# 区块链的应用价值与发展趋势

作者：Gate.io 研究院 M.Esteban，Z.Zian，C.Jill

## 摘要

区块链技术起源于比特币，又因公链以太坊而被更加广泛地开发。所以探讨区块链应用的价值与未来发展离不开比特币本身技术与公链的发展情况，本报告将从这两点入手，从技术本身出发，以区块链应用的发展趋势为最终目的进行探索。本文主要采用取样调研的方式，去探讨区块链在区块协作、数据处理、安全与隐私、数据/资产非同质化四个方面上应用的发展趋势。

## 要点摘要

- 比特币去中心化、防篡改、可追溯、匿名和共享性等特点发展出现有区块链应用的格局，其账本和共识技术等特点又为早先的技术开发提供了蓝本，同时比特币技术上的缺陷也是后来区块链应用技术突破的关键，而闪电网络正是金融应用上较为突出的代表；
- 公链的格局是围绕着以太坊进行多元化发展，未来的发展将围绕去中心化、性能和安全性三方面的权衡而开展，而且存在对任意区块链和资产间互操作性的跨链技术的巨大需求；当下要成为优质的公链，一方面需要市场&运营，另一方面需要特色化的技术开发道路；
- 从比特币本身技术和公链的发展情况判断，目前区块链资金层面重点发展在 DeFi 和 NFT，技术应用最具价值和优先发展的四个方向在区块协作、数据处理、安全与隐私、数据/资产非同质化四个方面上；
- DeFi 和 NFT 遇到的主要瓶颈在于资产的使用效率低和交易费用高，在未来加密货币和区

块链价值共识的增强将提高相关生态的参与率和使用率，layer2 的技术改进将进一步降低交易成本，DeFi 项目中支付和资产上链具有更好的前景，NFT 在短期价格泡沫后的资产价值发现回归理性；

- 区块链应用在区块协作上，将跨域协作的概念延升到行业的可重构开放式商业模式，未来经济发展的核心将可能从“资本”转移到“资本+数据”的模式；
- 传统企业将更多地应用区块链数据处理，其他发展将主要在泛金融应用和产业供应链两个领域，前者发展的关键在性能高 TPS 和跨链交互上，后者发展的关键在数据处理的及时与高效性上；
- 对比现今区块链隐私所受威胁和保护机制，区块链应用在安全性上的发展一方面可以结合其他行业技术比如人工智能，另一方面可以将需求性能和安全性的链或者项目分开处理；
- 从现有资产/数据非同质化的应用上来看，价值锚定机制还需完善，通证资产实际价值将会落地并缩小地域间的价值差异；
- DeFi 和 NFT 的成功源自传统资本运作的延续与创新，技术应用的发展源自市场对技术突破当下存在较大需求，虽然存在一定的限制条件，但是区块链应用未来具备广袤的发展空间。

# 目录

# 1 比特币价值

2008 年 11 月 1 日，一个自称中本聪（Satoshi Nakamoto）的人在 P2P Foundation 网站上发布了《比特币：一种点对点的电子现金系统》，提出了一种全新的“去中心化”的电子现金支付系统，力图摆脱当下“中心化”的种种掣肘。比特币发展至今十余年，参与者从最开始的少数特定技术群体，到资本方的陆续登场，再到广泛普通投资者的热情涌入，加密货币共识在全球范围内显著提高。加密货币从“技术链圈”拓展到“货币币圈”，币圈的繁荣又反过来刺激链圈的技术突破，资金与技术不分家的格局成为当下加密货币的投资与价值逻辑。

## 1.1 比特币及区块链的价值特点

比特币作为一种新型货币系统，本质上是一个共享的分布式账本，其“新”主要在于发现了区块链技术。区块链技术为比特币的诸多特性赋能，其价值特点主要体现在：

- 去中心化（去信任）→ 避免中心化风险。去中心化是比特币的安全和自由的保证，比特币不通过中心化机构发行，而是由全网旷工的共同记账来自证其信。也就是说，比特币网络中的每笔交易不存在任何中介机构，所有的交易都是交易人直接发生，按照交易时间被记录在交易人的客户终端，从而避免中介交易风险（中心化风险），真正实现“点到点”。
- 开放性→ 广泛参与维护稳定。这是针对区块链公有链而言的，任何人都可成为网络体系中的节点，可以参与区块链的交易与记账。通过广泛的网络节点参与，以社区共同治理的模式来维护区块链网络的稳定性。
- 防篡改性和可追溯性→ 保证信息真实一致性和安全性。区块的数据由特定算法按照时间

顺序进行上链，时间的不可逆性和不可更改性使得区块链数据也不可随意篡改。要更改区块链中的信息存在很大的成本和难度，一般而言需要达到网络中 51%的算力才能更改数据，这一点在现实中很难做到。同时，哈希指针的应用使得区块链信息具有唯一标识性，在验证和追溯查询区块数据上具有很强的实用性。

- 匿名性→ 保护所有者的信息安全。匿名性是基于算法实现是通过地址来寻址，而非个人身份。不用提供任何个人身份信息即可发送和接受比特币。
- 共享性与透明性→ 个体不产生群体影响 。网络中各个节点都可看到区块链上所有的交易信息，共享数据账本。这就意味着当某个区块数据出现问题时，并不会导致链上所有的交易信息和数字资产遭到负面影响。

就比特币作为一种货币工具而言，其区别于传统货币的特点有：

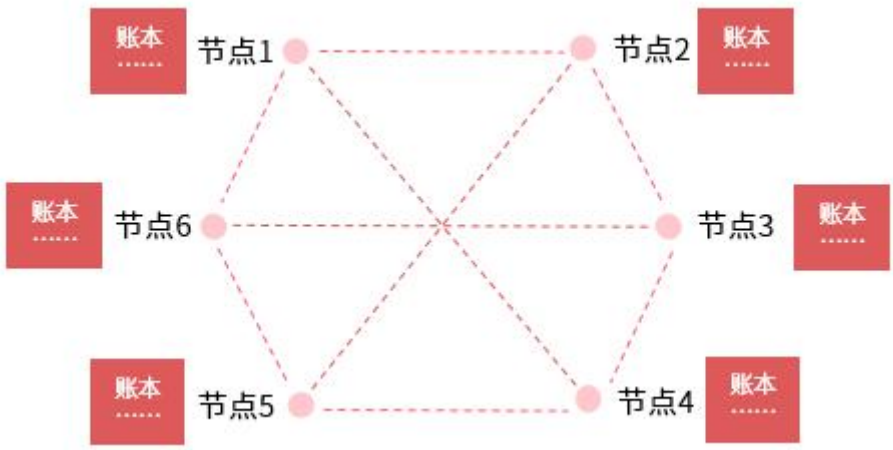
- 稀缺性→ 遏制通货膨胀增强货币信心。比特币是一种通缩性货币，总数恒定在 2100 万枚，通过调节难度系数来维系发行的稳定性。比特币平均每十分钟出一个数据区块，初始矿工奖励每个新区块 50 个比特币，之后每四年减半，预计 2140 年发行完毕。
- 转账成本低→ 增强流动性。用比特币转账，通常只需要支付较低的费用，转账手续费自由设定，而无中介或中心化机构进行中间的交易撮合，支付较昂贵的费用。
- 全球流通便捷→ 打破跨境流通障碍。在任何国家，任何接入互联网的智能终端都可进行比特币的转账和交易，减少受到各国政策监管的跨境资金管制。

## 1.2 比特币的基础技术

### 1.2.1 区块链技术——去中心化

**分布式账本**

区块链的本质是分布式账本，即多个节点分布在不同的地理位置或多个机构组成的网络里进行数据信息分享的资产数据库。在网络中并不存在中心节点，网络通过某种机制生成唯一真实的账本，每个节点都可拥有网络的唯一真实的账本的副本。当网络中发生交易，唯一真实账本也发生改动，各个节点的账本副本也几乎同步更新。



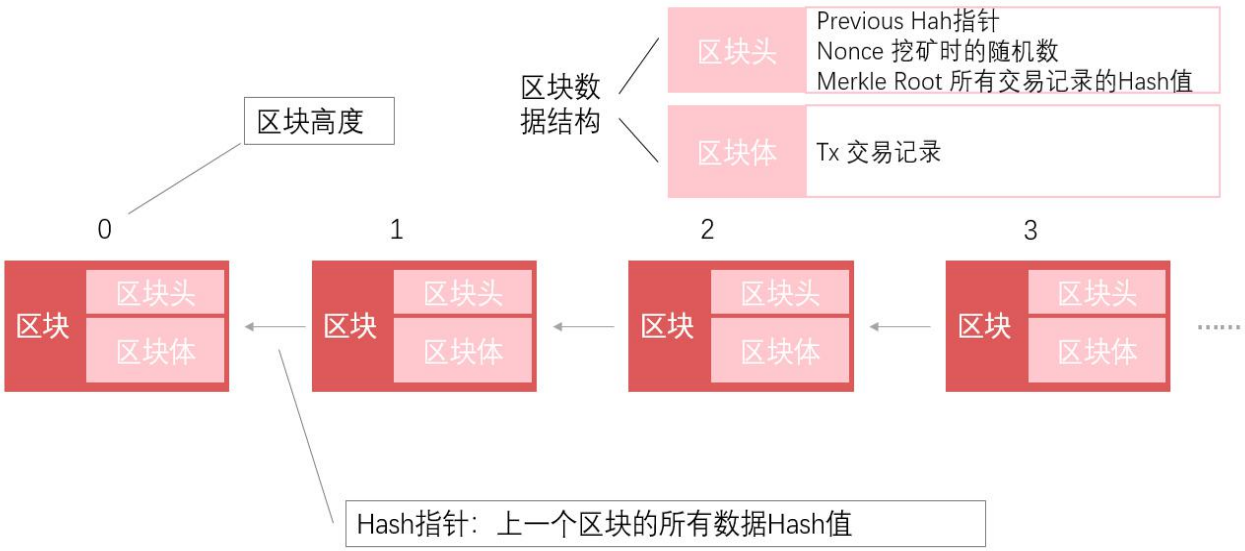

*图片：Gate.io 研究院*

**区块链机制**

在网络发生交易之后，记账传导过程为：交易——全网广播——全民记账——共识机制——单笔记账权。这样的过程周而复始进行下去，一条条的交易记录便生成了上述的分布式账本，账本在区块链上的存储形式叫做区块，将区块连起来便是区块链。这一过程中并没有出现中心化机构的身影，所有的交易和资产信息更新在激励机制下由广泛的节点或矿工抢夺记账权而进行，

在链上将信息同步。

从字面上理解，区块链是一个记录数据的链式结构，在链上包含许多区块，区块上的数字代表区块高度，中间通过 Hash 指针（后文会讲述 Hash 算法）进行连接和指向，即子区块存储其父区块所有数据的 Hash 值，每个区块通过 Hash 指针对链上数据进行唯一串联绑定。




*图片：Gate.io 研究院*

### 1.2.2 哈希算法与 Merkle 二叉树——不可篡改性与可溯源性

哈希算法，又称散列算法，是指将任何长度的数据提炼出固定长度数字的方法。在哈希算法中有一个输入和输出，输入时任意长度的数据，在算法内部不管输入的数据是何种形式，都以单纯的比特序列来处理，其实就是一串由 0 和 1 组成的二进制数。哈希算法具有不可逆性和无冲突性，输入值和输出值没有规律，只有完全一样的输入值才有同样的输出值，但不能通过输出值来计算输入值。

