区块链

盘点公链（2020H1）：扩容至深水区，DeFi、代付渐成标配

增持（维持）

2019 年 10 月 24 日召开的政治局集体学习会议将区块链定位为“核心技术自主创新的重要突破口”，而公链是区块链发展的基石，其发展动向可以看作区块链产业的风向标。本篇报告梳理了 2019 年以来重要公链为突破性能瓶颈做出的种种努力和在安全性和链上与链下应用方面的进展。

公链交易处理性能和安全性领域出现多种优化方案。交易处理性能方面，链上与链下扩容方案“齐头并进”。1）POA（权威证明机制）获得更多关注。Vechain、波卡等项目采纳的 POA 在前期或是解决公链性能问题的较为直接而有效的路径。2）POS（权益证明机制）探索之路漫漫。以以太坊为代表的诸多知名公链正在探索 POS 机制，以摆脱当前流行的 POW 共识算法下的诸多问题（例如性能）。其中，以太坊或将在 2020 年上线采用了 POS 共识的信标链，前景可期。

安全性方面，尽管以太坊共识机制转型延期，其他项目共识机制的转变和防范大规模攻击取得进展。例如，Algorand 采用随机算法实现拜占庭算法的大规模扩展；达世币专注升级链锁以免疫 **51%**算力攻击；Neo 将降低非投票节点可获得燃料代币的数量，将当前的 Neo 升级至 Neo3，以提升投票率和安全性。

DApp 竞争格局稳定。从交易额、交易笔数、活跃用户数量等方面来看，波场 TRON、EOS、ETH 居于全球前三。其中，TRON 在活跃用户和交易量等方面增速最快；2019 年，EOS 在交易额和交易笔数上处于领先地位；ETH 活跃用户和 DApp 数量均为第一，且在 2020 年一季度在总交易额上获得领先地位。

以太坊仍是标杆，DeFi、“为普通用户代付费用”渐成标配。我们预计，2020 年及未来，会有更多公链项目兼容以太坊，抱着追赶以太坊的态度，不断捕获以太坊与培育自身链上资产，吸收其他公链“放开链上资源租赁”“为用户代付链上资源使用费（参考 EOS、Nervos、VeChain 等）”等做法，使资源与用户的匹配更精准，降低普通用户的使用门槛和合规风险，并寻找区块链与传统商业世界的结合点。

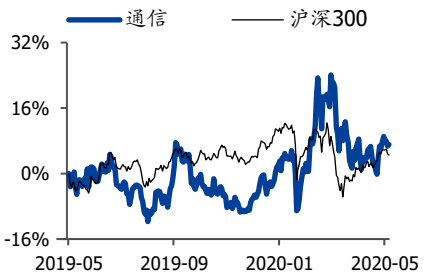
DeFi 生态繁茂，安全事件引担忧。被锁仓的加密货币市值已经高达 12.3 亿美元。而 2020 年年初以来，MakerDAO “黑色星期四”、bZx 闪电贷事件、Lendf.Me 被黑客攻击等几起与 DeFi 相关的风险事件引发担忧。这暴露出 DeFi 的安全性受制于底层平台，我们认为，作为一种金融服务，DeFi 应高度关注风险控制这一生命线。

投资建议：推荐关注有望受益于区块链技术持续发展的相关标的：1）东港股份、易见股份、安妮股份等（区块链应用）；2）央行数字货币：恒宝股份、新大陆等；3）欧科集团、火币科技（数字资产交易相关）；4）嘉楠科技（比特币矿机厂商）。

感谢以下机构与个人对本报告提供的资料支持（排名不分先后）：Nervos 吕国宁；Conflux 张元杰；VeChain 周子衡、任之劼；Qtum 郑义、帅初；Neo 达鸿飞、高原、李雅君；EthFans 以太坊爱好者 阿剑。

风险提示：区块链技术发展不达预期，区块链商业模式落地不达预期，监管政策宽松度不达预期。

行业走势



作者

分析师 宋嘉吉
执业证书编号：S0680519010002
邮箱：songjiaji@gszq.com
研究助理 孙爽
邮箱：sunshuang@gszq.com

相关研究

1、《区块链：比特币第三次“减半”，挖矿市场波澜不惊》2020-05-11

2、《通信：新基建如何落地？物联网、REITs 与国产化》2020-05-10

3、《通信：通信行业 2019 年报及一季报综述：春日将至，沃土生花》2020-05-06

内容目录

图表目录

1 概览：区块链迎来性能、安全、应用三方面的边际革命

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式（《中国区块链技术和应用发展白皮书》，工信部 2018 年指导发布）。它是以比特币、以太坊为代表的加密货币普遍采用的底层技术，有助于保证链上信息不易篡改，有助于对信息溯源，有助于多方协作。例如，比特币致力于不依赖银行、支付公司等第三方即实现点对点的价值转移，其交易流程为：为获得比特币奖励，用专用计算机求解比特币网络给出的数学题，成功解得者获得记账权，将交易打包入块，各区块按照被记录的时间，在最长链后逐个相连，由全网节点见证，比特币 2009 年上线，最新市值已超过 1600 亿美元（Coinmarketcap，2020.5.2）。

公链是区块链生态的重要组成部分。根据分布式账本记账权开放权限的不同，区块链可分为公有链、私有链及联盟链。其中：公有链记账权对互联网上的所有人开放，例如比特币、以太坊；私有链一般用于组织内部，不对其他人开放记账权；联盟链记账权对特定的组织和机构开放。

本文将回顾 2019 年以来部分知名公链的技术进展、链上应用（Dapp）发展情况并展望其未来。1）技术进展：公链存在实现“去中心化、高系统安全性和高交易效率”三个目标难以同时解决的“不可能三角”问题，各条公链致力于解决这一点，但路径有所不同。**2）应用情况：**公链的应用情况也是关注研究的重点领域，本文将介绍 2019 年在 DApp 方面较为领先的几款公链项目。

图表 1：比特币、以太坊等公链 2019 年技术回顾与 2020 年展望

	最新市值（亿美元）	24 小时活跃地址数	TPS（每秒交易笔数）	Dapp 数	2019 年回顾	2020 年展望
比特币（BTC）	1624	921407	3.8	/	闪电网络快速普及。	比特币闪电网络的快速普及，有望促进小额、实时、海量支付网络的形成。
以太坊（ETH）	236	408829	9.0	2585	技术升级利好 Layer-2 方案。	将优化 Gas 消耗（以太坊网络使用费用），提升性能，为扩容做准备。
比特币现金（BCH）	47	23998	0.5	/	运用 Schnorr 签名提升交易效率，通过其线性特点支持更多智能合约和多重签名。	继续通过技术提升交易效率。
BSV	39	25152	6.4	/	完成创世区块发行，取消区块限制，将默认区块大小从 128MB 提升到 2GB。	消除区块上限等人为限制，恢复比特币脚本的原始功能。
EOS	29	/	/	633	Dapp 格局上，EOS 在交易额和交易笔数方面处于领先地位。	EOS 会继续做出了一系列创新性的举措如升级主网至 v1.8 来提升用户使用体验，提升交易效率。
波场（TRON）	10	/	/	683	在活跃用户和交易量等方面增速较快。	深耕娱乐型 Dapp。
波卡（Polkadot）	/	/	/	/	通过中继链技术能各公链上的代币转入类似多重签名控	2020 年 5 月发布新路线图。

					制的原链地址中，提升区块链可扩展性。	
Cosmos	5	/	/	/	通过中继链技术能各公链上的代币转入类似多重签名控制的原链地址中，提升区块链可扩展性。	继续采用类似实用拜占庭容错的共识算法，实现代币安全快速地从一个空间传递到另一个空间，大幅提升区块链的互操作性、可扩展性以及无缝更新性。
达世（Dash）	7.8	66899	0.3	10.1	专注升级链锁以免疫于 51%算力攻击。	/
Nervos（CKB）	0.69	11000	/	/	成功启动了 CKB 主网，从头开始构建并如期交付了功能完备的 Layer 1 区块链.	除了持续进行CKB协议层和链上开发的改进外，还将重点关注开发者体验、Layer 2、研究以及社区建立。
Bytom（BTM）	0.71	1243	16 万（侧链 Vapor）	/	上线一主多侧的 BaaS 平台和侧链	基础协议层提出通用的跨链开放式网关协议，计划在 Layer2 前沿领域有所突破
Conflux（DAG）	/	/	/	/	声称能同时满足去中心化、高安全性、高性能。	继续为同时满足去中心化、高安全性、高性能努力，主网上线在即。
VeChain（VET）	2.5	4353(当日活跃账号数)	230	125	进一步落地在包括食品安全、可持续时尚、跨境供应链管理等领域的项目。	发布与落地 POA2.0 算法
NEO	7.14	226 万地址（其中 54%持有资产）	1000+	68	斥资 1 亿美元支持生态建设，推进链上互操作性协议的实现。	完成 Neo3 升级，大幅优化协议层、完成包括分布式存储，内置预言机与分布式身份在内的组建层搭建，并探索更多数字资产的应用场景。
Qtum	1.45	2221（全球节点数）	0.01（实测的最近 24 小时每秒交易量，不代表实际交易能力）	/	实现了 Qtum-BTC 原子交换，发布 Qtum2.0	离线 Staking，Qtum Phantom 隐私解决方案和 Qtum Neutron 虚拟机架构三大更新

资料来源：Coinmarketcap，区块链浏览器、国盛证券研究所（BTM、VET 的数据更新至 2020.5.8，Nervos 数据更新更新至 5 月 13 日，Qtum、NEO 数据更新至 5 月 15 日，其他公链的数据更新至 2020.5.2）

2 性能：百花齐放，以太坊信标链或于 2020 年上线

交易处理性能的衡量标准是每秒处理交易笔数（Transactions Per Second， TPS），比特币等区块链项目出于自身安全性和去中心化的需要，对区块规模大小和区块产生速度等进行了严格限制，导致项目的交易处理性能较差。处理性能不高势必导致用户在使用该项目进行收付款时面临高延迟、高堵塞的窘境，因此项目很难在日常生活消费中普及，而只能运用在高额支付中以确保交易安全性，这与比特币等项目的发起初衷是违背的。**提升 TPS、保证去中心化水平、提升区块链的可扩展性是公链技术未来发展的方向。**根

