全球区块链产业全景与趋势报告

（2018 上半年）

火币区块链研究院

2018.5

Huobi Research

全球区块链产业全景与趋势报告（2018 年上半年）

2018 年 5 月

【作者】

袁煜明
朱翊邦
肖　晓
郭大治

huobiresearch@huobi.com

摘要：

2017 年数字资产市场经历了自比特币问世以来的第三次牛市，这次牛市不再是比特币一枝独秀，而是“智能合约系”数字资产百花齐放，**代表了数字资产行业从点对点现金的共识到智能合约共识的进步**。市场自 2018 年初开始转冷，直到 4 月中旬，伴随**多个 DPoS 共识机制项目的超级节点竞选，**才逐步企稳并伴有回暖迹象。投资者情绪调查显示**大众对未来市场走势仍然乐观**，71%认为下半年总市值将上升 30%以上。

2017 年数字资产众筹经历爆发式增长，成功项目合计融资额达到 2016 年同期的 23 倍。**2018 年新增众筹项目破发率走高，3 月一度达到 67%，**但仍有如 Zilliqa 等优质项目市场价格突破众筹价的 34 倍，未来资金将进一步向头部项目聚拢。2018 年上半年出现**首例成功的 DAICO 模式众筹，**此类众筹模式将被更广泛的地采用，同时**美国众筹正转向合规，Reg A+，Reg D 也将开始流行。**

未来数字资产市场将存在六大逻辑。**渗透逻辑：**加密金融向传统金融渗透；**应用逻辑：**市场将由“场景+区块链”的升级逻辑引领；**并购逻辑：**将出现更多数字资产对互联网流量级应用的并购，让优质应用在上链赋能的同时实现数字资产退出；**用户逻辑：**用户数量继续增加，且将有更多二级市场机构进场；**代际逻辑和性别逻辑：**用户平均年龄由青年转向中年，女性比例有望进一步提高。

合规和监管方面，**2018 年 2 月美国 SEC 明确了大部分数字资产众筹的证券属性，并类比证券市场强化对其监管，预计将有更多国家效仿。**另外，日、韩率先成立自律组织，未来各国将呈现**集中监管和自律组织并行的状态**。短期之内**世界联盟监管仍存在空窗期。**

我们将区块链产业划分为硬件、基础设施；区块链底层平台；通用技术；垂直应用；服务设施五大板块。2017 年平台与基础层的竞争尤为激烈。**下半年仍需重点关注底层平台和通用技术**，随着接下来几个月各大平台的主网上线，底层平台的竞争格局或将逐步清晰。

技术方面，目前区块链的性能尚不能支撑大规模的应用落地，**扩展性、隐私性、互通性**是主要瓶颈，但过去一年中各方面都有新的解决方案不断涌现，且近期出现了 **DAG、哈希图等区块链之外的新型分布式账本技术**。预计 2018 下半年区块链技术的迭代将进一步加快。

目录

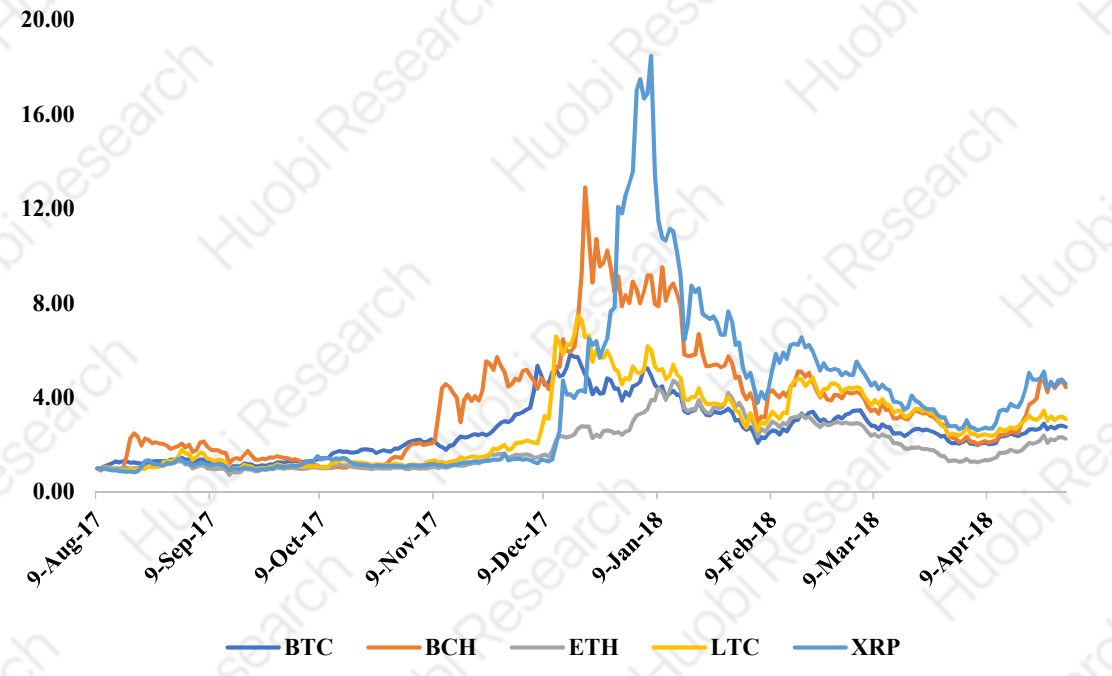
一、数字资产投资市场回顾与展望

自比特币 2009 年初诞生起，数字资产市场开始出现。根据 Coin Market Cap 数据显示，截至目前，全球共有超过 1,600 多种活跃数字资产在市场中交易，同时有更多的数字资产存在于我们周围，这些数字资产，共同构成了区块链数字资产主要的投资交易市场。

1.1 数字资产市场转为冷静，蓄势待发

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 4 月中旬，前五大数字资产“比特币”、“以太坊”、“瑞波币”、“比特币现金”、“莱特币”的价格跌至去年 10 月左右水平，价格亦较顶点缩水 70%以上。

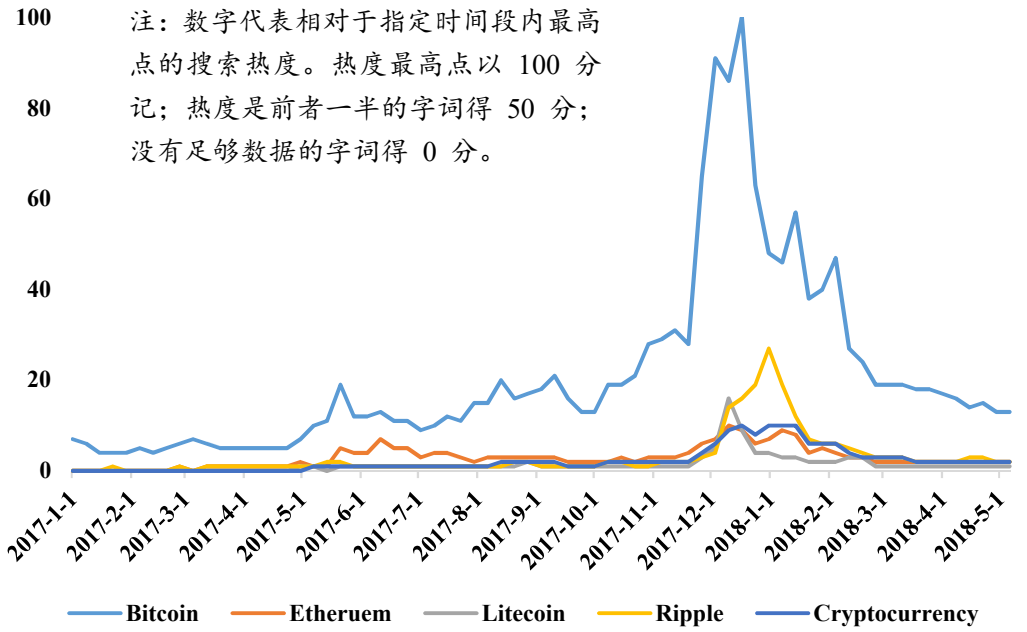
图1：前五大数字资产价格指数走势图



来源：火币区块链研究院整理

除价格大幅下跌外，数字资产市场的活跃度也大幅下滑：

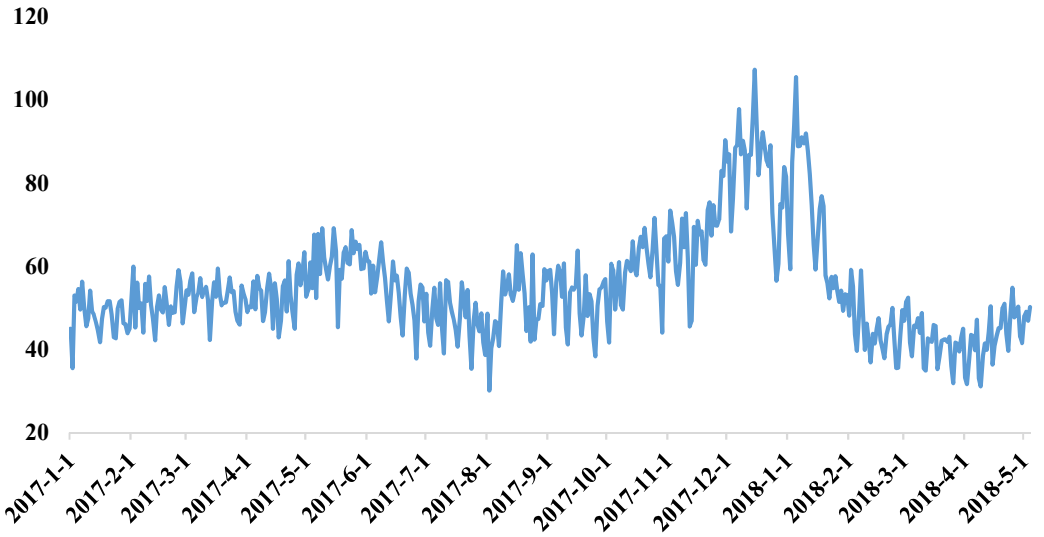
图2：数字资产相关搜索指数



来源：Google Trend，火币区块链研究院整理

比特币在数字资产中关注度较高。2017 年网友对比特币等数字资产的关注逐步上升，于 12 月达到最高点。2018 年，主要数字资产关注度有不同程度的下滑，比特币的关注度下滑最快，4 月底搜索热度最低点仅为最高点的 12%。

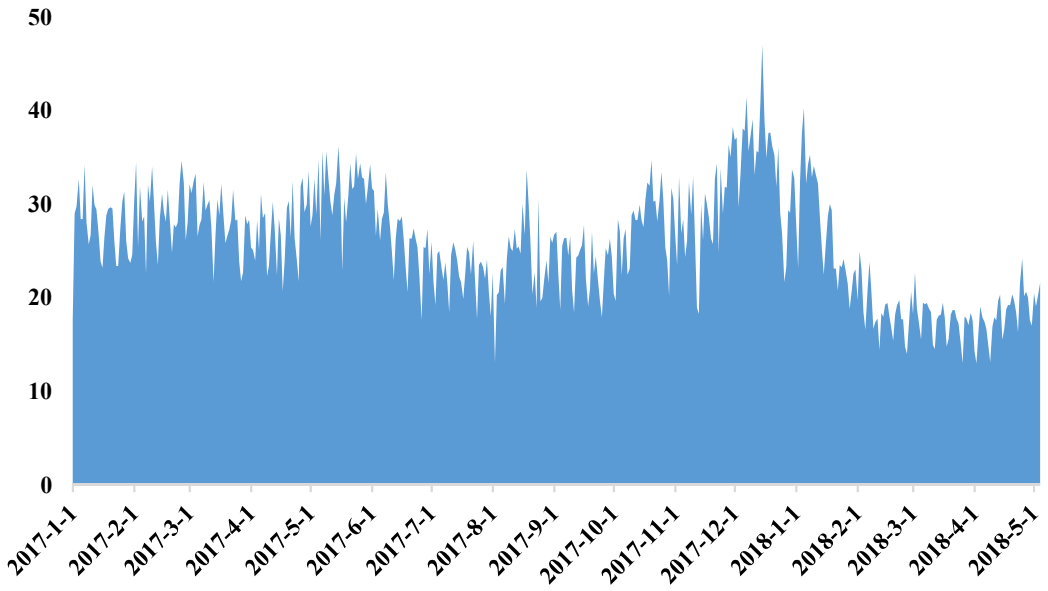
图3：比特币日活跃地址数（万个）



来源：Quandl，火币区块链研究院整理

除 11、12 月的明显上升外，2017 年比特币日活跃地址数整体较为稳定，但进入 2018 年以来明显下降，2018 年 4 月 9 日，比特币日活跃地址数达最低点，相比 12 月 15 日最高点的 107.3 万个相比下跌了 71.0%，直至 4 月活跃度才稍有回升趋势。

图4：比特币日交易量（去除最活跃的 100 个地址的每日比特币交易笔数：万笔）



来源：Quandl，火币区块链研究院整理

与关注度和钱包活跃度对应，2017 年比特币日交易量稳中有升，2017 年 12 月 15 日，比特币日交易量超过 47 万笔，达到历史最高点。而自 2018 年以来，随着数字资产市场行情转冷，比特币日交易量也一路下跌，4 月 2 日达到一年半一来的最低点 13 万笔，较最高点下滑 72.4%。

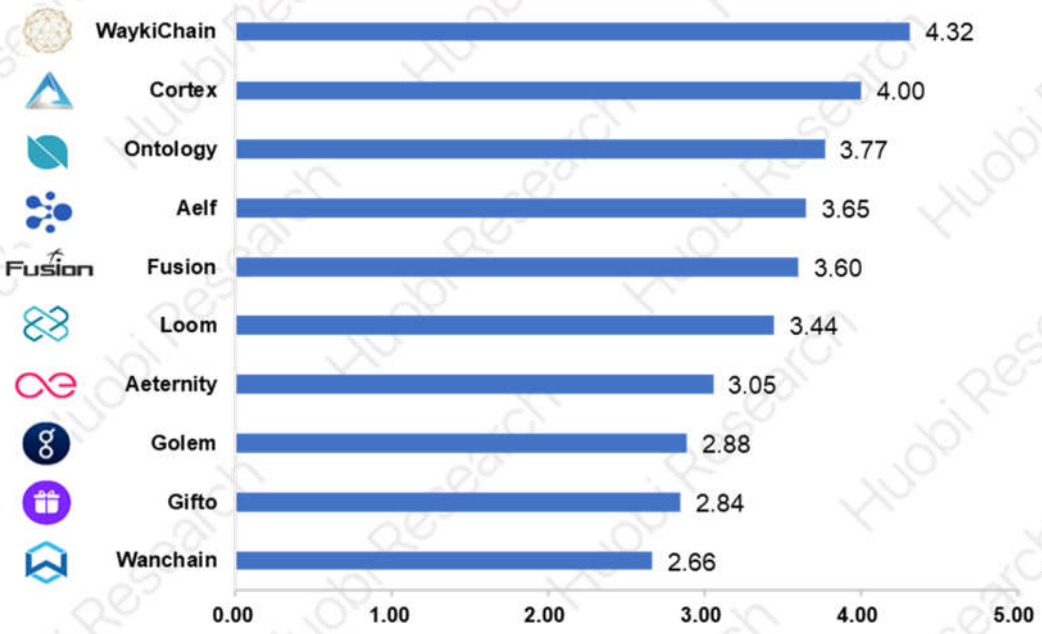
进入二季度后，随着美、日税季结束，市场二次探底无果，市场情绪有所恢复，行情逐步开始呈现分化态势，小行情出现：

- **超级节点竞选引爆小行情**

进入 4 月中旬，数字资产市场逐步企稳，在多个采用 DPOS 共识机制的项目如 EOS、CMT、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。火币区块链研究院跟踪了市值排名前

100 的主要数字资产，2018 年 4 月，涨幅前十的数字资产如下（包括部分冲入前 100 的数字资产）：

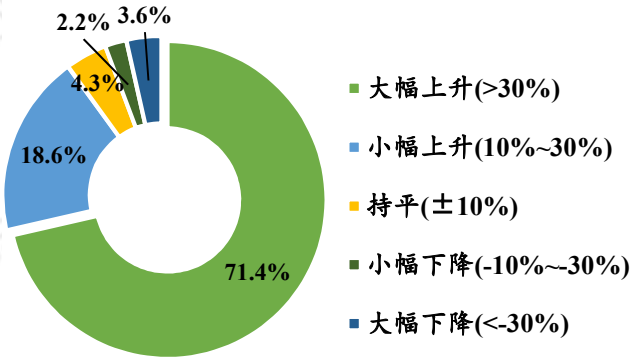
图5：2018 年 4 月起 TOP100 数字资产中涨幅前十榜



来源：火币区块链研究院整理

➢ 市场情绪仍看多 2018 年下半年走势

图6：投资者数字资产市场期望-中期



来源：火币区块链研究院市场情绪调查

虽然进入 2018 年后，数字资产市场整处于下跌趋势，但市场对 2018 年仍旧看好。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 2018 年下半年走势仍较为看好，认为将小幅上涨。根据最新的市场情绪调查，90.0%的投票者认为未来半年的数字资产总市值会上升，其中 71.4%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 数字资产众筹市场略有降温，但整体金额仍较大

