能通过某一标准化跨链协议进行链接，区块链系统间能协同工作，为更多的用户、更多的服务提供支撑。不同的是：**互联网是信息自由流通的网络，而区块链跨链网络则是价值自由流通的网络。跨链技术的成熟将成为价值网络时代到来的充分条件。**2018 年，跨链领域动态动态如下：

（1）跨链功能目前基本已成公链类项目标配

2018 年是一大波公链项目落地的元年，除了解决目前底层平台性能低等问题，各公链项目也将目光不约而同地投向了跨链网络的方向。经火币区块链研究院整理分析，**目前市值 TOP100 的平台类项目中，有约 65%的项目将支持跨链功能、侧链/子链，或提供跨链相关接口和协议，为平台未来的可扩展性早早打下基础。**

未来，谁的链能更好地与其他链兼容，更好地支持跨链互通将成为影响其生死存亡的关键因素。孤掌终究难鸣，还需兼容和互通打通生态圈，这意味着能链接更多的资源和用户，有更多引流渠道，生态建设也将更水到渠成。

（2）跨链资产互换逐步向跨链资产转移发展，但还有待成熟

跨链资产互换通常指两条链上的不同用户之间进行资产互换，但每条链上的资产总量并无增减，只是资产所有权发生了变化，且这个所有权改变的过程需在

两条链同步发生。跨链资产转移，是资产价值的转移，各链中可用的资产总量将相应增加或者减少，即真正将资产从一条链转移到了另一条链。

跨链资产互换的实现较为简单，只要保证两条链之间的交易为原子交易即可，通常通过哈希时间锁技术实现，例如比特币闪电网络，以及部分跨链项目均实质上采用的均是这种技术；这种模式的跨链需要用户同时在两条链上都有账号，仅仅能实现资产交换。而**跨链资产转移的实现难度就相对大很多，在保证原子交易的基础上还需要确认在两条链上的交易有效性，可以通过公证人、中继或是槲卯模式来具体实现**[3]。资产转移的模式实现了资产真正在链间的流动，可实现跨链资产交易、跨链钱包、跨链交易所、跨链预言机等多种功能。

随着跨链价值流通需求的日渐强烈，去中心化跨链交易所、跨链钱包的呼声越来越高，跨链资产互换的简单功能已难以满足未来可能爆发性的资产转移需求，跨链资产转移功能已成为跨链项目的必要功能。**但是该技术目前还并不成熟，未经历过时间的检验，也未大规模应用过，安全层面存在较高的风险。**

（3）2018 年，三大类跨链项目开始落地

2017-2018 年是跨链项目启动之年，诞生、落地了一批以跨链平台、侧链平台或者母子链平台为主题的项目。主要包括三大类跨链项目：

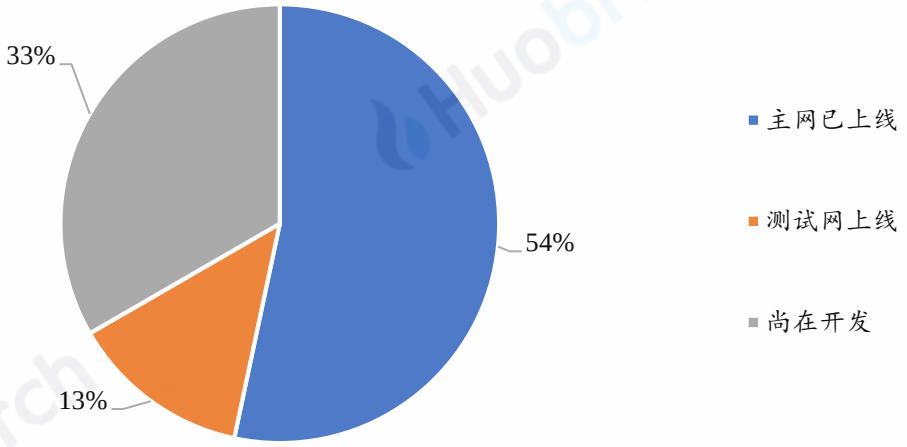
- 一类是想通过**侧链或子链**的设计实现底层平台的交易扩容，支持高并发、高 TPS，以 Loom Network、Liquid、Lisk、Aelf 等为典型；
- 第二类是搭建**主动兼容型跨链**平台，主动去兼容已有的区块链项目，他们通常是有不同数据结构、不同共识机制的异构链，并会一条一条地去适配已有的异构链，将其接入到跨链平台，Wanchain 是该类项目的典型；
- 第三类是建立**被动兼容型跨链**平台，为区块链项目建立一个同构化的底层平台，基于这个平台可快速开发独立的区块链并可方便地促成跨链互联，实现被动兼容，Cosmos 和 Polkadot 是这类项目的典型代表。

2018 年，从跨链项目的开发进度来看，约 54%的跨链项目已上线主网。也有 33%的项目还在开发过程中。**目前主网上线的项目以第一类和第二类项目为**

[3] 详细介绍请参考《火币区块链产业专题报告-跨链篇》

主，即侧链/子链和主动兼容跨链平台项目为主，第三类项目难度系数较大，有望在 2019 年主网落地，若其被证可行，则将为我们打开区块链跨链网络一扇全新的天窗，新的价值网络雏形或将诞生。

图 31：跨链项目落地数量比例汇总



来源：火币区块链研究院整理，以 2018 年 12 月底为基准

4.4 区块链以外分布式账本技术动态

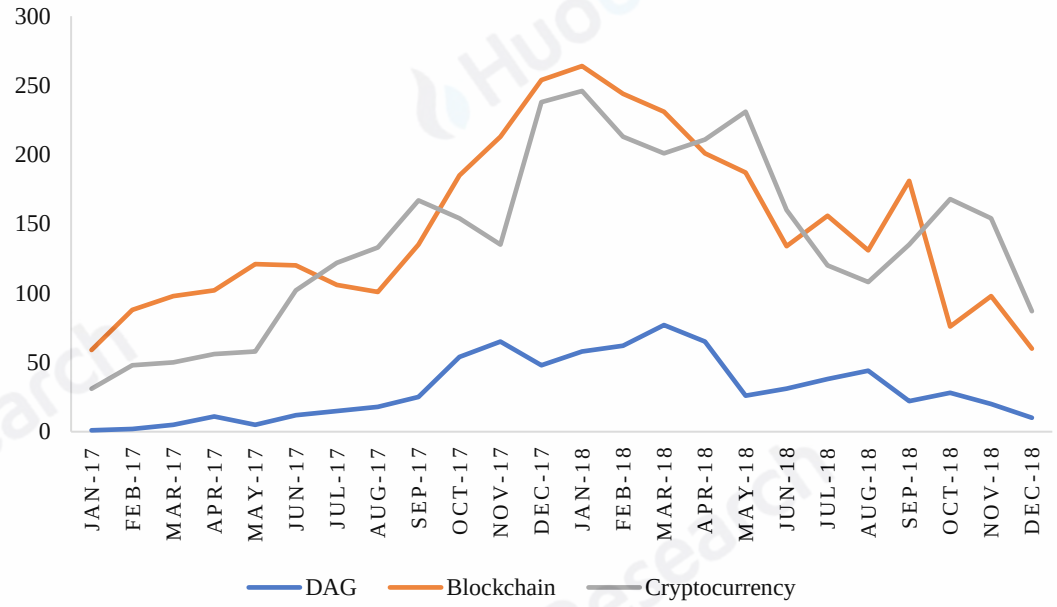
区块链是一种分布式账本技术，而分布式账本技术却不局限于“区块链”这一种具体技术体现形式。为了改进原有技术、满足更多的实际业务应用场景，更多的分布式账本技术正在被探索和应用当中。其中最重要的便是 DAG：

（1）DAG 的另辟蹊径，1.0 版本回顾

DAG（Directed Acyclic Graph，有向无环图）是目前除了“区块+链”式结构以外的另一种用于实现底层账本技术的数据结构，表现为一张有向图，并且从图中的任意顶点出发都无法回到该点（无环）。基于 DAG 的分布式账本技术在近年来被提出后，被认为有希望替代狭义上的区块链技术。对比传统区块链网络，每个区块中有很多笔交易，矿工打包好后统一发送；DAG 网络中并没有“区块”概念，最小单元是“交易”。**DAG 就是通过这种方式来突破扩展性的限制。**

DAG 的概念在 2018 年受到了相对较高的关注度。我们在 Reddit 上进行了词频统计。可以看到，DAG 的相对热度在 2017 年底和 2018 年一季度相对较高，前者与 DAG 1.0 项目 IOTA 于 2017 年底市值快速爆发有关，而后者与部分 DAG 2.0 项目在一季度开始逐步涌现有关：

图 32：DAG 词条热度变化图



来源：火币区块链研究院整理

（2）从“DAG 1.0”向“DAG 2.0 ”发展

DAG 的发展其实和狭义上区块链技术的进展是有类似之处的，即早期的一些 DAG 项目和狭义的第一代区块链都是以**支付作为其主要手段**的，而当 DAG 实现智能合约等较强可编程功能支持以及实现较高的交易扩展性后，可认为其进入第二代的阶段。**2018 年，DAG 技术即处在从 1.0 向 2.0 的发展阶段。**不过这一演进过程并不顺利。DAG 尽管具有异步、高并发的特性，**但在具体实现上仍然需要考虑到共识、智能合约等问题的具体解决方法**。2018 年，DAG 技术正在这些问题上在探索新的解决方案。

- **共识问题及解决尝试：**

DAG 异步通讯的特性一定程度上提高了双花攻击的可能性。除了 IOTA 的 Coordinator、Byteball 的 Witness 等比较经典的解决方案以外，不少 DAG 项目在尝试用新的思路来解决这类技术问题：

- 一些项目，例如 HyCon、Conflux 等是通过传统的 PoW 并采用 SPECTRE、GHOST 等策略来实现共识；
- 还有一些项目，如 Logos Network，是通过拜占庭共识协议或综合多层共识的方式来解决一致性问题；
- 另一些项目，如 Mixin 等，是在共识的基础上加入了 TEE（可信执行环境）来进一步增强安全性及交易可靠程度。