据 PANews 在 2020 年初的调查，有超过 7 成的用户认为 TPS 对公链发展至关重要，同时有超过一半的用户认为需要在提升 TPS 的同时保证去中心化程度。

目前区块链项目主要通过扩容的方式满足日益扩大的用户群的交易需求，主要扩容方式有三种，分别是 **1）直接增加区块容量。**移除原先中本聪对比特币容量 1MB 的区块上限；**2）发展跨链技术。**跨链技术的主要目标是实现单个公链内外信息、资产的相互沟通读取，这样可以显著提高区块链的可扩展性、速度和延展性，目前主要形式有闪电网络、侧链扩容等，在比特币区块链之外构建新的交易渠道进行小额交易；**3）分割区块。**主要形式有隔离见证等，将用以证明交易真实性和合法性的见证数据隔离在区块基本信息之外，只保留交易状态数据。

图表 2：跨链主要技术

主要技术	主要内容
公证人机制	以瑞波和 BTC Relay 为代表，关注资产转移。
侧链/中继	以 Polkadot 和 Cosmos 为代表，关注跨链基础设施。
哈希锁定	以闪电网络为代表，通过建立交易通道实现海量小额支付。
分布式私钥控制	以万维链为代表，链内交易的分布式账本均能接入万维链，实现不同区块链的连接。

资料来源：百度百科，国盛证券研究所

2019 年以来比特币及其分叉币、以太坊等项目有明显进展。

- 比特币和以太坊：主要采取了发展第二层网络的形式。2019 年比特币的闪电网络技术迅速普及，使比特币的小额实时海量支付成为可能；以太坊完成了君士坦丁堡和伊斯坦布尔两次升级，利好 Layer-2（二层网络）方案。
- 比特币现金（BCH）：利用 Schnorr 签名扩容。BCH 推出了改善扩展性和隐私性的 Schnorr 签名功能，大幅提升交易效率。
- BSV：完成创世升级，直接取消区块限制。2020 年 BSV 完成升级，消除了对协议施加的人为限制，如区块大小的默认上限，基本实现了最终扩容愿景。
- Polkadot 和 Cosmos：利用中继技术实现区块链互操作性和可扩展性。这两个项目通过中继链技术将私有链、联盟链融入到公有链的共识网络，为区块链项目提供跨链基础设施或协议，提升交易效率。

2.1 链上扩容路线——扩大区块

比特币现金（BCH）运用 Schnorr 签名提升交易效率，BSV 完成创世区块，取消区块限制。BCH 成功实现两次升级，Schnorr 签名功能具有重大意义，可以通过其线性特点，支持更多智能合约和多重签名，大幅提升交易效率，而安全证明和不可延展性进一步提升交易安全。BSV 仍旧遵循中本聪愿景，不断扩容。继 2019 年 7 月将默认区块上限提升到 2GB 后，2020 年 2 月 4 日 BSV 完成了创始升级，消除了区块上限等人为限制，恢复比特币脚本的原始功能，其扩容和大区块愿景已基本实现。但由于 BSV 的实际交易量不像比特币那样巨大，交易需求相对较小，因此实际扩容效果有限。2020 年其创始人 CSW 郁金香信托案件的诉讼结果将对其币值产生重要影响。

2.1.1 BCH 推出 Schnorr 签名

由于针对比特币的扩容方案不同而又无法统一，比特币出现了大量分叉币，其中以比特币现金（BCH）、比特币黄金、比特币钻石、BSV 等为主要分叉币。

图表 3：各比特币分叉币基本情况（截至 2020 年 5 月 2 日）

币种	分叉时间	单价（美元）	已发行量（万枚）	最新市值（亿美元）	与 BTC 的不同
比特币现金(BCH)	2017.8.1	256	1838	47	1）区块容量不同，BTC 为 1MB，BCH 删除了隔离见证，最大可支持 8MB 区块大小。2）算法难度不同，BTC 算法难度随着被挖数量增加而增加，而 BCH 生产难度会根据全网算力调节。
比特币黄金(BTG)	2017.11.13	10	1837	1.85	PoW 算法不同。BTC 采用 SHA256，BTG 采用 Equihash 以消除大矿工对算力的控制，这样可以做到更强的去中心化。
比特币钻石(BCD)	2017.11.25	0.59	18942	1.1	1）区块大小不同，BCD 支持每个区块大小为动态值。2）出块速度不同，BCD 出块速度约为 BTC 的 5 倍。3）BCD 降低转账手续费和用户参与门槛。
BSV	2018.11.9	209	1838	38.5	BSV 希望解除各种代码限制，如区块大小限制、防尘交易限制、非标脚本限制、OP_Return 空间和数量限制。

资料来源：coinmarketcap，国盛证券研究所

比特币现金（BCH）成功升级两次，Schnorr 签名提升交易效率和安全性。2019 年 5 月 15 日，BCH 推出了 Schnorr 签名功能和恢复意外发送资金的隔离见证（Segwit）恢复功能。比特币采用的是椭圆曲线数字签名算法（ECDSA），其固有缺陷是可延展和非线性特点，可延展性影响了签名的安全性，而非线性导致签名占用了过多空间，影响交易效率，而 Schnorr 签名算法则通过其线性特点，支持更多智能合约和多重签名，大幅提升交易效率。

图表 4：2019 年闪电网络技术特点

	椭圆曲线数字签名算法（ECDSA）	Schnorr 签名
签名验证	每个签名都必须运用点乘运算单独验证，广播一笔交易需要数千台计算机的验证，占用大量空间和费用。	Schnorr 方程是线形的，可互相加减，从而节省计算能力（加法比点乘法计算容易得多）
安全证明	ECDSA 不存在类似于 Schnorr 的安全证明。	当哈希函数足够随机且签名中使用的椭圆曲线离散对数问题（ECDLP）足够困难时，Schnorr 签名安全性很容易得到证明。
延展性	可延展，可以使无法访问私钥的第三方更改现有有效签名并双花资金。	不可延展，安全性更强。
多重签名	本身不支持多重签名，必须通过 P2SH 智能合约，但其交易成本较高、隐私保障较少。	线性，多个参与方可以协作生成对其公钥总和有效的签名，这是提高效率和隐私的基础，例如多重签名和其他智能合约。

资料来源：巴比特，国盛证券研究所

Segwit 恢复可以帮助网络用户在意外将其资金发送到隔离见证地址时收回资金。2019 年 11 月 15 日，BCH 实施 Minimaldata 规则，此更改使网络上的大多数 BCH 交易均不可篡改。同时 BCH 还扩展了 Schnorr 签名，几乎所有签名检查操作都将支持 Schnorr 签名。

2.1.2 BSV 完成创世升级不设上限

BSV 遵循中本聪愿景，不断扩容。BSV 始终遵循通过区块链交易存储方式来访问网络数

据的目标，不断扩容。2019 年 7 月，BSV 将默认区块大小从 128MB 提升到 2GB，而 2020 年 2 月 4 日，BSV 已经完成了“创世”升级，主要改变有：1）消除对协议施加的人为限制，如区块大小的默认上限。2）恢复比特币脚本的全部原始功能。3）删除对比特币的部分更改，如不再支持 P2SH 地址。“创世”升级意味着 BSV 的扩容愿景和大区块路线已基本实现。但由于 BSV 的实际交易量不像比特币那样巨大，交易需求相对较小，因此实际扩容效果有限。

2020 年 1 月 14 日，BSV 的币值出现大幅拉升，主要原因是 BSV 创始人“澳本聪”（CSW）自称掌握了证明自己是比特币创始人中本聪的关键证据，并拥有了能够解锁“郁金香信托”中 110 万比特币的密钥，一旦 110 万比特币投入市场，将对比特币市值产生重要影响。目前，克莱曼指控 CSW 通过伪造文件骗取其哥哥的郁金香信托遗产，美国法官裁定 CSW 需在 3 月 12 日前提交郁金香信托相关文件，这遭到了 CSW 的拒绝。案件仍在进一步审理中。一旦 CSW 败诉，其信用危机或将对 BSV 的币值产生重大影响。

2.2 链上扩容路线——改变共识算法

2.2.1 Conflux：引入“父边”“引用边”，打造树图结构

Conflux 是致力于在不牺牲任何去中心化程度及安全性的情况下实现高 TPS 的公有链。Conflux 使用基于树图结构的可扩容共识算法，通过节点并行出块来提高整个网络的吞吐量，以解决高并发网络中因分叉造成的计算资源浪费问题，使共识不再是区块链性能的瓶颈。

举例来说，综合橙皮书的研究，下图中 Conflux 为区块排序的步骤为：

1）父块与枢轴链

矿工在打包一个新区块的时候，必须选择前面的某个区块作为自己的父块，并且只能选择一个，子块最多的区块根据前后顺序组成“枢轴链”（这就是“最重链原则”）。

例如，下图中黑线代表“父块”顺序，则枢轴链为“A→C→G→J→M→N”。

2）引用边

除了父边，每个区块还必须把自己看到的其它分叉上未被引用的区块引用起来，作为引用边。

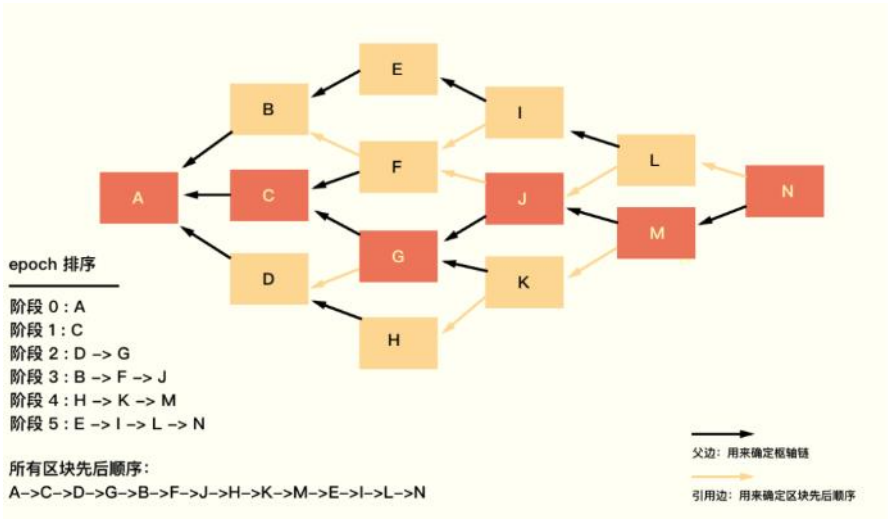
例如，下图根据引用边可以确定的区块顺序为“D→G”” B→F→J→L→N”” F-I”” H→K→M”。