数字资产众筹，指代围绕数字资产进行的一种众筹方式。在众筹过程中，一定量的众筹份额，会以数字资产的形式出售给投资者，以换取如比特币、以太坊等主流的数字资产。

2017 年新兴数字资产爆发，相关融资金额快速增长。据 Token data 数据，2017 年，总共有 435 个数字资产众筹项目成功发行落地，占同期 913 个发起的数字资产众筹项目的 47.65%，成功率接近一半，上述成功项目合计融资金额超 56 亿美金，大幅超越 2016 年同期金额 2.4 亿美金，另有部分数字资产众筹项目融资金额达 1 亿美金，包括基础设施项目“Filecoin”筹集 2.57 亿美金，公有链项目“Tezos”筹集 2.32 亿美金，以及跨链项目“Polkadot”筹集 1.45 亿美金等。

图7：2017 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
Filecoin	分布式存储	2017 年 9 月	$257,000,000
Tezos	公有链	2017 年 7 月	$230,498,884
Sirin Labs	硬件设备	2017 年 12 月	$157,885,825
Bancor	数字资产交易	2017 年 6 月	$153,000,000
Polkadot	跨链设施	2017 年 10 月	$145,171,723
Qash	数字资产交易	2017 年 11 月	$106,400,000
Status	社交应用	2017 年 6 月	$107,664,907
Kin	去中心化市场	2017 年 9 月	$98,500,326
Cosma	跨链支付	2017 年 11 月	$95,614,242
TenX	支付结算	2017 年 7 月	$80,000,000
合计			**$1,431,735,907**

来源：ICO Drops、火币区块链研究院整理

2017 年也是众筹数字资产增值幅度较大的一年，部分 2017 年的头部项目，至今增值幅度仍高达甚至接近百倍，极少数项目增值幅度超越千倍。其中，以法币计价，截至 2018 年 4 月 30 日，增值幅度最高的项目 Spectrecoin，其众筹至今增值幅度为 741.42 倍，而若是按其最高点价格，增值幅度更是高达 8,288.18 倍，而其余头部项目中，明星项目 Qtum 增值幅度最高也达 347.97 倍。

图8：2017 年增值幅度前十大数字资产众筹项目

	项目名称	众筹时间	众筹价格	目前价格	增幅	最高增幅
	Spectrecoin	2017-1	$0.001	$0.60	741.42x	8,288.18x
	Particl	2017-4	$0.134	$16.70	124.87x	384.10x
	Neblio	2017-8	$0.178	$15.06	84.83x	365.40x
	Populous	2017-6	$0.301	$24.50	81.35x	251.25x
	Qtum	2017-4	$0.307	$22.64	73.71x	347.97x
	Augmentors	2017-2	$0.015	$0.96	64.00x	140.00x
	OmiseGo	2017-6	$0.326	$17.55	53.83x	76.13x
	Icon	2017-9	$0.106	$4.59	43.30x	107.83x
	Tron	2017-9	$0.002	$0.085	42.80x	99.20x
	Zrx	2017-8	$0.048	$1.23	25.63x	52.71x

来源：ICO Drops、火币区块链研究院整理，截至 2018 年 4 月底数据

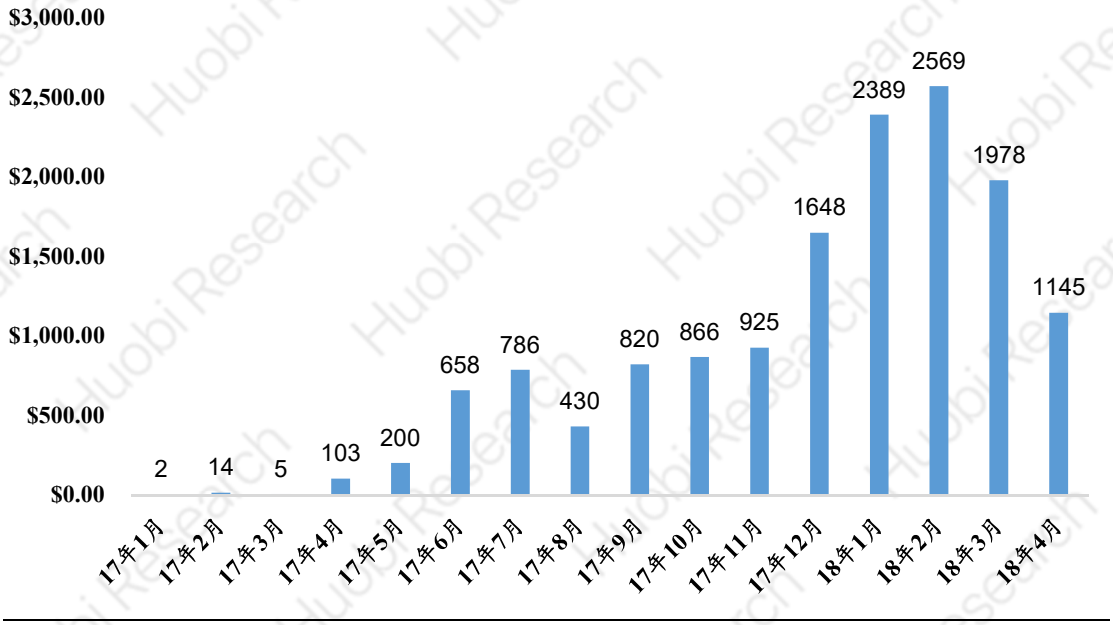
进入 2018 年，数字资产众筹市场有所降温：

- **融资金额环比下降，但整体金额仍较大**

火币区块链研究院持续跟踪市面上的数字资产众筹项目。进入 2018 年，数

字资产众筹项目融资金环比逐步下降，4 月份数字资产众筹融资金额为 11.45 亿美金，与 2 月高点金额 25.69 亿美金相比已缩水约 55%，但从整体来看，2018 年数字资产众筹融资金额仍较大，且已超过 2017 年全年总和。

图9：2017 年至今数字资产众筹融资金额（单元：%、百万）



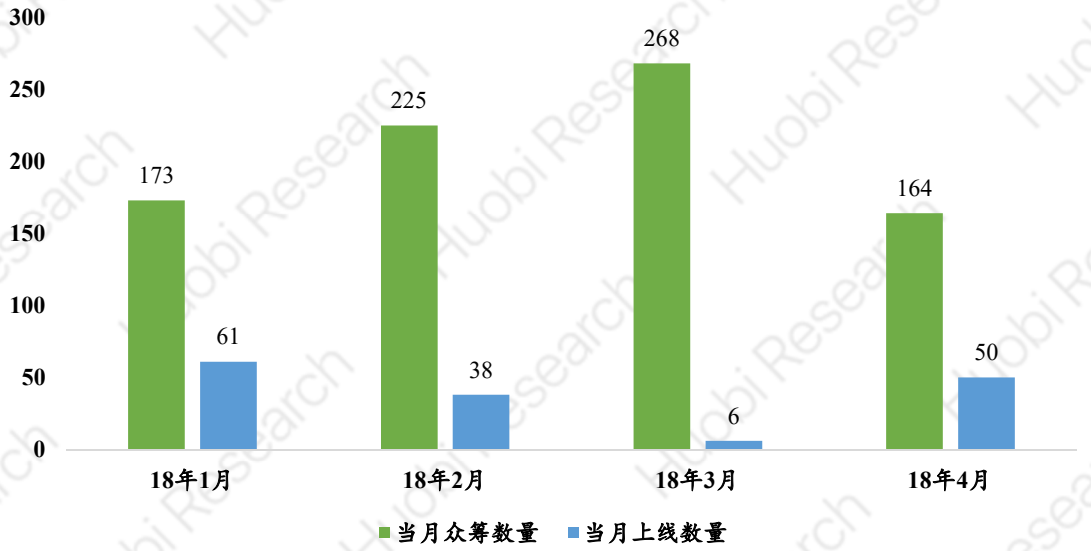
来源：Token Data、火币区块链研究院整理

2018 年数字资产众筹融资金额仍较大，主要是受到部分头部项目影响所致，Telegram 于 2018 年 2 月及 3 月分别筹集约 8.5 亿美元，合计筹资 17 亿美元，另 EOS 持续进行众筹，根据 Token data 数据，截至 4 月底，自 EOS 开启众筹以来，已合计筹集约 33 亿美金，若剔除相关影响，2018 年，数字资产众筹融资金额环比下降幅度则更大。

- **监管强化，流动性降低**

火币区块链研究院跟踪每月新增数字资产及其当月底上线交易所的比重。2018 年 1-4 月，新增数字资产当月上线率分别为 35.62%、16.89%、2.23%及 30.49%，呈现逐步下降态势，并于 3 月达到最低点，4 月快速回升。2-3 月新增数字资产上线率快速走低，主要系全球监管机构尤其是美国 SEC 对数字资产流通交易方面的限制，另一方面，市场环境较差，项目方主动推迟上线。直到 4 月中下旬，市场迎来小行情，新增数字资产项目上线率回升，流动性略有改善。

图10：2018 年数字资产众筹当月上线率统计（单位：个）

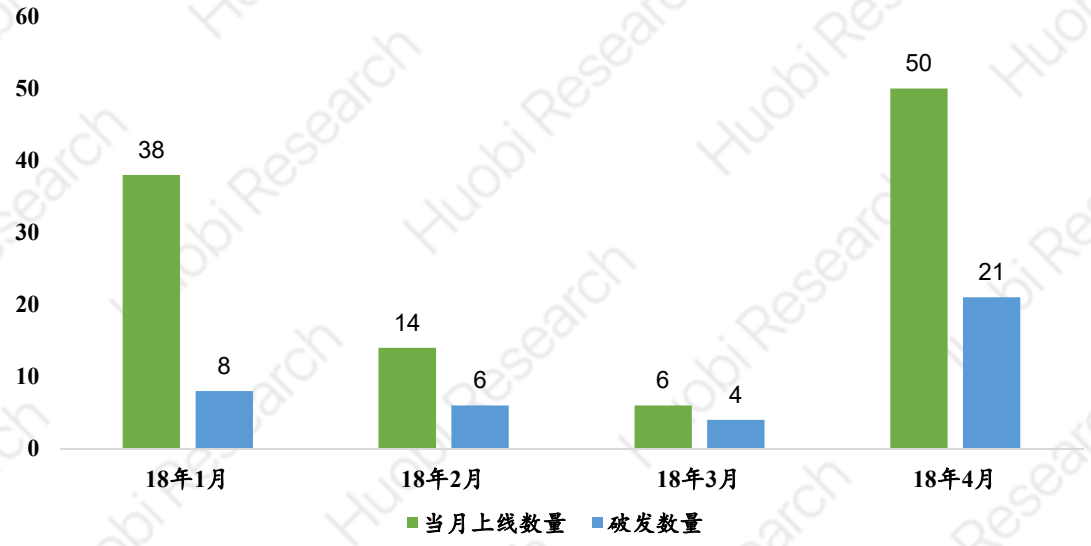


来源：www.icodata.io、火币区块链研究所整理

➢ **市场滑铁卢，破发率快速上升，但头部项目增值幅度仍较高**

2018 年，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，受到过多众筹项目对二级市场资金分流，以及以太坊本身价格下跌的影响，新增数字资产价格面临滑铁卢。2018 年 1-4 月，新增数字资产项目破发率分别为 21.05%、42.86%、66.67%和 42.00%。

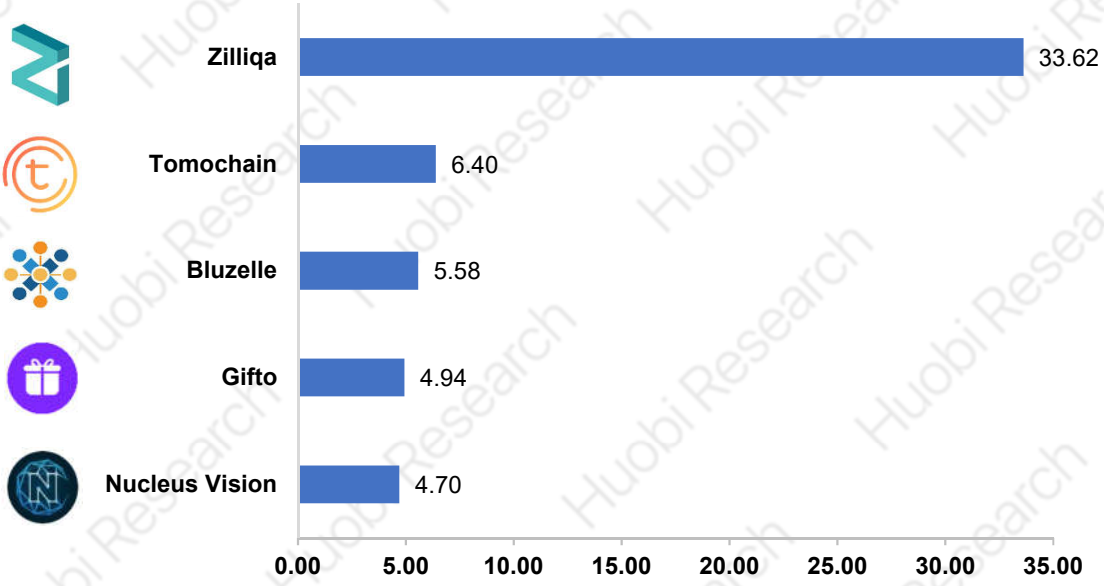
图11：2018 年数字资产众筹破发数量统计（单位：个）



来源：www.icodata.io、火币区块链研究所整理

虽然 2018 年上半年数字资产众筹项目上线后破发率走高，但是部分头部优质项目仍保持了较高的增值幅度，其中，收益率排名前五的为 Zilliqa、Tomochain、Bluzelle、Gifto 以及 Nucleus Vision，4 月底市场价格分别为众筹价的 33.62 倍、6.40 倍、5.58 倍、4.94 倍和 4.70 倍。

图12：2018 年数字资产众筹项目至今增值幅度（单位：倍）



来源：火币区块链研究院整理，以截至 4 月底数据为基准

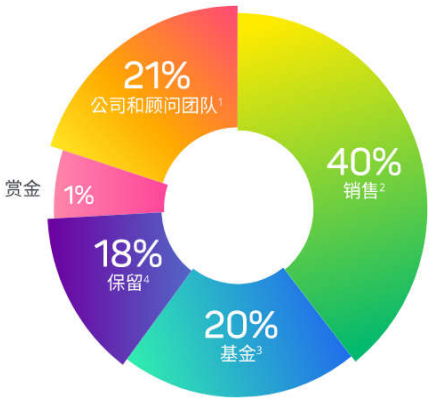
数字资产众筹市场降温，回归理性是必然趋势。未来，我们可能将不太轻易见到百倍、千倍的项目，但我们会越来越容易看到，资金向优质项目集中，尤其是向合规、合法背书项目集中，新的逻辑正在涌现：

- **数字资产众筹 2.0：以 DAICO 形式募集资金**

传统数字资产模式的局限性在于，信息的不对称性，以及投资者对项目方缺乏有效的约束性。不对称性体现在，众筹融资大多系“白皮书”融资，创业者掌握所有信息，而投资者掌握信息量较少，真假难辨；投资者对项目方缺乏约束性体现在目前还不具有相关的机制、法规对项目资金使用、落地执行、信息披露等进行约定，完全依赖项目方的自我约束，作为一种“先融资、再创业”的典型，圈钱跑路等行为时有发生，给投资者，特别是普通散户投资者造成了巨大的损失。

2018 年 1 月，以太坊创始人 Vitalik Buterin 提出新的数字资产众筹融资模式——DAICO。该模式将去中心化自治组织的功能加入了传统众筹中，为众筹加上一层智能合约，给项目方募集的资金安上“资金阀”。DAICO 模式下，资金募集完成后，项目方并不完全拥有资金的自由支取权利，资金的使用最终取决于项目的推进情况，并由数字资产持有者投票进行决定；同时，在极端情况下，项目方欺诈，项目开发不理想时，数字资产持有者也可以通过投票，终止智能合约，剩余的资金将按照持有数字资产的比例原路返还给投资者。

图13：The Abyss 数字资产分配结构



来源：The Abyss、火币区块链研究院整理

分布式游戏分发平台 The Abyss 是第一个采用 DAICO 智能合约进行募集的项目，该项目于 2018 年 4 月 18 日启动发行，5 月完成募资，共筹集 18,511 个 ETH，199,901 个 BNB，合计金额约 1,536 万美金。根据约定，分配给公司的 ABYSS 数字资产将由 DAICO 智能合约冻结两年，分配给基金的 ABYSS 数字资产将由 DAICO 智能合约冻结一年。