智能合约实现问题及解决尝试：

另一个在实现 DAG 时需要关注的重点是可编程性或智能合约的实现。由于 DAG 自身特性，智能合约的实现存在一定难度。目前的解决思路包括**首先实现非图灵完备的智能合约或可编程脚本**，或者采用**类似 Layer2 的分层理念，将智能合约运行在更高层次的子链、侧链或状态通道内**，底层仍然使用 DAG 来实现 Layer1 的账本扩展。

不过整体来看，DAG 类项目在 2018 年整体进展并不快：已实现“DAG 1.0”的项目在努力加入可编程的扩展特性；一些原先就定位在“DAG 2.0”上的项目，一部分推迟了主网上线时间，另有一些则仍然依赖于主链或 Witness 等中心化的方式来运行测试网。这些探索的结果都有待在 2019 年进一步观察。

五、年度回顾与未来趋势展望

5.1 2018 年度十大影响力事件盘点

2018 年度，万众期待的区块链经历了由狂热到理性的转变，中间起起伏伏，发生了一系列的重大事件，火币区块链研究院筛选了我们认为最具影响力的十大事件，进行了盘点和点评，具体如下：

1、EOS.IO 掀超级节点竞选热潮，DPOS 机制受热捧

2、“交易即挖矿”模式的兴与衰

3、EOS Ram 启示，人机交易/IBO 雏形，但 IBO 未如期爆发

4、Fomo3D 引发 Dapp 游戏思考

5、传统巨头开始布局区块链领域

6、区块链公司拥抱传统资本市场

7、USDT 面临信任危机，合规稳定币出世，而算法稳定币出师不利

8、监管不再限于纸面，落地执行开始，并以美国为典型

9、谁是真正的信仰者，从 BCH 分叉看公链治理

10、安全、黑客事件频发，区块链安全机遇显现

（1）EOS.IO 掀超级节点竞选热潮，DPOS 机制受热捧

EOS.IO 被认为是区块链 3.0 的代表，致力于为商业级分布式应用提供底层设施。其主要通过“DPOS”共识机制以提升区块链平台的扩展性和吞吐量，并以独特的“超级节点”模式席卷了整个市场，吸引了大量资金：区块生产者（俗称**超级节点）总计 21 个，通过投票从所有候选人中选出，可分享每年 EOS.IO 网络增发的 5%EOS 通证中的一部分（目前为 21 个节点平分 0.25%部分，及所**

有候选人平分 0.75%部分），但作为交换，节点需为整个网络提供算力，投入足够的服务器硬件，承担收集、验证网络交易信息并进行记账和维护账本的职能。

以“代议制”这种间接式的民主，通过 21 个代理人实现小范围达成共识，是这种机制最为核心的特性，其以牺牲一定的去中心化为代价，实现了相对更高的效率。而继 EOS 之后，包括 Tron、Cybermiles 和 Ontology 为主在内的公链项目都纷纷开始模仿并推出了自己的节点竞选计划，同时为了鼓励更多参与，或多或少降低了竞选门槛，一时间，DPOS 这种“效率—去中心化”妥协均衡模式，得到了市场追捧。然而我们也必须看到，DPOS 机制本身并不一定是完美的：

- **“公地悲剧”**

对于大部分通证持有者来说，其利益并不一定与真正的社区一致，或者说很多对社区有益的提案并无法真正激励通证持有者去投票，投票参与率较低，发生“公地悲剧”。而真正愿意进行投票的，大多是参选的节点本身，因为可以通过成为记账节点而获取出块收益，对于普通通证持有者来说，是没有激励的。这种情况下，投票的有效性会打一定折扣，而选出的记账节点，可能亦并不是最优的。

- **潜在的联盟和集聚效应**

由于 21 个节点轮流记账，并获得出块收益，随着时间推移，节点实际上会越来越倾向于固定，并倾向于形成相对稳固的几个联盟。一方面，新增的通证会被分配给这些记账节点，使其在投票中会越来越具备优势，另一方面，一票多投的机制，让节点之间更倾向于合作和结盟，而若采用一票一投，虽可一定程度避免结盟的情况，但却可能因为投票率过低，以及放大大户的投票权重，而失效。

综合来看，公链治理机制的设计永远是一个让人热议和探讨的话题，即便是更去中心化 PoW 机制，也会倾向于决策权、主导权被矿工、矿主所掌握，有的，只是利弊的权衡去取舍。

（2）“交易即挖矿”模式的兴与衰

“交易即挖矿”把用户在平台上的交易行为视为一种“挖矿”行为，并以此发行平台通证。具体来说，用户在平台上交易产生的手续费部分或全部通过等值平台通证的形式返还给用户，**其本质类似用户通过手续费持续不断认购平台通证**

和 0 成本的“免手续费交易”活动。而采用“交易挖矿”模式的交易所，其平台通证的主要价值在于能够获得平台手续费收入分成，用户按照账户中持有平台通证占已流通平台通证（已挖出或已解锁）的比重获取分成。

“交易挖矿”模式始于新加坡数字资产交易所 DragonEX，其于 2017 年 11 月发行平台通证 Dragon Token，但被真正热捧始于 2018 年 6 月 Fcoin 交易所的横空出世，仅仅半个月时间，成为了全球交易量最大的交易所，并带来了一大波的模仿者，主要包括**进行交易挖矿改造的交易所**和**新兴设立的挖矿交易所**两类：

来源：火币区块链研究院整理，其中部分交易所已取消“交易挖矿”

然而经过一段时间后，“交易即挖矿”模式难以为继，很大一部分挖矿交易所均出现了交易量、平台通证价格双跌的死亡螺旋。究其本质来看，“交易挖矿”+“手续费分成”模式下，通证具有类股权性质，价值主要源于可获得的预期手续费分成的折现。而根据“资产价值=负债价值+权益价值”公式：

- “资产价值”即平台整体预期手续费的折现值
- “权益价值”即通证的总市值，是通证持有者可获取的手续费分成部分
- “负债价值”即给予通证持有者之外的手续费分成部分（团队、运维等）

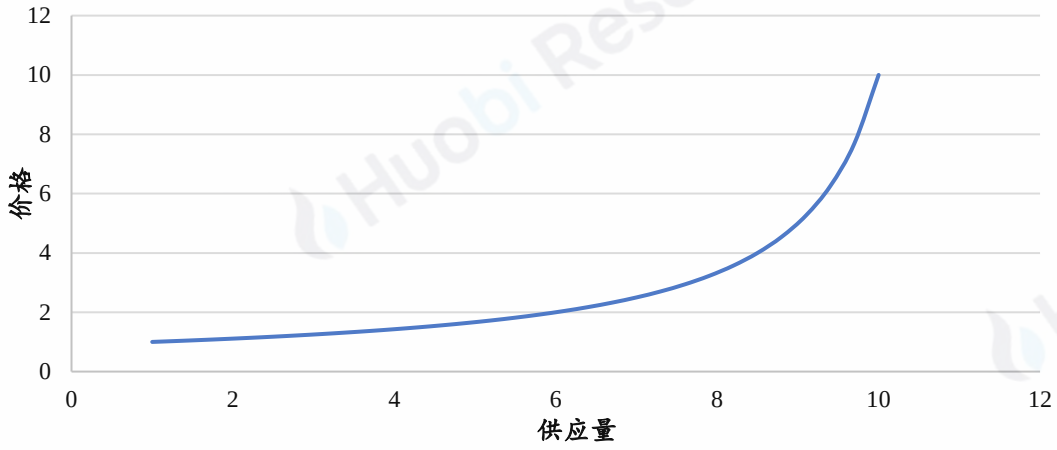
“交易挖矿”模型中，在平台通证不断发行的前提下，要求左端资产价值不断增加，且至少快于平台通证发行的速度，才可以支撑单位通证的价值。而左端资产价值取决于平台交易量以及手续费比例之积，是内生的，极易与通证价格相互影响，通证价格上涨，挖矿具备吸引力，交易量提升，进一步推升单位通证价值，而价格下跌，挖矿吸引力减弱，交易量减少，进一步拉低单位通证价值，进入死

亡螺旋。可以说，交易挖矿更多适合于一种短期的冷启动或营销，而若持续运作，长期来看，在机制上是存在极大不确定性和风险的。

（3）EOS Ram 启示，人机交易/IBO 雏形，但并未如期爆发

RAM 全称 Random Access Memory，即随机存取存储器，可通俗称呼为“内存”。EOS RAM 是 EOS.IO 中基础资源的一种。在 EOS.IO 中，RAM 主要用于存储账户信息和智能合约执行信息等数据，需要通过交易和购买获取。**而与传统的人与人之间发生交易不同的是，RAM 的交易被设置成了人机模式**，设计原理参考了 Bancor 算法。简单来说，**RAM 剩余量越少，RAM 的价格越高，RAM 的价格是严格按照公式推导计算出来的，这保证了交易的即时性和深度，并为市场提供了近乎无限的流动性。**此计一出，引发了市场对这样一种公平、透明、自做市的人机交易模式的极大期待，认为 RAM 实质上奠定了人机交易的雏形，甚至衍生出了名为“IBO”的这样一种必须质押资产才能发行新资产的模式。

图 33：RAM 价格与 RAM 供应量曲线变动关系



来源：火币区块链研究院整理

然而事实上，以 RAM 为首的人机交易，在经历了前期的火爆后，并未持续下去。RAM 本质是系统内的资源，更多代表的是使用型需求，而其前期的火爆，更多是市场资金看到其未扩容情况下的炒作空间所带来的一种结果，当 RAM 持续扩容后，炒作空间不再，便回归了常态，与 Dapp 的生态发展本身挂钩。具体 RAM 价格变化示意图如下（最高接近 1RAM=1EOS，目前 1RAM=0.06EOS）：

图 34：RAM 价格变动示意图

来源：Tradingview、FeeXplorer

不过，截止目前，市场上亦未出现更多类似 RAM 的人机交易案例，我们认为主要原因在于，适合采用 Bancor 算法人机交易的通证必须要符合：Token 的价格必须可由公式计算，系统账户内的准备金无法被转移，不需要跨链，**而符合上述条件的通证本身较少**，需要是**衍生型通证**或**锚定型通证**才可以：