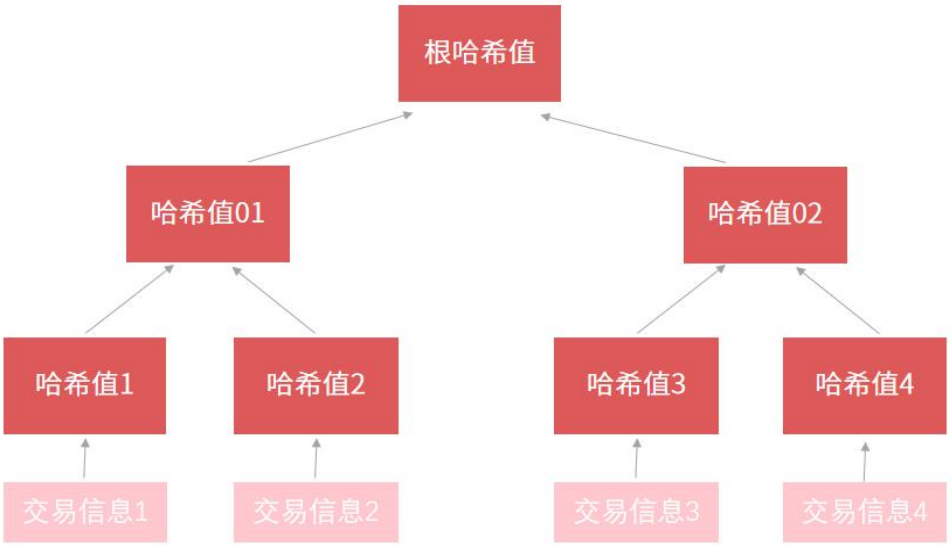
哈希算法在区块链中指的是计算区块的哈希值，通过生成区块头部的随机数来调整每次哈希的结果，使得计算出来的哈希值符合一个特定的标准。简而言之，哈希算法在区块链的应用如下：

**数据加密**

- 识别区块数据是否被篡改。对区块头进行哈希得到的哈希值可唯一确定某一个区块，可理解为身份证号。任意节点通过简单哈希计算可获得该哈希值，哈希值匹配则数据被未篡改。
- 将区块串联成区块链。区块与区块之间正是通过哈希值这一身份证号进行串联，从而形成一个链式结构的区块链。

**追溯地址**

- 通过 Merkle 二叉树快速定位每笔交易。在区块头中有个 Merkle Root 的哈希值，Merkle 实际上就是一个二叉树的数据结构，一分二、二分四、四分八等一直分下去就叫做二叉树，最上面的节点就是根。区块链的根数据由每笔交易的哈希值得出后，两两哈希再持续哈希，直到最顶层的根哈希值。通过这样的二叉树结构可以快读定位目标交易地址。
- 检验数据是否被篡改。二叉树中的任一哈希值有任何的变动都会导致 Merkle Root 的变化，若有错误发生，可快读找到错误出处。




*图片：Gate.io 研究院*

### 1.2.3 工作量证明机制

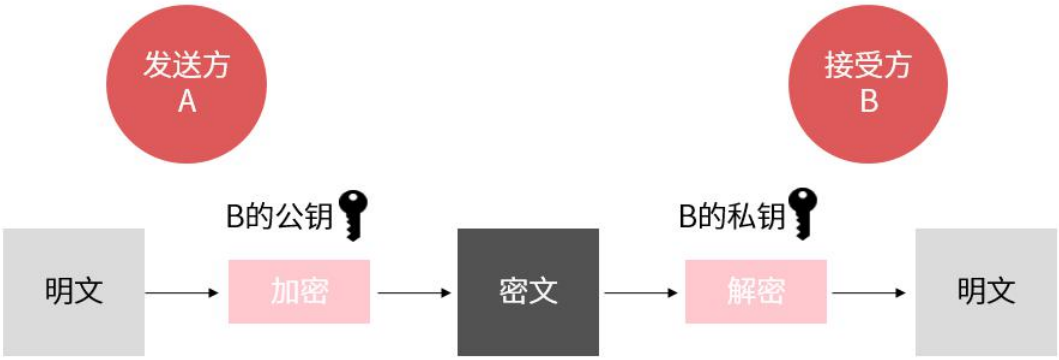
在比特币的设计当中，比特币的出块机制就是工作量证明机制。挖矿实质上指的是矿工们在解决哈希谜题，也就是算力的比拼，出块数量比例反映矿工在全网的算力比例。矿工的工作主要涉及两方面，通过不断重复两个步骤进行穷举运算，直到找到哈希指针值：

- 修改随机数 Nouce。块头部或币基交易中各有一个随机数，一般先更改头部随机数，在更改一圈之后仍未找到特定标准的哈希值则修改币基交易的随机数，这会引发 Merkle 数的重新生成并改变顶层的 Merkle Root
- 计算哈希值。将 Merkle Root 作为输入值通过哈希算法生成哈希值，并确认是否符合特定标准。

### 1.2.4 非对称加密技术——信息安全

在密码学领域有两个主要概念：对称加密算法和非对称加密算法，区别在于前者在加密和解密时使用的是同一个密钥，而后者需要两个密钥，即公开密钥（公钥）和私有秘钥（私钥），公钥和私钥成对存在，区块链采用的正是后者。通过私钥经过一系列算法是可以推导出公钥的，即公钥是基于私钥而存在的。但是无法通过公钥反向推倒出私钥，这个过程的单向的。

非对称加密及解密过程可简化如下：假设 A 向 B 发送信息。B 将自己的公钥告诉 A，A 通过 B 的公钥对明文进行加密并发送，B 接收密文后用自己的私钥解密，获取原文信息。在这一过程中，即使 B 的公钥泄露也不会导致信息泄露，因为只有 B 自己掌管的私钥才能解密。同样，当 B 向 A 发送消息，B 通过 A 的公钥加密，A 通过自己的私钥解密。




*图片：Gate.io 研究院*

## 1.3 比特币技术缺陷与闪电网络

### 1.3.1 比特币技术缺陷

比特币在货币创新与区块链应用等方面都有惊人的创新亮点，但在技术层面，其背后的共识机制 POW 存在一些令人质疑的不足之处：

- 耗能大，资源浪费。挖矿出块的过程是矿工们在不断计算哈希值，算力的比拼需要大量的矿机和电力投入。这一缺点在比特币之后的一些加密货币的共识机制创新得以解决，如 POS 机制。
- 区块交易效率低。全网进行算力竞赛和记账权争夺，同时全网节点要验证区块并达成一致，这使得系统运行的速度受限。比特币每秒交易次数低于 7 次，成功记账时间间隔为 10 分钟，这与当今动辄每秒上万的金融交易难以比较。要解决这一交易速度和可拓展性问题，layer2 的概念逐步兴起，比特币领域的闪电网络便是最受关注的一项扩容方案。

### 1.3.2 闪电网络

闪电网络（Lightning Network）是在比特币区块链上的第二层支付协议，其目的是实现交易双方的即时交易，同时最大限度的保证个人的隐私。该技术允许两个节点在链上锁定一笔资产开启一个支付通道，在锁定价值之内双方在链下进行快速的即时确认的交易。闪电网络是基于微支付通道演进而来，创造性提出两种类型的交易合约：

- 序列到期可撤销合约 RSMC（Recoverable Sequence Maturity Contract），主要解决通道中币单向流动问题，即链下交易的确认问题。

- 哈希时间锁定合约 HTLC（Hashed Timelock Contract），主要解决币跨节点传递的问题，即支付通道的问题。

在整个交易中，智能合约起到中介的作用，区块链则是确保最终的交易结果被确认。

**RSMC 的实现机制**

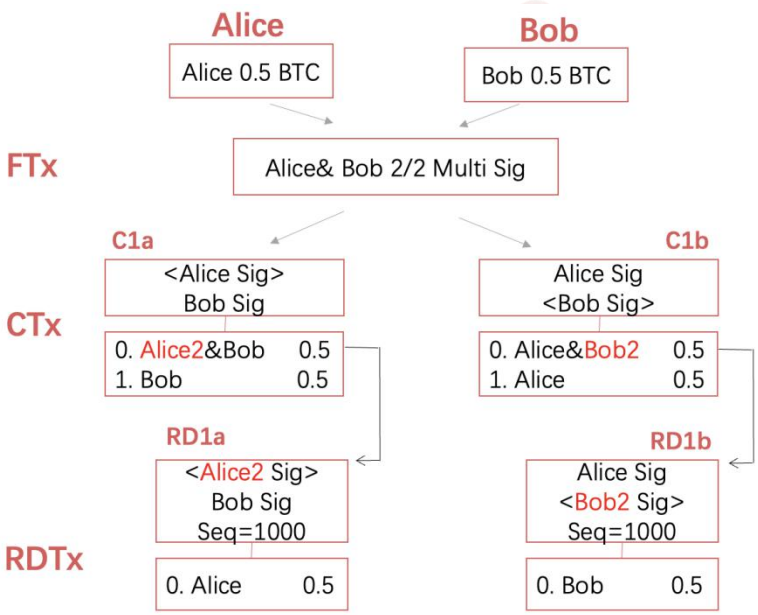
假设 Alice 和 Bob 是交易双方，比特币交易往来较频繁，于是两人设想构建链下的支付通道以避免链上的拥堵。链下进行交易，链上进行资产余额的更新。

A、 **初始创建：**创建抵押交易 FTX（Funding Transaction） 承诺交易 CTx（Commitment Transaction）和可撤回交易 RDTx（Recoverable Delivery Transaction） 互换 CTx 和 RDTx 签名 互换 FTx 签名 广播上链。其中，FTx 为共同可见，CTx 和 RDTx 为个人持有。

- Alice 和 Bob 各自拿出 0.5BTC，构建 FTx，输出为两人的 2/2 多重签名，此时 FTx 未签名也未广播。
- Alice 构造 CTx：C1a，并交给 Bob 签名。C1a 第一个输出是 Alice 的另一把私钥 Alice2 与 Bob 的 2/2 多重签名，第二个输出是 Bob 0.5BTC。
- Alice 构造 RDTx：RD1a，并交给 Bob 签名。RD1a 是 C1a 第一个输出的交易结果，输出为 Alice 0.5BTC，但此合约带有 Sequence，即带有一定区块数量的延时，矿工会判定这笔交易与其指向的交易存在区块间隔，只有在特定数量个区块（假设 1000）之后才会认为是合法的。
- 同理，Bob 构造 CTx：C1b 和 RDTx：RD1b，并交给 Alice 签名，结构上与 Alice 的两个交易合约对称。

- 双方将构造的 2*2 个合约互换并签名之后，由于此时未对 FTx 签名，任何一方均无动机作恶，任何一方不会有任何损失。
- 双方对 FTx 互换并签名，此时将 FTx 广播。

**安全机制：单方广播交易终止合约的一方会延迟到账，另一方可立即到账。**由于 C1a 和 C1b 是来自同一个输出的对称关系，所以两者只需一个广播出块。若 Alice 广播 C1a，则 Bob 可立即获得 0.5BTC（C1a 第二个输出），Alice 需等待 1000 个区块确认后才能拿到 0.5BTC（RD1a 的输出）。同理，若 Bob 广播 C1b，则 Alice 可立即获得 0.5BTC，Bob 需要等 1000 个区块确认后才能拿到 0.5BTC。