➢ 以证券形式合规募集资金

与 DAICO 模式刚刚开始试水不同的是，目前已有一批区块链项目正转向传统 IPO 审核背书的形式募资。关于数字资产众筹是否属于证券发行，历来存在较大的争议，由于未经注册或豁免进行证券销售系违法行为，此前，大部分项目方多借助将数字资产认定为“Utility Token”的形式规避监管和注册审查。

进入 2018 年后，随着美国证监会启动对各类数字资产众筹项目及相关机构的调查，越来越多的区块链项目正抛弃“Utility Token”这种可能存在合规隐患的方式，转而承认数字资产的证券属性，规避法律风险，同时获取法律信用背书。目前，大部分区块链项目正逐步接受通过如下豁免注册证券发行条款的形式进行募资：

Reg A+ offering

适用于小型初创公司的 IPO 规则，隶属 2012 年美国 JOBS 法案的一个条例，2015 年施行，允许美国、加拿大注册的中小企业在 12 个月内向大众投资者公开筹集最多不超过 5000 万的美金，可进行公开宣传，无限售，不涉及注册证券，但需提交发行通知，较白皮书信息披露更为详实，但代价是必须在证监会注册的国家级证券交易所进行交易。

Reg D offering

系美国证监会制定并于 1982 年实施的关于私募证券发售规则，下设 Rule 504，Rule 506（b）和 Rule（c）三类发行准则。ICO 项目多采用后两者，Rule 506（b）无融资金额限制，不可公开宣传，需向合格投资者发行，对合格投资者数量无限制，要求非合格投资人数量控制在 35 人以下，Rule（c）无融资金额限制，可公开宣传，但只能对合格投资者销售。发行证券后 15 日内需向美国证监会提交发行通知，且有 12 个月禁售期，另必须在证监会注册的国家级证券交易所进行交易。

Reg S offering

系美国证监会为保护本国投资者利益出台的离岸证券发售规则，该规则允许向非美国本土投资者离岸出售的证券豁免注册，离岸指代投资者不在美国本土，交易市场位于境外。

来源：SEC、火币区块链研究院整理

1.3 回望过去：最近这次牛市和曾经的牛市有什么不同？

比特币从诞生至今，共经历了三次牛市，而最近的这一次，与过去不同：

图14：第一次：2011 年 4 月至 2011 年 6 月，冲顶大会，来去匆匆

历时约 60 天，完成从 0.75 美金到 30 美金的上涨，涨幅逾 38 倍，而此时距比特币最初诞生时的 0.06 美金，已暴涨 492 倍。这一次的暴涨主要由于当年 3 至 4 月比特币与英镑兑换交易平台上线，随后《时代周刊》、《福布斯》等美国主流媒体相继发表比特币相关文章，来自更多国家的投资者疯狂涌入炒币行列。此轮暴涨后不久，便爆发了著名的“门头沟”黑客事件，比特币价格快速暴跌，至 11 月的 2 美金最低点，跌幅 94%。

来源：Coindesk、火币区块链研究院整理

图15：第二次：2013 年 1 月至 2013 年 12 月，比特币点对点现金共识

历时约 330 天，完成从 13 美金到 1,147 美金的上涨，中间经历了一小波 230 美金至 66 美金的大回调，合计涨幅超 82 倍，而此时距离比特币最初诞生价已上涨近 2 万倍。这一轮牛市，源于塞浦路斯债务危机所引发的传统金融机构信任危机，后由 2013 年下半年欧洲部分国家出台比特币友好政策所刺激，更多的人知道了比特币，投机客涌入。此轮暴涨后，比特币暴跌至 2015 年 1 月的 210 美金最低点，跌幅 82%。

来源：Coindesk、火币区块链研究院整理

图16：第三次：2017 年 1 月至 2017 年 12 月，区块链智能合约共识

历时近一年，完成了从 789 美金到 19,343 美金的上涨，中间经历了“9.4”事件，比特币价格从 4950 美金至 3226 美金的回调中继，合计涨幅约 20 倍，此时距离比特币最初诞生价已上涨 32 万倍。这一轮牛市，源于以太坊 ICO 爆发所引发；同年，比特币分叉，比特币现金诞生。同过去的暴涨类似，其结局也伴随着暴跌，2018 年 2 月 6 日，比特币跌至 6000 美金，较最高点跌幅达到 68.98%。

来源：Coindesk、火币区块链研究院整理

比特币、数字资产市场存在一定的周期性，其周期性一定程度源于每四年一

次的产量减半，2013 年的牛市系 2012 年比特币产量减半，2017 年的大牛市系 2016 年比特币产量减半。但与过去不同的是，2017 年的牛市不再是比特币的一枝独秀，真正驱动市场上行的逻辑也从原先点对点现金共识，变成区块链技术特别是智能合约的共识，由以太坊为代表的“智能合约系”项目所引领，2017 年：

- **比特币市值占数字资产市场总市值：**87.32%下降至 40.99%
- **比特币市值增长 VS 以太坊市值增长：**13 倍 VS 96 倍
- **数字资产数量：**617 个增长至 1335 个，增长率 116%
- **比特币地址数量增长 VS 以太坊地址数量增长：**1 倍 VS 18 倍

来源：Coin Market Cap，火币区块链研究院整理

1.4 展望未来：数字资产市场去向何方，会有什么新的玩法？

未来，数字资产市场市值将由什么驱动？对于这个市场，未来的一些新的逻辑和玩法可能是什么？火币区块链研究院总结了六大可能影响这个市场的逻辑：

➢ 渗透逻辑：加密金融将向传统金融渗透

图17：数字资产渗透跨境支付

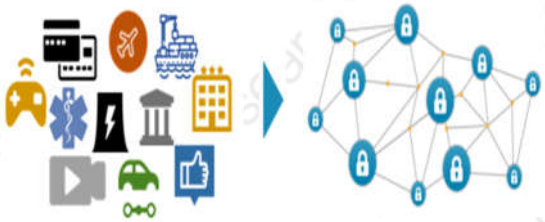
来源：火币区块链研究院整理

数字资产对传统金融体系最大的冲击一方面在于支付，尤其是跨境支付，另一方面在于业务模式。使用比特币等数字资产作为汇款媒介，汇款时间可大大缩短；同时，区块链的分布式登记、清结算，以及可编程的智能合约，可大大降低金融的运营及法律成本，改变金融机构的商业模式。另外，传统金融模式下，资源配置优先向头部靠拢，虽然有助于效率，但丧失了普世价值，很大一部分人事实上并没有享受到金融服务带来的好处，而区块链所衍生出的加密金融，是对每一个人开放的，每一个人都可以拥有一个账户，并享有与之匹配的金融服务，

让金融实现真正阳光普照。我们认为，数字资产由于其在匿名性、无国界性、低门槛等方面的优势，未来，在网络效应的推动下，对传统金融各应用领域的影响会不断加大，分布式的加密金融将会爆发。

➢ 应用逻辑：“场景+区块链”才能真正引爆市场

图18：“场景+区块链”模式

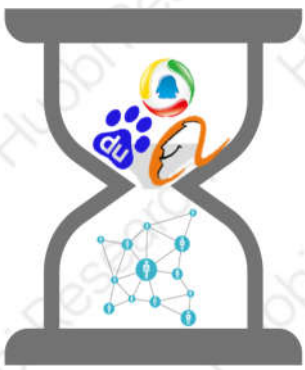


来源：火币区块链研究院整理

火币区块链研究院对市面上基于以太坊的分布式应用 DApp 进行了跟踪。目前，日活排名靠前的应用，除了如 IDEX、以德等去中心化交易所外，主要为部分区块链游戏，然而由于区块链底层的不完善，目前大部分区块链应用，仍是“区块链+场景”，属于自下而上路径，从技术找匹配场景，且与区块链游戏类似，主要通过带有投资、投机性质的玩法吸引用户，实际的体验仍旧较差，难以比拟传统中心化应用。火币区块链研究院认为，只有“场景+区块链”，即从现有针对大众的场景、应用出发，自上而下，通过叠加区块链技术，优化应用生态和体验的模式，才能引爆市场。虽然区块链技术还不成熟，短期之内较难实现“场景+区块链”，但是，仍有一部分低频场景，可进行区块链化，亦或可优先将一部分急需透明化、共识的内容上链，实现落地。核心是，非为了区块链而区块链。

➢ 并购逻辑：区块链将反向收购流量级应用上链

图19：区块链收购流量级应用



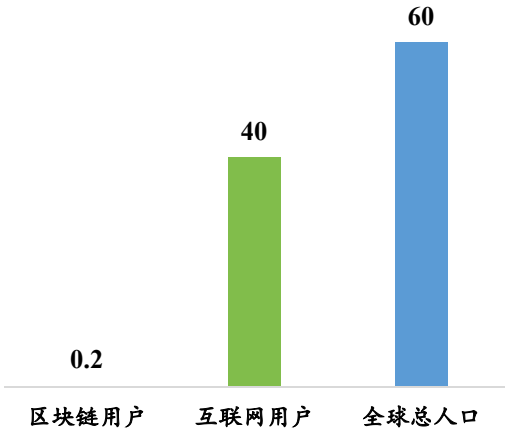
来源：火币区块链研究院整理

传统金融市场中，市值增长主要源于 IPO 新股发售及并购重组。分布式的加密金融市场中，新生数字资产的流通即类似新股上线，而这也是目前数字资产市场总值快速增长的主要原因。我们认为，未来，随着区块链基础设施的不断完善，以及各个领域区块链场景地基搭建完毕，我们也会看到传统金融领域的并购重组方法在区块链中不断得到运用，大量的基础层项目，为了完善其

应用生态，通过数字资产对优质的流量级应用进行收购，实现上链，而一部分优质的应用类初创企业，也会从原先传统并购市场退出，转向区块链数字资产退出。

➢ 用户逻辑：用户数量增长空间大，将助推市场热情

图20：区块链用户数量（亿人）

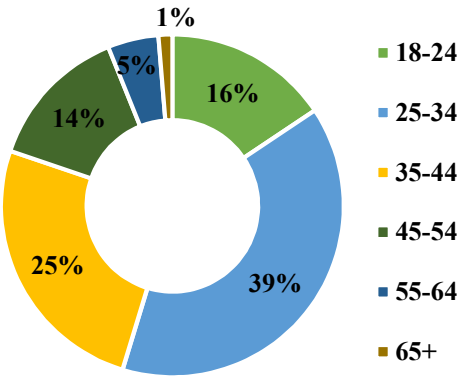


来源：火币区块链研究院整理

目前，全球比特币钱包地址数大约 2400 多万个，以太坊钱包地址数大约 3200 多万个，实际用户可能仅 2000 万，不到全球总人口数的 0.3%，而根据“We Are Social”和“Hootsuite”披露的 2017 年数据，全球互联网用户数已经突破了 40 亿大关，区块链用户数渗透率仅约 0.5%。火币区块链研究院认为，用户的数量增长将刺激区块链社区的活跃度，加快区块链社区建设，进而推动数字资产市值，这就好比新的生产力推动经济体的 GDP 增长。另外，未来将有更多机构，尤其是二级市场的机构投资人将数字资产用作新的投资资产类别，他们的进场将极大扩大资金池，增强市场流动性，并加速规范市场环境。

➢ 代际逻辑：从年轻到普及

图21：比特币社区参与者年龄分布



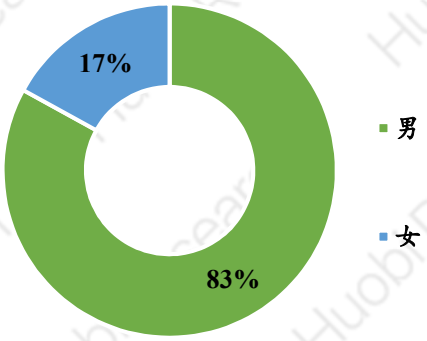
来源：火币区块链研究院整理

火币区块链研究院最新研究表明，比特币社区中大部分用户在 25-34 岁年龄段，约占总用户的 39%。与 CoinDesk 于 2015 年中发表的数据相比，35 岁以下的用户整体占比由 60%降低到目前的 55%。我们认为，随着区块链技术以及数字资产市场的成熟，它们将不再是只有年轻人接受的新兴概念，而是被更广泛年龄段的人所接受的事物，不仅体现在更多拥有经济实力和风险承受能力的中年人把数字资产当做一种资产配置手段，更表现

在针对不同年龄层次的分布式应用出现。

➢ **性别逻辑：从男性到女性**

图22：比特币社区参与者性别比例



来源：火币区块链研究院整理

火币区块链研究院经研究得出：目前，比特币用户中大约有 17%是女性用户，与 CoinDesk 于 2015 年中的 10%相比有较为显著的增加，女性正越来越多参与到区块链、数字资产的新兴潮流中来。一方面，我们认为女性投资人更加谨慎，偏好长远、可持续的投资，更多的女性加入数字资产市场将使得市场更加理性；另一方面，女性作为消费能力最强的群体，也将改变很多分布式应用的开发方向。

总之，我们认为，未来的数字资产市场，从长期来看，可能有如下三大趋势：

第一，将逐步由投资驱动，转向“投资+实用”并进的市场，目前，大部分数字资产的市值主要反映的仍旧是未来预期的折现，投资属性较强，未来，随着 Dapp 生态的成熟，对数字资产的使用型需求会增加。

第二，各类应用场景使用型的需求将会越来越多被数字资产化，并反映到整体市值中去，即上链，而上链所带来的数字资产市场市值的膨胀，可能超乎预期，并成为推动市场爆发的最大因素。

第三，使用型需求的增加，以及各 Dapp、区块链生态之间的交互越来越多，将导致数字资产之间的兑换需求更为频繁，而数字资产与法币之间的挂钩程度越来越弱。

二、区块链及数字资产合规、监管回顾与展望

2.1 区块链、数字资产监管现状及未来主旋律展望

2017 年是区块链技术共识的大年，区块链行业及数字资产众筹趋势在全球呈愈演愈烈之余，也涌现出不少乱象。火币区块链研究院根据世界各主要国家及地区 2016 全年 GDP 以及 2018 年上半年数字资产和众筹政策整理了最新的监管全景图：

图23：世界主要国家及地区数字资产及众筹政策监管最新全景图

来源：火币区块链研究院整理

随着数字资产的热度升级，各国监管对其重视程度越来越高。2017 年底、2018 年初，多个国家政府都逐步开始制定相关的监管框架，对行业进行规范。火币区块链研究院认为应重点关注未来监管领域的如下趋势：

- **美国或将成为世界监管的风向标，吸引各国监管机构效仿：**进入 2018 年后，美国正逐步强化 SEC 对数字资产市场的监管职责，并类比证券市场逐步对数字资产强化在运营牌照、证券发行注册、税项等一系列层面的监管。而继

美国之后，德国、新西兰等国家也将数字资产纳入证券监管范畴。2018 年 4 月，纳斯达克 CEO 宣布时机成熟后将考虑进军数字资产交易，或将进一步促使美国加速相关监管政策的出台，包括“证券类数字资产”与“实用类数字资产”的划分标准等，火币区块链研究院认为，未来可能将有更多国家效仿美国，基于证券监管体系推衍数字资产监管体系；

- **监管制度方面，未来将形成集中监管和自律组织并行的状态：**数字资产还处在早期发展阶段，且存在较高的专业性和技术性，需要集中化的政策指导，日本是典型通过立法确立数字资产合法地位，并采用牌照制监管的国家，美国是实操层面实用类数字资产和证券类数字资产分级管理的国家，未来，火币区块链研究院认为，将会有更多国家采取类似的集中化监管体系。另一方面，行业自律组织是集中式监管的有效补充，在全球监管政策尚未完善之前，成立自律组织有利于推动行业健康发展，比如在日本数字资产交易所 Coincheck 遭到黑客攻击后，由 16 家注册数字资产交易所组成的数字资产商业协会（JCBA）宣布将合力制定行业内投资者安全标准，包括数字资产众筹准则，又比如韩国也于 2017 年 12 月成立区块链协会，目前已有 23 家数字资产交易所加入，致力于实施自我监管并制定相关行业准则；

- **代表性国家的法律完善将推动全球联合监管，但短期内联盟政策出台尚需时日：**在 2018 年 3 月的 G20 峰会上，各国都表达了对待数字资产监管问题的立场，但由于各国态度仍存在分歧，最终并未明确具体监管措施。在此之前，法、德并在加速建立自己的相关监管制度的同时，也曾向 G20 主办国发信，呼吁对其采取跨国界的行动，并对外宣布将大力推动欧盟监管体系的完善。我们可以期待，在世界主要国家和地区落地自身完善的相关法律体系之后，跨国界的联盟监管体系也将应运而生。