- **衍生型通证：**RAM 本身作为一种 EOS 系统内的资源，并不需要额外进行募资，就是一种衍生型 Token。发行方首先设计衍生 Token 和主 Token 之间的价格兑换曲线，然后设置系统账户和智能合约，然后就可以发行可与主 Token 自由转换的衍生型 Token。衍生型 Token 不存在流动性问题，而衍生型 Token 需要使用主 Token 购买，会促进市场对主 Token 的需求，并且大量主 Token 存在系统账户内，会让主 Token 的流通量减少。
- **锚定型通证：**和主 Token 有锚定关系的 Token 也可以使用 EOS RAM 的人机交易模式进行交易。比如 Bitcoin Cash 社区曾提出一种虫洞协议，用于解决主链上的智能合约问题，并发行了 Token WHC。WHC 和 BCH 锚定，兑换比例为 100：1。如果是通过 Bancor 算法设计出一种锚定型 Token，可以突破原来固定比例的限制，并且自由兑换和转账。

另外，“IBO”作为一种采用 Bancor 算法的通证发行方案，并未得到市场的广泛认可，我们认为也是有如下的原因：

- **项目方难以获得所有或至少部分资金，融资功能不顺畅。**理论上，使用

Bancor 模型发行通证的团队是无法获得任何资金的，因为所有投资者用于购买通证的资金都存在系统账户中（例如，所有用于购买 RAM 的 EOS 都存在 eosio.ram 这个账户中）。不过，项目方确实也可以通过调整 Bancor 的曲线来实现部分募资，但整体融资功能并不顺畅。

- **只解决了流动性、深度问题，但并不解决背书问题和合规问题。**Bancor 模式很好解决了创业项目早期的通证流通性不足和做市问题，然而，“IBO”并无法解决资产发行涉及的合规问题，亦无法给项目质量增加背书，在数字资产发行监管强化的趋势下，“IBO”难以独善其身。

（4）Fomo3D 引发 Dapp 游戏思考

7 月，一款基于以太坊的 Dapp—“Fomo3D”火遍全网。从 7 月 4 日正式上线，至 7 月 21 日活跃度达到顶峰，Fomo3D 创下了逾 1 万的日活跃用户和逾 4 万以太坊的日流水（按当时以太坊价格为近 1900 万美金）巅峰成绩，并引发了 Dapp 的热潮和讨论，**而这皆源于其“博弈”、“分红”、“推荐奖励”、“抽奖”四大创新游戏机制，以及其无限重复性对人性的持续诱导和刺激。**四大游戏机制分别对应了其游戏中的如下玩法，并成为了之后 Dapp 竞相模仿的对象：

- 博弈：通过智能合约打造一款刚性兑付的新兴博弈式彩票，时间走完（24 小时）之前的最后一个游戏 Token 购买者获得全部奖金，奖池完全透明，源于之前购买游戏 Token 花费的以太币的一部分，实现以小博大；
- 分红：用户可根据自己持有的游戏 Token 的数量占总的游戏 Token 的数量的比重，获得来自之后购买游戏 Token 花费以太币一定比例的分红，让参与博弈之人不空手而归；
- 推荐奖励：用户花费少量以太币即可获得推广链接，任何通过推广链接加入的新用户，其购买游戏 Token 花费的以太币均有部分分配给推广者；
- 抽奖：用户购买游戏 Token 花费以太币的一定比例会进入空投奖池，用户购买游戏 Token 时会有一定概率获得该奖池中的以太币。

而 EOS 以及后续 TRON 的崛起，为 Dapp 和区块链游戏带来了新的血液，也诞生了新的玩法，**除了沿用上述四大重要游戏机制外，大部分 Dapp 还加入了**

“挖矿机制”，即玩家可以在游戏之中获取 Dapp 的通证，而持有通证可以获得 Dapp 收入的分成，以此作为冷启动和刺激玩家的重要手段，EOS 和 TRON 之上的 Dapp 生态亦快速繁荣了起来：

图 35：EOS、TRON 之上 Dapp 活跃度排行榜

EOS 上 Dapp：

排名	名称	分类	公链	24h活跃用户	24h交易笔数	24h交易额(EOS)	7天活跃用户	7天交易笔数	7天交易额(EOS)
1	Endless Game	竞猜	柚子	19549 ↑+25.79%	166068 ↑+30.83%	28395 ↑+81.2%	19090	1533069	233936
2	FRA糖果盒	其它	柚子	7856 ↓-9.71%	64668 ↑+12.97%	0	12915	519356	0
3	EOS骑士	游戏	柚子	5667 ↓-5.53%	247109 ↓-2.02%	3029 ↑+33.55%	7163	1962716	23711
4	ENBank	其它	柚子	5518 ↓-0.5%	44661 ↓-26.35%	0	6940	312404	0
5	VSbet龙虎斗	竞猜	柚子	4160 ↑+7.24%	140723 ↑+10.36%	327144 ↑+76.88%	6940	690632	3872373
6	PokerKing	竞猜	柚子	3810 ↑+3.06%	23882 ↑+12.92%	322594 ↑+52.91%	4080	115764	919758
7	BIG GAME	竞猜	柚子	2942 ↑+13.85%	50580 ↑+12.32%	16527 ↑+36.88%	3701	330963	107560
8	FAST	竞猜	柚子	2680 ↑+38.89%	337037 ↑+434.2%	202244 ↑+905.54%	4247	895399	1091083
9	EOSBet	竞猜	柚子	2629 ↓-0.08%	124309 ↓-18.39%	153893 ↑+88.88%	3011	1253147	1102519

TRON 上 Dapp：

排名	名称	分类	公链	24h活跃用户	24h交易笔数	24h交易额(TRX)	7天活跃用户	7天交易笔数	7天交易额(TRX)
1	Epic Dragons	游戏	波场	6368 ↓-1.77%	6828 ↑+2.61%	331821 ↓-2.61%	7082	44857	1918219
2	WINToken Games	竞猜	波场	5659 ↑+111%	9995 ↑+183.42%	314655 ↓-42.47%	6486	52734	2677018
3	ALLBET	竞猜	波场	3806 ↑+16.46%	23104 ↓-44.91%	26808718 ↓-0.97%	3760	216246	232427987
4	TronVegas	竞猜	波场	3269 ↑+26.95%	74203 ↓-43.52%	3596973 ↓-4.31%	3987	751462	34805848
5	TRONbet	竞猜	波场	2759 ↓-2.41%	383966 ↑+4.14%	193581476 ↓-33.87%	7546	2732999	1430025962
6	钓鱼简单	游戏	波场	2415 ↓-1.11%	5684 ↓-15.23%	631775 ↑+14.52%	16715	46914	5035707
7	摇骰水果机	竞猜	波场	2302 ↑+3.18%	2306 ↑+2.81%	1015 ↓-91.69%	3083	7096	36335
8	Dice 3D	竞猜	波场	2058 ↓-34.54%	67325 ↓-54.97%	8244737 ↓-72.53%	3819	2592110	500424529
9	抽红包	竞猜	波场	1918 ↑+541.47%	2124 ↑+92.39%	292150 ↑+6.95%	1561	3835	665213

来源：Spider Store

根据 Spider Store 数据，EOS 生态目前共有 348 款 Dapp，部署的智能合约数量 599 个，每日活跃用户数约 7 万，24 小时交易额在 700 多万 EOS 量级，其中有占据主导的竞猜类 Dapp 的贡献，也有如 EOS 骑士这样的典型链游 Dapp 的贡献，虽玩法简单，操作性不强，但 EOS 骑士以其稳定的 5500 左右日活及 3000EOS 至 5000EOS 左右的日交易量牢牢占据了 EOS 生态前三 Dapp 的位置。

TRON 生态目前共有 172 款 Dapp，部署的智能合约数量 318 个，每日活跃用户数约 4 万，24 小时交易额在 3 亿 TRX 量级，其中 1 月中旬上线的 Epic Dragon 链游 Dapp，已经获得了 6000 多的日活，30 多万 TRX 的日交易量，排名第一。

不过，我们也应该看到，由于目前数字资产用户量少，Dapp 的开发成本和门槛仍较高，这导致了多数开发者选择了一条偏向于快速回收成本的道路，**大部分 Dapp 依旧具有较强的资金游戏性质。而同质化、各类 Dapp 相互间的抄袭和换皮亦较为严重。如果无法真正降低用户入场门槛，解决“法定货币-数字资产”支付通道问题，引入更多的潜在用户，或是进一步简化优质游戏区块链改造成本问题，**Dapp 仍只会是一个供求两端均缓慢发展的小圈子，难以独立于目前数字资产市场投资、投机驱动的生态环境，走出属于自己的一条道路。未来究竟会有哪些变数，就让我们拭目以待。

（5）传统巨头开始布局区块链、数字资产领域

2018 年，对于整个数字资产、区块链领域最有风向标意义的，或许是传统领域的认可以及巨头的加速布局，这体现在：**1）传统金融机构加速布局交易所、托管等领域；2）传统科技公司探索区块链领域应用。**

在传统金融机构加速布局交易所、托管等领域方面，除了纽交所母公司 ICE 集团发起的 Bakkt 交易所、纳斯达克投资的 ErisX 交易所等加速数字资产方面的布局外，也有高盛、纽约梅陇银行、野村控股宣布适时将提供数字资产托管业务的动态，**上述公司借助其在客户资源、金融风控、资本实力方面的优势，将会为这一市场注入不一样的血液和驱动力，并加速投资市场的合规化、机构化。**