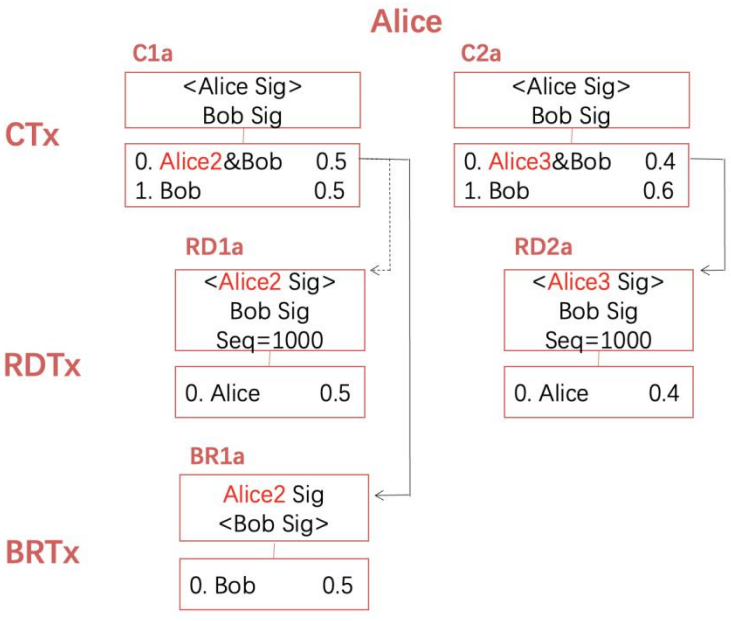

*图片：Gate.io 研究院*

**B、交易更新：**假设 Alice 想转 0.1BTC 给 Bob，创建新 CTx 和 RDTx 交出私钥、作废旧 CTx 和 RDTx、构造违约补救合约 BDTx（Breach Remedy Transaction）。

- Alice 和 Bob 根据交易后的新余额进行调整，分别构造新的 CTx：C2a 和 C2b，RDTx：RD2a 和 RD2b，过程与上面类似。


*图片：Gate.io 研究院*

- 提交私钥给对方，对方可构造 BRTx。如 Alice 将 Alice2 的私钥交给 Bob,表示 Alice 放弃 C1a，承认 C2a。Bob 得到 Alice2 签名后修改 RD1a 的输出给自己，形成 BR1a。




*图片：Gate.io 研究院*

**安全机制：特定数量区块确认时间内可对违约一方进行没收全部代币惩罚。**若 Alice 想违约，在 C2a 存在的情况下依然广播 C1a，则系统将惩罚没收其全部的抵押代币。Alice 交出 Alice2 的私钥或者对 BR1a 进行签名，两者效力等同，都是对 C1a 的放弃。同理，Bob 交出 Bob2 私钥便放弃 C1b，承认 C2b。此时 Sequence 的作用提供实施惩罚的窗口期，阻止后续交易进块（RD1a）。当发现对方毁约时，便有 1000 个区块确认的时间实施惩罚，即广播 BR1a 代替 RD1a。若错过 1000 个区块确认时间，则无法实施惩罚。

**HTLC 的实现机制**

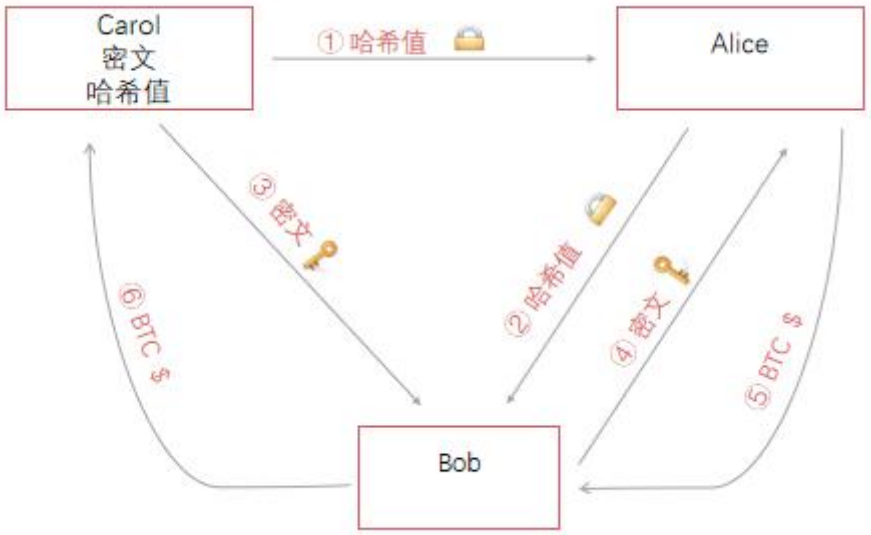
HTLC（Hashed Timelock Contract）哈希时间锁定合约，是在当双方没有直接的微支付通道时，通过第三方的通道介入来进行交易与支付。如果说 RSMC 属于无条件的微支付渠道，那 HTLC 则是带条件的资金支付方式，这个条件便是哈希值。在 HTLC 中，支付的前提是收款方需要提供一个字符串，该字符串满足哈希值等于 HTLC 的哈希值，这里利用了哈希函数的不可逆性，匹配的哈希值也即意味着收款方得到了付款方的授权。

假设 Alice 想向 Carol 转账 1 个 BTC，引入 Bob 作为中介通道，其实现过程如下：

- Carol（收款方）选择一个随机密文并得到哈希值，并将其交给 Alice（付款方）。（哈希值可理解为锁，密文便是钥匙）
- Alice 收到哈希值后，构建与 Bob（路由节点）的交易通道，这笔交易需要 Bob 拿到 Carol 的密文才能解锁，若 Bob 未在限定的时间里解锁成功，则资金退回 Alice。
- Bob 从 Alice 拿到哈希值后，构建与 Carol 的交易通道，Carol 需拿密文来解锁。
- Carol 提供密文从 Bob 获得 1 个 BTC，Bob 拿密文从 Alice 获得 1 个 BTC，这就完成了从

Alice 到 Carol 的转账交易。

在实际交易中，有两点需要注意：1、Alice 给 Bob 的转账金额需要大于 1 个 BTC，多出的部分以作为奖励 B 作为路由节点的费用。2、交易之间的哈希时间长度限制，第二步时间必须长于第三步，否则 Bob 在 Alice 关闭交易之后拿到 Carol 的密文，Bob 则无法向 Alice 拿回 1 个 BTC。




图片：Gate.io 研究院

综上所述，闪电网络通过 RSMC 和 HTML 两个合约搭建了 BTC 交易和支付的微通道，通过链下处理交易，链上公布交易结果的方式，极大缓解了比特币链上的交易拥堵情况。正是由于存在链上拥堵问题和闪电网络的扩容先行方案，激励了后续的像以太坊等公链项目积极追求更高的网络交易处理效率，在 layer2 寻求种种突破。

### 1.4 小结

比特币诞生的同时催生了区块链这一具有革命意义的新型技术，区块链的分布式思维和去中心化思想逐渐渗透，激励了越来越多诸如以太坊、ADA 等优秀公链的诞生，后来的公链也对 BTC 的 POW 工作机制提出质疑和许多优化方案，如 POS 和 DPOS 等。比特币的货币属性让人们对于新兴货币或加密货币有了更多的思考，其去信任的支付特点为传统金融机构提供了更高效、更低成本的技术考量，同时闪电网络的提出初步解决网络支付拥堵的情况，带动了 layer2 扩容方案的发展，为区块链技术的实际应用减少阻碍。

## 2 特色公链的发展

目前区块链公链市场已形成明显的格局，以太坊占据着最主要的市场，其次便是 BSC、ADA 和 DOT 等主流公链凭借着商业运作或者创新技术形成了一定的市场分流，新进公链项目比如 SOL 不凭借着巨大的资本运作已难以进入该市场。以太坊当下的发展很清晰，在通过硬分叉升级之后，扩容是最主要的发展方向。所以为了探究公链未来的发展趋势，本报告主要从拥有特色技术的其他主流公链出发，通过调研其商业模式、独立技术和企业愿景等方向，最终结合以太坊和其他特色技术去说明可能的发展趋势。

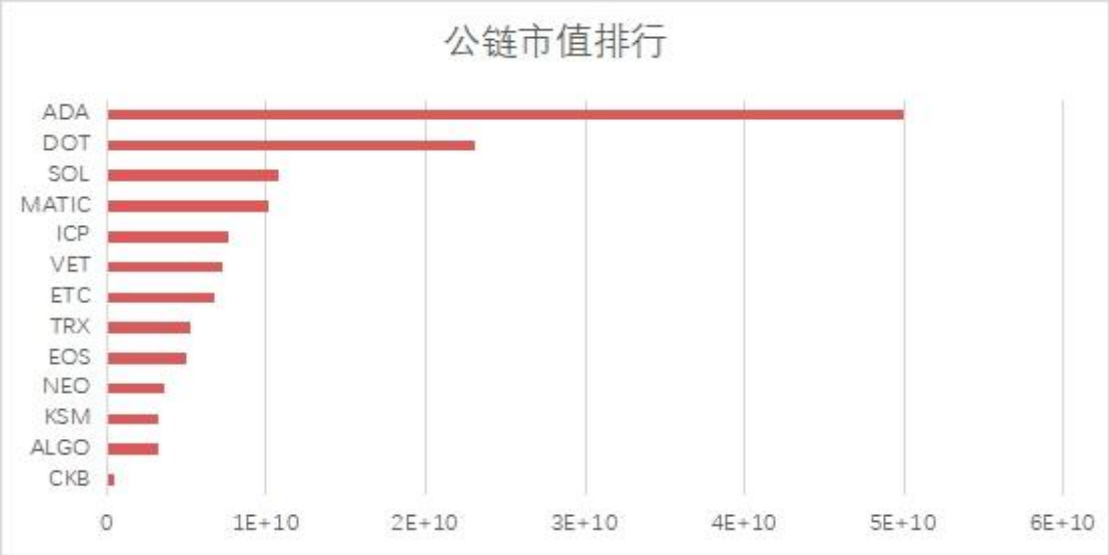
### 2.1 各主流特色公链产业现状（以太坊除外）

本部分取样调研部分独具特色的公链项目，包括 ADA、DOT、SOL、MATIC、ICP、ALGO 和

GateChain，去分析其资金实力、产业模式、技术特色和发展情况等方面。

**资金实力**

公链除以太坊以外，ADA 和 DOT 的市值远超其他项目。而这其中，ADA、SOL 和 ICP 等新进项目后来居上。所以在二级市场上，新进项目依然有通过资本的运作抢夺一定市场的机会。




*来源：coinmarketcap，图片：Gate.io 研究院*

据烯牛数据不完全统计，市场上主流公链项目多从 17 年开始发展，其中 SOL 和 ICP 具有公开数据上最多金额的融资，前期技术开发和市场抢占具有最充足的资本。ADA 在这之中属于较早期项目，ALGO 同期获得同级别融资，但是前者能够超越 EOS 等老牌公链抢占公链市场，后者却在市值上与 DOT 的测试网 KSM 属于一个级别。

| 项目 | 市值排名 | 融资金额 | 融资机构 | 时间 |
|---|---|---|---|---|
| ADA | 5 | 超 6222 万美元 | 未披露 | 2015-2018 |
| DOT | 8 | 超 1.4 亿美元 | Chain Capital，IOSG Ventures 等 | 2017-2020 |

| | | | | |
|---|---|---|---|---|
| SOL | 14 | 超 3.96 亿美元 | OKEX、MXC 等 | 2018-2021 |
| MATIC | 15 | 未知 | 未披露 | |
| ICP | 18 | 超 4.67 亿美元 | Polychain，Village Global 等 | 2017-2018 |
| ALGO | 30 | 超 2.36 亿美元 | Algo Capital，USV 等 | 2018-2019 |