3）阶段

枢轴链上的每一个区块独自代表一个“阶段”，按照阶段先后顺序排列所有区块。枢轴链区块引用的块、被引用的块的父块或其引用的块，如果还没有被排序，那么都同属于同一阶段。同一阶段内，有两个引用块彼此无法确定先后顺序，就采用哈希 ID 来排序。

例如，下图中各阶段及其内部的排序为：阶段 0（A），阶段 1（C），阶段 2（D、G），阶段 3（B→F→J），阶段 4（H→K→M），阶段 5（E→I→L→N），则下图中所有区块的排序为 A→C→D→G→B→F→J→H→K→M→E→I→L→N。

图表 5：Conflux 树图结构例示（局部）



资料来源：橙皮书，国盛证券研究所

在内部测试网中，Conflux 已经实现 3000-6000TPS 的高吞吐量，即将上线主网。Conflux 第一阶段（Pontus）会采用 PoW 共识机制，该阶段在 2020 年 4 月已上线，第二阶段将引入矿工社区，其后大约两个月后，将释放经济模型，技术升级通过硬分叉实现。

2.2.2 VeChain：引入链下权威节点，改进 POA 算法

2020 年 2 月，VeChain 发布 POA（权威证明）2.0 论文预印本。该算法的理念是：现有的共识机制 PoW 必然走向算力中心化、大矿场集群的终局，甚至将产业链上游逐步演变为传统制造业的商业逻辑。同理，PoS 看似解决了 PoW 的中心化问题，实则大节点依然靠线下的声望、资源关系彼此维系，这种类似传统金融业的商业逻辑。对两种共识机制而言，公链演变成中心化系统只是时间问题。因此，该算法的做法是，在现实中选择一些合格的、有一定声望的、符合 VeChain 生态标准的节点。

VeChain POA 2.0 中采用了新一代共识算法 SURFACE，该算法的特点是：1）在每一轮共识中，通过一种基于可验证随机函数（VRF）的机制来选择一个由多个节点组成的委员会，并让他们对出块节点生成的区块进行背书。因此，除非能够在委员会中控制多数节点并合谋，记账节点无法用其记账权利生成不同的区块，于是分叉的概率大大降低，而系统可以做到在正常的网络环境下稳定并高效地出块。它可以根据所测得的网络实际情况，通过调节委员会大小来最大化传输效率和最小化确认延迟。2）采用了一个基于 HotStuff BFT 的三阶段共识机制，把 BFT 共识过程分为连续的三个阶段，每个阶段都要求超过 2/3 的节点达成共识，以加强安全性。

2.3 链上扩容路线——分片：以太坊信标链 2020 年或将上线

以太坊于 2015 年 7 月 30 日挖出第一个区块，它与比特币区块链的最大不同是，它致力于成为“世界计算机”，而不只是“世界账本”，它允许开发者在它之上运营各种可自动执行的智能合约（例如发行数字资产），被称为比特币之后的“区块链 2.0”，并在 2017 年，成为诸多区块链项目首次代币发行（ICO）募集资金的工具。

以太坊计划进入 2.0 阶段，会将共识机制从当前的 PoW（工作量证明，拥有更多算力者

拥有更多出块/记账即获得代币奖励权)转变为 PoW 和 PoS 混合的共识机制 Casper FFG，进而转换为 POS（权益证明机制，拥有更多代币者拥有更多出块/记账即获得代币奖励权），还会引入分片（Sharding）机制，**每个分片中的交易仅由网络中的部分验证者验证，以此来提升性能**。分片的 GitHub 官方介绍称其目标为每秒处理万余笔交易。以太坊转换共识机制和引入分片机制的主要目的是在保持去中心化的同时解决其认为的 PoW 机制下存在的性能问题，届时当前的 PoW 链会退化为一个分片或者主存储合约。也就是说，最终以太坊 2.0 可能成为以太坊的主链，而现有的以太坊则作为 1.X 成为 2.0 管理的分支。

根据以太坊基金会及各以太坊开发团队的披露，我们推测，以太坊 2.0 的 POS 共识产生的运作机制可能将是:

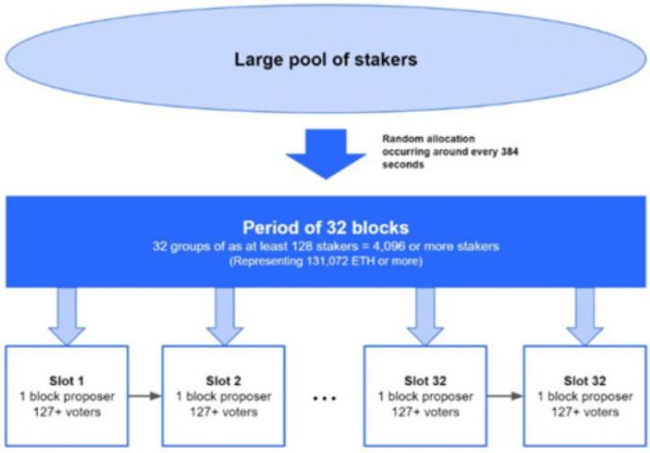
1、成为验证者
当前代币 ETH 的持有者每质押 32 个 ETH 可获得 1 个 ETH2.0 上的代币(以下称作“ETH2”)，并通过向网络告知自己公钥的方式自动在信标链注册成为验证者/staker。为了激励用户将手中的 ETH 转换为 EHT2，前期以太坊网络可能设定较高的质押回报率，即以太坊网络会增发代币，并将部分代币直接“送给”staker。

2、构建投票委员会
验证者进入投票委员会，并被随机选入各分片工作。每个分片的投票委员会包含 128 个验证者， 其中 1 个验证者会被随机选为出块者（block proposer），其余 127 个会成为投票者（voters）。信标链（beacon chain）会关联 64 个分片，各分片都将自己的最新状态的哈希存到信标链的区块上。每个分片并不直接了解其他分片，而要连接到信标链。

3、投票
每 12 秒产生一个“插槽”（slot），每个 slot 内最多可容纳 64 个投票委员会。投票委员会在给定 slot 内对区块内交易/提案表决，即构造区块，并将区块发送给信标节点。

4、确认交易
每 32 个插槽组成一个“阶段”（epoch）。每个 epoch 的产生大约需要 6.4 分钟。投票委员会引用和表决历史上的某一区块，这一关联性（crosslink）被提交到信标链上，以此来确认区块产生的最终性。最终性过程大约需要两个 epoch，也就是说，最终性过程大约 12.8 分钟。

图表 6：以太坊 2.0 投票委员会的构成



资料来源：BitMex Research，国盛证券研究所

为了促使矿工转向以太坊 2.0，以太坊还设置了“难度炸弹”。“难度炸弹”会使挖矿难度系数呈指数增加，出块时间显著增加，直到最后几乎挖不出区块，以太坊进入“冰河期”（Ice Age），届时，矿工除了转向新的 PoS 协议将别无选择。出块时间增长对 Dapp 开发者和使用者来说也十分不友好。难度炸弹原定于 2017 年底“引爆”，此后在拜占庭升级、君士坦丁堡、缪尔冰川三次升级中分别推迟 300 万个、200 万个区块、400 万个区块执行，这反应出以太坊网络并未对从 PoW 共识转向 PoS 共识做好准备。

信标链原定于 2019 年上线，也未能达成目标，原因是尚未解决安全问题（分片更容易被攻击）。不过，**2019 年上半年，信标链规范已确定，2020 年或将上线。**其后的阶段 1 是分片结构的试运行阶段，将解决分片链的共识和最终性，并允许信标链监控分片链的执行。阶段 2 中的以太坊 2.0 将完全集成分片，将实现状态执行和智能合约功能。

图表 7：以太坊发展规划与历次分叉

阶段序号	阶段名称		上线时间	内容
	奥林匹克（Olympic）		2015.5	第 9 个，也是最后一个测试网，概念验证（POC）
1	边境（Frontier）		2015.7	允许挖矿和 Dapp 开发；区块奖励为 5ETH
2	家园（Homestead）		2016.3	第一个生产环境版本；加快了交易速度
	DAO		2016.7	去中心化自治组织 The DAO 通过代币发售筹集了 1.5 亿美元资金。6 月，The DAO 被黑客攻击，价值 5000 万美元的 ETH 被黑客劫走。以太坊社区的大多数参与者决定实行硬分叉，恢复钱包中被盗的 ETH 并修补漏洞（未恢复被盗 ETH 的原始链为以太坊经典）。
3	大都会（Metropolis）	拜占庭（Byzantium）	2017.10	允许以太坊开发人员对 zk-SNARKs (零知识简洁非交互式知识证明) 执行有效的链上验证，提高隐私性；调整挖矿难度，使挖矿更困难，为过渡至 PoS 机制做准备；区块奖励由 5ETH 降为 3ETH；难度炸弹推迟 300 万个区块
		君士坦丁堡（Constantinople）	2019.2	新增可提前预测合约地址的合约创建方法，更好地支持基于状态通道或者链下交易的扩容解决方案；区块奖励由 3ETH 降为 2ETH；难度炸弹推迟 12 个月（200 万个区块）
	伊斯坦布尔		2019.12	
	缪尔冰川（Muir Glacier）		2020.1	推迟难度炸弹 400 万个块
4	宁静（Serenity）/以太坊 2.0	阶段 0（信标链）	2019.6.30 规范已确定	启用 PoS 共识，信标链部署完毕后，将使用 PoW/PoS 混合机制 Casper FFG 进行股权证明；暂不支持 Dapp 开发
		阶段 1（分片）	/	引入基本的分片结构
		阶段 2（分片的 EVM）	/	完全实现分片；引入智能合约
		阶段 3（轻客户端）	/	链下状态存储
		阶段 4	/	分片智能合约