在传统科技公司探索区块链领域应用方面，我们则是能看到像 Facebook 这样的互联网社交网络企业调整组织架构，新设立区块链部门，积极探索区块链技术与 Facebook 在社交、数据、隐私等等方面的结合，并于 12 月被彭博社爆出正致力于开发稳定币，可在印度市场被用于汇款；另外还有像网易，在旗下的《逆水寒》、《流星蝴蝶剑》以及《新倩女幽魂》三款游戏中引入“伏羲通宝”，而“伏羲通宝”是基于区块链技术生成的有价值的资产，可通过挖矿机制产出；而华为也于 3 月正式公布了云区块链服务平台，发布了《华为区块链白皮书》，并希望用 5G 技术予以赋能；此外，微软也于 5 月发布了其 Azure 区块链市场，为

开发者提供工具包等服务，并于 10 月以 75 亿美元的价格收购了存储着大量区块链项目代码的开源代码托管库 Github。**上述公司本身庞大的用户群体，若能借此逐步接触、参与区块链和数字资产，则有望大幅加速区块链市场的扩大，并能让区块链真正能与应用深度融合。**

（6）区块链公司拥抱传统资本市场及传统金融工具

区块链、数字资产领域与传统领域的交融，不仅体现在传统巨头正加速布局，也体现在区块链公司也同时正拥抱传统资本市场，包括了：**1）区块链公司寻求上市；2）收购上市公司进行资本运作；3）并购优质产业链上下游资产。**

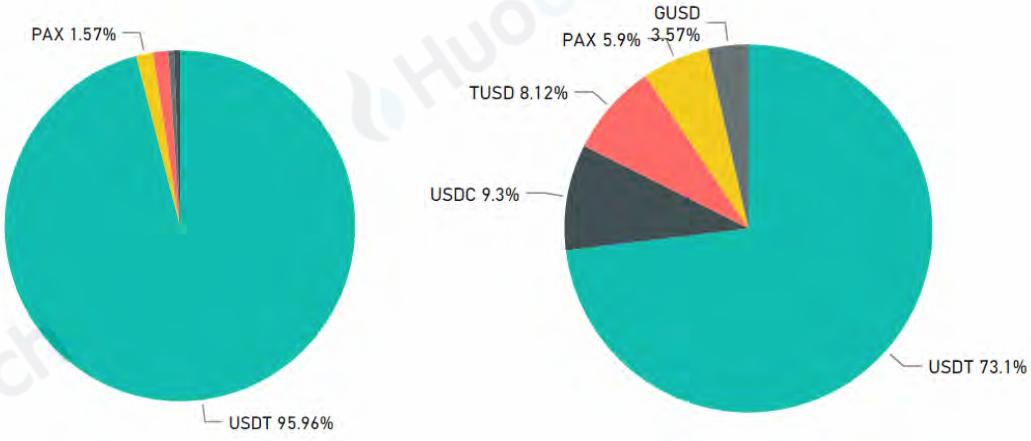
2018 年，我们看到了三大矿机厂商—比特大陆、嘉楠耘智和亿邦国际冲击 IPO 上市，数字资产投资公司 Galaxy Digital 登陆加拿大多伦多证券交易所创业板，还有美国数字资产交易所 Coinbase 对 IPO 上市亦跃跃欲试。而与直接上市不同，也有部分区块链公司通过收购上市公司的形式拥抱传统金融市场，最典型的，还包括区块链公司 Penta Global Blockchain Foundation 首创用其发行的通证 PNT 以每股 0.02 澳元的价格收购澳大利亚物联网上市公司 CCP Technologies Limited 的 2800 万股，获得了澳大利亚证券交易所的认可，另外也包括火币集团以均价每股 2.27 港元的价格，合计耗资 6 亿港元获得了桐城控股的控制权，以及 OK 集团收购香港上市公司前进控股。另外，区块链公司通过并购的方式获取产业链优质资产的案例亦开始出现，2018 年 7 月，波场基金会就以 1.4 亿美元收购 BitTorrent。

（7）USDT 面临信任危机，合规稳定币出世，而算法稳定币出师不利

稳定币源于泰达公司发行的美元稳定币 Tether USD（简称 USDT），其价值锚定 1 美元，自 2015 年 2 月推出，于 2017 年下半年开始规模快速提升，成为各大主流交易所的核心交易对和市值排名前 10 的数字资产。然而一路走来，由于其在透明性、监管背书性等方面存在一定弱势，面临了较多的争议和不信任。2018 年 11 月 15 日，USDT 价格出现波动，出现了较大幅度的下跌，并一度使得各大交易平台上 BTC/USDT 的价格大幅上涨。**可赎回性实质是像 USDT 这样的法币抵押稳定币的价值核心，换句话说，法币抵押美元稳定币本质就是链上美元，其价值是由可赎回性所保证的，没有通畅的购赎体系予以支持，便难以获得信任。**

USDT 的改良版 PAX、GUSD、TUSD 和 USDC，便是在这一种环境中获得的发展空间，且与其说是在合规性、透明性以及美元储备安全性上做了优化，**不如说是上述币种相对通畅的购赎体系尤其是可赎回性，获得了市场的认可，USDT 的市场份额，正有一部分被上述改良版法币抵押稳定币所逐步获取。**

图 36：2018 年 Q4 各法币抵押稳定币交易量　　2018 年底各法币抵押稳定币发行量



来源：火币区块链研究院整理

而除了法币抵押稳定币外，致力于通过其他模式实现价值稳定的稳定币也在今年不断涌现，其中，算法调节稳定币，凭借其完全独立性，不依赖外部信用，成为了最受瞩目的品类，Basis，Carbon，Terra，uFragments，Reserve 均是这一波稳定币浪潮中的崛起者。**然而，12 月 13 日，起步较早的 Basis 项目向社区宣布项目终止，算法稳定币师出不利，**而背后深层次的原因，则是与其机制设计中的“债券币”和“股权币”存在非常大的联系：由于“债券币”的溢价回购属性和“股权币”的分红属性，其会被多数监管机构认定为证券，以美国为首，**若涉及证券，则只能在合格投资者之间流转，且会有 12 个月的限售期，一旦如此执行，便会大大降低市场参与度，而 Basis 体系的稳定性非常依赖上述两个币种的存在，尤其是当 Basis 价格低于 1 美金，系统回购 Basis 的资金源于“债券币”销售带来的资金之时，证券的定性，会严重影响其稳定机制的发挥。未来，算法稳定币作为一种和比特币一样的极客尝试，究竟走向何方，仍存在一定未知数。**

（8）监管不再限于纸面，落地执行开始，并以美国为典型

2018 年起，各国、地区除了在数字资产、区块链监管体系上不断完善，另一个很重要的变化是**监管正不再限于纸面，而是开始落地执行，体现在部分国家、地区监管机构开始对违规项目进行追溯、调查和处理，以美国 SEC 为典型。**而 SEC 在这一轮执行浪潮中，亦是从**对欺诈型违规行为的处罚，转向包含对非欺诈型违规行为的处罚，态度系“处置+整改”并行，已能明显感知到美国监管态度的强化，未来预计会有更多的项目被波及：**

- **违规的数字资产发行、销售行为，**以 11 月 16 日对 Paragon Coin 和 CarrierEQ（又称 Airfox）项目的处罚决定为典型，SEC 认定上述数字资产发行属证券发行，并认为其并不符合豁免证券注册的条件，处置决定包含了罚金，要求重新进行证券注册和后续向 SEC 进行持续信息披露，以及赋予投资者按法定货币退回当初的款项附加利息的权利。
- **违规的数字资产交易、流通行为，**以 11 月 8 日对中心化交易平台 Etherdelta 的处罚决定为典型，SEC 认定该平台未经注册为“全国性证券交易平台”或获得相应豁免，擅自为包括美国公民提供部分已被认定为证券的 ERC20 通证撮合交易，处置决定包含对其创始人的罚金。
- **违规的数字资产投资、咨询行为，**以 9 月 27 日对比特币经纪商 1Broker 的处罚决定为典型，SEC 认定该平台未经注册为证券经纪商，擅自在全球各地招揽包括美国用户在内的客户到其平台用比特币购买证券掉期类衍生品，处置决定包含永久关停，没收所有非法所得以及罚金。

11 月 16 日，SEC 发布的《关于数字资产证券发行与交易的声明》，则是继 2017 年 7 月 27 日著名调查报告“DAO Report”之后，SEC 再一次的对数字资产监管态度的重申，即 **SEC 对数字资产的监管参考的仍是传统的联邦证券法体系，只要数字资产符合联邦法律定义的“证券”，即被纳入全面监管，**而判别是否会被纳入监管，除判断是否属于“证券”外，还有三大重要原则，均源自 “DAO Report”：**第一，只要涉及向美国公民销售证券或提供相关服务，即受监管；第二，去中心化组织亦可以成为证券发行或相关服务主体，并受监管；第三，以法定货币或数字资产形式销售证券或提供相关服务，并不影响监管效力。**

（9）谁是真正的信仰者，从 BCH 分叉看公链治理

2018 年，BCH 社区最知名的开发团队之一，“Bitcoin ABC”，提出在 11 月 15 日进行一次“硬分叉式”的客户端升级。原本是 BCH 的例行升级，但因为 BCH 社区另一知名开发团队“NChain”（即 Bitcoin SV）提出的另一种提案而陷入不确定性之中，**二者主张的分歧在于，区块大小的制定、若干个新的 Opcodes 以及对待智能合约的态度。这一分歧，直接导致了后来 BCH 的分叉。**

然而本次分叉**与以往的硬分叉有所不同的点在于，短期内两条链无法“共存”：由于客户端没有重放攻击保护，区块链有遭遇重放攻击的危险。**在 ABC 版本链上的交易，也可以在 SV 版本链上重新广播并打包，部分持有者可能会出现 Token 被故意取走的情况。这意味着两条链关系会趋向于激烈竞争而非各自独立，直到一方加入新的重放攻击保护机制才能结束。因而这次硬分叉会引发“算力大战”，BCH 矿池、矿工以及比特币的算力持有者和租借者都可以是参与者。

从结果来看，双方都有不同程度的损失，BCH-SV 由分叉中新生，但为了实现其愿景，仍旧有很长的路要走。最重要的是，BCH 因为分叉，实际上让凝结的共识和算力分裂，这不禁让我们对公链治理进行深思：