*来源：烯牛数据，图片：Gate.io 研究院*

**产业模式**

产业模式通过调研项目团队构成大致可以分为两种：偏市场和运营、偏技术。

首先，通过 ADA 和 DOT 在其经济模式（加密货币交易/市值）上的运营结果来看，重视市场运营的项目往往在二级市场能收获更高的“股价”。而这两个项目主要的团队人员配置在社区的经营上，其中 ADA 尤其重视社区运营，社区大使总计 55 人，人员分工明确，横跨大约 16 个国家，是其团队的一个重要组成部分。

| 项目 | 团队构成 | 产业模式 | 产业运营特点 |
|---|---|---|---|
| ADA | 市场&运营 61%，技术 39% | 偏市场&运营 | 重点运营社区 |
| DOT | 市场&运营 57%，技术 43% | 偏市场&运营 | 重点运营社区 |
| SOL | 市场&运营 25%，技术 75% | 偏技术 | 偏技术开发 |
| MATIC | 市场&运营 40%，技术 60% | 偏技术 | 偏产品开发 |
| ICP | 市场&运营 33%，技术 66% | 偏技术 | 偏技术开发 |
| ALGO | 市场&运营 29%，技术 71% | 偏技术 | 偏技术开发 |

*来源：Linkedin，各公链官网，图片：Gate.io 研究院*

最后，SOL 和 ICP 作为后来居上的公链项目，产业模式同样偏技术却赢得公链的优势，除了资本的运作，很可能是其技术上的创新十分的迎合当下的价值投资，因此而吸引众多的投资者。

**技术特色**

主流公链项目都以以太坊为模板，除了解决以太坊高额的 GAS 费外，现阶段的技术创新点集中在对去中心化、性能和安全性三个方面的权衡（具体公链技术产品介绍见附录）：

去中心化：DOT 创新 NPOS 共识机制，减少寡头效应，从较小的集合中选择验证人，从而使较小的持有者可以提名验证人来运行基础结构，同时仍然可以获得系统的收益，而无需运行自己的节点；ICP 的阈值签名接力（Threshold Relay Technology）可以在任何一个能建立「虚拟计算机」的安全抗攻击网络中，让大量客户端节点共同协作，并使用加密技术来创建随机性，按照几乎不可摧毁、不可操纵、不可预测的方式，按需选择相应的网络参与者，去中心化的同时提高安全性。

性能：ADA 的 Ouroboros 权益证明共识机制和递归网络架构（Recursive InterNetwork Architecture，RINA）可节约大量计算资源和解决网络带宽问题；SOL 的时间证明共识机制（POH）、Gulf Stream、sealevel 和 Pipelining 等技术提高处理交易的效率的同时，构建横向扩展，可将 TPS 提升到 5 万；MATIC 可将以高达 65000 的 TPS 处理交易；ALGO 的 ASA、原子交易和无状态合约与有状态智能合约等技术更是满足金融的高交易需求，并同时实现一些产品所需特性；而这其中，ADA 和 ICP 的相关架构在理论上更是可以实现无限扩容。

安全性：GateChain 的保险账户（Vault Account）具备转账可撤回、私钥可恢复等功能重要安全性功能，为个人、企业和银行业提供全新的资产安全解决方案；MATIC 的 Polygon chain 可以通过牺牲部分独立性和灵活性提供高水平的安全性；ICP 的神经网络系统（NNS）可以完全控制网络的各个方面，包括面对黑客攻击让所有方恢复正常等。

| | ADA | DOT | SOL | MATIC | ICP | ALGO | GateChain |
|---|---|---|---|---|---|---|---|
| 技术特色 | 不依赖比特币和其他加密货币系统的技术基础，从扩容出发，解决规模化通信障碍，打造大规模的 DAPP 首选平台 | 打造更底层的区块链基础架构，做“链生态”，可将已有的链和其生态纳入自己的网络，包括以太坊 | 打造单一区块链，解决项目之前可组合性的问题，更适用于急需扩展性的项目 | 以太坊扩容方案之一，拥有四层技术，开发者可以自由组合，并最终接入以太坊。 | 将人工智能与区块链技术结合，重点提升区块链性能和安全性，并有望利用区块链技术重构互联网垄断、重构 IT 系统并大幅削减成本。 | 专注打造金融平台，做金融资产和金融产品的专用公链 | 利用 EVM 模块实现无成本以太坊产品迁移，拥有全新的多功能和高安全性账户 |
| 优于以太坊 | 1.基础技术独立，不依赖与从比特币或其他加密货币系统获得的技术基础。<br>2.Ouroboros 运行成本低，可节约大量计算资源，并可解决交易量上限的问题，完成后理论上 TPS 可无限。 | 1.NPOS 比 POW 和 POS 更安全，更去中心化。<br>2.更优化的升级方式，升级无需硬分叉。 | 1.高达 5 万的 TPS，POH 高效率的交易处理机制，与以太坊高 GAS 费和低效率形成对比，非常适合高频的区块链应用，比如 DeFi。<br>2.单一链解决分片后可组合性问题。 | 1.高达 65000 的 TPS 和远低于以太坊的 gas 费。 | 1.神经网络系统（NNS）可以完全控制网络的各个方面，包括面对黑客攻击让所有方恢复正常等，用户安全性体验优于以太坊。<br>2.以太坊分片扩容有上限，DFINITY 将共识、验证和存储分为不同层次的架构理论上可以无限扩容。 | 1.越是简单的应用就越可以用简单的逻辑去实现，这不仅让应用更容易开发，同时也更保证了应用的安全性。<br>2.专注承载金融资产和产品，比以太坊更能满足金融交易速度的需求，以及更能实现金融产品所需特性。 | 1.更高级别的安全性<br>2.低迁移成本，甚至无需跨链迁移资金 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3.区块链规模越大，所需网络带宽也越多，RINA 解决每个节点支撑通信所需的网络带宽问题，使节点间自然地进行规模化通信。 | 3.平行链是以太坊分片技术的进化版。以太坊做“币生态”，波卡做“链生态”，波卡可将已有的链及其生态纳入自己的网络，包括以太坊。 | 3.比以太坊更注重性能和扩展性。 | | | | |
| 支撑未来经济发展的大规模任务关键型 DApp 的首选平台 | Layer-0，倾向于成为更底层的区块链基础架构，乃至成为互联网的下一代平台 | 不与以太坊竞争，为需求扩展性的项目提供最好的平台 | 构建和连接与以太坊兼容的区块链网络的协议和框架，是以太坊扩容方案之一 | 用 AI 取代代码，将传统互联网垄断行业重构开放式商业，利用区块链计算机系统重构 IT 系统并大幅削减成本，希望大部分技术可用于以太坊，二者相互完善 | 做一个金融平台，承载各种金融资产和金融产品。 | 最安全的公链 |

企业愿景

*来源：各公链官网，图表：Gate.io 研究院*

而要再将上述主流公链细分的话，ADA 是名副其实的以太坊竞争者，DOT 旨在做以太坊的上游将所有区块链“万物互联”，其他的公链则是对以太坊去中心化、性能、安全性和专项经营（ALGO）的补充。

值得一提的是，除了 ADA 和 DOT 有宏大的愿景之外，本节认为 ICP 的愿景最为宏大。ICP 将人工智能和区块链技术相结合，推广发展到传统行业，利用人工智能完善区块链技术，利用区块链技术影响传统行业，有望打破传统互联网行业垄断重构开放式商业，重构 IT 系统降低人力需求从而大幅削减成本，甚至可能影响整个人力资源市场。

综上所述，各大主流公链在去中心化、性能和安全性三个方面技术开发的偏重如下（根据公链已完成的独立技术分类，详见附录）：

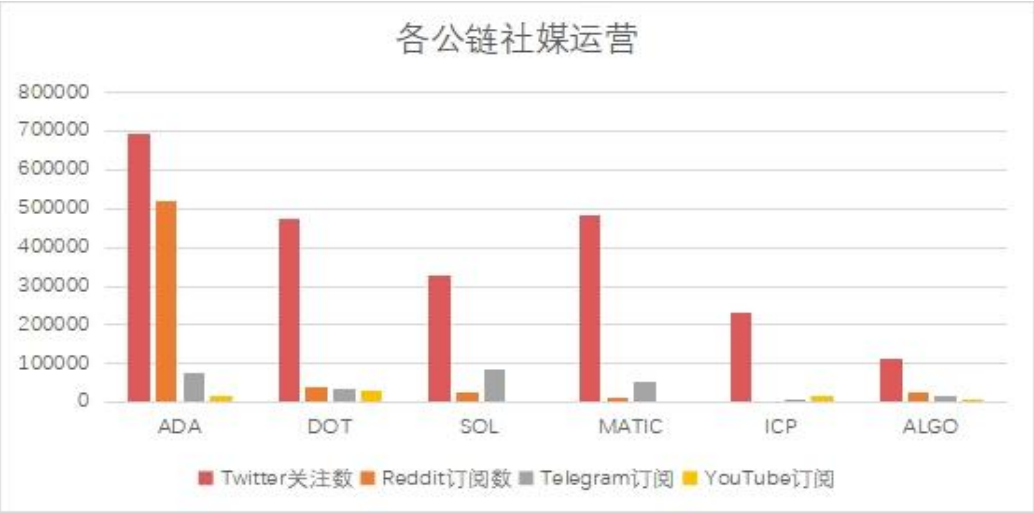
| | ADA | DOT | SOL | MATIC | ICP | ALGO | GateChain |
|---|---|---|---|---|---|---|---|
| 去中心化 | ☺ | ☺ | | | ☺ | | |
| 性能 | ☺ | ☺ | ☺ | ☺ | ☺ | | ☺ |
| 安全性 | | ☺ | | ☺ | ☺ | ☺ | ☺ |

*图表：Gate.io 研究院*

**发展情况**

区块链产业发展迅速，在这个产业发展的上升阶段，技术、企业或项目的革新迭代也是非常迅猛的。各个特色公链作为企业运营来说，其业务的拓展和市场的开拓在这个市场突飞猛进的时期尤为关键。

根据前文提到的团队构成和下图中社媒的数据显示，再次印证了 ADA 和 DOT 近期的经营重点在市场&运营，二者都已在业内获得极高的关注度。值得一提的是，以太坊近期最大的技术突破就是二层扩容，而 MATIC 作为其扩容方案也收获较大的关注度，区块链公链技术依然存在围绕以太坊展开的迹象。




*来源：Twitter、Reddit、Telegram、YouTube（截止 20210618）*

## 2.2 公链的发展趋势

综上所述，公链市场围绕着以太坊进行技术开发的格局已有了多元化发展。公链的未来发展趋势将依然以“以太坊的竞争者”（ADA）、“以太坊的技术补充与改善”（DOT、SOL、MATIC、ICP）和单项领域发展公链（ALGO）为主而展开。

其次，公链的发展将围绕去中心化、性能和安全性三方面的权衡这个难题而继续开展技术研发。以太坊近期大力开展的扩容便是在性能寻求优化，但扩容之后节点增加节点的安全性又是令人担忧的地方，所以完美的公链就是在去中心化、性能和安全性达到完美平衡的以太坊。目前市场上已经有了大量的 rollup 等优质扩容方案，后续安全性和隐私性革新的解决方案或许是以太坊下一个发展目标，也是公链下一个发展目标。

再者，SOL 提供了一种单一链的公链经营模式，这样专一经营的模式满足“小众”的需求，短期更易实现应用的价值。但这同时也对区块链间与资产间的互操作性提出要求，所以如同

DOT 和 CKB 一样能够提供任意区块链和任意资产间的跨链技术的项目，也将是未来公链发展的方向之一。

最后，从前文的数据来看，优质的公链更需要优质的市场运营来维持，而技术开发是重中之重，也需要特色化的技术开发道路。从目前公链市场的发展趋势来看，特色化的公链技术发展道路有条：一是充足资本，扩大规模与市场运营，在去中心化、性能和安全性中发展重点技术，提供供应，寻找需求，进而抢夺市场；二是开创自有领域，创立特色的企业愿景，比如 DOT 创建 Layer-0，ALGO 创建金融应用专用公链；三是将区块链与其他高新技术结合，创建其他新进企业难以实现的技术，比如 ICP 结合区块链与人工智能。