2.2 世界主要区块链国家和地区监管透视

火币区块链研究院对世界主要区块链、数字资产国家和地区的监管政策进行了跟踪，并制定了如下评估体系，对监管程度进行考察：

- **是否允许数字资产用于支付**
- **是否允许数字资产交易所境内运营**
- **是否允许首次数字资产众筹**
- **是否允许公民进行数字资产投资**

同时，我们引入监管严格指数，综合上述评估体系，对各国家和地区对区块链、数字资产的监管程度按照强弱进行评分：从一颗星到四颗星，星数越多，代表该国家和地区监管程度越强，政策越紧，对数字资产态度偏保守和不认可，星数越少，代表监管程度越弱，政策越宽松，对数字资产态度越接纳。

（1）北美地区

美国：由松变紧，强化数字资产证券属性，监管严格指数：★★★

是否允许数字资产支付

美国国家税务局（Internal Revenue Service，简称 IRS）出于税收的考虑，早在 2014 年发布的投资者指南和规则（IRS Notice 2014-21）中就将数字资产等视为资产而非货币，投资者需对长期和短期的资本利得缴纳相应的税收。总体来看，美国政府并未在法律层面承认数字资产的货币属性，但亦未禁止商户接受数字资产支付。

是否允许交易所境内运营

历来，对于提供数字资产服务公司的管理权主要集中在各州政府手中，各地均有所不同，但大多实施牌照化管理，颁发相应许可证，例如美国数字资产交易所 Coinbase 便在纽约州获得比特币经营牌照。

2018 年 3 年 7 日，美国证券交易委员会（Security Exchange Committee，简称 SEC）发布公开声明，要求交易符合证券定义的数字资产平台必须在 SEC 注册为国家性质的证券交易所或者得到豁免。根据 SEC 国家性质的证券交易所名单显示，主流的 Coinbase、Bittrex、Poloniex 三家美国主流数字资产交易所目前无一在列。这一事件意味着美国监管再一次强化。若交易所涉及证券类数字资产的交易，则可能面临非法销售证券的诉讼。

是否允许首次数字资产众筹

2017 年底，数字资产众筹受到美国 SEC 的不断关注。2018 年 1 月，美国 SEC 查没了德州数字资产银行公司 AriseBank 所持数字资产，叫停了该公司正在进行的 6 亿美金的数字资产融资；2018 年 2 月，美国 SEC 主席 Jay Clayton 在国会的数字资产听证会上申明大部分数字资产可能属于证券，意味着数字资产众筹被允许，但原先数字资产项目以“Utility Token”（服务类数字资产或实用型数字资产）的名义，实际发行证券性质的数字资产已不再容易，数字资产众筹将受到美国 SEC 的监管，并需要进行注册，监管强化。

是否允许数字资产投资

由于美国政府将数字资产认定为资产，因而并未限制数字资产投资，然而在税收层面，相关监管正逐步强化：

2017 年底，IRS 通过联邦法院下令，让全美最大的数字资产交易所之一的 Coinbase 交出其 2013 至 2015 年的客户记录，据 IRS 统计，2013 年到 2015 年，只有不到 900 人为比特币投资交易报税，但有超 1.4 万个 Coinbase 用户进行了比特币交易。Coinbase 后对此进行了反抗，但以败诉告终。2018 年 1 月 31 日，Coinbase 向网站的美国用户邮箱中发送了 IRS 专用的 1099-K 税务表单，并最终将 1.4 万个用户的交易记录上交。另外，2017 年底，美国总统特朗普签署了新的税收法案，认定数字资产交易都将成为应税事项，包括两种数字资产之间的相互交易。

（2）亚洲地区

日本：总体仍宽松，数字资产众筹法规呼之欲出，监管严格指数：★★

是否允许数字资产支付

2017 年 4 月 1 日，日本内阁签署的《支付服务修正法案》生效，承认比特币等数字资产的合法支付地位。之后，比特币支付得到大规模推广，并被预计为日本经济贡献 0.3%的国内生产总值。

是否允许交易所境内运营

日本是少数较早在国家层面对数字资产交易所进行牌照化管理的国家。2017 年 4 月 1，日本内阁签署的《支付服务修正法案》生效，该法案为交易所制定了一系列标准和规则，要求数字资产交易所必须获得日本财政部和金融厅的授

权，并在九月底前向金融厅提交注册登记文件。截至目前，日本已批准了 16 家数字资产交易所。

2018 年 1 月，日本 CoinCheck 交易所发生 NEM 被盗事件，引发了日本金融厅对国内数字资产交易所的强化审查，3 月，金融厅对所管的 Coincheck、GMO Coin、Mr. Exchange 等多家数字资产交易所作出行政处分，并对其他部分数字资产交易所要求限期业务整改。在这样的监管环境下，截至目前，8 家已经提交申请的交易所撤回了牌照申请。虽然监管有所强化，但整体来看，依旧持支持和鼓励态度。

是否允许首次数字资产众筹

针对首次数字资产众筹行为，日本尚无明确的法规，而 2017 年 4 月 1 日生效的《支付服务修正法案》亦不足以对相关行为的法律性质予以明确。

2018 年后，日本金融厅开始监控对日本投资者进行的各类数字资产众筹。2 月，日本金融厅对 Blockchain Laboratory 这家位于澳门的数字资产众筹机构发出警告，声明其在的运作未得到官方许可，并要求其停止向日本投资者的募资行为。未来，相关法律法规或将推出，予以明确。

是否允许数字资产投资

日本对于数字资产投资持较为开放态度，但投资人将面临不同程度的征税。2018 年 2 月，日本国税厅推出了针对数字资产税收全方案，裁定数字资产收益属于个人“杂项收入”，按照累进制税率进行报税，从 15%到 55%不等，如果投资者当年含数字资产资本利得的收入超过 4000 万日元（约合 36.5 万美元），那么超出部分就将征收 55%的最高税率，远高于对投资股票、外汇等征收的 20%左右的所得税。

韩国：交易监管强化，反洗钱是重点，监管严格指数：★★★

是否允许数字资产支付

韩国未有相关法律承认数字资产在支付领域的合法地位，但通过比特币等数字资产进行支付并未禁止。

是否允许交易所境内运营

韩国允许交易所在境内运营，并接受电子商务法监管，根据该法，企业按照电子商务网站进行注册，便可以开展数字资产交易类业务。韩国区块链协会虽也发布《数字资产交易所自律控制案》，并于 2018 年 4 月公布了数字资产交易所自我监管框架，对交易所设定了一定的资质和运营要求，但目前，整体准入门

槛仍相对较低。

随着数字资产市场的快速发展，韩国政府正逐步强化对交易所的监管：2018 年初，韩国金融服务委员会宣布要求数字资产交易所实施实名制等规则，之后，银行开始拒绝为较小的交易所发行新的虚拟账户，只向四大数字资产交易所提供法定存款服务；同时，韩国政府宣布将对数字资产交易所征收 22%的企业税及 2.2%的地方所得税。

是否允许首次数字资产众筹

韩国自 2017 年 9 月至今仍全面禁止首次数字资产众筹。2017 年 9 月初，韩国金融服务委员会透露，将处罚数字资产众筹项目，其中也包含进入别国进行募资的韩国项目，紧接着在 9 月底，韩国金融服务委员会全面禁止了首次数字资产众筹。目前政策暂未实质性变化。

是否允许数字资产投资

韩国允许民众进行数字资产投资，并暂未对相关投资收益进行征税。进入 2018 年后，相关监管有所加强：1 月 23 日，韩国金融服务委员会发布一系列措施，禁止在韩国交易所进行匿名交易，并且未成年人和外国人禁止交易数字资产。

新加坡：政策稳定，且未来有望进一步开放，监管严格指数：★

是否允许数字资产支付

新加坡税务局（IRAS）在 2014 年发布的加密货币指南（IRS Virtual Currency Guidance）中将比特币等数字资产认定为“货物”而非货币，使用数字资产进行支付被视为“物物交易”，需要缴纳商品增值税，税率为 7%。2017 年 11 月，新加坡金融管理局发布《支付服务法案》（草案）第二个征询意见稿，希望通过一个独立的法案来简化对所有支付服务的繁复监管，未来，比特币等数字资产的支付地位有望得到法律认可，并颁发相应许可证。

是否允许交易所境内运营

新加坡允许在境内开设并运营数字资产交易所。2017 年 11 月 14 日，新加坡金融管理局发布《数字代币发行指引》，文件表明，新加坡数字资产相关的中介机构，包括数字资产交易所，若涉及提供被视为资本市场产品、证券或期货合约的数字资产交易，则需要获得相应牌照、批准，若仅提供币币交易，且不涉及上述被视为资本市场产品、证券或期货合约的数字资产，则无需相关牌照，但仍需要符合反洗钱相关规定。

是否允许首次数字资产众筹

2017 年 11 月 14 日，新加坡金融管理局发布《数字代币发行指引》，肯定了首次数字资产众筹，并明确了监管范围，即当数字资产属于《证券及期货法》项下定义的资本市场产品时，数字资产众筹受到监管，需要获得新加坡金融管理局的审批，若数字资产不属于资本市场产品，则不需要受到监管，只需遵守反洗钱等常规性要求即可。

是否允许数字资产投资

新加坡对数字资产投资持开放的态度，针对投资数字资产的收益，暂不征税，但新加坡政府仍旧多次发表声明，就数字资产潜在的风险对投资者进行提示。

香港：基本保持不变，强化执行，监管严格指数：★★★

是否允许数字资产支付

香港未从法律上承认数字资产的法定支付地位，但亦未禁止比特币等数字资产用于支付。

是否允许交易所境内运营

香港允许开设数字资产交易所，但若涉及向香港公众提供证券类数字资产的交易服务，依据 2017 年 9 月 5 日香港证监会发布的《有关首次代币发行的声明》，则受监管，需获取相关牌照或向证监会注册，发牌规则参照《证券及期货条例》规定。

2018 年 2 月 9 日，香港证监会发布《证监会告诫投资者防范数字资产风险》公告，声明已先后致函 7 家位于香港或与香港有联系的数字资产交易所，警告它们不应在未领有牌照的情况下买卖属于“证券”的数字资产。

是否允许首次数字资产众筹

香港并未禁止首次数字资产众筹，2017 年 9 月 5 日，香港证监会发布《有关首次数字资产众筹的声明》指出，部分项目数字资产可能属于《证券及期货条例》所界定的“证券”，并且就该类“证券”类数字资产，若以香港公众为对象，则需证监会发牌或向证监会注册。该声明同时指出，若某首次数字资产众筹项目被认定为证券，则不仅是参与到该代币的一级市场做市商、咨询机构、以及机构投资人等需获得相关牌照，并且二级市场的参与者（包括交易平台）也需要证监会发牌或向证监会注册。

2018 年，3 月 19 日，香港证监会叫停发行人 Black Cell Technology Limited 的

数字资产项目，因其在未获认可的情况下，向香港公众投资者进行“证券”类数字资产销售。

是否允许数字资产投资

香港允许公众投资数字资产，针对投资数字资产的收益，暂不征税，但香港证监会多次发布声明告诫投资者防范数字资产风险。

（3）欧洲地区

俄罗斯：由紧转松，逐步转向明确，监管严格指数：★★★

是否允许数字资产支付

2014 年 2 月 28 日，俄罗斯总检察院发表声明禁止在俄罗斯境内使用比特币，并全面封杀以比特币为代表的数字资产交易，之后，俄罗斯数字资产的禁令虽有所松动，但整体仍持高压态度。

进入 2018 年，俄罗斯对数字资产态度快速转变，1 月，俄罗斯财政部提出《数字金融资产法》草案，3 月，俄罗斯国家杜马议长 Vyacheslav Volodin 和议会立法委员会主席 Pavel Krasheninnikov 提出了修改意见，提议数字资产可在法律规定的情况和条款下被用作支付工具，但数字资产并不会被强制作为支付、存款、转账和记账单位；数字资产的数量及使用者的相关信息会被收集，数字确认将与书面声明和签名一样有效。这标志着俄罗斯对数字资产地位合法化迈出了第一步。

是否允许交易所境内运营

自俄罗斯 2014 年全面禁止比特币等数字资产后，2017 年 9 月，俄罗斯央行再次发表声明，重申现阶段不会批准任何正规交易所进行数字资产交易，也不会批准将该技术用作基础设施，即俄罗斯官方不允许任何数字资产交易所境内运营。

进入 2018 年，俄罗斯对数字资产交易所立场巨大改变，财政部提出的《数字金融资产法》草案规定，俄罗斯允许境内开设数字资产交易所，但需要符合俄罗斯联邦证券市场法等框架，并需要在俄罗斯中央银行注册。

是否允许首次数字资产众筹

2017 年 9 月，俄罗斯央行发表声明，呼吁警惕数字资产和数字资产众筹存在的高风险。

2018 年，财政部颁布《数字金融资产法》草案，其中明确了数字资产众筹的合法性，规定个人或法人都可以进行数字资产众筹，其中需要提供一系列资料和签名以保证信息披露的完整性和可靠性。

是否允许数字资产投资

2018 年，俄罗斯财政部提交《数字金融资产法》草案，基于该草案，若不属于《俄罗斯证券市场法》中规定的合格投资者，则只能获得不超过 5 万卢布的数字资产且只能记录于特殊账户（该特殊账户由交易所提供），若为合格投资者，则可以合格投资者的名义开设数字钱包用于保护数字资产信息和访问数字交易账户。原数字资产交易禁令正逐步放开。

英国：政策仍不明确，但并未予以限制，监管严格指数：★

是否允许数字资产支付

英国并无相关法律对数字资产的属性进行明确，但对数字资产支付等行为仍持自由开放态度，并未予以禁止。

是否允许交易所境内运营

英国允许交易所在境内设立，目前英国有 Bitstamp、CoinEgg、HitBTC 等交易所，但还局限于币币交易，暂不需要受英国金融市场行为监管局监管，但若交易所涉及法币，或与数字资产有关的衍生工具，如期货和差价合约，则需要受到监管，并要满足反洗钱等规定。目前政策未变化。

是否允许首次数字资产众筹

英国并未禁止首次数字资产众筹，对其是否属于监管的范畴采取的是一事一议的方式。对于数字资产众筹所涉及的风险，2017 年 9 月，英国金融市场行为监管局曾发出过警示。2018 年 2 月，英国金融市场行为监管局宣布将从国家法律层面对数字资产众筹融资机制的适用性进行深入研究，以确定“进一步监管行动”的必要性，未来，有望出台相关政策。

是否允许数字资产投资

英国不限制数字资产投资，同时，数字资产投资收益暂不征税，目前政策未变化。

瑞士：总体友好，政策不断完善，监管指数 ★

是否允许数字资产支付

瑞士各地允许数字资产支付，且不会涉及征收增值税，不过部分数字资产支付会受到《反洗钱法》的监管。瑞士楚格州在国际上已经成为了有名的“数字资产山谷”，当地政府早在 2016 年就已经宣布将允许其市民使用数字资产支付政府服务。2017 年 9 月，瑞士基亚索市政当局也宣布将开始接受使用数字资产进行纳税，税款支付额度不能超过 250 瑞士法郎（大约 265 美元）。

是否允许交易所境内运营

瑞士允许数字资产交易所在境内开设，态度相对开放，但是瑞士并未对数字资产交易所单独设立合规牌照。目前，主要的瑞士本土的数字资产交易所，都拥有 VQF（Financial Services Standards Association）会员资格，会员资格中包括了对数字资产的经营范围。

是否允许首次数字资产众筹

瑞士对首次数字资产众筹持肯定态度，目前，其监管法规也正逐步完善。2017 年 9 月，瑞士金融市场监督管理局颁布的一项关于数字资产众筹的指导意见中指出，目前瑞士还未制定针对数字资产众筹的完整法规，但是依据数字资产众筹的组织形式，数字资产众筹的部分环节需符合当前金融市场的监管法规：当所筹数字资产为支付工具时，该活动将会受到《反洗钱法》的监管；当涉嫌吸收公众存款时，发行主体需要持有银行牌照，并受银行法监管；当所筹数字资产具有类似证券性质时，筹集主体需要有证券经纪商的牌照；当筹集到的资金由外部第三方管理时，还需要符合集合投资计划的相关规定。

随着瑞士数字资产众筹数量的增加，2018 年 2 月，瑞士金融市场监督管理局发布了另一份指导意见，意见中将数字资产分为可相互重叠的支付类数字资产、功能类数字资产、资产类数字资产三大种类，其中，最后一类会被归类为证券，同时，只有当功能类数字资产的唯一目的是授予应用程序或服务的数字访问权限时，并且只有在发行时已具备此种用途时，方不属于证券。