资料来源：EthFans（以太坊爱好者），国盛证券研究所

2.4 链上扩容路线——多链

2.4.1 波卡（Polkadot）：采纳 POA，通过中继链实现跨链通信

波卡旨在解决目前区块链即时扩展性和延伸性低的问题。波卡计划将私有链/联盟链融入到公有链的共识网络中，同时又能保有私有链/联盟链的原有的数据隐私和许可使用的特性。它可以将多个区块链互相连接。在波卡看来，其它区块链都是平行链，波卡通过中继链（relay-chain）技术能将各公链上的代币转入类似多重签名控制的原链地址中，对其暂时锁定，在中继链上的交易结果将由这些签名人投票决定其是否生效。它还引入了钓鱼人角色对交易进行举报监督。通过波卡可以将比特币、以太币等都链接到波卡上，从而实现跨链通信。

与以太坊长期兼容，连续升级增加基础功能。波卡发布了去中心化的区块链项目 Kusama 网络，截至目前服务器已经历 20 多次升级，添加了可扩展的分布式身份联盟系统、多重签名、假名和事务批处理功能。另外，波卡发布了确保与以太坊兼容的四点计划，包括：1）令 Substrate 与以太坊 EVM 兼容；2）开发基于 Substrate 的 Parity-PoA 以太坊桥；3）开发 2.0 版智能合约语言 ink! Language，智能合约将受益于广泛的编译正确性保证；4）智能合约工具集将在 2020 年实现倍增，增加文档、优化和互操作性基础架构。

根据波卡 2020 年 5 月公布的路线图，其发展将分为多个阶段：
第一阶段：采纳 POA 共识机制，仅允许 Web3 基金会的 6 个验证者维护；
第二阶段：采纳 NPOS 共识机制（提名权益证明机制），Web 基金会启用有访问治理功能的超级账户 Sudo，发起第一次验证者选举，网络通过跟验证者绑定的经济权益确保安全；
第三阶段：如果大型验证者集成良好，Sudo 密钥将支持波卡中的治理模块套件，也就是支持理事会、技术委员会以及公众投票的模块；
第四阶段：公众投票发起升级，将 Sudo 移出，从此代币持有人掌握网络；
第五阶段：支持余额转账、平行链与跨链等核心功能。

2.4.2 Cosmos：通过跨链协议 IBC 实现跨链通信

Cosmos 采用 Tendermint 共识算法，是一个类似实用拜占庭容错共识引擎，具有高性能、一致性等特点。在其严格的分叉责任制保证下，能够防止怀有恶意的参与者做出不当操作。Cosmos 网络的中心及各个空间可以通过区块链间通信（IBC）协议进行沟通，代币可以安全快速地从一个空间传递到另一个空间，Cosmos 中心会记录每个空间所持有的代币总量。这一架构有助于提升应用程序互操作性、可扩展性以及无缝更新性。

2.5 链下扩容/二层网络（Layer-2）/侧链路线

二层网络（Layer-2）扩容路线，也被称为“链下扩容”“侧链”“状态通道”路线。它的常见方案是将交易状态放入主链之外生成，用户在主链抵押/存入一定金额的代币，其后在侧链开通与其他用户的交易通道，交易金额不得超过抵押金额，当需要提现时，才通过主链确认交易。比特币和以太坊等主流公链均在探索这一方案。

2.5.1 比特币：大力推广闪电网络，优化交易处理性能

比特币交易处理性能较差。比特币是一种不依靠货币机构发行且采用工作量证明（PoW）作为共识机制，因此其拥有较高的去中心化程度和安全性。但在交易处理性能方面，比

特币等待 6 个块的可信确认导致约 1 个小时的最终确认时间，远低于传统的金融交易系统。比特币的每秒处理交易笔数（TPS）约为 7，而支付宝在 2019 年“双十一”时最高 TPS 可达 54.4 万笔/秒，VISA 可达 5.6 万笔/秒，PayPal 2019 年总交易笔数为 125 亿笔，因此年平均 TPS 约为 393 笔/秒。

比特币主要参数仍保持中本聪要求。中本聪在设计比特币指出就选取每 10 分钟生成一个区块，区块容量不超过 1MB，区块生成时间和区块大小的限制也局限了全节点数据量，使得大部分电脑都可以运行，从而降低全节点的门槛并实现高度的去中心化，整个网络将更加安全，但这些限制也直接导致了比特币 TPS 较低，交易效率不高。

图表 8：比特币主要参数（截至 2020 年 5 月 2 日）

主要参数	数值
平均出块时间	9 分 7 秒
已出块数量	628586
区块大小	905.003KByte
每区块奖励	12.5BTC
奖励手续费率	5.89%
出块难度	15，958，652，328，578
总大小	320.71GB

资料来源：bitinfocharts，国盛证券研究所

图表 9：比特币成功实现的发展规划与历次分叉

上线时间	阶段名称	内容
2015.12	BIP141（隔离见证）	移除比特币交易过程中的签名字段，将交易和签名分离开，在不扩大区块大小的情况下实现“扩容”，这被称为技术性扩容方案。
2017.3	BIP148（用户激活软分叉）	由矿工决定是否升级更改比特币网络，转向由用户、交易所、支付处理商等来决定。该协议将原本由算力决定的锁定信号交给由全网节点来决定。
-	BIP141+闪电网络	主链区块 1M 大小不变，采用隔离认证（segwit）+闪电网络的方案解决比特币交易拥堵的问题。
2015.6	侧链扩容	Samson Mow 创立 Liquid Networks 侧链项目，通过创建点对点的侧链网络，达到扩容目的。
2017.6	UAHF（用户激活硬分叉）	更改节点软件，使先前无效的区块在 flag day 后生效，更改无需绝大多数算力执行。

资料来源：乐链网，国盛证券研究所

闪电网络：小额实时海量支付的交易网络。闪电网络先假定交易双方之间存在一个“微支付通道”（资金池）。双方都预存一部分资金到“微支付通道”里，之后每次交易，就对交易后的资金分配方案共同进行确认，同时签字作废旧的版本。当需要提现时，将最终交易结果写到区块链网络中，最终确认。也就是说，在闪电网络下，只有提现的时候才需要通过区块链。由于不实时依赖比特币主链，闪电网络可以不受不可能三角的束缚，提升交易处理性能。

闪电网络的流程主要分为三个步骤：开启通道、通道内交易、关闭通道。

- 开启通道
  - ✓ 交易双方将部分比特币转给一个由两人共同控制的多重签名地址。在地址中进行交易不会被链记录，交易速度快，几乎零手续费。
  - ✓ 主要技术包括多重签名技术，它指的是多个用户同时对一个数字资产进行签名，表现形式为 m/n，一共 n 个私钥可以给一个账户签名，而当 m 个地址签名时就可以支付一笔交易。
- 通道内交易
  - ✓ 交易双方在通道内各自记账，基于哈希时间锁定和哈希密钥锁定保证双方的诚信。最终双向支付通道扩展成闪电网络，构建人群之间的支付通道，每个人都充当一个中间的路由节点。
  - ✓ 主要载体为双方支付通道，而为了在缺少第三方记账的情况下保证交易的诚实可靠，需要用到哈希时间锁定和哈希密钥锁定。其中，哈希时间锁定指在交易脚本里面设置时钟，必须要等设定时间之后，才能用地址的私钥签名解锁地址里的比特币；哈希函数可以把一串输入转换成 256 位固定长度的输出，计算过程称为一次哈希运算，其中输入称为密文，输出称为密文的哈希值。可以把一个密文的哈希值放入交易的输出当中充当哈希密文锁，也就是必须得输入该哈希值对应的密文才能解锁脚本中的比特币。
- 关闭通道：单方面强制关闭，即某一方将自己控制的最新交易签名后广播出去，关闭一方会受到延时惩罚；另一种关闭方式是商议后关闭，双方从最开始的多签地址构建交易。

去中心化的闪电网络促进比特币流通。根据检测网站 1ML.com 的统计数据，截至 2020 年 5 月 2 日，闪电网络可访问节点数达到 12519 个，较上周环比增长 3.73%，交易通道达到 36191 个，较上周环比减少 0.1%，交易容量达到 958.21BTC，较上周环比增长 3%。

闪电网络的普及使用促成了比特币小额支付的可能。原先由于比特币 TPS 只有 7 笔/秒，当比特币普及之后由于交易数量过多而导致了通道拥挤，这造成了交易时比特币无法即时到账，也无法满足使用者海量的支付需求，而对于日常生活中频繁、小额的支付行为如购买商品等比特币网络无法有效应对。闪电网络的普及解决了比特币交易处理性能过低的问题，使得小额、实时、海量的支付成为可能，将有利于比特币在日常生活中的支付应用。

2019 年闪电网络应用增长迅速，快速向世界普及。2019 年 1 月，比特币爱好者发布了“闪电火炬”运动，通过闪电网络传递少量比特币，使得闪电网络技术不断得到普及。另外，Bitfinex 等交易所也开始加强闪电网络的部署，促进闪电网络的普及发展。闪电网络的技术也开始了升级，2019 年出现了交易反欺诈监控设施“瞭望塔”以及大额支付解决方案“多路径支付”。根据闪电网络最新发布的公告，lnd v.0.10-beta 更新已准备就绪，在这次更新中，协议正式添加了多路径功能。“部分签名的比特币交易（PSBT）”的功能也已添加到闪电网络，得益于此功能，用户现在可以通过一次交易将资金发送到多个不同的渠道。