- 对于采用 PoW 共识机制的公链来说，**矿工**承担着维护数字社会共识与信任的重任，以算力代表着话语权；**技术团队**推动公链技术的发展，掌握着代码；而**用户**代表着拥趸，使用数字资产，会用脚投票来维护权益。**若一套机制维持者三者的平衡，那么链上治理也就是成功的。**
- 在 BCH 的案例之中，BCH-ABC 一方专注于技术团队的代码权，BCH-SV 一方则将矿工的算力权奉为圭臬，**大矿主对算力的控制强，用户、普通矿工的利益和诉求在这个生态中并没有很好的表达途径**，以至于造成了后来的局面，而算力大战的产生，本身也是大矿主对生态控制力偏强的一种体现。**如何能有一种完善的方案，能让算力权、代码权和用户权得以平衡，是值得公链系统开发者们深思的。**

（10）安全、黑客事件频发，区块链安全机遇显现

2018 年，区块链安全事件从上半年开始随着数字资产行情的涨落而变得频繁。火币区块链研究院将 2018 年的一些重大安全事件汇总如下：

领域	安全事件简介
交易所	1 月 26 日，Coincheck 遭到攻击，价值超过 5.3 亿美元的 NEM 被非法转移
	2 月 8 日，Binance 发生严重宕机事故，服务中断近 60 小时
	2 月 11 日，意大利交易所 BitGrail 遭遇攻击，价值 1.95 亿美元的 NANO 被盗
	2 月 15 日，LLC 交易所遭受攻击，损失约 200 万美元
	3 月 7 日，Binance 部分用户权限被黑客窃取，并被用来拉高 VIA 币价格获利。Binance 回滚了异常交易，但仍引起市场恐慌
	3 月，OKEx 出现近 1 个半小时极端异常情况，并在事后对异常交易进行回滚
	4 月 12 日，印度交易所 Coinsecure 的 438 个 BTC 被盗，为印度迄今为止最大的一次数字资产被盗事件。
	6 月 10 日，Coinrail 的账号被以钓鱼方式窃取，损失超过 5000 万美元
	6 月 20 日，Bithumb 疑似员工电脑遭恶意代码植入后服务器攻击，价值 3000 万美元的数字资产被盗
	9 月 20 日，日本交易所 Zaif 遭受黑客攻击，损失近 6000 万美元
	9 月，C-CEX 交易所遭遇“短地址攻击”，价值上百万美元的数字资产被盗
公链	3 月，慢雾团队披露利用以太坊节点缺陷，恶意调用 sendTransaction 合约的上亿规模盗窃事件
	5 月，360 安全团队发现 EOS 主网上线前的版本存在缓冲区溢出漏洞，会导致 EOS 网络被黑客控制
合约	4 月 22 日，BeautyChain 合约出现重大漏洞，可生成大量 token
	4 月 25 日，Smartmesh 出现溢出漏洞，据估损失约 1.4 亿美元
	4 月 28 日，EDU 合约出现重大安全漏洞
	7 月，Bancor 智能合约出现安全漏洞，导致 2350 万美元的资金被盗取
	7 月 25 日，EOS Fomo3D 遭到连续攻击，损失约 60000 多个 EOS
	9 月 2 日，EOS Win 随机数算法被破解；并在 9 月 15 日遭到“假币攻击”，导致 EOS Win 暂时关闭
	9 月 10 日， DEOSGames 的随机数算法被破解，约 2.4 万美元 token 被获取
	9 月 14 日，EOS Bet 合约由于 token 名称检查上的 bug，遭受“假币攻击”，导致无成本生成了大量 token 并在之后被转移走
	10 月，黑客利用 EOS Bet 在检验收款方时存在的漏洞“伪造转账通知”盗取了合约中的 EOS
	10 月，World Conquest 遭到攻击，奖池中的几乎所有 EOS 均被黑客转走
	12 月，众多 EOS 的 DApp 遭遇回滚攻击，按时价计算损失超过 500 万人民币
钱包	4 月，Coinsecure 钱包遭窃取，438 个比特币被盗
	4 月，MyEtherWallet 遭 DNS 劫持，持续几个小时，损失约 215 个 ETH
	12 月，BitPay 的 Copay 钱包早黑客入侵，疑似因使用的第三方 JavaScript 库被修改，注入了恶意代码
矿池	6 月，嗨池位于阿里云的服务器遭到连续攻击，导致其近 10 万 FAB 被盗，进而造成矿池永久关闭

来源：火币区块链研究院整理

可以看到，**以密码学作为底层逻辑的区块链和加密数字资产在 2018 经历了交易所、公链底层平台、合约/DApp、钱包、矿池等多个维度上的重大攻击，进而使很多人产生了对区块链的担忧。**

不过，在区块链生态暴露在巨大的安全风险的同时，2018 年安全防护方面也显露出了巨大的机遇。不少在信息安全具有丰富经验的技术专家、白帽子等纷纷成立了区块链的安全公司，开始从事区块链方面的安全审计工作。尤其是智能合约的审计服务，已基本成为区块链安全公司的标配。在 2018 年上半年，就有慢雾、PeckShield、链安、降维科技等专注在区块链安全领域内的公司成立并迅速发展，**在信息安全范畴内细分出了一个新的行业垂直领域赛道。**

于此同时，一些已具规模的安全公司也在嗅到了区块链安全的巨大商机后，开始布局区块链安全业务。其中，最典型的是 360 公司在 2018 年 5 月发现 EOS 漏洞后，进而宣布进军区块链安全领域，主打区块链安全与开放平台。其他目前已提供区块链安全服务的公司还包括猎豹区块链安全、长亭科技、知道创宇等等。

5.2 2019 年度十大重要预测

对于区块链的未来，我们依旧充满信心，前途是光明的，然而道路永远是曲折的。如果说 2018 年对于区块链来说是由狂热回归理性的一年，那么 2019 年则是痛定思痛和重新积蓄力量的一年，火币区块链研究院对 2019 年做了十大预测，与大家共勉（部分预测源自火币大学 GBLP 创世班 18 年 12 月课程讨论结果）：

1、缺少造富效应，融资项目出清，2019 年市场寻底后将宽幅震荡

2、ETF 不会一帆风顺，但个性化衍生品将持续涌现

3、公链改良循序渐进，然性能已非痛点，有效场景才是

4、一站式区块链部署或成新宠，跨链互通催生区块链落地多样性

5、Web 3.0 到来，5G 和基于 IPFS 的分布式存储成重要推动力

6、矿业金融化变革推动洗牌，改弦更张者上位，抱残守缺者离场

7、传统应用掀 Dapp 化浪潮，一个崭新的流量世界将浮出水面

8、资产通证化案例涌现，通证锚定权利逐渐丰富，但规模化仍存障碍

9、稳定币从交易转向应用和支付，基于稳定币的“PayPal”将会出现

10、主流国家监管持续优化，示范效应引多国效仿，牌照、沙盒将普及

（1）缺少造富效应，融资项目出清，2019 年市场寻底后将宽幅震荡

从历史角度看，2013 年那一轮牛市后，花了一年多时间，到 2015 年 1 月触及底部，之后 2015 年经历反复震荡，于 2015 年 11 月才开始摆脱底部宽幅震荡区域，**震荡盘整的时间长达 10 个月之久**。若参照历史，那么理论上 2019 年也应是真正触底的一年，并且亦将会在很长一段区间内低位震荡，直至再次逐步上行。

图 37：2014-2015 年熊市图（黄色系震荡盘整区域，持续近 10 个月）

来源：Tradingview、火币区块链研究院整理

不过我们认为，与上一轮熊市 15 年初就寻得底部不同的是，这一轮熊市的底部，目前还没有被真正触及，而 19 年第一季度亦难具备形成上行的条件：

- **融资项目还未出清完毕，资金仍处于被分流状态**

各类公链项目以及无数应用层融资项目的存在，拖慢了这一轮“牛-熊”周期的出清速度，上一轮牛熊市只有数百个项目，且大多复刻比特币，这一轮牛熊市涉及的项目达数千之多，还需要一定时间予以消化，**这部分未出清的项目，持续分流着存量市场中的资金，难以形成集聚效应。**

- **区块链项目的失败、证伪，也会传导至机构投资者，形成较大抛压**

2017 年和 2018 年，大量的区块链、数字资产基金设立，并专注于寻找和投资该领域的优质资产。然而区块链领域本身仍处于早期，潜在的失败率相对较高，大量项目失败、被证伪，会传导至该领域的大量机构投资者，并带来非常大的负面影响（尤其是该领域的机构投资者存在大量扎堆同一项目的情况，这一传导效应将会更加明显），由此引发**机构投资者在 LP 的压力下清盘，则会进一步给本身就脆弱的数字资产市场，带来较大的抛压，拖累市场的上行。**

- **美日税季即将来临，对市场影响不可小觑，一季度难具备大幅上行条件**

根据主流国家尤其是美国、日本等国的数字资产政策，每年的 3-4 月，均是重要的报税季时间窗口，日本截止日在 3 月 15 日，美国截止日在 4 月 15 日。**虽然，数字资产市场经历了 2018 年的大跌，“资本利得—税收”效应带来的抛压会相较于 2018 年 4 月小很多，**然而熊市下跌之中亦有波动机会，且有部分投资者通过卖空赚取不少收益，这一部分亦需缴纳税款，对市场影响不容小觑。这也使得我们认为，一季度市场难以具备上行的条件，反倒是很可能的见底时间窗口。

我们认为，**每一轮熊市结束，牛市周期开启，大多都会伴随着“价值发现”—“造富效应”—“资金效应”三个阶段：**其中，**“价值发现”是前提，而只有“造富效应”从而带来的大量资金流入，产生“资金效应”，才能构筑牛市。**17 年的牛市，由以太坊以及相关的数字资产众筹带来的全局性“造富效应”所推动，而目前来看，**显然短期之内，甚至一段时间之内，我们找不到一个真正可以带动全局的主题，自然无法集齐上述条件。**