是否允许数字资产投资

瑞士并未限制数字资产投资，同时，数字资产投资收益暂不征税。

德国：政策相对明确，并正积极完善，监管严格指数：★★

是否允许数字资产支付

德国对于数字资产用于支付的态度非常积极，早在 2013 年 8 月 19 日，德国财政部就宣布比特币是一种“记账单位”并可以被用于支付。

2018 年 2 月 27 日，德国财政部进一步下发指示文件，用户用比特币及其他数字资产支付时，买卖双方其实是在提供法币和数字资产兑换的“补充服务”，根据 2015 年欧盟法院对增值税（VAT）的裁决，除了已经包含在商品价格中的增值税，双方将无需缴纳其他税项。

是否允许交易所境内运营

德国目前对于数字资产交易所没有出台明确的监管政策，但或将纳入德国联邦金融监管局(BaFin)的监管范畴。BaFin 在 2018 年 3 月 28 日发布的针对数字资产众筹的指导意见中，要求提供与数字资产及数字资产众筹相关服务的市场参与者在处理相关业务时必须审慎考虑数字资产的分类及对应遵循的法规。2018 年 1 月 29 日，柏林数字资产交易所 Crypto.exchange GmbH 由于其欺诈行为被 BaFin 要求立刻停止金融证券业务。

是否允许首次数字资产众筹

德国对首次数字资产众筹持保守态度，但目前并未予以禁止，且正在积极完善相关的监管法规。2017 年 11 月 9 日，德国联邦金融监管局(BaFin)曾发出警示公告提醒广大投资者首次数字资产众筹是极具风险、带有投机性质的行为，并列举了一系列的风险点，鼓励公众在参与首次数字资产众筹之前做好详尽的研究。

随着德国数字资产众筹的数量增加，BaFin 又于 2018 年 3 月 28 日发布了进一步指导意见，明确了数字资产众筹所涉及的数字资产属于金融工具，将落入证券监管的范畴。BaFin 将针对具体数字资产众筹项目给对应数字资产分类，决定它是《德国证券交易法》（WpHG）及《德国金融工具市场指导》定义的“金融工具”，还是《德国证券招股说明书法》（WpPG）定义的“证券”，还是《德国资本投资法》（VermAnlG）中定义的“资本投资”，然后决定所需遵循的对应的政策法规。除以上几条法规外，如果条件满足，数字资产众筹还将遵循《市场滥用行为监管条例》（MAR）等国家及欧盟级别证券监管范畴内的其他法规。

是否允许数字资产投资

德国目前暂未限制数字资产投资，但 BaFin 多次发出公告提示投资人注意风险，并鼓励投资人在投资前仔细研究区块链及数字资产技术，了解自身所面对的风险。

对于投资收益所需缴纳的税项方面，暂无明确政策法规，但鉴于 BaFin 宣布数字资产需落入证券监管范畴，未来数字资产的投资或将遵循与证券投资类似的税务规定。

（4）大洋洲地区

澳大利亚：环境宽松，法规完善，保持稳定，监管严格指数：★

是否允许数字资产支付

澳大利亚政府是世界上少数全面放开以比特币为代表的数字资产交易和流通的国家之一，2017 年 7 月 1 日，澳大利亚政府正式认可比特币的货币地位，并正式实施免除对比特币的双重征税、交易税以及商品与服务税政策。在 2017 年 7 月 1 日之前，澳洲数字资产的消费者需要支付两次消费税（Goods and services tax，简称 GST），一次是在购买数字资产时，另一次是在使用数字资产购买其他商品和服务时。

是否允许交易所境内运营

澳大利亚正推行对数字资产交易所的注册登记制。2017 年底，澳大利亚参议院正式批准通过了《2017 反洗钱和反恐怖融资修正案》，授权该国金融情报机构——澳大利亚交易报告分析中心（Austrac）监管比特币交易所，该法案规定，澳大利亚的比特币交易所需要在 Austrac 登记注册，在“数字资产交易所登记册”上留底，此外，交易所还要制定一系列风险防范措施，包括寻找反洗钱和反恐怖主义融资的解决方案，验证客户的身份信息，报告任何可疑的活动，国际交易或有超过 1 万澳元的大额交易也需上报 Austrac。交易所还需要将部分交易记录以及客户身份信息保留长达 7 年的时间。

上述政策于 2018 年 4 月 3 日正式施行，政策期限为 6 个月，若在此期间内没有遵守条款，交易所将被采取强制措施；此外，若交易所的注册申请处于审核当中，Austrac 将考虑通过过渡期的方式允许现有公司继续提供服务，但必须在 5 月 14 日前进行注册。

是否允许首次数字资产众筹

澳大利亚政府对数字资产众筹的态度较为包容。2017 年 9 月 28 日，澳大利亚证券和投资委员会（Australian Securities and Investments Commission，简称 ASIC）发布了监管指引，指出：首次数字资产众筹的法律性质取决于某一个具体的数字资产项目是如何构成及操作的，以及所筹数字资产背后所代表的权利，监管机构将依据项目所涉及的行业与业务的差异适配于不同的法律法规。

是否允许数字资产投资

澳大利亚对数字资产投资持开放态度，但在特定场景下将对其收取相应的资本利得税。

一方面，如果出于投资目的持有数字资产（即追求投资回报或用以维持某个公司的运营等），则该项数字资产在增值时需要缴纳资本利得税；但若持有该项数字资产超过 12 个月，税务局会给予一定的税务优惠。如果出于个人使用目的持有的数字资产（如主要用来支付或做等价交换其他消费品），金额 10000 澳元以内的无需缴纳资本利得税。

新西兰：态度持续保守，政策依旧较紧，监管指数 ★★★

是否允许数字资产支付

新西兰央行对数字资产支付持保留态度，并未认可数字资产的法定地位，认为数字资产扩展了人们可以相互交易的机制，但数字资产“交易量较小”、“匿名性与信贷发放不匹配”，“暂时无法替代传统的支付系统”。

是否允许交易所境内运营

新西兰对数字资产交易所实施严格的管理，新西兰金融市场管理局明确指出，数字资产属于证券，要求交易所、钱包以及经纪商等所有涉及数字资产的服务供应商都需要依据《金融市场管理法》在金融服务供应商登记系统（FSPR）中登记，支付申请费用、税款，以及遵守公平交易规则，履行反洗钱法规定的义务。目前政策暂未变化。

是否允许首次数字资产众筹

新西兰金融监管局认为，所有数字资产都是证券，属于《金融市场管理法》监管范围，并且，在某些情况下，根据数字资产的特征和经济实质可将其归为金融产品，如债权证券、股权证券、托管投资产品或衍生品。其他情况下，若不属于金融产品，发行方企业必须遵守“金融市场管理法”下的“公平交易法”（Fair Trading Act），且这项法律不仅适用于国内产品，也适用于新西兰境外提供的数字资产产品。此外，数字资产众筹方还需遵从其他进一步的监管，如反洗钱法等。目前，相关政策暂未发生变化。

是否允许数字资产投资

在数字资产投资方面，新西兰政府并未禁止投资者参与，但整体态度相对保守，曾向用户警示数字资产投资的风险。

三、区块链产业链回顾及展望

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，我们将区块链产业链分成五大板块：

- **硬件、基础设施：**为各种区块链提供、整合底层算力和硬件支持；
- **区块链底层平台：**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：**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：**将区块链应用于各个行业及场景，服务最终用户；
- **服务设施：**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、基础设施

为各种区块链提供、整合底层算力和硬件支持：（排名不分先后）

- 矿机生产商

BITMAIN Canaan EBANG

比特大陆　嘉楠耘智　亿邦通信

- 矿池

ANTPOOL ViaBTC f2pool

蚂蚁矿池　ViaBTC　鱼池

- 芯片厂商（含代工）

NVIDIA AMD HISILICON

英伟达　超微半导体　台积电

➢ **现状及未来趋势：**

目前矿机主要用于以比特币为主的使用 PoW 共识机制的币种挖矿。专业矿机多使用 ASIC 芯片，其计算效率可以比显卡等高出很多倍，但只能针对特定的算法打造，即只适用于单一币种或者某些算法相似的币种。另外，专业的 ASIC 矿机也造成了区块链网络的算力集中，且在挖矿过程中消耗掉了大量的

电力能源。火币区块对链该领域的看法有三点：

- **专业 ASIC 矿机的竞争格局已初具雏形，未来头部效应将更加明显：**目前专业矿机使用的 ASIC 芯片主要由矿机厂商设计架构，再由台积电等传统芯片厂商研发和代工生产，即核心研发技术由芯片厂商掌控，但仍需要矿机厂有芯片架构设计能力，这就形成了一定进入壁垒；另外，随着挖矿需求的增加，ASIC 芯片的价格也显著升高，对小规模、议价能力低的矿机厂商造成一定压力，整个行业出现优者更优的现象。
- **显卡矿机未来将以长尾形态与 ASIC 矿机并行存在：**显卡矿机与 ASIC 矿机相比通用性更强，可以针对多个币种，就像加强了显卡配置的电脑，更适用于公众。且在图形算法方面显卡的计算速度更高。另外，为了防止 ASIC 矿机集中算力，不计成本地进行 51%攻击，未来可能将由更多区块链项目采用对抗 ASIC 的共识机制，比如 PoS 或 PoW+PoS 等。但是，挖矿显卡的设计技术掌握在英伟达、AMD 等传统厂商手中，任何使用这些显卡的设备都可以作为矿机，因此将不会有专业的显卡矿机厂商出现，而是长尾地分布在多数用户手中。
- **未来行业的机会在于低能耗的矿机：**无论是 ASIC 矿机还是显卡矿机，在挖矿的过程中都消耗了大量的电力能源，而挖矿的过程仅仅是重复进行公式计算，没有产生太多价值。未来，类似 CDN 挖矿的低能耗挖矿需求可能会增加，将给矿机厂商带来新的机会。

3.2 区块链底层平台

为各种区块链应用提供底层架构、开发平台和生态：（排名不分先后）

- 通用基础链

以太坊　EOS　卡尔达诺　Stellar　NEO　Qtum　Icon

- 垂直领域基础链

➢ **现状及未来趋势：**

经火币区块链研究院不完全统计，目前至少已有数十个基础链平台项目，该领域已经极度拥挤。底层基础链相当于区块链的操纵系统，是区块链应用的基础。可以说，谁能做出好的区块链底层平台，谁就有大概率成为区块链巨头。目前该领域头部效应已经开始出现，预计短期之内竞争还会加剧，但未来竞争格局将进一步集中。未来基础链有以下几个发展趋势：

- **跨链交互性成为重要的评判标准：**随着区块链底层技术的逐渐成熟，跨链交互需求也日益增加，也有越来越多的跨链平台应运而生。跨链的优势主要在于：**1）性能提升：**跨链是解决区块链可扩展性的途径之一，这也是跨链最直接的价值；**2）信息交互：**虽然区块链去除了国界的限制，但是各个独立的区块链本身还是类似一个个的局域网络，跨链带来的信息交互可以让数据、信任在各个局域网络之间传递，形成一个互联、互通、互信的通讯网络；**3）价值转移：**每一个独立区块链都是一个价值经济体，在各自的体系中产生各自特有的价值，跨链区块链是连接独立区块链的中枢，只有实现跨链才可实现不同经济体之间的价值交换，连接不同行业，使区块链真正变成一个价值流通平台。

- **性能不是唯一评判标准，用户对“开发者友好”的要求会越来越高：**过去的几年里公有链领域在提高 TPS 性能方面做出了众多探索，包括闪电网络、分片、侧链、改进共识机制等等。但目前还没有出现非常“开发者友好”的底层平台。火币区块链研究院认为，未来会有更多“好用的”平台出现，比如针对更多通用的应用场景嵌入成型的开发模块，降低对应用程序开发者的要求。

- **垂直应用领域的基础链机会出现：**我们知道 TCP/IP 协议定义了互联网的标准协议，而与之相比，区块链的世界更加复杂，不同场景和行业对共识机制等区块链逻辑都有不同的需求。火币区块链研究院认为，未来并不一定是通用的基础链一统天下，每个垂直领域内的基础链也存在机会。目前已经有少数垂直行业的基础链出现，未来随着“区块链+行业场景”的深度磨合，各个垂直领域将有更多的业务逻辑上链。

3.3 通用技术

让区块链应用更方便部署和应用，为开发者和用户服务：(排名不分先后)

- 分布式存储

Filecoin　Siacoin　Storj　GNX

- 去中心化交易

ZRX　路印协议　Kyber Network

- 数据服务

公信宝　ChainLink　Bluzelle　海洋协议

- 分布式计算

Golem　Enigma　TrueBit

- 安全服务

Certik　Quantstamp　Zepplin　哨兵协议

- 隐私、加密服务

Nucypher　Rockchain　Keep Network

- 开发者工具


Lisk


Stratis


Arcblock


Etherparty

- 扩展性解决方案


Loom


Raiden Network


Trinity

➢ **现状与未来趋势：**

由于区块链本质上是一种技术解决方案，其在行业应用中也有非常多的共通性。区块链通用技术层主要目的就时满足各个垂直行业在应用区块链时的共通需求，如分布式数据、分布式数据交易、代码审计、隐私加密服务等，可以将其理解为部分区块链技术的外包。火币区块链研究院认为，未来，区块链通用技术的发展较为明确，且将呈现螺旋上升的良性循环：

- **通用技术的普及加快行业应用的落地：**通用技术平台降低了区块链应用开发的门槛，加快了应用落地的进程。如新的应用可以直接采用现有的 IPFS 等分布式数据存储解决方案，而无须自己开发，好比互联网世界的应用直接采用阿里云、百度云等现有存储方案，无需从零开始。
- **各垂直行业区块链应用的成熟将催生新的通用需求：**模式的成熟使得共通性更加明显，随着区块链的普及，通用技术领域必将出现新的机会。我们可以猜想，应用程序入网身份验证也是每个区块链项目的必需品，未来这方面可能也将出现通用的技术平台。

3.4 服务设施

帮助资金、信息等流动，为产业链参与者提供专业服务：(排名不分先后)

- 数字资产交易所


火币


币安


Bitfinex


OKEX


Bithumb


Gate.io


Bittrex


Poloniex


IDEX


Nex

- 媒体、社区


Coindesk


Bitcoin Magazine


巴比特


金色财经


币世界


链得得


火星财经


火讯财经

- 行情、资讯终端


Coin Market Cap


AICoin


Mytoken


非小号


CoinGecko

- 数字资产钱包


Imtoken


Kcash


qbao


火币钱包

➢ **现状与未来趋势：**

区块链产业链上的周边业务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。随着行业的发展，该产业链环节具有**较为明确的发展前景**，但同时，由于该产业链环节本身的特性(最接近互联网，核心逻辑是资源整合)，未来都将是一个**头部效应不断强化、强者恒强**的领域。

- **去中心化数字资产交易与中心化数字资产交易可能并存：**数字资产交易目前主要是通过交易所“链下撮合”的方式进行，即并未实际记录在区块链上，并且，流动性是分割的，分散在不同的中心化数字资产交易所。随着区块链技术的发展，去中心化的数字资产交易，即“链上撮合”方式进行的交易会越来越普遍。但由于在交易体验上的差异，未来一段时间内，去中心化的数字资产交易可能更偏向面对各类分布式应用的用户，提供简单、友好的数字资产兑换服务，而中心化的数字资产交易，则会更多面向投资、交易驱动型的用户，提供极致的交

易体验。

- **行情、资讯终端可能会充当交易聚合的入口：**由于目前中心化数字资产交易存在的流动性分割现状，用户需要在不同的交易所注册不同的账户进行交易，过程繁琐，而行情、资讯终端，凭借其在交易用户端积累的优势，将会逐步渗透至提供聚合交易服务，让用户通过一个账户，实现在各个交易所交易的功能，成为数字资产领域的“同花顺”。
- **钱包从长期来看可能成为各类应用的入口：**移动互联网时代，如同各类 App 作为用户感受移动互联网的窗口，未来，区块链时代，各类 Dapp 也将成为用户直接参与区块链的主要方式。由于用户与 Dapp 的交互需要消耗数字资产，而钱包作为协助用户管理各类数字资产的工具，其重要性不言而喻，可能会成为新时代的应用商店，成为区块链 3.0 时代真正的超级流量入口。

3.5 垂直应用

该领域项目将区块链应用于各行业场景，服务最终用户。（涉及项目排名不分先后）

目前，从区块链的技术特点来看，区块链赋能的应用场景主要与以下几个方面相关：（1）交流效率低、信任成本高的领域；（2）对信息可验证性、共识有极大需求的领域；（3）对大体量数据分享和计算有较大需求的领域。

支付、清结算等货币市场应用

现阶段商业贸易的交易支付、清算都要借助银行体系。传统的银行体系下，支付需经过开户行、对手行、清算组织、境外代理银行（若涉及跨境支付）等多个组织及较为繁冗的处理流程，往往需要依赖第三方的中央清算机构，造成了支付及清结算费用高且效率低。尤其是对于小额跨境支付来说，高昂的手续费及漫长的等待时间所造成的负担尤其沉重。区块链带来的效率提升主要来自两方面：利用无地域限制的通用数字资产作为支付媒介，减少中间流程；以及