图表 10：2019 年闪电网络发展进程

时间	技术或活动	主要内容
2019.1	闪电火炬	一位名为“hodlonaut”的比特币爱好者在 Twitter 发起了“闪电火炬”接力活动。他通过闪电网络将 10 万聪比特币（（1 比特币=1 亿 Satoshi/聪，即约 3.4 美元），赠予在帖子下随机挑选的一位回复者。每次接棒的人，向后传时需要增加 1 万聪比特币。Twitter 首席执行官 Jack Dorsey、《精通比特币》的作者 Andreas Antonopoulos、世界首位比特币项目投资人 Roger Ver 等知名人物参与了活动。
2019	钱包	2019 年初有 6 款左右的钱包支持闪电网络，2019 年底达到 18 个（其中部分 app 已宣布停止开发）。
2019.12	交易所	Bitfinex 成为首家支持闪电网络的主流加密货币交易所。用户可以通过闪电网络对自己的账户进行 BTC 的充值或提现。一周时间累计发生超过 800 次的闪电网络转账，其中 600 次为充值行为，总充值金额超过 7 个 BTC。
2019.6	瞭望塔	可以实时监控闪电网络中是否有欺诈交易，如果存在则帮助用户修正问题，并让欺诈者损失所有资金。
2019.12	多路径支付	Blockstream 表示完成了实现多路径支付可互操作的测试，将大额付款分成较小的部分，以便可以快速、廉价地发送大量比特币。
2020.4	PSBT 开启通道	新增支持使用 MPP 发送资金，在使用 PSBT 开启闪电网络通道的功能中，用户将可以使用单笔链上交易为多个闪电网络通道提供资金

资料来源：链闻，国盛证券研究所

2.5.2 以太坊：完成两次升级，利好二层网络方案，为扩容做准备

以太坊还有多种可以与分片兼容的二层网络扩容方案。例如，Plasma 与以太坊主链相连，用户将资产从主链发送并存储在 Plasma 上，资产可以撤回到主链上。不过，相比于节点更多的以太坊主链，Plasma 的安全性较低。

以太坊的另一种链下扩容方案雷电网络与比特币的闪电网络类似，都属于状态通道。用户将 ETH 存储于以太坊的某个智能合约中，将其作为抵押，在雷电网络开启一个通道，与另一个用户相连，两者交易金额不得高于用户存储的 ETH 金额。用户之间可以通过其他通道相连，但需支付手续费。

以太坊技术升级利好二层网络方案。君士坦丁堡升级延期完成，伊斯坦布尔升级如期完成，优化了 Gas（以太坊网络使用费用）消耗，提升性能，为扩容做准备，进一步利好二层网络方案。

2.5.3 Nervos：成功启动 CKB 主网，2020 年进一步关注技术开发

Nervos：成功启动 CKB 主网，2020 重点关注开发、研究以及社区。Nervos 的目标是创造去中心化的加密经济世界，具体做法是运用 Layer 1 来存储全局的状态共识，Layer 2 负责的是状态生成，即计算功能，追求高效率。2019 年 11 月 13 日，Nervos 成功启动 CKB 主网“Lina”。CKB 是一个全新的基于 PoW 共识机制的底层区块链。它进行了一系列的自主创新，包含独家定制的共识机制、哈希算法、编程模型、虚拟机以及经济模型等。

图表 11：2019-2020Nervos 大事件及技术进展

时间	事件
2019.3.9	Nervos 经济模型提案发布
2019.3.21	Nervos 项目发展路线图更新
2019.5.18	Nervos CKB 测试网 Rylai 正式上线
2019.6.19	CKB 共识协议提案发布
2019.6.30	Nervos 与火币合作打造金融公链
2019.7.20	挖矿算法 Eaglesong 发布
2019.10.16	Nervos 上线 Coinlist 并首次公售
2019.11.16	Nervos CKB 主网 Lina 正式上线
2020.1.9	Nervos 启动 Grants 计划并为其设立 3000 万美元基金，助力外部开发者在 Nervos CKB 上进行开发。
2020.5.6	Nervos 开启 CK Labs 计划 帮助区块链初创公司孵化构建 dApp，并帮助其连接主流加密领域投资者，并助力将其产品推向市场。
2020 开发	重点关注开发者体验和 Layer 2，提供更多可选的智能合约编程语言，更强大的 RPC，更成熟的 SDK 以及更完备的文档。
2020 开发	打造用户自定义 Token（UDT）标准，使得所有 UDT 共享相同基础代码，用户在链上独立拥有余额，大幅提升 Token 的可扩展性。
2020 开发	Neuron 钱包方面，将支持灵活的 UDT 标准并探索如何帮助用户更轻松访问主网上的 DApp。
2020 开发	构建多个使用高级语言或 DSL 的框架来促进 CKB 上智能合约的开发。
2020 开发	持续优化 CKB 浏览器的用户体验，并提供额外的功能，深层次地挖掘数据并进行分析。
2020 开发	轻客户端协议方面，支持移动端钱包、网站等的自我验证，且无需信任第三方。
2020 研究	探索通道、基于链的协议和基于 zkp 的协议。积极参与零知识证明协议的研究，并且搭建基于 zkp 协议的原型及通道的原型。
2020 社区	通过两个计划部署资源，以此鼓励开发者们优化体验和进行 Layer 2 项目开发。

资料来源：NervosNetwork，国盛证券研究所

2.5.4 Bytom：频繁上线商业应用，在 Layer2 领域继续寻求突破

Bytom：商业应用频繁上线，2020 年加大技术开发和应用进展。2019 年，Bytom 的 layer2 网络 Bystack 进一步起到操作系统和 DApp 商店的作用：1）一主多侧结构的 Bystack Baas 平台上线，它为开发者提供了区块链能力的一站式解决方案。2）Bystack 侧链 Vapor 上线，性能极限为每秒钟 16 万笔交易。3）基于比原链已在中国、欧洲和美国建立起跨链交易、物流、支付等多个领域的应用。2020 年 Bytom 将进一步扩展技术产品化，在基础协议层提出通用的跨链开放式网关协议，在 Layer2 前沿领域有所突破，而在应用层将持续设计有价值的新商业模式。

图表 12：2020 年 Bytom 技术进展规划（部分）

时间	事件
2020Q1	落地基于多签与门限混合密码学方案的开放式网关协议，支持将比原的主链、侧链与比特币、以太坊等主流公链进行去中心化的资产跨链。Vapor 侧链上线首个二层协议 Mov——一个基于磁力合约的资产交换撮合协议。基于 Bystack 架构， 提出完整的企业级区块链应用框架（Devchain）规范， 包含身份、合约、隐私、共识、跨链、资产交易等组成模块。
2020Q2	推出 Blockchain App 多语言完整 SDK。探索 DeFi 应用，基于 MOV 协议构建链上开放式生态 BApp，致力于与合作方推出多个实际产品。完成 Devchain 的部分模块开发。
2020Q3	推出完整的 Devchain 工具栈（ToolStack)， 可兼容现有的知名联盟链的 API 接口规范。Bytom 公链的协议整体升级。比原链 DEVCON3 开发者大会。
2020Q4	多领域企业级应用案例推出完整的从端到端的解决方案。积累区块链相关知识产权，在学术上参与 IEEE 区块链标准、DID 标准、MPC 联盟标准制定，并获得成果。

资料来源：巴比特，国盛证券研究所

依照比原链官方的规划，2020 年 3 月 30 日，作为第二代去中心跨链 Layer2 价值交换协议的 MOV 成功上线。MOV 打造资产托管和资产流转两大 DeFi 基础设施。随即比原链官方在 4 月 26 日宣布了保底 100 万美元 BTM 的销毁计划。在计划发布 4 天内，MOV 跨链资产超过 500 万美元。

3 安全性篇

区块链的安全性主要由其共识机制和加密算法决定。加密算法决定了区块链项目在单笔交易过程中是否存在漏洞，导致交易方出现“双花”现象，而共识机制则决定了全网各节点在验证和确认一笔交易时的公正性，它决定了作恶方能否发起 51%算力大规模攻击从而直接导致货币崩溃。目前，加密算法方面各项目已逐渐成熟，它们将更多的精力花在共识机制的改进和发展上。

共识机制的产生缘于拜占庭将军问题，该问题主要讨论了存在少数节点作恶可能性下的一致性达成问题。目前主要有四种可以防范节点作恶的共识机制以及几种防范节点故障的共识机制。

主流的四种共识机制分别是工作量证明机制（PoW）、权益证明机制（PoS）、委托权益证明机制（DPoS）以及实用拜占庭容错算法（PBFT）。其中，PoW 和 PoS 等机制通过提高作恶成本以降低作恶节点出现的概率; PBFT 等机制致力于在允许一定的作恶节点存在的前提下，依然使得各节点之间达成共识。

图表 13：公链的主流共识机制

共识机制	本质	主要内容	特点
工作量证明（PoW）	全网节点维护拥有最大工作量的链。算力越大，记账成功率越高。	通过消耗大量能源来计算一个满足条件的 Hash 值来获得记账权（发起提案），某个节点成功找到满足条件的 Hash 值之后，会马上对全网进行广播打包区块，网络中的节点收到区块后，会立刻对其进行验证。如果验证通过则立即接受该区块，同时记账节点会得到代币奖励。假如节点有任何的作弊行为，都会导致验证不通过，并直接丢弃其打包的区块，作弊的节点不但得不到奖励，还损失了巨大挖矿成本。	实现了完全去中心化和高安全性，破坏系统需要投入极大的成本。但是浪费能源，共识效率较低，而且算力集中，难以满足商业化应用的需求。
权益证明（PoS）	持有币的数量越多、时间越长，获得记账权的成功率越高。	一定程度上缩短了共识达成的时间。	不需要消耗大量能源挖矿，但性能提升有限，容易导致代币大量集中，流动性变差。
委托权益证明（DPoS）	不再需要所有参与节点验证，而是委托部分代表。	PoS 的改良版本，先通过投票选举达成极少数可信的见证人共识，见证人之间再达成交易验证共识。	大大提高了整个系统的共识效率，但容易导致过度中心化。
实用拜占庭容错算法（PBFT）	让系统中大部分的诚实节点来覆盖恶意节点或无效节点的行为。	用户端向主节点发送使用服务操作的请求，主节点通过广播将请求发送给其他副本，所有副本执行请求并将结果发回用户端，用户端需要等待 F+1 个不同副本节点发回相同的结果，作为整个操作的最终结果。	算法效率有所提升，但容错率相对较低。