# 3 区块链的应用价值与发展趋势

## 3.1 区块链行业概况

随着 2008 年比特币的横空出世，区块链作为一项具有信息产业革新意义的技术开始蓬勃发展。区块链发展至今十余年，行业参与者从特定群体拓展到各大投资机构和著名企业，不管是金融市场投资、价值支付方式接纳、区块链技术研发和应用等均有欣欣向荣之迹。一级市场区块链投融热情高涨，二级市场加密货币市场市值已超 2 万亿美元，区块链企业爆发式增长，区块链技术专利领域形成一定气候，区块链在各行各业的应用也呈现百花齐放的格局。咨询研究机构 Gartner 预计，到 2030 年，区块链技术创造的商业价值将达到 3.1 万亿美元，足以判断区块链技术的发展势头非常强劲。

### 3.1.1 区块链行业发展模式

目前区块链的发展主要呈现两种发展模式：

- 原生区块链货币价值模式：基于去中心化的区块链技术，在基础技术上寻求突破与创新，实现价值传递和交易等。以 BTC 为代表，在新型货币和支付手段上对标传统金融，解决“去信任”的问题。
- “区块链+”技术价值拓展模式：将现实传统场景和区块链底层协议相结合，企图提高效率、降低成本。区块链除了最初的交易属性（价值属性），在存证属性、信任属性、智能属性和溯源属性上均有广阔的价值挖掘空间，当传统场景的痛点与需求和区块链的技术属性相匹配时，便能产生巨大的商业价值。区块链在当前区块链的行业应用主要在第二种模式，ETH、ADA、DOT 等公链搭建各种应用场景所需的基础平台，场景应用项目在其上进行应用空间的想象与落地。

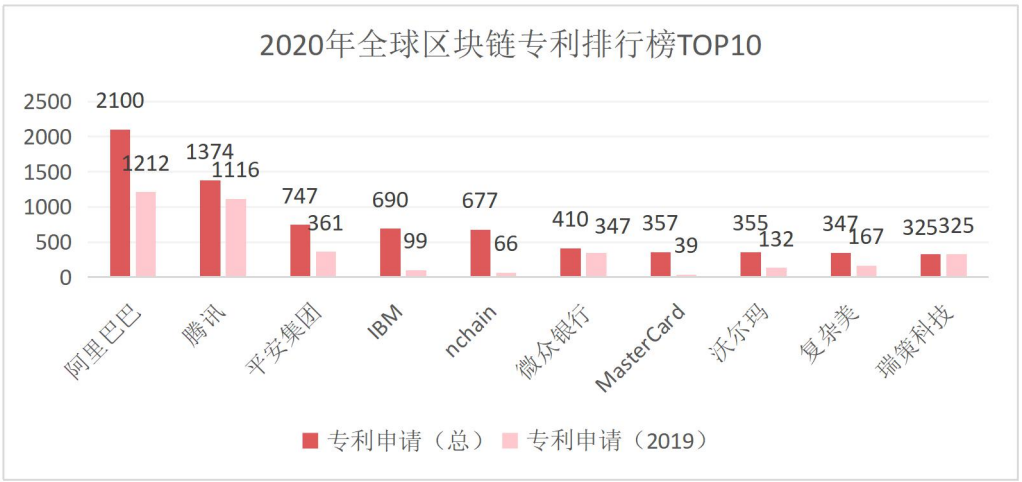
### 3.1.2 区块链行业市场形态

当前的区块链行业已形成了比较明晰的产业链结构：上游基础设施，中游通用技术拓展，下游区块链应用领域。上游为区块链系统的正常运作提供必要的操作环境和物理设施，同时也包含公链的搭建；中游的通用技术是在区块链走向应用端的必要环节，区块链开发者的技术调用和服务提供更加便捷、效率更高；下游的垂直应用是区块链技术的价值呈现的最佳体现，通过区

块链赋能传统行业，为传统经济增添新活力。


*图片：Gate.io 研究院*

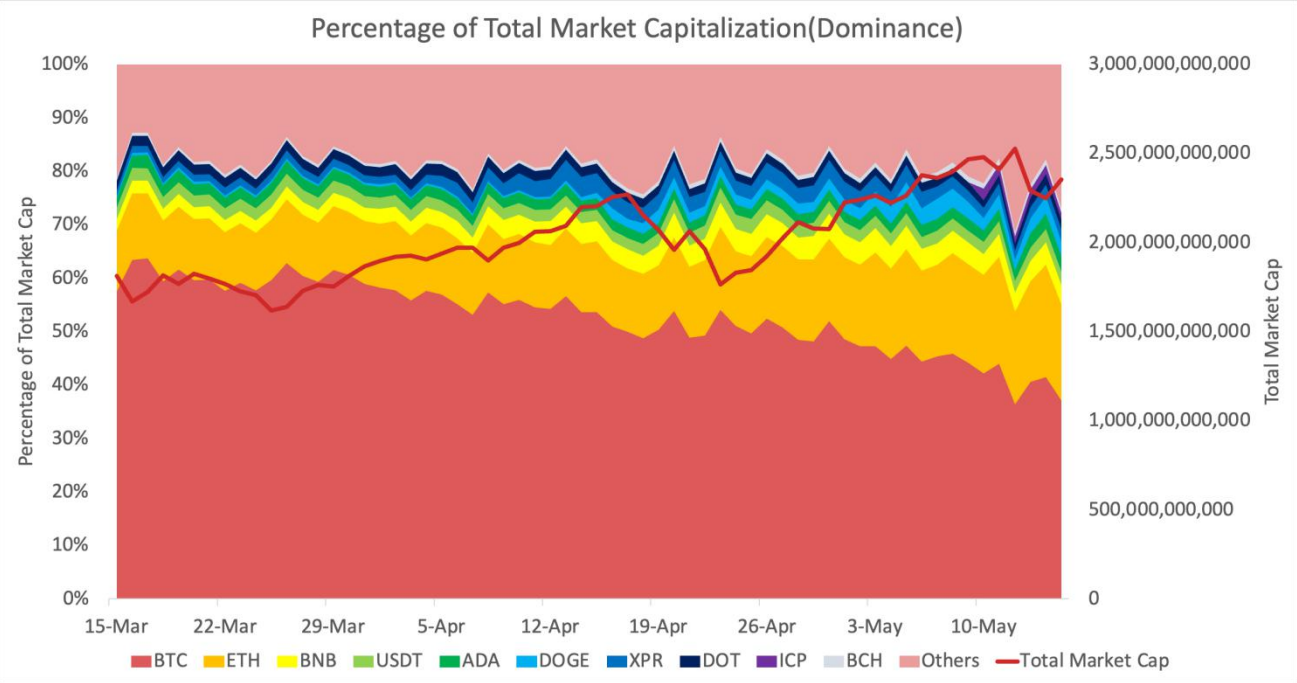
区块链作为一种“分布式账本”，其在信息传输链条上的“去中心化“、在信息存储的透明度和安全性上等优点，吸引当今越来越多的企业布局区块链。截止 2019 年末，全球共计约 6000 家公司申请区块链专利，数量超 3.8 万，涵盖中、美、日、韩、新、澳等 47 个国家。据零壹智库统计数据，在 2020 年区块链专利排行榜 Top100 中，中国有 52 家公司上榜，Top10 中占据 6 位，其中阿里巴巴、腾讯和平安集团三家公司稳居前三，可见中国在区块链技术上占据绝对优势。




*来源：零壹智库，图片：Gate.io 研究院*

### 3.1.3 区块链行业竞争格局

区块链技术以代币发行的形式为投资者参与区块链生态发展的提供投资敞口，加密货币市场的市值反映不同区块链技术或项目在投资者心中的价值认可程度。Coingecko 近几个月的加密货币市值数据显示，当前市值前十的加密货币分别是 BTC、ETH、USDT、ADA、DOGE、XPR、DOT、ICP 和 BCH。加密货币鼻祖 BTC 的市值占据半壁江山，在价值认可上始终保持优势，闪电网络的应用也解决了部分交易效率上的问题；ETH 通过智能合约的搭建使其成为之后诸多公链的模范，如今 ETH 2.0 和 layer2 也正如火如荼进行中；公链赛道 ADA、金融垂直应用 XPR、跨链代表 DOT、新一代计算机互联网 ICP 等也都具有各自的特点和发展前景。




*来源：coingecko，图片：Gate.io 研究院*

## 3.2 区块链行业发展趋势

### 3.2.1 共识增强和技术发展解决瓶颈，DeFi 和 NFT 仍具长远发展空间

DeFi 和 NFT 的火热令无数投资者跃跃欲试，但从客观理性角度来看，当前的过热态势带有资本炒作的性质。DeFi 的资金使用效率受人诟病，NFT 的价值锚定与定价机制仍较混乱，一旦加密货币市场行情走颓便呈现巨幅波动，其真正的区块链应用价值处于初步探索阶段。研究院认为，目前两者遇到的主要瓶颈在于资产的使用效率低和交易费用高，在未来加密货币和区块链价值共识的增强将提高 DeFi 生态的参与率和使用率，layer2 的技术改进将进一步降低交易成本，NFT 在短期价格泡沫后的资产价值发现回归理性。因此，将来区块链将仍会在 DeFi 和 NFT 有较长远的发展。

### 3.2.2 “区块链+”和商业模式创新将成为区块链技术价值最大体现

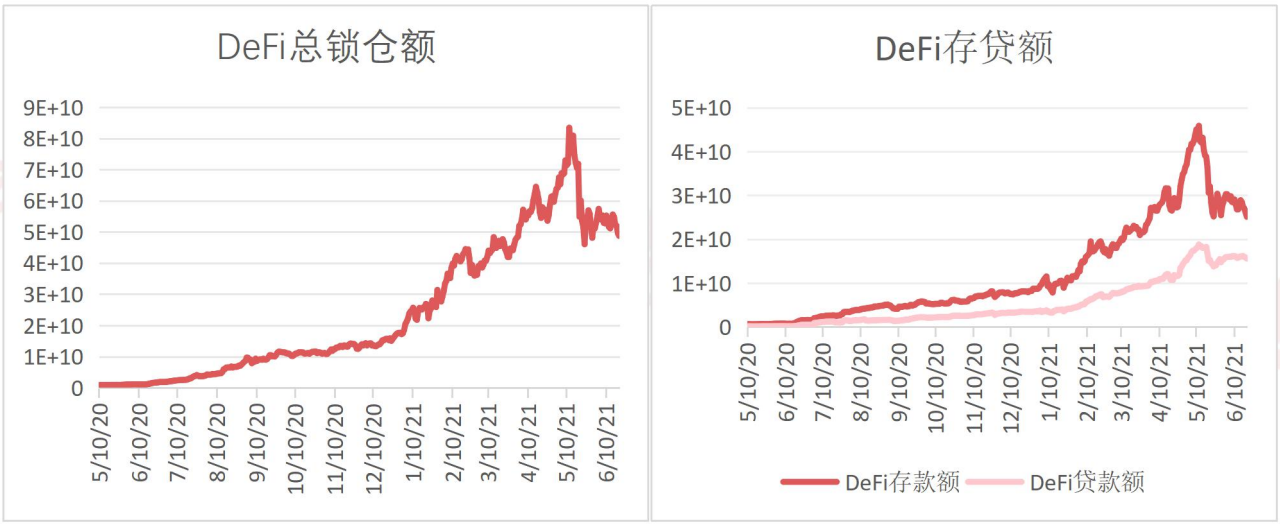
另外，区块链技术的创新不仅仅是技术本身，其应用落地的可设想空间和对于经济形态或商业模式的创新思考或是更具价值的体现。区块链代表的是一种“分布式”和“去中心化”的思想，在信息存储和价值传递上具有优势，对于传统应用的降低成本和提高效率等方面均有成效。另外，区块链技术一方面做到数据安全与信息保密，一方面在透明性和公开性做到极致，在此基础上，企业的商业模式和企业间协作模式可予以创新思考。传统的企业内或企业间的信息存储和传播需要中心化机构管理，有时容易产生权限管理混乱、信息不对称等瓶颈，而区块链技术的应用能够构造更加开放和谐的商业共享和管理模式。