利用去中心化共享账本技术，减少清结算效率。主要项目如下：


Ripple


OKLink


BitBay


Veem


wyre


Abra

火币区块链研究院认为，未来区块链在这一领域将有两种普及路线：

- **短期来看，以数字资产作为支付汇款的媒介货币将有极大前景：**目前已经有很多家利用数字资产做支付（尤其是跨境支付）的服务商，比如提供企业间汇款的 BitPay，Veem，Wyre 和提供个人用户间小额支付的 Abra。这些公司使用数字资产作为媒介货币，利用其无国界性节省跨境支付中境外代理银行所涉及的时间和中间人成本。比如 BitPay 提供的比特币跨境汇款服务可以将汇款时间从 4 个工作日降低到 1 个工作日，汇款手续费从 7%降至 1%。同时通过差价合约等金融产品对货币进行对冲，确保支付账单的实际价值不会发生变化。BitPay 公司月汇款金额已超过 100 万美元，且已与 Lush 等大型快消品牌合作。火币区块链研究院认为，这种汇款方式正在逐步被大型企业接受，该领域短期之内即将开始进入规模化阶段。

- **长期来看，区块链将从协议层变革支付和清结算领域：**支付的协议层变革在上述数字资产汇款的基础上更进一步，为银行后台账本制定标准规范，使得银行间共享清结算数据更加容易，从根本上提高支付效率。目前在全球跨境支付市场上，最先使用区块链技术完成其商业化应用的是由瑞波币实验室研发的跨境支付网络 Ripple，它借助区块链协议为全球大型银行提供跨境汇款方案，试图打造基于区块链的全球金融传输网络以取代 SWIFT。类似的支付网络还有美国支付协议网络 Stellar 和中国跨境支付项目 OKLink，二者主要针对中小型持牌金融机构。我们认为长期来看，基于区块链技术的支付网络是解决支付和结算流程成本和效率问题的最好方案，尤其可以解决中小型机构的支付痛点，大力促进普惠金融。

证券、票据、另类投资等资本市场应用

目前金融资产交易依赖于中心化的确认。比如证券交易体系中，全部证券登记及结算任务由中央登记结算机构负责完成，该中心化结构体系的维持和运行，依赖复杂的规章制度和审计流程。区块链技术带来的去中心化能够让各参与主体在无需相互信任的情况下进行完全自由的交流，各个节点只需信任整个网络以及网络所带有的共识机制，这样一来可以缩减由信息不对称造成的信任成本，以及层层中央结算流程造成的时间成本。主要项目情况如下：

Tzero

Polymath

Global Reit

ReitsChain

上海票据交易所

未来，这一领域可能存在的方向和趋势有：

- **证券市场区块链化方面已有美国“正规军”进入，未来将有更多发达国家相继效仿：**2015 年 12 月，美国证券交易委员会（SEC）已批准 Overstock 旗下区块链证券交易平台 T0 交易并结算证券。该平台通过区块链技术发行债券、股票等数字资产，构建一个更加快速透明的“交易即结算”的证券发行交易平台。2017 年 10 月，证券类数字资产发行平台 Polymath 上线，为证券类数字资产的发行、确认和交易提供服务。火币区块链研究院预计，随着各国区块链及数字资产的政策日益完善，未来将有更多交易所效仿美国，将区块链技术应用到证券市场。

- 票据市场中国央行率先尝试，落地在即，有望产生示范性效应： 2017 年中国人民银行推动的基于区块链的数字票据交易平台已测试成功，这标志着在全球范围内，中国央行将成为首个研究数字资产及真实应用的中央银行。

- **更多资产相继上链，推动各垂直领域的资产交易平台形成：**在另类投资领域，也有不少企业做出了尝试。早在 2015 年 10 月，纳斯达克就在和区块链初创企业 Chain 合作下正式上线用于私有股权发行及交易

的 Linq 平台。REITs 方面，也有创业公司 Global REIT、瑞资科技等多家公司做出尝试，将房产信息数字化之后作为链上资产，并利用分布式账本和分布式存储技术对其定期审计，提高效率。在能源领域也有中国的能链众合等公司开始结合区块链，基于区块链上的碳排放量等资产开发结构性金融产品。火币区块链研究院认为，分布式资产交易平台在模式上有着极大共通性，一旦某一个垂直行业的平台落地就会极大刺激其他行业的探索和发展，未来跨行业复制效应会极其明显。

医疗健康

目前医疗领域区块链技术研发主要集中在电子病历，远程医疗，医疗保险方面。应用主要凸显了区块链在信息真实，信息安全，隐私保护，去中心化储存，智能合约的特性，解决了医疗数据零散存储，隐私保护不足，信息安全性欠佳等问题。目前 Medicalchain 和 Medibloc 团队集中于电子病历和远程医疗区块链技术的开发。Medicalchain 通过非对称加密和 Hyperledger 来保证用户拥有 100%的信息权限控制。Medibloc 通过零知识代理重加密和 IPFS 实现完全的信息权限控制和去中心存储。目前在互助保险方面 Medishares 通过智能合约提升互助资金池安全并为理赔核准问题提供解决方案。主要项目如下：

MedicalChain　MediChain　MediShares　Mediabloc　Hashed Health

我们认为未来围绕大健康和医联体分级诊疗制度而构建的区块链应用将成为热点：

- **大健康多维度个体健康管理与疾病预防得到实现：**结合 IOT，可穿戴设备，链上电子医疗病历，机器学习技术构成的长期健康管理闭环将通过点对点存储，重加密，子母链，以及链下支付通道实现信息访问权限资本化，促进医疗人工智能技术开发和技术普及，实现生命全周期长期健康呵护和疾病预防。用户可以选择将日常体征数据租赁给人

工智能开发者和医学研究机构，数据有助于 AI 技术关键环神经网络的开发，可应用的 AI 技术又反过来为用户健康提供多维度测评并给出个体解决方案，从而形成闭环。火币研究院认为在机制设计上对于参与者行为进行正向引导，思考各方面真实诉求，形成共赢机制的平台将会脱颖而出。

- **促进现代分级诊疗制度发展：**通过智能合约和上链保证了信息真实与透明，提高了保险运营效率，促进了商保直赔。有助于解决医保支撑不够导致的医院之间报销差异明显和基层人才首诊激励动力不够问题。通过去中心电子病历存储和重加密技术降低集中控制的风险，以及信息存储成本，保障了患者隐私，解决上下转诊信息调阅难。助力远程医疗和国际医疗第二建议的普及。

供应链溯源及金融

区块链对供应链领域的变革主要有供应链溯源及确权和供应链金融两个切入点。供应链溯源及确权方面，目前已经存在多种解决方案，包括唯一图案标记、二维码、RFID 芯片等。大体思路都是给货品赋予一个唯一的数字 ID，从生产环节开始记录原材料信息、生成地信息、货品物流信息等。这些传统解决方案的问题在于防伪数据存储在了中心化结构上，易于篡改。而基于区块链的防伪溯源，将货品的实时数据存储在去中心化结构之上，任何人都无法篡改，公信力更高。更重要的是，基于区块链可以生成智能合约，实时确定货品的所有权和处置权的归属，使整个供应链更加自动化。

供应链金融方面，银行和核心企业供应链生态系统内的企业可以建立共享的账本及交易信用历史，提高银行在处理贷款信用审核的效率，且基于区块链溯源和货品确权系统，银行审核企业仓单等抵押物的流程将进一步简化，缩短宝贵的贷款周期。就融资成本来说，银行优先服务于大型供应商，而中小企业虽然手握优质的供应链资产，还是由于自身的信用缺乏而难以从银行处获取低

成本的资金。区块链可以将核心企业应付/账款、各方库存、商业票据等供应链资产转化为链上可以拆分、流转的数字资产，并引入信用背书机制，使得企业的身份和信用可以得到多维的认证，比如供应链上下游的“按时交货”、“按时付款”都可以作为信用的背书，这样一来信用可以在各个核心企业的供应链上下游传递，实现多级融资。具体这一领域相关项目或玩家如下：

Vechain

布比

京东

Chained Finance

菜鸟

复杂美

未来，这两个切入点将可能有较大的发展机会：

- **供应链溯源及确权领域，大型企业和小型企业需求共同驱动区块链的普及：**2017 年 3 月，国际海运第一巨头马士基航运已经与 IBM Hyperledger 项目合作，完成了对施耐德电气货物跨大西洋运输的全过程测试，过程中利用区块链共享账本及智能合约技术节省通关文件审核以及清点货物的时间，将原本需要 60 天的运输流程降低到两周，并节省了厚达 25cm 的纸质文件；国内目前已有电商巨头京东于 2017 年 7 月发布区块链防伪追溯开放平台，面向京东生态内的品牌商免费开放；另外还有一系列创业企业，如为头部奢侈品公司提供防伪溯源的唯链（Vechain）项目，以及服务于小型画廊的艺术品防伪溯源项目天权优成等等。我们认为，防伪溯源不仅仅是大型公司的需求，类似小型画廊的小众、高客单价的领域也具有极大发展空间。该行业发展将由两极需求共同驱动。

- **供应链金融领域，核心企业为主要助推作用力：**核心企业作为整个供应链体系的关键节点，常常希望能利用自己的信用帮助供应链上有的供应商更好的稳定现金流，以便自己能拥有稳定的供应链并及时收到上游货品。2017 年初，富士康集团推出了首个区块链供应链金融平台 Chained Finance，利用区块链技术实现多级融资，主要服务于自身供应链上的供应商。2017 年中，海航集团与创业公司复杂美合作推出了基

于区块链的供应链票据平台“海票惠”，服务于自身供应链。2018 年，京东、阿里及腾讯也发布了其各自基于区块链的供应链金融解决方案。火币区块链研究院认为，虽然中小型供应商在供应链金融领域的痛点更加明显，但由于供应链金融涉及的相关企业繁多，不是依靠一家之力就能实现落地，所以行业发展将呈自上而下头部推动的趋势。

- **未来基于溯源及确权系统的供应链金融将衍生出更多产品，想象空间极大：**供应链参与者可以基于区块链设置智能合约，将赋予供应链金融新的玩法。比如在某种特定状态下自动为货品确定所有权，这样一来货品在运输过程中也可以实现动态的质押，且所有权已经记在区块链上，如果发生纠纷可以轻易的发起仲裁。

版权确认及交易

随着互联网，特别是移动互联网的发展，数字内容及版权交易已经形成较为完整的产业链，然而盗版、侵权仍旧制约了数字内容行业的发展。同时，版权所有者在互联网体系中的话语权较小，盈利空间被渠道挤占，严重打击了创作积极性。区块链则通过时间戳的形式，将内容和信息进行记录、传输和存储，并无法篡改，良好解决了当前版权保护的注册、确权和验证问题。同时，区块链也可构建起一个去中心化的版权交易网络，提高创作者本身的地位，让内容产生的收益从平台流向创作者本人。该领域相关项目如下：

原本 Primas　墨链　YoYoW　Mediachain　CNN　Bitmark

未来，区块链有望在如下方面对该领域进行持续渗透：

- **紧迫的需求和日益提升的用户付费意愿是区块链确权落地的基石：**区块链的防篡改性与版权确认的需求有天然的结合性，目前该领域已经有众多玩家进入，如中国的版权确认及文化资产交易平台“墨链

（Ink）”，由中国版权保护中心和华夏微影文化传媒中心联合打造的微视频登记、确权、监管、交易、分享和结算平台“微视频 360”。音乐媒体巨头 Spotify 也于 2017 年收购了纽约创业公司 Mediachain，用于维护原创作者的版权。另外，内容产业是基于用户付费的逻辑，随着知识产权意识的普及，用户为优质 IP 付费的意愿越来越强，进一步为区块链确权在内容产业落地营造了优越的市场环境。

- **基于区块链确权的版权交易使长尾内容价值凸显，推动市场扁平化：**传统内容产业中，头部 IP 效应明显，而许多头部 IP 都是由平台炒作而成，被哄抬后的市场价格可能超出公允价值。另一方面，众多腰部和尾部内容由于没有大型平台支撑，而无法获取足够的市场关注度，价值被低估。我们认为，随着区块链去中心化技术的落地，平台所产生的推动效果减弱，头部及尾部 IP 都将获得更合理的市场化定价，缩小头尾部的价格差距。

- **区块链确权促进内容产业跨界结合，推动产业升级：**2017 年 6 月起，美国个性化人工智能公司 ObEN 与女团 SNH48 达成合作，基于 PAI 公链为 SNH48 成员制作全球首款明星虚拟人工智能形象，在线上与粉丝互动。在这个过程中，如何证明区块链上的形象是对应明星自己的形象，而不是其他人基于明星的照片和声音仿制出来的山寨产品，就需要借助区块链确权系统。火币区块链研究院认为，过去被确权问题及盗版现象限制的 IP 跨界合作将随着区块链的落地活跃起来，带来内容产业与其他诸如社会服务业、制造业、高新技术产业（如人工智能）等其他行业的进一步融合。

数字广告

数字广告行业经历了传统购买阶段（广告位投放）、广告网络购买阶段（媒体组合投放）和程序化购买阶段（智能精准投放）。虽然数字广告领域的智能

化、程序化趋势越来越明显，但也大幅提高了很多参与者的门槛，广告主需要依赖专业的第三方进行广告投放、程序化采购，然而各方之间数据不互通，其结果便是相互之间的信任不断丧失，链条上引入越来越多的环节，比如广告验证、数据监测、广告拦截等。而区块链的透明、不可篡改、可追溯等特性正好可以解决广告链条上的信息割裂、欺诈问题，为共识奠定了基础。涉足数字广告领域的相关项目如下：


BAT

DATA

Prochain

AdEx

DATx

AdChain

RebelAI

我们认为，未来：

- **区块链将率先改造低频次的广告场景：**数字广告已进入程序化购买阶段，实时出价交易可达毫秒级的确认速度，然而，目前的区块链技术暂无法实现高并发，各条基础链大多每秒仅能支持几十、上百左右的交易数，且所有的应用共同占用一整条链的资源，相互挤占，一定程度上限制了其对数字广告领域的变革。我们预计，在未来一段时间内，区块链将更多侧重于满足低频次的场景需求，例如广告发布、文案及内容推广、品牌营销等。
- **区块链对广告领域的改造将逐步从反欺诈、去中介化直接营销等演化为广告效果综合管理及评估工具：**传统数字广告领域，投放效果归因一直是一个重要却较为复杂的问题，由于从广告投放到用户转化会经过多个环节，可能涉及多次曝光，如果按照点击或转化付费，则部分媒体的曝光作用可能被忽略。而基于区块链及其可追溯的特性，量化的问题就能被解决，升级成为广告主的媒介综合管理及评估工具，而媒体也能有更透明的收益分成机制。

游戏

游戏作为具有海量用户、原生数字化的领域，天生契合区块链技术。火币区块链研究院认为，区块链对游戏的改造，并不在于其体验和玩法，而在于为游戏设定更为开放、公平和互信的环境和机制，将原先控制在开发厂商手中如同黑箱的游戏，逐步开源、透明化。区块链游戏领域，相关项目如下：


Decentraland


Enjin


Refereum


DMarket


Bit.Game


Etheremon

除此之外，未来，游戏领域与区块链还可能会有如下的结合点：

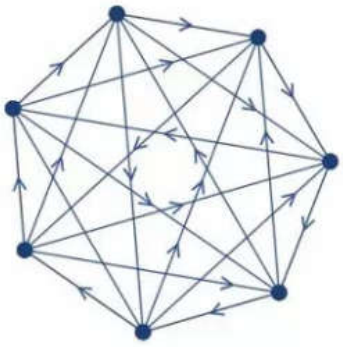
- **玩家数字资产交易是一大重点方向：**传统游戏中的虚拟资产，包括游戏装备、皮肤、坐骑等的所有权最终属于游戏厂商，且依赖游戏的存续，用户无法通过正规途径将虚拟资产向现实资产进行转化；同时，游戏中的虚拟资产大多处在封闭体系之中，缺乏共通性。区块链技术的存在，则有望改变虚拟资产流通方面的局限，通过虚拟资产上链，用户借助数字资产进行交易，且能大大降低玩家的交易风险，目前，DMarket 以及 Bit.Game 均有在尝试搭建基于区块链的游戏资产交易所。而虚拟游戏 Decentraland 之中可进行的土地拍卖流转，也正是虚拟资产通过区块链进行交易的体现。

- **区块链有望改变传统游戏分发、营销模式：**传统游戏模式下，游戏推广及分发大多依赖于大型的游戏渠道，包括 Steam 游戏平台、腾讯的 Wegame 游戏平台等，但该部分渠道成本相对较高，对中小开发者造成较大的压力。区块链可以将玩家、开发商等聚集在一个经济体系中，开发商事先购买数字资产，转入智能合约奖励池中，玩家通过转发、完成任务等形式可获得这部分奖励，并可用于购买游戏等，以此实现低成本的游戏推广。2018 年，去中心化的游戏分发平台 Refereum 开始在这方面进行尝试，并与游戏直播平台 Twitch 及游戏引擎公司 Unity 达成了合作。