当然，我们也并不否认 8 月莱特币减产对市场的推动作用，**事实上，莱特币减产很可能是 19 年 5 月起到年中最重要的行情窗口。**不过可惜的是，减产更多是与上述“价值发现”相关的一个引子，**它可以带来市场热点，并引发阶段性的行情，成为探底后宽幅震荡的一个重要推动因素，**但其并无法真正带来牛市。正如过去的牛市，也并非独因减产而发生一样，唯有不断探索区块链以及数字资产的场景，扩大其内在价值，形成健康的循环，才能让这个市场摆脱大起大落的短周期特性，才能真正迎来属于数字资产市场和区块链行业的“黄金十年”。

（2）ETF 不会一帆风顺，但各类信托、期货等金融衍生品将不断涌现

自 2017 年底，CBOE 和 CBOT 的比特币期货推出后，比特币 ETF 即将通过的声音便此起彼伏，市场对于传统金融市场介入数字资产市场的期望居高不下。然而天不遂人愿，2018 年， Proshares 和 Direxion 的比特币 ETF 申请，双子星（Gemini）交易所创始人 Winklevoss 兄弟提出的比特币 ETF 申请，以及被认为最有希望的 SolidX、VanEck 提出的比特币 EFT 申请，均铩羽而归。

不过与很多人认为的比特币 ETF 将很快破冰不同的是，我们预计其在 2019 年仍不会一帆风顺，目前的市场基础还并不足以支撑 ETF 的存在：

- ETF 的本质系为投资者提供一种更为便捷的交易方式，参与者通过认购并持有这一类基金，便可获得相应底层资产的风险敞口。**其代表的是一个市场进入成熟期后，为了满足更多场外投资者资产配置的需要，才引入的一种投资产品**。其与期货这一类解决投机、专业风险管理需求的金融产品，或本身具有一定门槛的场外信托产品，是不一样的，这也就意味着其通过的难度更高。目前，整个数字资产市场的成熟度，还没有达到 ETF 本身定位所要求的一个状态，而其不成熟体现在如下几个方面：

- **市场流动性分散，深度不足，价格易受资金影响。**数字资产市场本身体量较小，参与人数并不多，共识尚未形成，而目前数字资产的交易又是分散在各个数字资产交易所中，造成了深度的分散，单一交易所的价格很容易受到资金的影响发生非理性波动，ETF 锚定价格存在风险。

- **监管机构对市场交易、清结算行为，以及客户身份等缺乏掌控。**就美国来说，其金融监管推行共享监管协议，协议各方，包括监管机构在内有权获得上述信息。而目前，大部分市场参与者的相关行为信息，其实并无法被监管机构很好地获知，且比特币 ETF 锚定价格所发生在的某个交易所，即便是受规管的签订共享监管协议的交易所，其规模可能亦不大，无法代表市场整体。

不过，比特币 ETF 即便有朝一日获批，其影响力可能亦并不如我们现在所预期的那么强大，届时，整个市场本身的覆盖面和成熟度，就已经远远甚于目前，推出 ETF 不过是水到渠成的事。比特币 ETF 更多代表的是一种象征意义，象征着比特币真正进入主流市场，以及传统市场对于数字资产的一种认可，**而若只是**

这一点，各类场外信托产品，期货产品的推出，就已经代表这个市场逐步走向正规化。我们毫不怀疑，2019 年各类合规的信托、期货类金融的个性化数字资产产品将会不断涌现，并为这个市场带来新的血液和力量，传统金融主流的入局，已成不可逆转的趋势。

（3）公链改良循序渐进，然性能已非痛点，有效场景才是

2018 年，对于公链来说，整体处于降温、欲速则不达的状态，间接拖累了应用类项目的落地进度。2019 年，不出意外，我们可以看到像以太坊 2.0 那样的公链改良方案循序渐进，**不过，要实现重大的技术突破还有不小的难度，大概率仍为现有体系延伸，涉及跨链、DAG、分片、分布式存储、VRF(可验证随机函数 Verifiable Random Function)的 POS 等已有技术的推进，这从 2019 年预计将上线的公链项目便可窥之一二，如下图。同时，公链改良还会涉及针对 2018 年的一些问题进行修补**，如区块链安全问题，我们预计将出现标准的安全审计流程，标准的安全沙盒测试以及同行代码安全审计等。

编号	项目名称	预计主网上线日期
1	Dfinity	2019 年 Q3
2	Polkadot	2019 年 Q3
3	Cosmos	2019 年 Q1
4	Irisnet	2019 年 Q1
5	Algorand	2019 年 Q2
6	Nervos	2019 年 Q2/Q3
7	Thunder	2019 年 Q1
8	Conflux	2019 年 Q3
9	PlatON	2019 年 Q3
10	QuarkChain	2019 年 3 月份
2018 年延误项目		
11	Cardano (合约层)	2019 年 Q1
12	Aeternity	2019 年 Q1
13	Aelf	2019 年 Q1
14	Hashgraph	2019 年 3 月份
15	Internet of Services	2019 年 2 月 25 日
16	Rchain	2019 年
17	Theta	2019 年 3 月 15 日

18	Zilliqa	2019 年 1 月 31 日
19	Filecoin	2019 年 Q3

来源：火币区块链研究院整理

不过就目前来看，公链性能已非真正痛点，是否有真实的场景和需求，才是决定这个行业生死的关键。实际上，大多数应用部署在区块链上所面临的性能问题，都可以通过非区块链的方式予以弥补。而区块链所要解决的，更多是把最有价值，最需要信任和公证的数据予以确认。**寻找这些真正面临痛点的场景，将其引入区块链，让需求反推技术发展，让真正有价值的数据上链，或许才是真正正确的道路。**过于关注技术实现或突破，认为底层的不完善大规模限制了应用和区块链的发展，事实上是并不公允的。

而 2019 年，或许是市场重新思考这些核心问题，并在公链体系设计上予以体现的重要时间窗口，我们需要摆脱目前创造需求的怪圈，转而服务需求，这是整个市场需要面临的转变。

（4）一站式区块链部署或成新宠，跨链互通催生区块链落地多样性

以太坊智能合约为代表的区块链 2.0，让 Dapp 应用得以方便地在链上部署智能合约，发行专属通证。但该类链上应用难以实现复杂逻辑和功能，无法对区块链底层的数据存储、共识机制、出块策略等做定制化开发。之后，基于侧链和子链进行 Dapp 开发的模式出现，侧链和子链通常和主链在数据结构或者是共识等方面是强关联模式，主要由主链来承担安全职责，侧链或子链负责各自应用数据的处理，做到了数据和计算的隔离和自定义。但侧链和侧链之间，或者子链和子链之间的互通性并不是首要考虑因素，实现上并不简单；且该模式可扩展性不强，一条主链上搭载的侧链和子链数量是有限的，未来发展受限。

2019 年，以 Parity 发布的 Substrate 开发框架为代表，通过模块化开发迅速部署一条公链的形式，我们认为将成为未来 Dapp 开发的新趋势，理由在于：

- **模块化开发，开发门槛被降低。**Substrate 是 Parity 团队开发的一个区块链开发框架，可以基于 Substrate 快速开发一条自己的公链，Polkadot 也是基于 Substrate 开发的，任何基于 Substrate 开发的链都能和 Polkadot 进行互联互通。这意味着，以前只能快速开发一个 Dapp，现在可以基于

Substrate 快速开发一条自己的公链，不仅定自定义账本数据结构、共识算法，还可以自定义各种接口，**大大降低了公链开发门槛，使得人人都可以快速发布一条自己的公链。为应用层 Dapp 的繁荣奠定了基础。**

- **可定制化程度高，支持高复杂性应用。**与智能合约、侧链或者子链的模块化开发不同，模块化公链的开发可更灵活地设计底层逻辑和架构，比如区块账本数据结构、出块规则、共识算法、对外接口以及数据存储方式等。**这种一键发链的模式能支持更复杂的应用场景，满足多样化需求。**
- **包含跨链基因，增加应用多样性。**按照统一框架进行开发的公链，他们在底层架构上的一致性让其有着天生的跨链互通基因，而跨链互通的能力又将为应用的多样性带来突破性的空间。比如跨链资产流通、跨链数据服务、跨链资产金融服务等等，跨链信息交互与价值流通将开拓更丰富的应用场景，催生落地多样性。

总得来看，2019 是跨链平台真正意义上的落地首年，其带来的一站式区块链部署以及跨链互通功能将带给我们更多的想象空间和应用场景。

（5）Web 3.0 到来，5G 和基于 IPFS 的分布式存储成重要推动力

Web 1.0 解决了用户读取信息的需求，信息可以通过用主动查询来获得；Web 2.0 则是解决了用户互动的需求，用户除了可以进行信息查询，同时还能进行互动，但所有的数据仍是通过寡头企业的服务器存储记录，存在隐私泄露问题；而 Web 3.0 则是提供了一个更加扁平的信息读取、交互方式，所有数据交换将基于分布式网络，以加密的形式存储在网络中，用户对自己的身份以及行为数据拥有绝对的所有权和控制权，同时应用亦是分布式的，没有中心化服务器。而这一切的实现离不开**分布式存储**、**网络通信能力**以及**区块链底层技术**的提升。

我们认为，2019 年，应当是 Web 3.0 开始到来的一年，基于：

- **5G 助力 Web3.0 移动端发展和网络通信能力提升。**随着移动智能终端的普及，移动端应用地位已占据非常重要的地位，Web3.0 的普及和兴起也必将伴随着移动端应用而发展，移动终端也将成为去中心化网络中关键的节点群组。因此，移动节点之间的通信传输成为目前核心的难点，而

5G 网络的建设正好是解决此问题的利刃。**5G 网呼之欲出，目前已开始小规模试验，2019 年也将是试验期的关键一年，虽然离大规模开通还有差距，然而与之配套的试验性应用也必将会随之同步开展。**