## 3.3 区块链应用主要领域

### 3.3.1 DeFi 与 NFT 现状和发展趋势

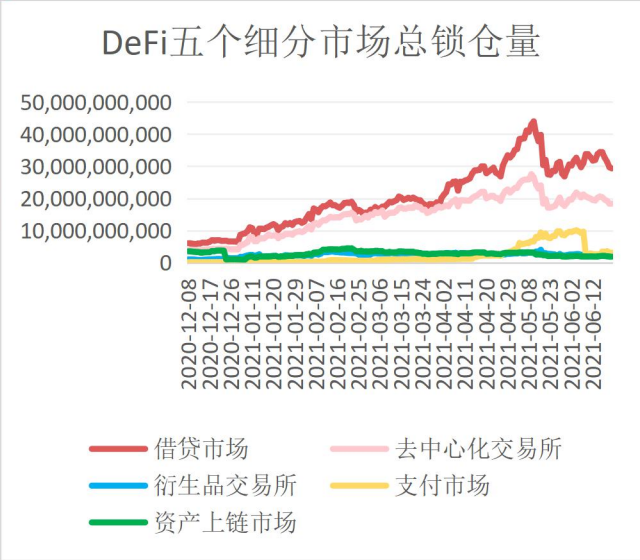
**DeFi**

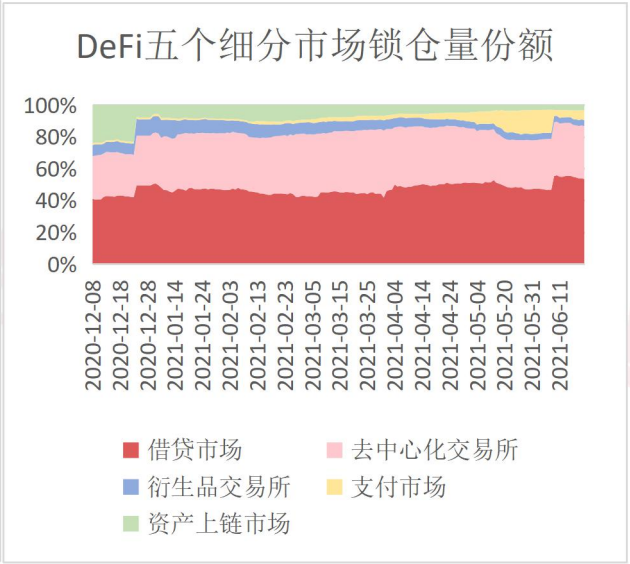
继 2020 年 6 月的“DeFi”之后，今年年初“NFT”概念也呈现爆发式发展。近一年来，Syhthetix、Compound 等项目的出现推动流动性挖矿/收益率耕种成为市场的宠儿，DeFi 成为加密货币估值的重要驱动力。数据显示，DeFi 的总锁仓量和存贷额稳步上升，均有超百倍的惊人增长，存款额与贷款额差异拉大，池内资金充足，资金流动性有保障。




*来源：QKL123，图片：Gate.io 研究院*

当前 DeFi 领域可划分为借贷、去中心化交易所、衍生品交易所、支付市场和资产上链市场这五个细分市场。其中，借贷市场是 DeFi 领域的龙头，借贷市场和去中心化交易所市场的锁仓量涨幅和市场占比具明显优势，两者占据超 80%的市场。衍生品市场和资产上链市场总锁仓量变化波动不明显，市场占比均有所下降。支付市场起步水平较低但后来居上，今年 5 月在 xdai 和 Lightning Network 的带动下迎来锁仓量大爆发。



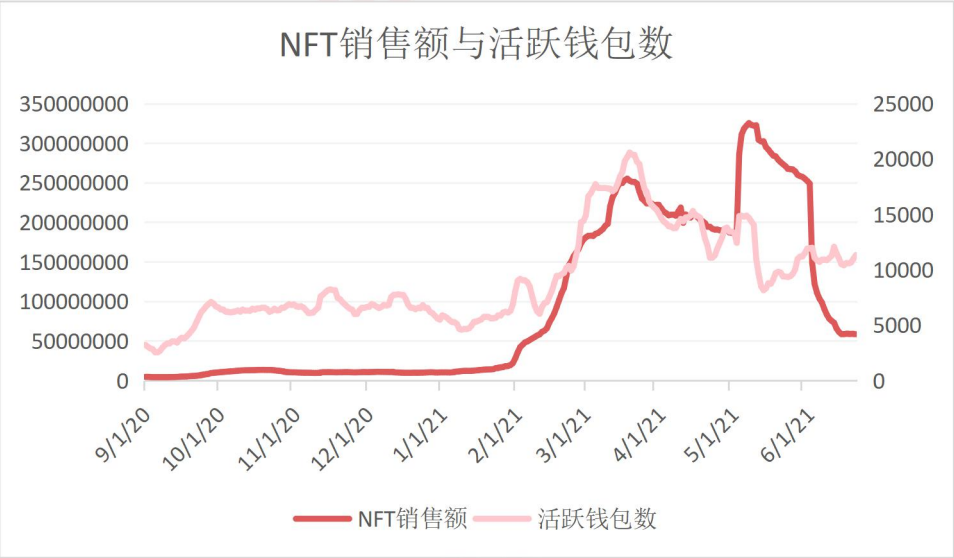

*来源：Tbanic，图片：Gate.io 研究院*

结合 DeFi 项目的使用现状来看，DeFi 领域目前的发展主要依靠热门投资主题拉动，在代币经济和锁仓量方面运作较好，但项目生态的运转状况（尤其是借贷资金效率和参与率）并与之相匹配，大量锁仓资产处于空置状态。问题主要在于参与 DeFi 的成本仍较高，目前主要集中在以太坊链，以太坊的拥堵情况尚未得到很好的解决，但当下各类扩容方案（如 layer2）的提出有助于克服这一瓶颈，未来可行技术的落地将会进一步推动 DeFi 的发展。

研究院认为，借贷是金融的核心，未来 DeFi 领域仍会以借贷市场占主导，支付市场和资产上链市场将迎来春天。当前代币多样化和碎片化的格局将伴随着 DOT 等跨链项目的生态逐渐完善而发生改观，未来不同链的扩展协作和资产互换会成为需求爆发点，开放式金融将带来广阔的前景，故看好支付市场和资产上链市场未来的商业价值。

NFT

NFT 的唯一标识性价值被挖掘，NFT 概念在今年一季度成为市场新风向标，尽管销售额近期有所回落但总体出现飞跃式增长。同时，活跃钱包数在市场行情下滑时未出现像销售额的巨幅下跌，反而小幅上升，或可说明投资者对于 NFT 仍具投资信心。




*来源：Tbanic，图片：Gate.io 研究院*

当前 NFT 市场的数字 Token 鱼龙混杂，代币发行的开放性和低门槛使得价值锚定出现严重背离，故可期待未来在这一方面的机制逐渐完善后会有新一轮的增长。在 NFT 领域中，资产上链会是持续备受关注的话题，在区块链中实现低成本的“万物可上链”、“万物附价值”。

### 3.3.2 区块链技术主要应用现状与发展趋势

#### 3.3.2.1 区块协作

区块链诞生以来，市场长时间聚焦加密货币的金融投机，而区块链技术本身能体现的数据信息

协作的价值一定程度上未得到重视。2020 年的新冠疫情让全球经济陷入泥潭，但同时基于区块链技术的远程协作分布式办公掀起一阵“基于数据经济的协作模式” 的热潮。

**区块协作的两大应用**

区块链技术赋能企业协作，其中具有代表性的应用有：DAC 和供应链。

## DAC：新型协作

分布式自治系统 DAC（Distributed Autonomous Corporation），其实是去中心化组织 DAO（Decentralized Autonomous Organization）的改进，是对 DAO 无所不包的应用边界具象在追求经济利益的“商业组织”当中。DAC 是指通过一系列公开公正的规则，可以在无人干预和管理的情况下自主运行的组织系统。DAC 是为了实现某个具体的商业目标，通过程序设定一套标准化规则，DAC 成员之间进行协作，不断创造价值。DAC 可以是某种数字货币，如比特币，通过一套标准化规则激励各个节点来维护数据安全，也可以是一个系统或实体机构等。

本质上，DAC 可以理解为构造一种新的开放性的组织模式和商业系统，完善市场运行制度，克服传统公司之间协作和治理方面的高成本、信息不透明、管控过程黑箱和交付结果不达标等问题。

Metis 协议是以太坊 layer2 的搭建 DAC 跨域协作的项目，其愿景是任何一方基于 Metis 协议可以构建一个 DAC 与分布式的其他方进行各种跨域协作，并对 DAC 中写作的过程进行管理。其主要通过 MSC 元质押合约进行协作方治理，通过 ComCo 框架进行协作过程管理。

- 协作方治理：融合了 Staking Economy、Optimistic Rollup 算法、博弈论和智能合约等机制，创新地提出 MSC 元质押合约（Meta Staking Contract），将质押保证金作为元协作双方履行条款或承诺的保障。在协作过程中，任何一方违反条款，守约方可申请仲裁，待退回的质押保证金会被回撤，元协作被解冻，仲裁官介入并对违约方进行惩罚。
- 协作过程管理：通过 ComCo 管理框架，协作双方在链下商议确定协作内容，链上只需公布协作结果的共识状态。

Metis 通过以上两方面在跨域协作上寻求可行方案，将经济价值数据化、标准化和结果可衡量化。不管是 DAO 还是 DAC，其作为新型组织管理模式备受关注的原因是其独有的特性：自动执行的统一规则、透明度、权益相关者表达诉求的便捷性；快速、无边界的业务决策；组织范围内的投票参与，这些正是能解决当下跨域合作当中出现的一些痛点。

## 供应链：信息共享

融合区块链供应链平台，搭建金融机构、产业链核心企业、链属企业、供应商等多方联盟信任体系和价值网络，构筑核心企业信用，降低产业链结算成本、融资成本、增强资金和资产流动性，促进整个供应链生态良性发展。在金融场景应用中，针对区块链股权的 PlatONE 和供应链金融领域的蚂蚁链走在行业的前列。这一部分也将主要讨论区块链股权和供应链金融两个方面。

**区块链股权**

市场经济的基石是财产权利的确定性，这种确定性也是交易的基础。

- 在传统金融领域，公司常常被法律赋予了较大的主动权来自行确立股权的权利，公司可以选择采用任何有成文记录的形式来维护股东名册，传统上上市公司多数采用纸质版进行保管，中央清算机构作为第三方公信力提供者来增强可信度；而对于非上市公司的股权，其背后并没有此类中央清算机构，由于缺乏完善的技术基础设施来确保每一份股权的唯一性，只能依赖工商局这种国家行政机关的公信力来进行“事后性”的确权公示，这样不免导致效率低下和违背市场经济私法原理（由当事人的意思自治来完成权力转移，而非公权力机关）等问题。
- 另外从投资者的角度看，股权交易前的背景调查往往是很繁琐的过程，特别是当一些公司存在股权错综复杂、管理模式混乱、公司故意隐瞒信息等情况，真实可信信息的获取难度较大，投资者的投资信心受到削弱；股权交易过程的繁琐、消耗时间之长等都直接影响投资者利益。