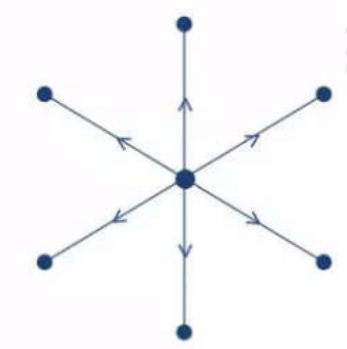
四、区块链技术发展回顾与展望

经济活动的发生依赖信任。今天，几乎任何一种形式的经济活动都需要一个可信任的第三方存在。引入第三方后，原先完成经济交换所面临的不确定便大大降低。然而，第三方模式也有一定的缺点。第一，需要支付费用，在某些场景下可能较高；其次，过分依赖第三方可能带来安全问题，部分敏感数据或保密信息可能泄露；另外，第三方的可信任程度依旧存在不确定性。这便是区块链技术存在的意义和需要解决的痛点，其本质是在公开、分散、对等的网络条件下实现大规模协作的工具，与传统的中心化调配具有较大的区别：

图24：区块链分布式协作与传统中心化协作对比



区块链：分布式协作



传统第三方：中心化调配

来源：火币区块链研究院整理

4.1 我们已处在激动人心的分布式、开放经济生态的技术攻坚阶段

区块链技术的现实应用，源于中本聪当年原始论文《比特币：一个点对点的电子现金系统》中提出的比特币及背后全新的价值转移方式。目前，比特币网络已正常运行近 10 年，比特币也已不再是唯一的数字资产及区块链应用。比特币进入主流的同时，也引发了关于区块链技术的激烈探讨。

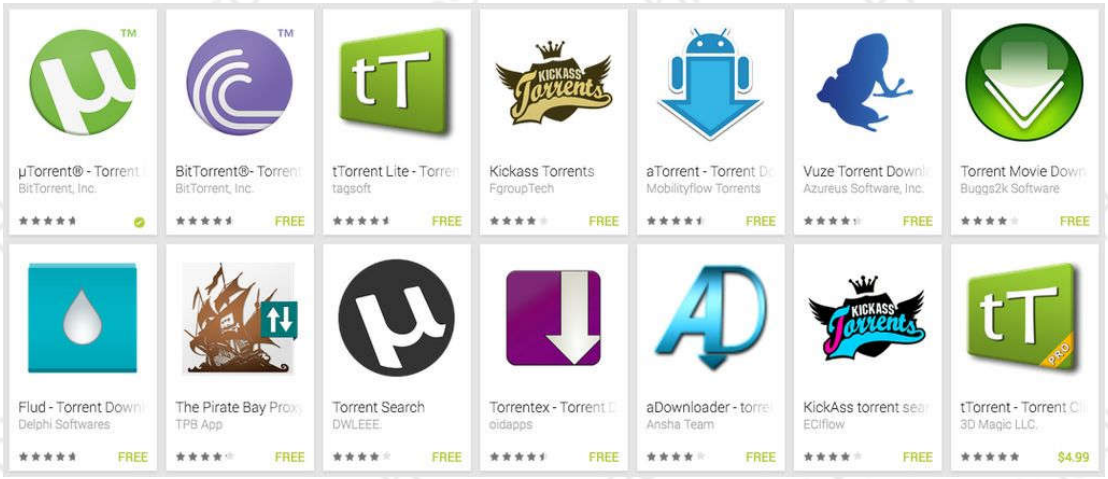
结合万向控股副董事长、万向区块链实验室发起人、分布式资本创始管理合伙人肖风先生提出的观点，火币区块链研究院认为，区块链将经历三个层次和阶

段的发展，而我们已处在最激动人心的分布式、开放经济生态的技术攻坚阶段：

第一层（阶段），分布式通讯、传输网络

区块链的最底层和初级阶段，是一个解决点对点沟通和传输的分布式网络。该分布式网络的核心在于一致性，换句话说，即如何在一个任何参与节点都能够发起、交互及广播信息的环境下，通过预设的算法、协议进行同步。在区块链的背景下，这一预设的算法、协议被称为共识机制。分布式网络技术早已有几十年的历史，而对于大多数人来说，感受最深的便是 BT 下载和“种子”这一类 P2P 分享传输应用。最早的 P2P 分享传输源于 1999 年一位美国的大学生肖恩范宁开发的一个名叫 Napster 的软件，用户启动该软件后，计算机就会变成提供上传下载服务的微型服务器，可为用户和其他使用 Napster 软件的用户提供传输和下载。

图 25：点对点传输下载应用



来源：火币区块链研究院整理

第二层（阶段），分布式账本

区块链的第二个层面和阶段，是一个借助加密的方式，进行分布式记账的账本。其衍生出的分布式金融体系，与我们传统的金融体系，是具有极大差异的。其最大的差异在于体系的维护成本，即当传统金融体系需要一整套复杂、繁重的设施保证其运行，分布式的金融体系只需要算法

和代码定义的规则。具体来说，传统的金融体系下，银行会通过严格的审核流程去评估用户的信用，并往往需要依赖于可信任的第三方例如中央清算所记录银行和不同主体之间的转账交易；分布式金融体系，相反地，是一个完全开放的网络，并且通过“全民参与”的方式记录和同步各类转账交易，不再依赖第三方，成为了一个去信任的账本网络。这一阶段，衍生出了比特币、莱特币、门罗、大零等一系列点对点现金，而这些数字资产均搭建在区块链分布式账本的基础上。

第三层（阶段），分布式、开放经济生态

区块链的第三个层面和阶段，是一个包含激励的分布式、开放经济生态。和传统股份制结构借助固定的雇佣关系与参与者绑定经济利益不同的是，区块链式的经济生态通过灵活的“行为—奖励”机制对参与者进行激励。在区块链式的经济生态中，参与者不再受到单一雇主的限制，相反地，参与者可通过完成一系列由规则预先设定好的任务或工作，例如求解哈希算法、共享资源、上传优质内容等从各个渠道获得报酬。同时，传统股份制下，参与者报酬通过法币形式发放，然而区块链式的经济生态中，报酬是通过数字资产，或可编程的数字资产进行发放，经济激励，第一次成为了可以自动化、智能执行的一串代码。

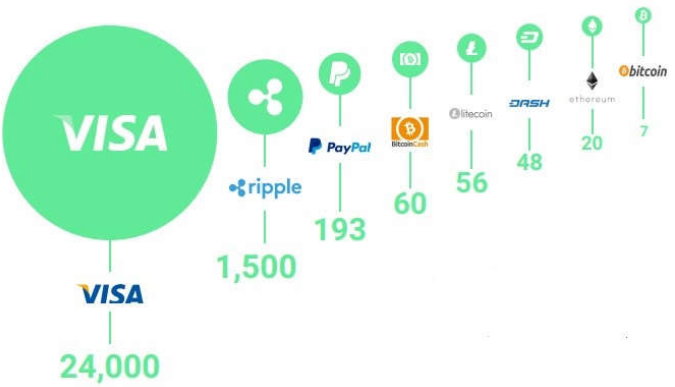
而我们正处于这一阶段，区块链技术，正通过改变人们交互和协作的方式，不断地向各个行业和应用场景渗透，并引发了科研界、产业界的热议。目前，区块链技术正努力夯实地基，为特定场景经济激励的全新商业模式的诞生奠定基础。

4.2 区块链应用落地面临的技术瓶颈与解决方案进展

虽然区块链技术发展势头迅猛，其落地应用仍旧面临不小的挑战。目前，区块链技术的性能及实用性并不能支撑大规模的商业应用搭建，扩展性、隐私性、互通性仍是瓶颈与主题，但新的解决方案正不断涌现：

➢ 可扩展性解决方案进展

图 26：每秒交易处理性能对比



来源：Token data、火币区块链研究院整理

可扩展性仍是区块链技术领域最核心和亟待解决的问题。交易吞吐量及延迟是商业应用落地的两大关键，目前，主流的区块链仅能支持数十笔交易，还远远不及 VISA 每秒可处理交易量的峰值 24,000 笔，另外，确认一笔交易区块链所需的时间很慢，比特币块时间是 10 分钟，而以太坊块时间是 14 秒左右，而 VISA 这一类服务，交易的处理是即时确认的。目前，可扩展性解决方案主要集中在共识机制（分布式网络层面）和交易验证机制（分布式账本层面）。

第一，共识机制：

公有链环境下，传统的工作量证明机制（Proof-of-Work）会面临能源浪费、效率低下的问题，为了解决节点验证效率问题，权益证明机制（Proof-of-Stake）、代理权益证明机制（Delegated Proof-of-Stake）、实用拜占庭容错机制（Practical Byzantine Fault Tolerant）逐步被开发和采用。

权益证明机制（PoS）

Cosmos　卡尔达诺 Ouroboros

Thunderella　Algorand

权益证明机制方面，除有卡尔达诺的 Ouroboros 以及 Cosmos 的 Tindermint 尝试，还有最新由 MIT 图灵奖获得者 Micali 提出的 Algorand 算法，系 PoS 机制的变种，以及康奈尔大学计算机教授 Elaine Shi 等人提出的 Snow White 算法（被用于其 Thunderella 项目）。

代理权利证明机制（DPOS）


Bitshares


Steemit


EOS

代理权益证明机制方面，最著名的案例便是 Bitshares、Steemit 以及 EOS，它的原理是让持有数字资产的人投票产生的代表记账。

实用拜占庭容错机制（PBFT）


超级账本


NEO

多用于非信任环境下的联盟链，典型案例超级账本，另小蚁对此进行了优化，形成了 Delegated Byzantine Fault Tolerant 共识机制。

来源：火币区块链研究院整理

第二，交易验证机制：

从交易验证机制角度出发，目前有侧链或状态通道、分片技术、子链或分层架构等多种扩展性优化解决方案：

- **侧链及状态通道**

该解决方案本质是将在区块链上发生的交易或运行的智能合约放在链下进行，交易双方通过开设链下通道的形式，进行小额、多笔次交易或智能合约运行，区块链仅作为结算层来处理最终交易，或在智能合约产生争议时在主链上进行公决，以此减轻主链负担。

侧链的典型案例包括比特币闪电网络、以太坊雷电网络、小蚁的 Trinity，以及“主链+侧链”结构的 Aelf 和阿希链，状态通道的典型案例包括被称为“欧洲以太坊”的 Aeternity。目前，闪电网络已上线测试网络，拥有近 900 个节点和近 2400 条网络通道，以太坊的雷电网络和小蚁的 Trinity 尚在部署之中，根据官方进度，Aeternity 也预计于 2017 年 6 月份上线主网。

- **分片技术**

分片技术将区块链网络切分成许多独立的小区域，称为“碎片”，并且每个碎片有专门的节点来维护，相当于把区块链分成了多个独立的区域，每个碎片只负责特定的事物。分片技术主要包括交易分片和状态分片两大层面。其中，交易

分片，专指每一笔交易只让一小部分节点看到和处理，由此实现交易的并发运行。状态分片，则是将存储区分开，让不同的碎片存储不同的部分，节点至负责托管自己的分片数据，解决原先主流公有链节点承担存储所有交易、智能合约和各种状态的负担。

目前，分片大多集中在交易分片，最典型的案例为 Zilliqa，已于今年 3 月 31 日上线代号“红虾”的测试网络 1.0，而状态分片实现难度相对较大，涉及跨片通信，且与交易的高吞吐量存在一定鱼与熊掌不可兼得的矛盾，目前，Rchain、Emotiq、Zilliqa 以及以太坊等项目均在状态分片、跨片通信等领域进行兼容方案的探索。

- **母子链或分层架构**

传统的公有链网络中，记账节点不仅需要负责完成交易清算，还需要承担运行智能合约及存储各类状态的职能。

分层架构的本质是将交易清算及智能合约的运行、计算进行隔离，独立运行，分担原先节点的压力，该方案的最著名的提出者为卡尔达诺，其将区块链网络分成了“清算层”和“计算层”，清算层负责数字资产的交易和流动，计算层提供智能合约，身份认证，通信等功能，并方便开发者进行应用开发，目前卡尔达诺已完成清算层的部署。

母子链架构则是将区块链分成主链和子链，母链负责交易清算，并存在众多的子链，每一条子链负责不同智能合约的运行，可定义自己专属的共识机制及执行模块，同时子链相互独立，互不影响，达到并行处理效果，子链与母链定期进行通讯，由子链将信息同步确认至母链上，典型的案例包括墨客、本体及 Nuls 等，墨客已于 4 月 30 日正式上线主网络，本体于 3 月 30 日上线测试网络，Nuls 于 3 月 31 日上线测试网络。

- **隐私性解决方案进展**

在公有链环境下，每一个节点都能获取系统账本，并且，所有的交易信息公开透明，然而这在某些对私密性要求较高的应用场景下却是致命的。尽管类似比

特币的主流区块链网络是“化名”的，即采用公钥哈希值作为交易标识，公钥哈希值与用户真实信息不绑定，然而我们仍旧可结合区块信息、转账记录以及 IP 地址等，对真实信息进行推断，因而区块链并不能完全实现“匿名”。

如何在保障隐私（隐匿交易信息）的情况下实现区块链的特性（可追溯、可验证等），目前的解决方案包括：“环签名（Ring Signature）”、“零知识证明（Zero-Knowledge Proof）”、“混币（CoinJoin）”，及“隐形互联网（Invisible Internet Project）”。

1、混币（CoinJoin）

达世币采用了混币（CoinJoin）的关键技术，借助主节点将多个用户（至少 3 个）的多笔交易进行混合、形成单一交易，同时，为了防止主节点被攻击，达世币引入链式混合（Chaining）以及盲化（blinding）技术，即用户的交易会随机选择多个主节点，并在这些主节点中依次进行混合，同时，用户不直接将输入输出地址发送到交易池，而是随机选择一个主节点，让它将输入输出传递到一个指定的主节点。

2、环签名（Ring Signature）

门罗币提出了一种不依赖于中心节点的加密混合方案——环签名（Ring Signature），每当用户发起一笔交易，用户使用自己的公钥会与其他用户的公钥中随机选出的若干公钥来对交易进行签名，以此隐藏发起者的真实身份，通过隐匿地址（Stealth address）技术，保证接收者地址每次都变化，从而让外部攻击者看不出地址关联性。通过环形 CT 来隐藏交易的金额。

3、零知识证明（Zero-Knowledge Proof）

大零币利用了零知识证明（Zero-Knowledge Proof）的密码学技术，可自动隐藏区块链上所有交易的发送者、接受者及数额信息，只用那些拥有查看密钥的人才能看到交易的内容，用户拥有完全的控制权，并可自行选择向其他人提供查看密钥，成为既可提供完全的支付保密性，又能使用公有区块链来维护的去中心化网络。

4、隐形互联网（Invisible Internet Project）

Verge 币是基于比特币技术的开源匿名数字资产，通过洋葱网络（The Onion Router）和隐形互联网（Invisible Internet Project）技术隐藏个人信息，比如 IP 地址和地理位置等，实现快速匿名交易，并无法追溯交易历史。

来源：火币区块链研究院整理

然而目前，区块链隐私解决方案大多集中在交易、转账隐私的保护上，并未涉及智能合约、信息存储、信息通讯层面的隐私问题，进入 2018 年后，一部分致力于填补上述市场空白的区块链项目开始涌现：包括致力于实现点对点加密通讯及信息传输的 Mainframe 项目；专注提供分布式的信息代理加密及解密服务的 Nucypher 项目，可满足公共区块链上私密信息的存储、共享和管理；以及目标成为公有区块链体系的私密层，可实现智能合约、信息的私密运算和交互的 Keep Network 项目。