- **IPFS 技术栈成熟成重要推动力。**IPFS 是唯一一个从网络底层协议开始逐步改进的分布式存储体系，可实现索引搜索功能，较其他只提供存储或证明功能的分布式存储方案有很大的优越性。我们认为，IPFS 技术体系的成熟将有利构建 Web3.0 数据存储的基础，**而 2019 年让人期待已久的 IPFS 应用层项目 Filecoin 若可如期落地，则真正第一次让通证激励与分布式存储进行挂钩，让分布式存储实现“全民参与”的初衷**，不仅可扩宽外界对 Web3.0 的认知，也可为 Web3.0 的落地提供技术基础。
- **公链底层技术提升是重要基础。**Web3.0 推崇数据平等，强调用户数据所有权，强调隐私和安全，这一切离不开底层区块链技术的发展，以实现数据确权，数据安全和平等。经过 2017 和 2018 各大公链平台的竞争，一些有技术实力的公链平台在 2019 年会进一步夯实基础，提高稳定性，为 Web3.0 的应用搭建提供可靠的区块链底层技术支持。

随着基于 IPFS 的分布式存储落地、5G 网络时代的逐步到来以及公链的成熟，Web3.0 的底层核心技术生态逐渐完善，为 Web3.0 的启动提供了技术和生态基础。

（6）矿业金融化变革推动洗牌，改弦更张者上位，抱残守缺者离场

自比特币十年以来，逐渐形成了以链、矿、币为代表的三大发展路径。而矿业更系因比特币而形成的独特产业，承担着数字世界最重要的任务：维护着共识与信任。从一开始单 CPU 竞争记账挖矿的理想，到目前由矿工、矿场和矿池等组成的明确产业分工，矿业一直在向精细化、专业化的方向发展。我们认为，**这一发展趋势会持续进行，并在这一轮熊市中进行深度洗牌。而与过去只是市场格局进一步集中，淘汰落后产能不同的是，2019 年，我们将会看到矿业从“制造业”真正逐渐步入“类金融业”，抱残守缺、固步自封的参与者或将离场，而改弦更张、开拓创新的玩家会迎来新的发展机遇：**

- **矿工迈向专业投资时代。**矿工是一个特殊的群体，他们参与竞争记账，

获取比特币挖矿奖励和手续费。十年以来，参与者的特点一直在变化，由极客逐步发展到个人投机/投资者，但整体逻辑基本在于持币、屯币，必要时卖币。而未来，会是专业投资者/机构的时代，挖矿作为一种特殊的数字资产投资手段，也会逐渐变得专业化，而推动这一趋势的重要原因在于期货合约等衍生品的出现，在币价波动剧烈时，传统“屯币”的矿工会在比特币波动的时候面临成本压力，而如果有专业的套期保值手段则会对减少损失，整个产业，将会越来越多运营各类金融手段去管理风险，真正告别粗放式管理，并成为行业的标配。

- **矿池看齐互联网与金融**。矿池的产生逻辑来源于“风险均摊”、“按劳分配”，当挖矿难度不断飙升，单个矿工挖出比特币期望降低，为了均摊风险，于是组成了矿池，大家一起挖矿，挖到的比特币按贡献的算力大小统一分配，看似无本万利，但其必须保持 3-5%全网算力的生命线，否则其预期挖矿收益波动太大，会造成矿工流失。因此拉新、留住用户（矿工）成为矿池第一要务。可以推测，熊市中，矿池或会学习互联网的玩法，进行“补贴大战”，在行情低迷时候利用充足的资金，不断拉升自己全网算力占比，以便在未来行情爆发时候获取更大收益。而除了补贴之外，矿池或也会向着矿业金融机构方向发展，逐步推出众多的金融衍生品，未来随着矿业投资价值被逐渐认可，许多投资者也不会再去购买机器、挑选矿场等这些繁琐的手段，可以直接从矿池手里购买各类衍生品，以更简便的方式获取矿业投资收益，例如算力的通证化等。

（7）传统应用掀 Dapp 化浪潮，一个崭新的流量世界将浮出水面

Dapp 可以追溯到 2017 年底，一款叫《加密猫》的游戏，玩家可以在游戏中拥有琳琅满目的可爱猫咪，并且可以让其繁殖后代来继承父辈的属性。每一只猫咪的背后都有一个 ERC721 标准的非同质化通证（NFT）和其绑定，以此来确保猫咪的唯一性和资产属性。之后，Dapp 浪潮正式开始，我们能看到《Decentraland》通过土地销售拍出地王，可以看到类似区块链炉石传说的《Zombie Battleground》和《Gods Unchained》还未上线便已备受瞩目，也可以从 EOS 和 TRON 生态中各类采用“游戏挖矿”机制的 Dapp 获得追捧，产生了“Dapp 矿工”这一新兴的

特殊群体。不过，**2018 年，Dapp 仍旧是独立的世界，与传统外界相对隔离。2019 年，我们认为，会有一波传统应用的 Dapp 化浪潮，新的流量世界会开始形成：**

- **开发成本正不断降低。**各类为传统游戏开发者将游戏部署至区块链的模块化组件正不断成熟，有基于以太坊网络的 Loom SDK 和 Enjin SDK，也有传统游戏引擎服务商 Cocos、Laya 和 Egretia 推出的模块化组件，可实现“一键转化”传统游戏为区块链游戏，这都会在 2019 年逐步成熟；
- **区块链部署、运维成本降低。**对于 EOS.IO 来说，开发者需要各类资源才能部署和持续运营一款 Dapp，成本不可以说不高，2019 年，随着多条 EOS.IO 侧链的逐步出现，这部分的成本将会大幅降低，也将大大减少传统应用转到区块链上的门槛。
- **以 EOS Knights 为首的新颖挂机类 RPG 游戏对开发者的启发。**随着 Dapp 的发展，已经有越来越多的真正游戏出现在区块链上，EOS Knights 作为 EOS 主网上的首款挂机类 RPG 游戏，弱化了 RPG 游戏中的操作感，将游戏重心放在英雄数值培养和道具的合成交易上，将游戏借助区块链予以数值化，获得了 5000+的 DAU 和 3000-5000EOS 的日流水，这一类低成本游戏的成功，将大幅启发和激发传统游戏开发者入场。
- **门槛更低的钱包、托管解决方案将助力传统用户入场。**目前，Dapp 很大部分的门槛来自于用户的私钥管理，“法定货币—数字资产”转化，而托管解决方案，以及门槛更低的钱包，例如可通过用户的手机号等信息直接登录的钱包的出现，将大大降低这一块的用户门槛。

对于传统应用 Dapp 化来说，其实现的是：账号系统区块链化；应用核心逻辑的数据化、上链化；应用经济模型通证化；应用内资产通证化四大功能，也是四个重要阶段：

- **第一阶段：账号系统和支付体系区块链化**

在这一阶段，项目本身的逻辑并不上链，还是在中心化服务器上运转，但是会和区块链用户进行，并支持区块链用户用加密货币进行支付。

- **第二阶段：应用核心逻辑数据化、上链化**

即应用中最为关键的逻辑，如概率事件、强执行事件等都会通过智能合约来执行，确保了项目的公平公正和不可篡改，但是非核心逻辑还是继续在中心化服务器上运作，一是为了降低运营成本，二是当前的区块链存储技术还不完善。

- **第三阶段，应用经济模型通证化改造**

在这一阶段，应用的商业逻辑会进行彻底的改变。从传统的封闭的经济模型（即项目内资源无法和项目外资源自由兑换）转为了流动性更好的通证经济。一旦完成了项目经济模型的通证化改造，项目会拥有数倍于之前的爆发力，因为用户在项目内的所有资源都可以快速、高效地变现，大大增强了用户的使用动力。

- **第四阶段，应用内资产通证化**

这一阶段是上一阶段的升级，也是通证化中的一部分，最为核心的资产需要用一套量身定制的通证来锚定其价值，这可以使得项目中的资产实现真正的“独一无二”以及获得项目以外的价值（比如收藏价值）。

而对于用户来说，Dapp 带来的是资产养成和流通的特性，其可将其投入的时间或金钱所获取的游戏内资源，通过交易进行变现和与其他游戏进行互通，而这一切的实现和发展，与去中心化交易的进步是不可分割的，Dapp 去中心化交易的共振，将真正让 Dapp 成为新的流量世界。

（8）资产通证化案例涌现，通证锚定权利逐渐丰富，但规模化仍存障碍

以 USDT 为首的稳定币，本身就是资产通证化的一种典型案例。2018 年，市场更多看到的是美元、黄金等基础资产的通证化。而 2019 年，我们将有望看到通证的底层资产越来越多样化，通证所被赋予的权利，除了所有权外，还可能有独立的收益权、债权甚至相关衍生的权利，而**证券类通证概念的普及，以及相关监管框架、生态的成熟，将成为促进多元化权益通证化和资产上链的催化剂。**不过，尽管如此，我们仍然认为，目前资产通证化的规模化发展还存在不小难度：

- **证券类通证交易平台的成熟尚需时日，资产端供给还未跟上。**由于资产的证券属性，因而此类通证需在证券交易平台进行交易，然而**多数以证券形式融资的通证均伴有锁定期**，例如通过美国 Reg D、Reg CF、Reg S 融资的通证都有 12 个月的禁售期（RegS 最短情况下 6 个月），**实际目前还无法广泛流通。**截至 2018 年 10 月，美国 SEC 总共只批复

了 39 个融资项目，其中还包括 Telegram 等以 SAFT 形式融资的功能型通证。以这种速度估算，证券类通证要大规模爆发，还需时日。不过好在我们已经能够看到除了利用证券类通证合规融资属性的项目外，真正的资产通证化项目出现，例如 10 月，纽约曼哈顿一处价值 3 千万美金的公寓在以太坊上被予以通证化，让我们看到了进一步发展的潜力。

- **多数国家对于数字资产融资的政策也还没有明确**，或者还在沙盒测试阶段。而各类资产通证化的前提，是监管机构对此类资产合法性的肯定，并有明确的监管方式。目前除了美国外，大部分国家在这一板块均还处于探索阶段，而**即便是美国，操作一整个证券通证发行，也需要消耗大量的时间和精力**，使得其难以像原本数字资产众筹那样快速爆发。