所以，当区块链作为一种分布式账本出现时，股份确权的形式将丰富起来，股权信息将更加透明，区块链在金融股权应用方面的价值值得进一步挖掘。

在区块链股权应用方面，PlatONE 是个典型的代表。PlatONE 是基于隐私计算的新一代联盟区块链平台，支持企业级应用。它通过广播加密和群签名来解决个体隐私与中心监管的矛盾，通过动态加密和零知识证明解决交易隐私和登记确权的矛盾，通过安全多方计算解决机构件数据隐私和数据协同利用的矛盾。通过 PlatONE，企业股权信息可以得到及时登记确认和维护，

通过分布式的数据架构来降低企业沟通与信息对接的门槛，股权数据的实时安全共享，区块链技术的不可篡改性和可追溯性保障了重要信息披露的真实性和安全性。在 PlatONE 联盟网络中，股权登记和查询平台可提高企业和股东股权登记、变更和交易等流程的效率和安全性，与工商、信息服务机构的对接也更加顺畅。

**供应链金融**

联盟链在供应链金融的应用价值，能够在多方主体参与、信息不对称、信用机制不完善、信用标的非标准的场景中得到显著的体现。

- 在供应链金融体系中，上中下游企业的沟通和信息传导与共享的效率与准确性至关重要，区块链数据系统能最大限度地整合供应链金融上的市场参与者，形成“产品信息流、商流、物流、资金流”为一体的链上格局，保障金融信息透明化，打破信息孤岛。
- 由于链上数据的真实可靠及不可篡改，传统金融中的企业信用随链条拉长而减弱的问题可得到解决，链上信息的地位平等，现实的企业债务债权情况映射在链上并进行真实传递，企业信用传递效率得到极大提升，融资成本也将有效降低。

蚂蚁集团在区块链的供应链金融的探索处于世界领先水平，蚂蚁链从 2016 年到 2020 年连续四年获得区块链专利申请数和授权数的全球第一，技术上可支持 10 亿账户规模、每日 10 亿交易量、每秒 10 万笔跨链信息处理。当前蚂蚁链的合作伙伴包括招商蛇口、英特尔、中远海运、上港集团等，与供应链上的多个节点搭建合作关系。在具体落地应用上，蚂蚁链走入大众，落地场景超过 50 个。


*图片：Gate.io 研究院*

## 区块协作的发展趋势：开放式商业模式

从上文分析可以知道，区块链的出现不仅仅是技术的突破，也正在重塑商务流程、商业链条和全球经济面貌，由此可打造“开放式商业模式”。开放式商业模式就是企业为了最大化商业价值，打破组织的界限，整合企业利益相关者的所有知识和资源来增强企业价值。因此可以认为，地理空间层面的“跨域协作”和组织体之间的“开放式协作”的商业特点与区块链的技术特点和应用场景相得益彰。

互联网发展三十年，信息传递的全球化使得全球经济面貌焕然一新，互联网企业深刻影响着当今的经济格局。尽管互联网本身是开放自由的，但互联网巨头的快速发展和资本逐利的本性使

得当今的经济结构逐渐变得僵化，它们利用技术优势和资本优势在市场上逐步走向垄断。垄断企业往往具有较完整的资源系统，一定程度上能产生积极的“领头羊效应”，但中小企业往往缺乏这样的资源体系，或缺少资本、或缺少数据的获取渠道等。过于依赖投资的格局导致越来越多的中小企业难以发挥自身优势，往往要么被迫选择站队或被收购，要么被边缘化。另外，互联网巨头筑起行业高门槛，将信息和数据集中化占有，其他公司要获取价值信息的高成本使得他们望而却步。

本节认为，互联网实现的是信息传递，区块链的出现能实现更深层次的价值传递。通过区块链分布式和链式的信息存储结构，信息共享和数据存储的真实性和安全性得到保障，由此形成的节点间或企业间的沟通更加顺畅，开放而可靠的协作模式便是商业模式的下一个发展方向。可以设想，未来经济发展的核心从“资本”转移到“资本+数据”，通过链上的交易行为和交易数据来描述协作各方的合作关系和合作成效，特定行业者的垄断性问题也将得到缓解。

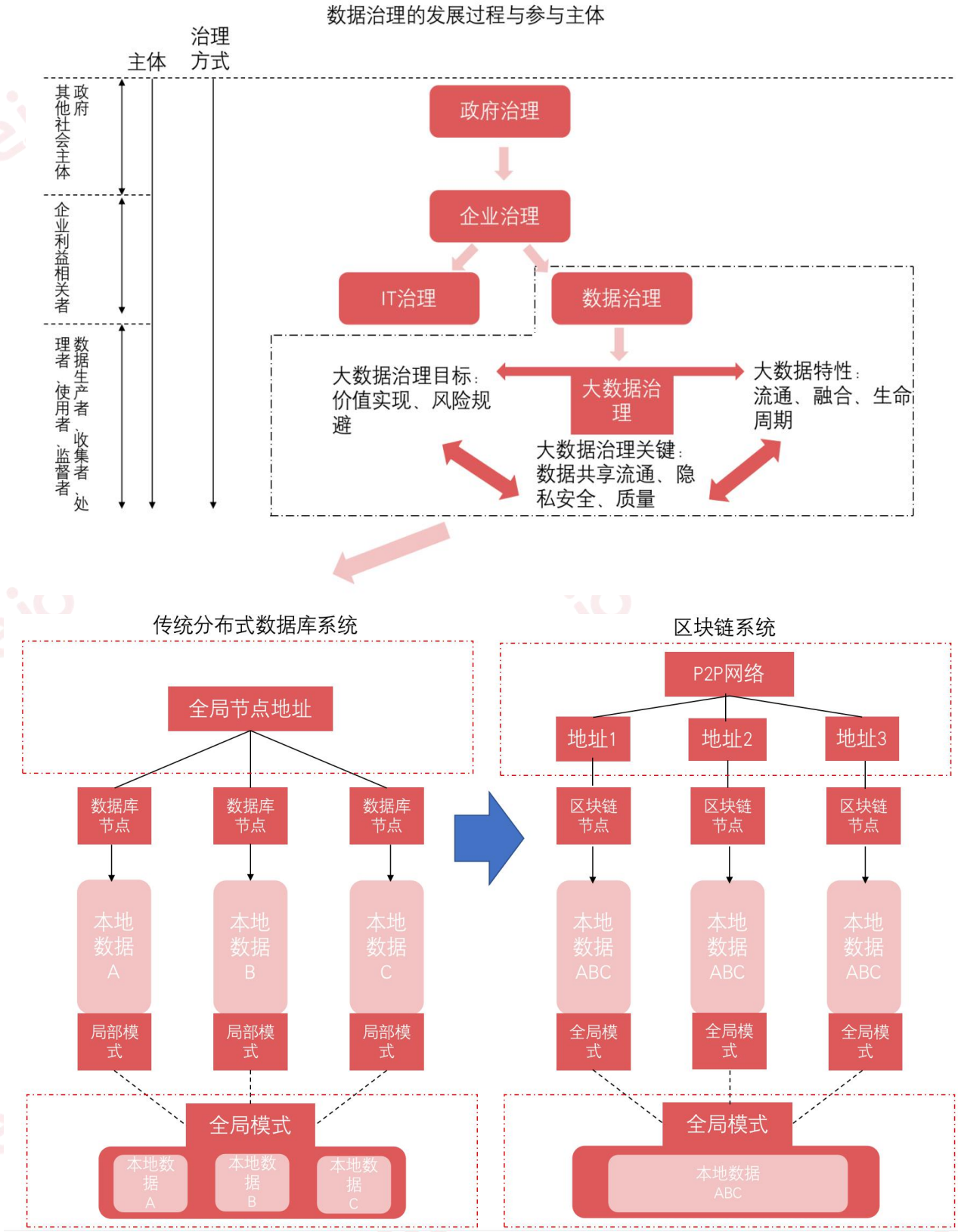
#### 3.3.2.2 数据处理

数据处理源自传统企业和相关业务的需求，数据处理的发展与现状是信息产业发展演变而来。区块链技术是信息产业的技术革新，欲探究区块链数据处理领域的未来发展趋势，还得回归传统企业和业务的需求本身。

## 从传统数据治理到大数据治理，再到区块链数据处理

首先，数据处理的主体一直在从中心化向去中心化发展，数据生产、收集、处理、使用和监督的角色也在从单一主体逐渐角色分化。传统数据治理方式在向大数据治理发展时，传统企业就已提出提高数据决策质量、评估与监管个人隐私数据使用和促进数据共享。可以说去中心化的发展是数据处理领域的一种需求和必要结果。

其次，传统数据处理从政府治理到企业根据相关业务进行数据自治，再到大数据治理，根据其特性、目标和治理关键，整个发展过程对数据的处理提出了三个要求：可审计的数据存储和处理，可溯源问责的数据获取和共享，可验证的数据分析和机器学习。




*图片：Gate.io 研究院*

区块链技术分布式数据库的机制（上图）有助于提高数据存储和处理的效率和质量，并提供审计、溯源和验证等解决方案。目前市场上各区块链项目在此基础上进行研究与创新，从不同的层面各自的角度提升区块链数据处理的性能。ICP 的网络被设计为在使用时，能存储无限量的状态，因此一个节点不可能维护所有庞大的数据副本。ICP 利用 USCIDs 技术，对跨节点的状态存储进行切分，要求每一个端口维护被分配的唯一状态数据副本，完成无限量的数据存储。

对比传统与区块链数据库，在完善区块链数据处理技术性能之后，只要二者性能相当，区块链数据库去中心化、效率、安全性等优势便可体现。因此，对于数据可审计、可溯源和可验证要求较高较急迫的行业，将区块链数据处理技术率先发展的方向。本报告认为，泛金融应用和供应链等行业更可能是区块链数据处理并应用的主要领域。

## 数据处理的发展趋势：泛金融效率与异构数据访问 & 供应链溯源

### 泛金融应用领域

首先，区块链系统能够为金融支付和管理场景提供更安全、便捷的自动交易和记账服务。蚂蚁金服的区块链跨境支付系统已经能够实现 1 分钟到账的效率，相比传统金融 VISA 系统的一周到账，效率提升是突破性的。所以未来区块链系统在交易验证的高实时性和高吞吐量是一个主要的发展趋势。VISA 系统的 TPS 在数千笔每秒，SOL 的时间证明（POH）处理机制提高 TPS 到 5 万，MATIC 作为以太坊二层扩容拥有高达 6 万 5 的 TPS，而 TPS 的数值还在一直被突破。

其次，现有金融领域存在众多金融组织，这意味着未来区块链金融领域将存在众多区块链系统，

所以区块链系统在存储上的异构将是数据审计、溯源和验证的一大壁垒。所以金融区块链间的跨链交互，是解决异构数据访问问题的关键。而这或许正是 DOT 和 CKB 等公链项目技术价值实现的关键。

**供应链领域**

供应链包括联盟链等产业模式，产业经营过程繁杂，节点数量庞大，信息量对数据处理技术也有极大的考验。区块链系统存储并管理供应链数据，拥有对数据溯源、查询和验证等核心功能，进而提高产业过程的透明度与相关行业的安全性。但因此对于区块链数据处理能否及时和高效地发现供应链中出现的问题有极高的要求，因此在溯源机制上能否开发切实有效的、基于技术和算法的自动管理体系，将是数据处理在供应链发展的关键。

#### 3.3.2.3 安全性、隐私性

##### 区块链隐私所面临威胁和现有保护机制

前文已多次提到区块链安全性的问题，以及本报告认为目前区块链技术的难点就是在于对去中心化、性能和安全性三个方面的权衡。所以隐私保护将会是区块链技术发展上长期面对的难点。

区块链隐私与威胁大致可以分为账本隐私与威胁、网络隐私与威胁：

- 账本隐私与威胁：分布式账本记录区块链运营中的所有事务数据，在加密资产领域、金融领域和企业间应用等方面上，区块链账本都主要记录交易数据。而目前区块链行业内，交易模型主要为 UTXO 模型和 account 模型两种。所以隐私内容主要是交易内容、账户地址