- **互通性解决方案进展**

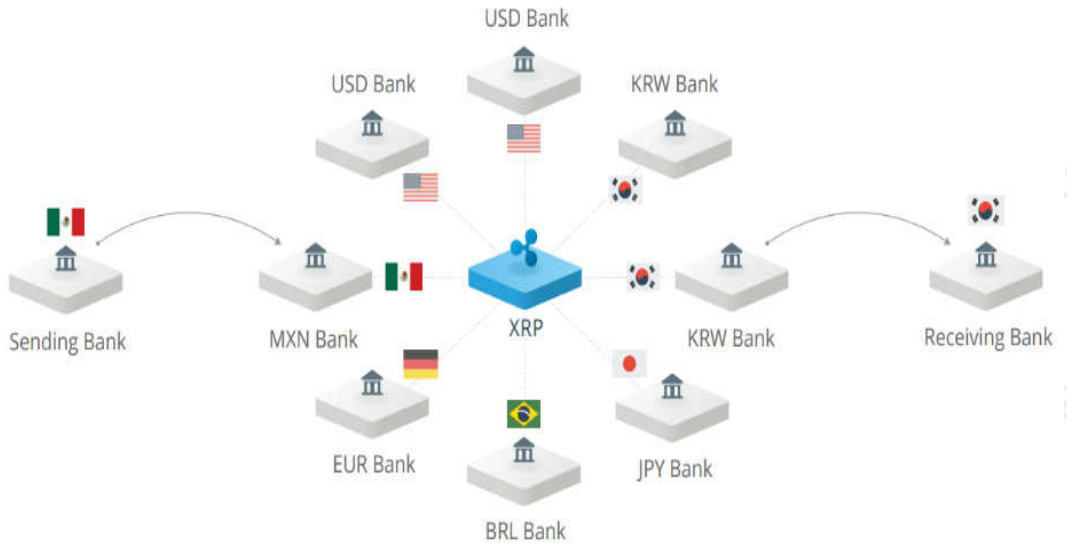
区块链体系分为私有链、联盟链和公有链。基于交易性能、容量规模、隐私保护等方面的考虑，联盟链和私有链往往被商业机构特别是金融机构更广泛采用，然而：（1）私有链、联盟链中的资产不能在不同的区块链间直接转移，主动或被动地导致了价值的孤岛；（2）同时，即便是目前的公有链，也只能和自己的生态系低成本交互，而无法高效率和别的区块链生态进行高效交互。由此各种连接不同区块链的跨链技术也被人们开始关注和探索。目前，关于区块链的跨链技术还在研究和试行阶段，方向主要分为价值跨链和状态跨链，以价值跨链为主，状态跨链有待进一步探索。主要的跨链方案包括：

- **公证人机制（Notary schemes）**

以瑞波为典型代表，其 Interledger 协议能连接不同账本，通过第三方“连接器”或“验证器”互相自由地传输货币。该协议采用密码算法用连接器为这两个记账系统创建资金托管，并通过受信任的一个或者一组团体向某记账系统声明另一记账系统上发生了某事件，或者确定该声明是正确的，这些团体既可以自动地监听和响应事件，也可以在被请求的时候进行监听和响应事件。当所

有参与方对交易达成共识时，便可相互交易。

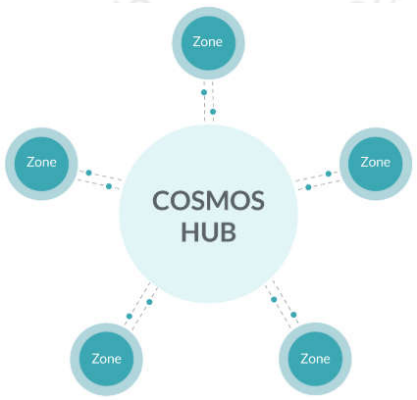
图 27：Ripple 的 Interledger 协议



来源：Ripple

- **中继技术（Relay）：**

图 28：Cosmos 的“Hub—Zone”异构链网



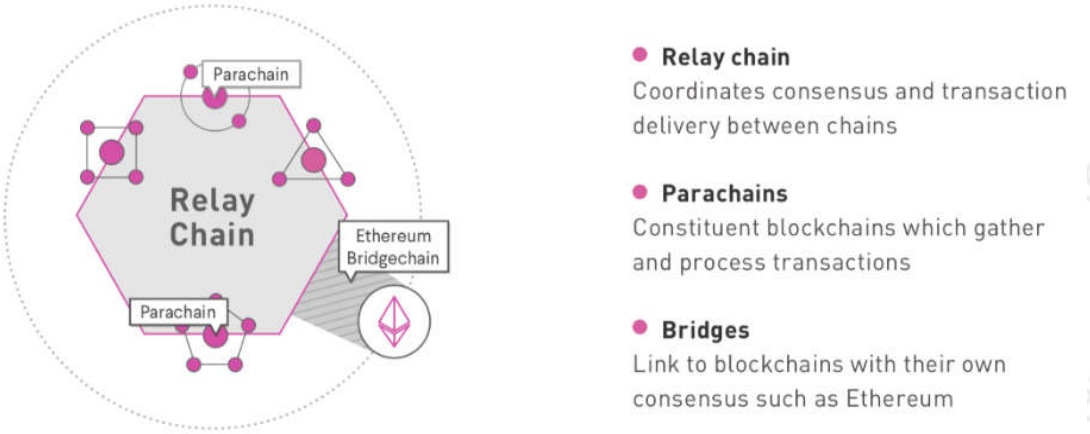
来源：Cosmos、火币区块链研究院整理

以 Cosmos 和 Polkadot 为典型。Cosmos 是 Tendermint 团队推出的一个支持跨链交互的异构网络，以其核心链—“中心（Hub）”为中继，与其余的链—“空间（Zone）”共同构成一个链网架构。链网架构下，中心及各个空间可以通过区块链间通信协议（IBC）进行沟通，代币可以安全快速地从一个空间传递到另一个空间，空间内部所有代币的转移都会通过中心，并会记录每个空间所持有的代币总量。2018 年 5 月初，Cosmos 测试网络已进入 Gaia-5000 阶段，可进行验证者的出块奖励。

而 Polkadot 系由原以太坊主要核心开发者 Gaven Wood 开发的一个可伸缩的异构多链网络。这个网络以 Polkadot 为核心的中继链（relay chain），并存在大量的可验证的、平行的动态数据结构，被称作平行链（para chain），通过 Polkadot 这一中继链，不同区块链

之间可以进行通信和数据的传递，并实现并发和扩展。

图 29：Polkadot 的“Relay-Parachain”可伸缩异构网络



来源：Polkadot Light Paper

- **侧链技术（Sidechain）**

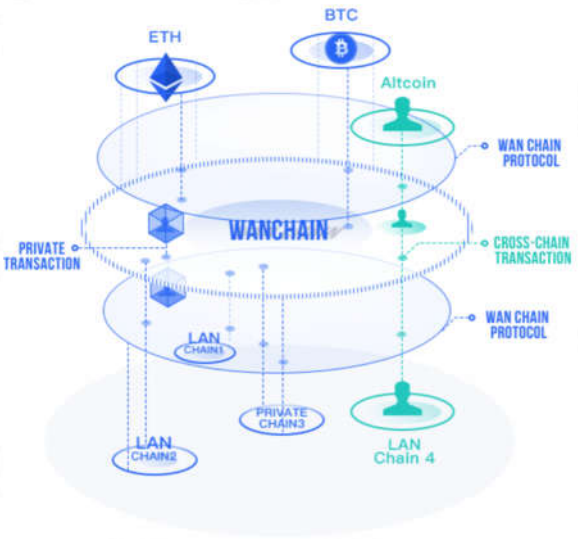
侧链是以锚定某种原链上的数字资产为基础的新型区块链。假设 B 链能拥有 A 链的所有功能，则称 B 链为 A 链的侧链，A 链为 B 链的主链。其中主链 A 并不知道侧链 B 的存在，侧链 B 知道有主链 A 的存在。通过将主链的区块链头写入侧链的区块中，让侧链使用和主链一样的共识验证方法，侧链便可以验证主链的交易。典型的侧链技术项目如比特币的侧链 Rootstock。

- **哈希锁定技术（Hash locking）**

以闪电网络（Lightning network）、雷电网络（Raiden network）为典型，在跨链支付层面被莱特币所率先采用。其核心在于哈希锁定技术（Hash locking），即在不同的区块链之间架设链下的支付通道，双方若无直接的点对点支付通道，只要网络中存在一条连通双方的、由多个支付通道构成的支付路径，闪电网络也可以利用这条支付路径实现资金在双方之间的转移。由于比特币和以太坊等区块链网络各自使用了不同的网络协议，导致很难在异构的区块链网络间搭建闪电网络的通道，目前的跨链闪电网络通道，主要存在于莱特币和比特币之间。

- **分布式私钥控制技术**

图 30：Wanchain 的跨链交易机制

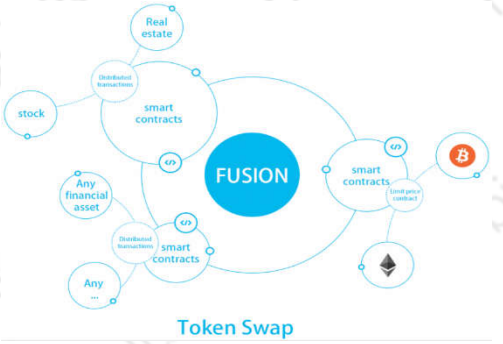


来源：Wanchain

以 Wanchain 和 Fusion 为典型。Wanchain 利用多方计算和门限密钥共享方案对跨链交易进行联合锚定，在不改变原有链机制的基础上通过跨链通信协议实现接入和交互。具体来说，对于转入交易，用户发起跨链交易请求，并将原链上的资产转入 Wanchain 位于原链的跨链锁定账户，之后用户可在 Wanchain 上获得新创造的同等价值的智能合约数字资产，进而可以使用相关应用或交易；对于转出交易，用户在 Wanchain 上被创造的数字资产清空，之后 Wanchain 位于原链的跨链锁定账户，会向用户提供的原链目标账户转入先前锁定的数字资产，等值的数字资产便会回到原有链。

Fusion 则是通过分布式私钥生成与控制技术将各种数字资产映射到 Fusion 公有链上，这一过程称为锁入，而后可实现对多种数字资产的控制权管理，被映射的数字资产可在 Fusion 公有链进行自由交互，通过智能合约进行抵押、托管、借贷、衍生品等应用。最后，再通过解锁，将数字资产的控制权还给所有者，与 Wanchain 不同的是，整个过程不涉及所有权转让。

图 31：Fusion 的多数字资产映射模式



来源：Fusion

4.3 区块链以外新的分布式账本底层正不断涌现

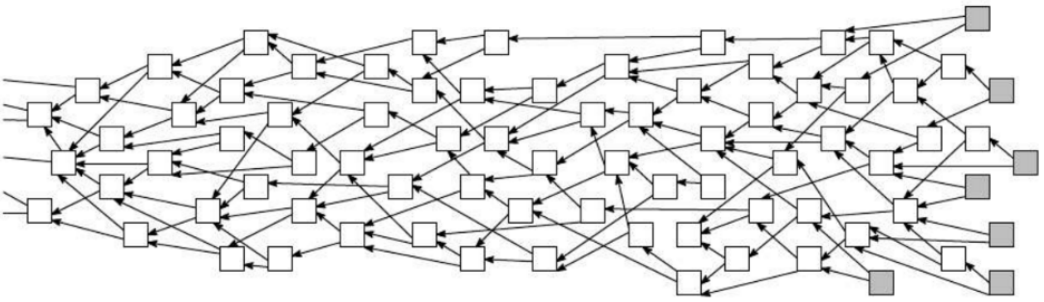
由于区块链技术目前面临“可扩展性—去中介化—安全性”的抉择，越来越多的项目寄希望于通过区块链以外的技术搭建分布式账本底层，以突破上述瓶颈。事实上，“区块链”是一种分布式账本技术，然而分布式账本技术却不等同

于“区块链”。目前，除区块链外的主流分布式账本技术如下：

➢ 有向无环图（DAG）

DAG 是一种使用拓扑排序的有向图形数据结构，无区块概念，不涉及将所有数据打包进区块，以及区块之间的串联，而是节点各自提交数据单元，包含签名，数据与父辈单元信息，不同数据单元之间通过哈希值进行关联，最终形成一个无回路的有向图数据结构。

图 31：有向无环图架构



来源：Wikipedia

与区块链同步记账不同，DAG 本质是一种异步记账，即数据信息录入操作异步化，用户可以自主异步地发起交易，并把数据写入 DAG 中，从而可以支持极大的并发量和极高的速度。目前，传统采用 DAG 架构的项目包括 IOTA、ByteBall、Nano，另外，也有新兴的如 TrustNote、Hycon、CyberVein 等项目涌现：

传统 DAG

IOTA

独创 Tangle（缠结）架构，无挖矿，整个网络均参与交易验证，节点每向网络中添加一笔新的交易，需验证网络中前两笔交易，进行一定的工作量证明，后等待其他节点对你发起的交易进行验证。2018 年 5 月 3 日，IOTA 基金会宣布 Qubic 项目，将会通过 Qubic 在 IOTA 中添加智能合约、预言机等，被认为是重大升级。

ByteBall

取消了区块链和工作量证明挖掘概念，在传统 DAG 架构上引入主链与公证人概念，主链即经过公证人认定的最短路径，是一道确定的交易时间序列，构成无序的有向无环图中的主干，公证人充当监管者的角色，帮助系统锚定交易发生的时间顺序，以避免潜在的双花问题。

Nano	原 Raiblocks，2018 年改名 Nano，独创 DAG 区块点阵（Block-Lattic）数据架构，非传统的单线程区块链架构，一个账户一条链，只记录、维护和更新自己的交易，从而实现高并发。具体来说，发送者在自己链上执行“发送”交易，并完成简单的工作量证明，以防止垃圾攻击，接收者在自己链上执行“接收”交易，后交易发送给验证节点，由验证节点进行比对和广播，无冲突，便确认，若有冲突，启动验证节点投票。
新兴 DAG	
TrustNote	TrustNote 改进了 Byteball 的公证人制度，采用了双层共识机制，在传统 DAG 验证的基础上，引入了被称为 TrustME 的公证共识，由超级节点通过竞争的方式获得公证人的权利，同样依据 DAG 架构中排出的主链定序避免双花问题。
Hycon	韩国的基于 DAG 数据架构的底层公链平台项目，使用称作 SPECTRE 的共识算法，在两组数据单元之间采用投票算法，以成对的方式对它们进行排序，以解决 DAG 异步记账模式下潜在的双花隐患。
CyberVein	在 DAG 数据架构的基础上附加可交互的智能合约，并使用自己的编程语言 Vein 和虚拟机 CBVM（CyberVein Virtual Machine）。与传统 DAG 项目节点在发布数据单元前需要做简单的工作量证明不同，CyberVein 引入贡献证明（Proof of Contribution），通过在网络中的贡献和适当的哈希计算，来决定交易费用的分配。

来源：火币区块链研究院整理

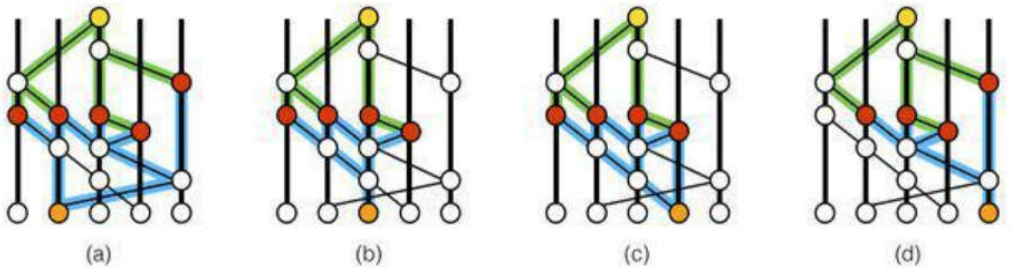
➢ 哈希图（Hashgraph）

哈希图是由 Swirds 公司持有专利的一种分布式账本技术和数据结构，根据其独创的流言协议（gossip about gossip protocol），每个节点需将自己的交易信息传递给相邻节点，又将相邻节点的交易信息传递给其他节点；并且，每一笔交易信息都会附上需要传递的他人交易信息的哈希值，以及该节点自己最近一笔交易的哈希值，当所有节点完成信息传递，便可以达成共识，完成记账，这一过程被称为虚拟投票（Virtual Voting）。通过上述方式，哈希图解决了传统 BFT 共识下消息复杂度高，大量消耗系统的网络带宽，无法很好的应对动态网络问题。

目前，哈希图主攻商业领域的联盟链，已在联盟链环境下实现二十五万笔

每秒处理速度，然而其在大规模公有环境下运行仍有待验证。

图 32：哈希图数据、信息传递结构



来源：Hashgraph

哈希图具备如下特征：

- 哈希图仍采用拜占庭容错算法，属于完全异步的拜占庭容错 aBFT，1/3 的容错率，不良节点低于总节点数的 1/3，就能保证共识无误，但一旦有更多的节点作恶，系统便会崩溃。
- 相较于区块链体系记账时间通常与实际交易时间存在差异，例如在 PoW 机制下，某一笔交易的优先级不够高，或者矿工费用较低，记账者就会优先打包其他交易，但哈希图机制下，实际交易时间与记账时间是一致的，交易发生后就传遍全网，便获得公认，因而更加公平。
- 无需挖矿，原先 PoW 的工作量证明机制，运行公有网络的成本高昂，同时，若两个矿工同时创建了两个区块，系统会默认选择最长的那条链，而丢弃另一个，造成浪费。

火币区块链应用研究院

关于我们：

火币区块链应用研究院（简称“火币研究院”）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
微信公众号：	火币区块链
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
Website:	http://research.huobi.com/

免责声明：

1. 火币区块链研究院与本报告中所涉及的项目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，报告中的结论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。