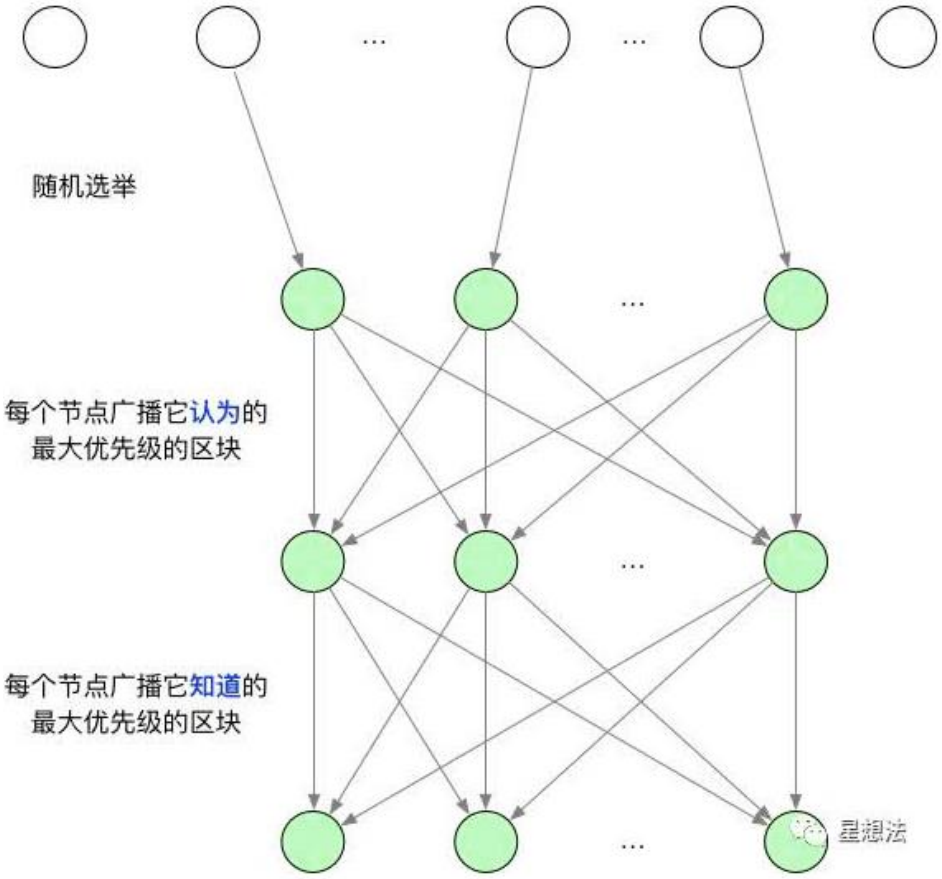
资料来源：准准网，国盛证券研究所

2019 年以太坊、Algorand 等项目进一步研究了共识机制问题以改善安全性，而达世币（Dash）也在安全性上有所突破。1）以太坊向 PoW 证明机制转变延期。以太坊信标链和难度炸弹延期，暂未上线，因此以太坊的共识机制转变将延期。**2）Algorand 实现了拜占庭共识算法。**该项目通过密码学抽签算法实现了拜占庭共识算法的大规模扩展，使其相比其他共识算法更安全和高效。**3）达世币升级链锁（Chainlocks）以免疫于 51%算力攻击。**共识机制虽然可以防范 50%共识以下的攻击，但一旦全网 51%以上的算力或权益达成共识，系统的崩溃也在所难免。达世币基于 PoW 共识机制提出链锁概念并进行多次升级以完全免疫大规模攻击。

3.1 Algorand：采用随机算法实现拜占庭算法的大规模扩展

Algorand 共识机制主要分为两个步骤：1）随机选举区块生成者生成区块 2）形成共识。随机算法主要通过可以生成随机数据的 VRF 函数和基于账户余额比例的权重随机确定区块生成和投票人。随机选举成功后，共识算法又分为两步，分别是同步确定最大优先级区块和确定该区块是否能稳定共识。

图表 14：Algorand 算法



资料来源：CSDN，国盛证券研究所

Algorand 算法可能更为安全、高效。Algorand 结合随机函数以及账户的余额比例选举委员会，并由委员会成员进行记账行为。因此通过上述拜占庭共识算法，Algorand 算法相较于 PoW、PoS 可能拥有更安全、几乎不分叉、更高效等特性。Algorand 于 2019 年末上线了 Algorand2.0，极大地扩展了可在 Algorand 平台上构建的去中心化应用程序的范围，预计 2020 年 Algorand 平台的 DApp 将迎来广阔发展空间。

图表 15：Algorand 主要技术特点

技术特点	主要内容
权重用户	对每个用户分配一个权重，该权重大小由相应用户所占有的资金数量决定。Alogrand 算法需要系统中占有 2/3 资金以上的为诚信节点方可避免分叉和双花。
委员会共识	随机选举一个小的节点子集运行 BA 算法从而实现 BA 扩展性。选举会依据节点占有的资金量分配相应的选中概率。
加密算法	为了防止针对委员会的恶意攻击，Algorand 在选举委员会的时候采用了一种私密且非交互的方式。每个节点通过运行 VRFs 以及自身私钥和来自区块链的公共信息计算自己本轮是否是委员会的成员。是的话将 VRFs 返回的证明信息广播给其他用户以证明身份。
参与者替换	在共识的每个阶段都会选举新的委员会， 各委员在将决策信息发送到网络之后就与接下来的共识过程无关。

资料来源：CSDN，国盛证券研究所

3.2 Neo：建设下一代互联网基础设施，优化治理模式和经济模型

Neo 是较早上线主网的公链，近期正在筹备从 Neo2 向 Neo3 的升级。Neo3 采用了全新的构架，也会产生新的创世块。Neo3 主网上线后，Neo2 会暂时与 Neo3 并行，以保证后续顺利迁移。某种程度上，Neo 正在做的升级不是硬分叉，而更接近于跨链。与以太坊类似，Neo3 的迁移或将为公链的转型升级提供全新范式。

Neo 链上有两种通证：NEO 和 GAS。NEO 是治理通证而 GAS 是燃料通证，GAS 在目前可以通过持有 NEO 获得。当前 Neo（Neo2）的基本治理模式是由 Neo 的持有者选出 7 个共识节点（其中 5 个由 Neo 基金会运行，一个为 Neo 开发者社区 CoZ，一个为荷兰皇家电信公司 KPN），共识节点负责出块。而在 Neo3 中治理模式将进行改变。

Neo3 新治理模式的主要特点是：1）Neo3 将由 NEO 持有人投票选出 21 个委员会成员，排名靠前的 7 名委员会成员或将成为共识节点。委员会成员有链上治理的责任，例如投票改变链上交易手续费。2）提升参与投票治理的 NEO 持有人的奖励，降低没有参与投票的 NEO 持有人收益，不参与投票的 NEO 持有人可获得的 GAS 收益预计将减少至 Neo2 时期的 1/10。

图表 16：Neo 发展大事记（部分）

2015.10	主网测试网上线
2016.4	发布共识机制 dBFT
2016.10	主网上线，Neo 理事会 7 个共识节点选出（均由 Neo Foundation 运行）
2018.7	Neo 开发者社区 CoZ 成为 7 个共识节点之一
2018.10	荷兰皇家电信（KPN）成为 7 个共识节点之一
2019.5	宣布将斥资 1 亿美元支持生态建设
2019.7	与 Ontology （本体）合作推出互操作性跨链协议
2019.4	Neo3 开发线路图公布，启动建设下一代互联网基础设施

资料来源：Neo，国盛证券研究所

Neo3 还将推进下一代互联网基础设施的建设，包括 1）Neo-FS：分布式文件存储，可以存储视频、大文件；2）Neo-ID：分布式身份协议，可以绑定身份，提供链上身份证明的

有关方面的功能;3)开发内置 Oracle,可以让区块链上的智能合约直接访问互联网资源,以增强跟互联网的互操作性。

3.3 Qtum：采用 POS 机制，非出块节点分享出块收益，延迟收益

POS 机制不存在算力竞争问题,挖矿的硬件门槛低,在某种程度上,有利于节点的加入,使节点能去中心化分布。Qtum 每个区块的出块奖励由 10 个矿工平分，其余奖励延迟 500 个区块，使攻击者无法预测区块奖励的多少，也无法立刻获得奖励，以此提高发动“垃圾合约”的成本。

Qtum 于 2017 年 9 月发布了主网，2019 年 1 月实现了 Qtum-BTC 原子交换，2019 年 10 月升级到 Qtum2.0，增加了隐私资产、通过智能合约实现离线 Staking 等特性。

3.4 达世币：通过仲裁链免疫 51%算力攻击

达世币（Dash）升级链锁（Chainlocks）以免疫于 51%算力攻击。基于 PoW 共识机制的区块链系统在整体算力较低且目前矿机算力逐渐集中在几家公司的情况下，很有可能遭遇 51%全网算力攻击而系统崩溃。而达世币 2018 年起提出了链锁概念并对其进行多次升级以完全免疫 51%算力攻击。

链锁主要基于长期主节点仲裁链，具体做法是基于“首次发现”规则进行网络范围的评估和投票。在每个块上，将从数百个主节点中选择长期主节点仲裁链，并且每个参与者将签署参与扩展活动区块链的第一个块。如果足够数量的参与者（例如 60%或更多）确认与第一块相同的块签名，则他们可以创建 P2P 消息并将其发布到网络。只有足够数量的仲裁链成员同意，P2P 信息才创建成功。即使 51%算力攻击成功，攻击者仍然无法执行深度重组，因为攻击者无法使先前的 P2P 消息无效，这可以证明原先的块是最长链。