（9）稳定币从交易转向应用和支付，基于稳定币的“PayPal”将会出现

2018 年系稳定币的大年，出现了多个致力于改良 USDT 的合规法币抵押稳定币，亦有了一批致力于通过其他模式实现价值稳定的稳定币项目。然而目前，**大部分的稳定币还是以充当交易媒介的形式存在**，通过**与交易所、OTC 批发商、机构交易者合作的形式拓展规模**，从区块链地址上看，大部分的稳定币被存储在交易所的冷热钱包地址，便是很好的例证。

2019 年，我们认为，这一现象有望被逐步改变，**稳定币将从交易转向应用和支付，而区块链时代的“PayPal”，基于稳定币的支付解决方案提供商也将会逐步浮现，而这是基于如下的理由：**

- **Dapp 的逐步发展，需要稳定的支付解决方案。**目前，用户在 Dapp 中使用的均是底层公链的通证，例如以太坊和 EOS，**其本身价格的相对波动性，对于 Dapp 沉淀资产和用户，是一个很大的挑战**，数字资产市场价格的波动，或多或少会影响用户在 Dapp 之中的行为和资金流入流出，这部分是 Dapp 开发者难以把控的，而采用稳定币，则可以很好解决用户的行为波动，让资金流入流出，只和 Dapp 本身有关。**另外，Dapp 的发展还面临传统用户“场外—场内”入金问题**，而各类合规法币抵押稳定币，由于具备入金功能，且有监管背书，则可以很好地解决 Dapp 的用户拓展问题。**我们坚信，这部分需求，会被基于稳定币的支付解决方**

案提供商所发现，为不同的链提供稳定币产品（无论是通过直接多链发行，还是借助跨链网关形式进行互通），并为相应链上的 Dapp 提供支付解决方案，打造新时代的“PayPal”，将成为 2019 年重要的一环。

- **数字资产支付服务商本身模式变革的要求。**目前大部分的数字资产支付服务商的业务模式，是通过一系列风险对冲手段和工具的形式，实现稳定。例如用户汇款法定货币，服务商收取法定货币后会兑换成数字资产，并与市场上的经纪商等主体签订差价合约（类似 Swap），之后向收款人地址汇款，并协助收款人将数字资产转换成法定货币。通过差价合约形式，价格上升时，服务商支付差价，价格下跌时，服务商收取差价，以此保证价值稳定。**这种方式相对复杂，要求较高，且依赖市场上有愿意做差价合约对手方的资金，而若直接通过稳定币，则省去了上述的步骤，业务模式更为简单、稳定和有效。**

（10）主流国家监管持续优化，示范效应引多国效仿，牌照、沙盒将普及

2018 年系数字资产市场合规化元年，全球市场正式进入合规阶段。虽然目前包括美国、新加坡、日本、香港等在内的主流国家和地区对数字资产的性质、发行与销售、流通与交易等重点行为进行了规定和约束，**然而客观地讲，很多监管条例仍处在摸索和初级阶段，其正确性尚未经过时间和市场的验证。**我们认为，如果说 2018 年是数字资产市场真正意义上的合规元年，那么 **2019 年便是监管规则逐步在执行中进行验证、优化和落定的一年，并真正开始引发资源、资金向监管体系更为成熟、完善和友好的国家流动，这一示范效应将促使多国积极效仿，甚至开启监管层面的竞争：**

- **“牌照+沙盒”将成为监管规则持续优化的重要特征。**目前数字资产市场还处在早期阶段，变化较快，因而对数字资产的监管本身理应是个动态的过程，且需要整个行业与监管机构的共同努力，单纯的集中式监管往往滞后，并难以满足行业发展需求。**采用“牌照+沙盒”结合的监管模式，对大部分基础、业务模式已相对固定的数字资产业务发放牌照，再对新兴、创新型的数字资产业务采用沙盒监管，**既能保证合规，又不至于束缚创新，真正实现监管体系在执行中验证、优化和落定。

- **监管体系完善所带来的资源、资金向监管体系更为成熟、完善和友好的国家流动，这一示范效应是促使多国积极效仿甚至在监管层面进行竞争的核心原因。**我们预计，2019 年，不同国家、地区针对区块链、数字资产的监管体系对地区性市场和行业的影响会越来越大。基于我们的观察，2018 年的监管更多是对“合规与否”进行定性，并对不合规的行为和相关业务进行处罚，2019 年的监管，我们预计，则会真正偏向于让优质的企业脱颖而出，对合规与不合规的企业、行为进行差别对待，是引流的，这将导致资源、资金的流动，大部分的企业、项目和创业者会倾向于集中至监管体系更为成熟、完善和友好的国家。而部分走在后面的国家，为了吸引优质的区块链企业，发展区块链产业，**亦会加入到这一场合规化进程中，甚至会在监管体系上形成国家层面的竞争，以此鼓励优秀的人才、资源入驻，而部分小国例如马耳他等对区块链展示出的极大友好，已经显现出这一端倪。**

六、火币研究院系列报告目录

目前，火币研究院的系列报告分为**不定期的 6 个系列深度报告、定期的 4 个系列常规报告**和**“演讲精华与访谈”系列**，火币研究院会根据市场情况持续完善相关报告类型，具体已撰写的系列报告目录如下，可在我们的官网（http://research.huobi.cn）或简书（搜索“火币区块链研究院”）查阅：

一、产业专题系列

2018-05 全球区块链产业全景与趋势报告（2018 上半年）

2018-05-28 火币区块链产业专题报告-公链平台篇

2018-08-01 火币区块链产业专题报告-游戏篇

2018-08-07 火币区块链产业专题报告-钱包篇

2018-08-30 火币区块链产业专题报告-区块链技术可扩展方案分层模型

2018-10-15 火币区块链产业专题报告-跨链篇

2018-10-28 火币区块链产业专题报告-合规基础设施系列（上）——稳定币

2018-12-3 火币区块链行业专题报告-区块链四层应用模型的构建与解析

2018-12-10 火币区块链行业专题报告-合规基础设施系列（中）——资产托管

二、精华演讲系列

【演讲稿】共赢 我们都在同一条船上

【演讲稿】区块链如何改造生产关系

【演讲稿】区块链的本质、意义与商业体系设计（清华 X-lab 公开课）

【演讲稿】我们现在处于区块链经济的 1776 年

【演讲稿】我们离真正的区块链经济有多远

【演讲稿】区块链重构云服务生态

三、火线视点系列

2018-04-01【火线视点】分钟回顾“麻吉宝”事件

2018-04-16【火线视点 1】怎样打造一款比“头号玩家”更火的爆款区块链游戏？

2018-04-30【火线视点 2】纳斯达克的区块链冲锋号角

2018-05-04【火线视点 3】从 ERC20 漏洞事件看区块链安全生态建设

2018-05-17【火线视点 4】CFTC 向左，SEC 向右？美国芝商所推出 ETH 汇率指数

2018-05-26【火线视点 5】马德里 DES 展会结束之际，为 GDPR 庆生

2018-05-31【火线视点 6】复盘 EOS 安全事件及再议区块链安全

2018-06-30【火线视点 7】火币区块链研究院带你认识 ERC721 标准

2018-07-05【火线视点 8】没有免费的午餐—从 EOS RAM 价格看公链通证经济体系设计

2018-07-22【火线视点 9】Fomo3D：天使还是魔鬼？

2018-08-13【火线视点 10】Vitalik 的“99%容错共识算法”解析

2018-09-06【火线视点 11】网易《逆水寒》，走出传统网游区块链改造的第一步

2018-09-10【火线视点 12】存证上链里程碑时刻：区块链电子存证法律效力得到最高院确认

2018-10-13【火线视点 13】软分叉将比特币链上扩容 3584 倍？Bitcoin Forward Blocks 剖析

2018-10-22【火线视点 14】DApp“FarmEOS”24 小时成交额破亿，EOS 生态应用潜力在哪？

2018-11-02【火线视点 15】香港数字资产监管新规解读：正式宣告进入全面监管时代

2018-11-13【火线视点 16】谁才是真正的比特币现金？BCH 社区或将迎来大规模“算力战争”

2018-11-19【火线视点 17】从“SEC 关于数字资产证券声明”看美国数字资产监管

2018-12-12【火线视点 18】以太坊的硬分叉升级—君士坦丁堡

四、超越白皮书系列

2018-05-08【超越白皮书 1】EOSIO 程序实测分析与技术建议

2018-06-01【超越白皮书 2】EOS 主网上线前夕的实测分析与技术建议

2018-07-12【超越白皮书 3】DAG 技术解析与实测

2018-07-16【超越白皮书 4】Bancor 算法的数学、经济学解析与参数测算

2018-09-06【超越白皮书 5】BFT 类共识协议概览与分析实测

2018-11-05【超越白皮书 6】智能合约技术研究与 EVM 实测分析

五、数海拾趣系列

2018-06-21【数海拾趣 1】火币区块链大数据产品及近期研究结论

2018-07-21【数海拾趣 2】比特币巨额转账研究

2018-09-04【数海拾趣 3】分类算法解析推测比特币持有者类别与流向

2018-11-19【数海拾趣 4】五种稳定币数据的深度解析

2018-12-28【数海拾趣 5】比特币十周年数据解析

六、难链的经系列

2018-05-16【难链的经 1】通证经济学的诺奖理论基础

七、火量学派系列

2018-07-03【火量学派 1】区块链行业 Smart Beta 的探索

2018-07-07【火量学派 2】Markowitz 投资组合理论在数字货币上的应用

2018-07-30【火量学派 3】海龟交易法则在数字资产上的应用

2018-09-27【火量学派 4】缠论在数字资产上的应用（一）：脉络梳理

八、定期报告系列

1、区块链行业周报（1-47 期，截止目前共 47 期）

火币区块链行业周报（第一期）2018.3.5-3.11

…

2、区块链大数据周报（1-30 期，截止目前共 30 期）

火币区块链大数据周度数据洞察（第一期）2018.6.6-6.13

…

3、区块链行业月报（1-12 月，截止目前共 12 期）

2018-01 全球区块链资产行业月报-1 月

…

4、情绪指数报告月报（3-12 月，截止目前共 10 期）

火币数字资产投资者情绪指数报告（2018 年 3 月）

…