4 应用：DApp 三足鼎立，DeFi 风险事件频发

DApp 即去中心化应用（Decentralized App），它直接运用区块链技术和智能合约，与交易数据、去中心化存储相关联。通过将应用前端界面和智能合约结合，确保信息无法被篡改，并与分布式数据库交互。

尚无面向个人的“杀手级”DApp 应用问世，ETH、EOS、TRON 在这方面较为领先。目前区块链应用仍处于起步阶段，各国政府机构和科技公司都在着力搭建区块链基础技术平台以促进自身业务效率提升。DApp 方面，金融 DApp 是 2019 年开发者的主要关注点，目前主要 DApp 都是基于以太坊构建的，因此以太坊 DApp 的活跃用户和 DApp 数量均为第一，在交易额和交易笔数方面，2019 年 EOS 处于领先地位，而 2020 年第一季度，以太坊则在总交易额上实现了 56.4 亿美元的规模，较去年同期增长 652%，超过了 EOS。

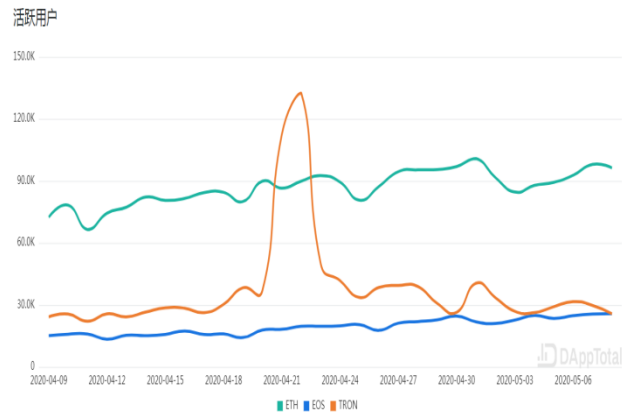
波场 TRON 和 EOS 的 DApp 生态稳定全球前三并不断提升用户体验。波场 TRON 深耕娱乐型 DApp，2019 年活跃用户数量和 DApp 数量均有显著上升。而 EOS 通过上线 REX 资源交易所，使得 EOS 交易门槛大幅降低。而在经历了 EIDOS 项目火爆所导致的网络堵塞后，EOS 也做出了一系列创新性的举措如升级主网至 v1.8 来提升用户使用体验。

图表 17：2019 年基于以太坊构建的 DApp 数量

	基于以太坊构建的 DApp 数量	代表 DApp
排名前 50 的金融 DApp	42	MakerDAO、OmiseGO
排名前 50 的交易所 DApp	44	Augur、Uniswap
排名前 50 的安全类 DApp	42	Quantstamp
排名前 50 的开发 DApp	43	Kauri、Golem、CrytoZombies
开发活动最多的前 50 DApp	44	-

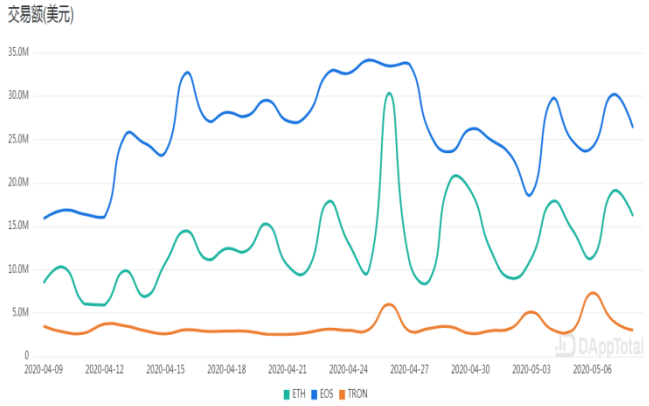
资料来源：陀螺财经，国盛证券研究所（注：排名基于"活跃用户、tx 容量、开发活动、配置文件及时度、CTR 和用户建议等多个因素"）

图表 18：2020.4.9-2020.5.8 各公链 DApp 活跃用户数量（单位：千）



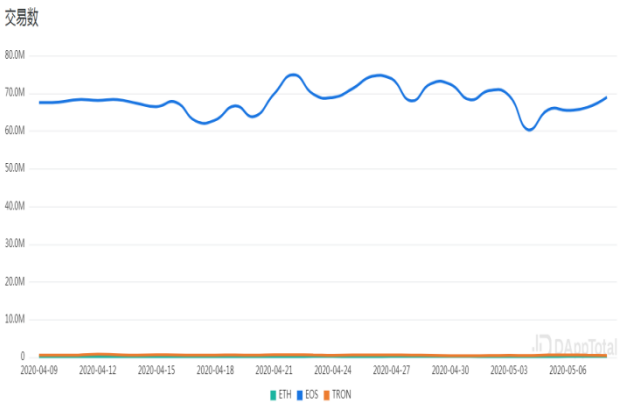
资料来源：DAppTotal，国盛证券研究所

图表 19：2020.4.9-2020.5.8 各公链 DApp 交易额（单位：百万美元）



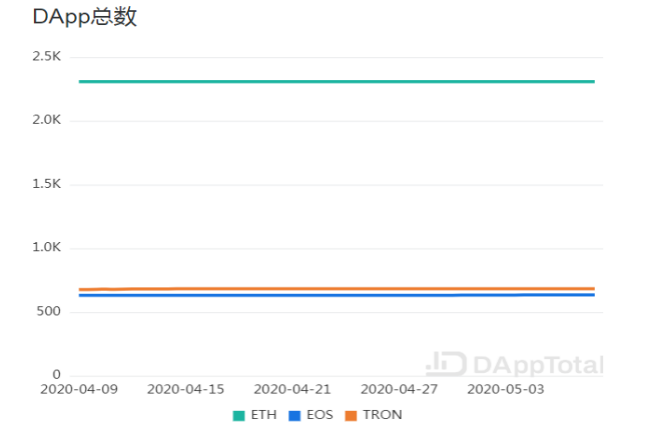
资料来源：DAppTotal，国盛证券研究所

图表 20：2020.4.9-2020.5.8 各公链 DApp 交易笔数（单位：百万美元）



资料来源：DAppTotal，国盛证券研究所

图表 21：2020.4.9-2020.5.8 各公链 DApp 数量（单位：千）



资料来源：DAppTotal，国盛证券研究所

4.1 波场：DApp 活跃用户和交易量等增长快速

波场币 DApp 增量最多、增速最快。2019 年，波场 TRON 在 DApp 生态方面稳居全球公链前三的位置，还在 DApp 活跃用户数和交易量等指标上都实现了对以太坊的反超（目前有所下滑），根据 DAppReview 发布的 2019 年 DApp 数据，网络上的 DApp 总数已高达 663 个（截至 2020 年 5 月 1 日，已有 683 个），活跃用户高达 98.93 万； TRON 过去一年总交易额高达 44 亿美元（2020 年第一季度为 4.15 亿美元），交易笔数超过 4 亿。而 DAppReview 发布的 2020 年一季度市场报告也显示，TRON 新增 DApp66 个，远超以太坊和 EOS。

图表 22：2019 年波场 TRON 技术发展历程

时间	事件
2019.3	波场宣布发行基于 TRC20 的稳定币 USDT(TRC20-USDT)。随后包括 OKEx、火币、币安在内的多家交易所相继宣布支持。后经历短短几个月，TRC20-USDT 总量就突破了八亿美金，一跃成为全球第三大稳定币，目前几乎占稳定币总供应量的 22%。
2019.8	波场正式发布 Sun Network 网络，通过链下扩容提升现有 TRON 公链的可用性。Sun Network 中的智能合约应用侧链、跨链通讯等技术，进一步扩大了波场网络的整体容量，提升波场整体的 TPS 以及智能合约执行效率。
2019.10	波场 TRON 与三星达成国际合作，并与三星区块链的密钥库(Samsung Blockchain Keystore)完成整合，三星开始支持 TRC10 与 TRC20 标准，波场也成为了三星支持的唯一一家“国产”区块链。
2019.12	基于区块链的内容直播平台 DLive 即将加入 BitTorrent 生态系统，并开始迁移至波场区块链。
2020.4	基于波场 TRON 的稳定币借贷平台 JUST 正式上线。依靠 TRON 网络强大的资源和社区能量，JUST 运行稳健，而这也是在 TRON 波场上运行的第一个 DeFi 项目。

资料来源：创氪网，国盛证券研究所

4.2 EOS：项目方代付 CPU，使用门槛大幅降低

EOS 向合规迈出重大一步，新用户使用门槛大幅降低。2019 年 5 月 2 日，REX（EOS 资源交易所）的上线意味着 EOS 拥有了一个系统级的资源租赁平台，CPU 的租赁也更为便利。另外 Dapp 项目方开始为用户代付 CPU，用户可以不消耗资源畅玩 Dapp，这些举措都大大降低了新用户的使用门槛，促进 EOS 网络下的 DApp 快速发展，交易额和交易数量世界领先。

图表 23：2019 年 EOS 技术发展历程

时间	简介	事件
2019.2.27	启动 DAPP 网络	通过将 DAPP 通证分发到此类服务包中，DApp 开发人员可以访问额外的存储容量、安全的通信服务和其他关键实用程序。
2019.5.2	REX（EOS 资源交易所）上线	REX 为用户和开发人员提供平台，使其可以租用 CPU/NET 资源供个人和企业使用，这使得在 EOS 区块链上构建和部署 DApp 更加便宜。
2019.5.31	EOS 在 Coinbase 上市	EOS 还被纳入 Coinbase 盈利计划，用户可以通过了解 EOS 的工作原理来赚取 EOS 通证。
2019.9.18	EOS 主网升级至 v1.8	此版本使 DApp 开发人员可以代替其用户支付网络资源，以确保流畅的用户体验，并简化新用户的进入过程。
2019.11.1	EIDOS 在 EOS 发行	EIDOS 是一个“空气币”项目。用户可以将任意金额的 EOS 币转账至 eidosonecoin 这个账户，智能合约会将等量的 EOS 返还至用户账户，并将 eidosonecoin 这个账户中存有的 0.01%EIDOS 作为空投奖励发送到用户账户。EIDOS 导致 EOS 出现了海量的交易和流通，占用了大量 CPU 资源导致 EOS 网络出现严重堵塞。
2019.10.2	与 SEC 和解	SEC 批准了 Block.One 的 EOS ERC-20 代币 ICO 豁免请求。有了这项豁免，现在可以确定 EOS 不是证券，而 Block.One 只需要支付 2400 万美元的罚款。

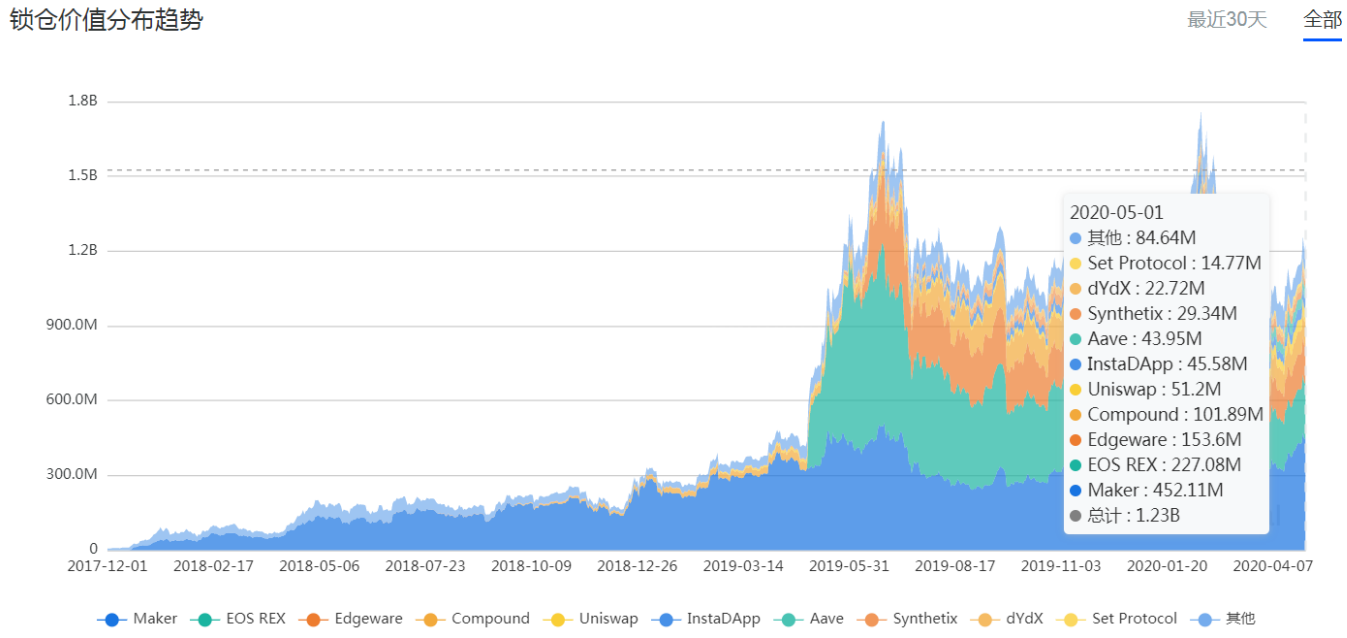
资料来源：区块链网络、玩币族，国盛证券研究所

4.3 DeFi：并非无本之水，安全性受制于底层平台

DeFi 意为 Decentralized Finance（去中心化金融），主要指去中心化借贷，即数字货币用户可以将持有的数字货币抵押给 DeFi 平台，获得利息，也可向 DeFi 平台借款，是近年来链上应用为数不多的亮点之一。

DeFi 锁仓规模约为 12.3 亿美元，竞争格局集中。其中，被锁仓的 ETH 个数约为 354 万个，占其供应量的 3.2%；被锁仓的 EOS 个数约为 8261 万个，占其供应量的 8.11%；在锁仓市场，Maker 锁仓规模约为 4.5 亿美元，市占比最高，约为 37%；EOS REX 次之，约为 2.3 美元，市占比约为 19%；Edgeware 约为 1.5 亿美元，市占比约为 13%，其他平台约为 3.9 亿美元，市占比约为 32%。

图表 24：被 DeFi 平台锁仓的加密货币价值约为 12.3 亿美元（M 为百万美元，B 为十亿美元，2020.5.1）



资料来源：Dapptotal，国盛证券研究所

DeFi 风险事件频发，受底层平台制约大。2020 年以来 DeFi 平台 MakerDAO 与 Lendf.Me 遇到的安全事件受到了广泛关注，反映出 DeFi 作为区块链链上应用，受到底层技术平台在性能和安全性等问题上的若干制约，难以独善其身，也反映出作为金融服务对风险控制这一生命线的掉以轻心。DeFi 不是无根之水、无本之源，其发展前景受到底层平台制约，也需引入更多金融人才，考虑更多极端情形，做好风控措施。

1）MakerDAO“黑色星期四”出现，有用户以 0 价格拍卖竞价，得到价值 833 万美元的 ETH。2020 年 3 月 12 日，以太坊拥堵，交易打包上链所需的 Gas 费飙高，此时 DeFi 平台竞拍者较少，部分竞拍者意识到这点后，利用了 MakerDAO 拍卖期短、单次拍卖的最大拍卖数量小（50ETH）等漏洞，免费拍到了高额 ETH。其后，MakerDAO 提高了单次拍卖的最大拍卖数量至 500ETH，并延长了拍卖期。这次风险事件反映出 MakerDAO 平台协议设置的不成熟和在底层技术平台方面以太坊本身固有的性能问题。

2) bZx 闪电贷事件。2020 年 2 月 18 日，恶意参与者操控 bZx 的经济模型，盗走了价值约 65 万美元的 ETH 。这已经是 bZx 平台一周之内第二次遭受攻击了。攻击者利用 DeFi 借贷协议 bZx 的“合约漏洞”，在一个以太坊区块时间内，充分利用 5 个 DeFi 产品互相的合约调用，在漏洞间操纵价格。

3）Lendf.Me 被盗 2500 万美元。2020 年 4 月 19 日，dForce 的去中心化借贷协议 Lendf.Me 遭遇黑客攻击，价值约 2500 万美元的数字货币被从合约中取出。此次黑客攻击主要是利用 Lendf.Me 和 ERC777 标准的兼容性漏洞进行了重入攻击，回调机制允许黑客反复将伪造的 ERC777 作为抵押物借出款项。在 dForce、星火矿池、慢雾、imToken、去中心化交易所 1inch 等机构与新加坡警方的合作下，4 月 21 日，黑客归还全部盗取的资产。尽管如此，Lendf.Me 合约状态已被污染，无法重启。这次事件反映中 DeFi 作为一种“乐高”式协议的组合，如果不能处理好各协议的兼容性问题，则其安全风险不容忽视。

5 投资建议

推荐关注有望受益于区块链技术持续发展的相关标的:
1）东港股份、易见股份、安妮股份等（区块链应用）;
2）央行数字货币：恒宝股份、新大陆等;
3）欧科集团、火币科技（数字资产交易相关）;
4）嘉楠科技（比特币矿机厂商）。

风险提示

区块链技术发展不达预期。当前区块链“去中心化、安全与效率不兼容”的“不可能三角”问题或长期无解。

区块链商业模式落地不达预期。例如，代币投资者对代币升值的预期和代币消费者对代币价格稳定的预期的矛盾或长期无解。

监管政策宽松度不达预期。公链商业模式的重要基础是代币，如果监管政策严格（例如将所有代币定性为证券），公链商业模式探索或将遇阻。

免责声明

国盛证券有限责任公司（以下简称"本公司"）具有中国证监会许可的证券投资咨询业务资格。本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告的信息均来源于本公司认为可信的公开资料，但本公司及其研究人员对该等信息的准确性及完整性不作任何保证。本报告中的资料、意见及预测仅反映本公司于发布本报告当日的判断，可能会随时调整。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司力求报告内容客观、公正，但本报告所载的资料、工具、意见、信息及推测只提供给客户作参考之用，不构成任何投资、法律、会计或税务的最终操作建议，本公司不就报告中的内容对最终操作建议做出任何担保。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素。

投资者应注意，在法律许可的情况下，本公司及其本公司的关联机构可能会持有本报告中涉及的公司所发行的证券并进行交易，也可能为这些公司正在提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。

分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的任何观点均精准地反映了我们对标的证券和发行人的个人看法，结论不受任何第三方的授意或影响。我们所得报酬的任何部分无论是在过去、现在及将来均不会与本报告中的具体投资建议或观点有直接或间接联系。

投资评级说明

投资建议的评级标准		评级	说明
评级标准为报告发布日后的 6 个月内公司股价（或行业指数）相对同期基准指数的相对市场表现。其中 A 股市场以沪深 300 指数为基准；新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以摩根士丹利中国指数为基准，美股市场以标普 500 指数或纳斯达克综合指数为基准。	股票评级	买入	相对同期基准指数涨幅在 15%以上
		增持	相对同期基准指数涨幅在 5%~15%之间
		持有	相对同期基准指数涨幅在-5%~+5%之间
		减持	相对同期基准指数跌幅在 5%以上
	行业评级	增持	相对同期基准指数涨幅在 10%以上
		中性	相对同期基准指数涨幅在-10%~+10%之间
		减持	相对同期基准指数跌幅在 10%以上

国盛证券研究所

北京
地址：北京市西城区平安里西大街 26 号楼 3 层
邮编：100032
传真：010-57671718
邮箱：gsresearch@gszq.com

上海
地址：上海市浦明路 868 号保利 One56　1 号楼 10 层
邮编：200120
电话：021-38934111
邮箱：gsresearch@gszq.com

南昌
地址：南昌市红谷滩新区凤凰中大道 1115 号北京银行大厦
邮编：330038
传真：0791-86281485
邮箱：gsresearch@gszq.com

深圳
地址：深圳市福田区福华三路 100 号鼎和大厦 24 楼
邮编：518033
邮箱：gsresearch@gszq.com