和用户身份等信息，这些信息记录在公开的区块链账本中，面临着攻击者的威胁。

- 网络隐私与威胁：区块链系统运营的本质是去中心化 P2P 节点间的通信，所以在增加链上扩展性的同时，节点和通信隐私面临着威胁。黑客可以通过部署监听节点，爬取网络中其他各节点的隐私信息和网络通信信息，甚至对其他节点发起攻击。

| 区块链隐私分类 | 隐私内容 |
| --- | --- |
| 账本隐私 | 交易内容 |
| | 账户地址 |
| | 用户身份 |
| 网络隐私 | 节点隐私 |
| | 通信隐私 |

图表：Gate.io 研究院

而现有的保护机制主要分为三类：通道隔离机制，信息隐藏机制和地址混淆机制。前文提到的闪电网络使用了通道隔离机制，主要通过 RSMC 和 HTLC 将交易在链下进行，将结果通报在链上进行，从而阻绝攻击，保证安全性；而以太坊和 ICP 都是通过其签名算法和共识机制来提高攻击成本，使攻击者入不敷出，属于信息隐藏和地址混淆机制两大类。

## 隐私保护的发展趋势：技术融合&分离处理

随着区块链技术的更加广泛应用，区块链系统的隐私保护变得越来越重要，这势必是未来该领

域发展的一个研究热点。但从其当下的隐私内容和所受威胁来看，区块链系统安全性提高的最大难点，依然是在与去中心化和性能两方面的权衡（比如扩容后将面临更大的节点隐私威胁）。

本报告认为其未来发展趋势可能在于两方面：一是结合其他行业技术，比如 ICP 结合人工智能技术开发出的神经网络系统（NNS），控制区块链系统的所有过程，面对黑客攻击可以让所有方恢复正常，达到安全性体验优于以太坊；二是将需求性能和安全性的链或者项目分开处理，摩根大通发起的项目 Quorum 通过分离公开和私有状态改进现有以太坊项目，增加私有事务与私有链上合约，增强系统隐私性和安全性。

#### 3.3.2.4 资产/数据非同质化

##### 确权保护的痛点及区块链的应用

版权保护问题和版权纠纷长时间以来是创作领域的痛点。中国政法大学专家李俊慧表示，当前版权在开发、管理和商业变现中，遇到的主要阻力的版权归属判定难，搬运、抄袭现象数见不鲜，版权运营的变现机制尚需要进一步完善。区块链技术具有不可篡改、追根溯源、分布式共识等特点，和数字版权保护具有天然的契合之处，两个结合可极大降低版权维权成本、提升版权保护效率，为网络版权的存证、交易和维权提供新途径。2021 伊始市场上最火热的投资主题“NFT”（Non-fungible Token，非同质化代币）便是内容确权在区块链上的体现，它定义了一种生态中不可分割的、具有唯一性的代币交互和流通的接口规范。抛开 NFT 的代币投机因素，区块链的应用创新地提出了一种标记原生数字资产所有权的方法，且该所有权存在于中心化机构或中心化数据库之外。基于这一点，区块链在唯一标识和内容确权方面可以在多个领

域发挥作用，如知识产权、实体资产、身份证明、金融文件和电子存证等。

**知识产权**

NFT 的非同质化和不可拆分性使得它与知识产权领域应用十分贴合，一幅画、一项专利、一首歌、一部影片、一段小视频、一张照片等，都可以将其在链上作为具有唯一标识性的数字资产。

**实体资产**

NFT 几乎可以锚定现实世界的一切资产，如房屋等实体资产，将实体资产上链形成可便捷流通的数字资产，交易和价值流通的便捷能极大不动产的流动性。

**身份证明**

传统身份认证模式中，往往需要委托中心化机构进行信息存储，透明度和安全性问题难以保证，再加上身份认证的低效率、存在不科学的流程、个人信息被特定企业控制而非个人等，传统身份管理模式需要创新。区块链可实现个人行为全记录，如身份属性、生物信息、个人特征等，具体来说包括出生证明、身份证、驾照、学历证明和护照等，再到个人征信、奖惩记录、社交资料、线上浏览记录等。将个人的数据在链上完整地记录和呈现，在一定的场景下不需要第三方验证，通过智能合约进行有效的身份交互验证，降低成本、提高安全性和隐私性。

**电子存证**

现实世界中的合同、文书等凭证均可进行链上去中心化存储。在金融应用领域，金融机构贷款交易业务频率高，一旦发生纠纷需要提交大量的案件证据。通过区块链技术将海量电子证据事

前存证、固证，技术上保障电子证据的真实性，保护交易数据原文等商业秘密，降低机构的证据保全成本。腾讯云推出的区块链可新取证 BTOE 能提供实时、高效、可信的在线取证、固证、公证服务，解决线上取证维权难题。通过细腻化取证环境，让电子数据全链路可信、全节点见证、全流程留痕，有效解决诉讼中存证难、取整难和认证难等问题。

### 非同质化发展趋势：价值锚定机制待完善，通证资产实际价值落地并缩小地域价值差异

当前的 NFT 市场存在各种各样的非同质化资产，其中绝大多数是数字艺术品、游戏物品和数字收藏品。区块链的开放性使得喜闻乐见的“人人可发行”成为现实，但伴随而来的是发行的非同质化资产的质量参差不齐和定价乱象，市场容易被投资者的盲目投机扰动，而背离了其真正的价值和经济逻辑。故本节认为，当前 NFT 或区块链数据资产非同质化的确权应用存在的主要问题在于非同质化数字资产的定价机制和价值锚定机制不完善，未来的发展方向也在于这两方面的改进优化。此外，通用资产的实际价值链上落地能最大程度发挥区块链在缩小地域定价差异的价值，将通用资产上链进行标准化定价，在全球全网络节点真正实现“一价定律”，削弱地域内其他因素的影响，使得价值共识达到全球统一。

## 3.4 主要应用领域的关键成功因素与发展可行性

区块链应用最成功的发展依然是在 DeFi 和 NFT 领域，而对于企业与机构的需求，区块链技术上的应用则又是重中之重，所以区块链应用当下的发展一方面是在资本的运作，另一方面是在技术的革新或者区块链为一些传统领域赋能。本节主要探讨前文应用领域的现阶段关键成功因

素与未来发展可行性，也将主要分为在资本层面上的运作（DeFi 和 NFT）和在技术层面的创新（区块协作、数据处理、安全与隐私、数据/资产非同质化）

### 3.4.1 现阶段关键成功因素

#### 3.4.1.1 DeFi 的成功是资本运作延续与创新

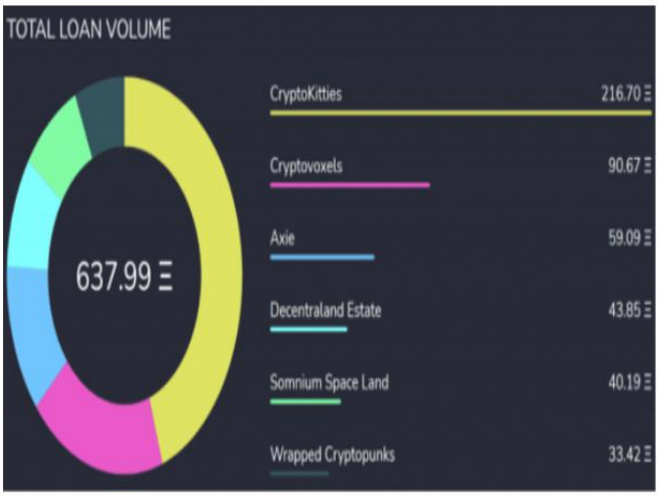
首先，在资本运作上，本报告并非认为 DeFi 和 NFT 没有技术（DeFi 和 NFT 具备相应的技术成分）而是认为 DeFi 和 NFT 成功的背后主要是资本的运作，对标传统行业，其成功的关键目前具有不可复制性且区块链领域本身的特点密不可分：

- 代币经济的运作。从 staking 原生代币到 yield farming 治理代币，Ox 等项目最早推出 staking 入口并开始发行治理代币，使 DeFi 的抵押有了更多的效用——收益权与治理权，随后 Compound 和 Aave 等项目开始推行流动性挖矿等现金机制来汇聚大量加密资产，用户将代币锁定到平台的流动性池中，平台则在系统中积极使用代币，DeFi 项目大多是紧密结合的，代币的价值便在流动中不断攀升。对比收益的吸引和投资的狂热，NFT 显得更加小众。非同质化代币从价值本身上剥离供应提升需求，从加密艺术到球星卡片等产品，

NFT 多是多版限量或者独一无二，对于认可其价值的投资者来说，升值空间是无可限量的。

DeFi总锁仓量和调整后总锁仓量


NFT作为借贷抵押品的价值

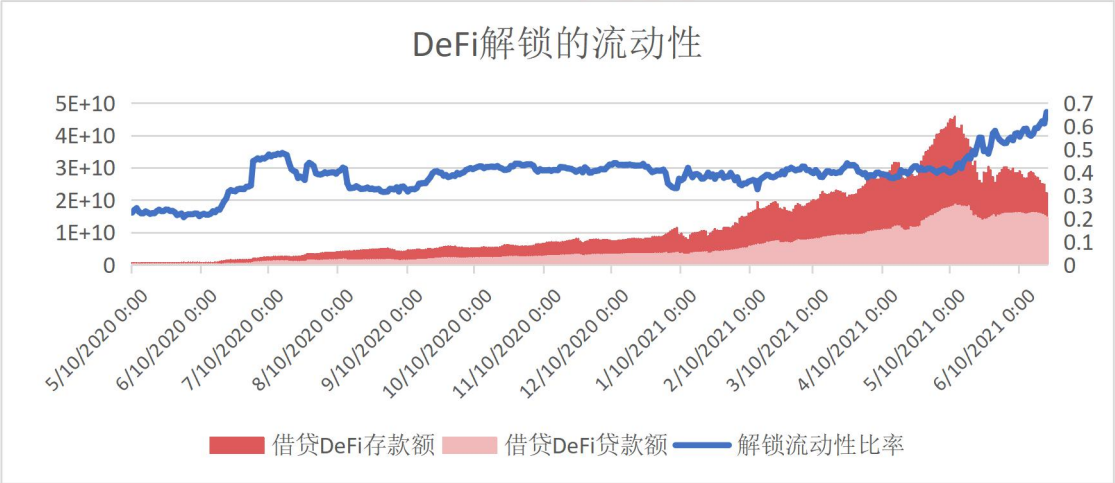



*来源：DappRader（左图数据截止 2021 年 6 月，右图数据截止 2020 年）*

- 通证经济是创新的商业范式。不论是 DeFi 还是 NFT，没有传统金融中所谓的纯投资人和纯消费者（例如消费者要参与 DeFi 和 NFT 生态就要拥有相关通证，拥有通证便拥有了投资者人的身份），生态的参与者身份是多元的，是利益相关者，既作为利益相关者，在相关的通证价值推动上就有了一定的动力。
- 传统投资模式赋能。比如，AMM 是使用恒定定价功能以任何价格进行做事行为的脸上流动性池，其大幅降低了流动性提供者的成本，Balancer 和 Curve 等成功就预示着 AMM 的巨大潜力。而 NFT 更加切合消费市场，在传统领域早已拥有追捧者，外加上 NFT 还具有社交的属性，DAO 等去中心化社区为其赋能、推广与炒作，作为具有实体的投资品能更快地为投资者所接受。

DeFi 在提供收益的同时，还解锁了巨大的流动性。随着 DeFi 被更多的投资者所关注，从 2020

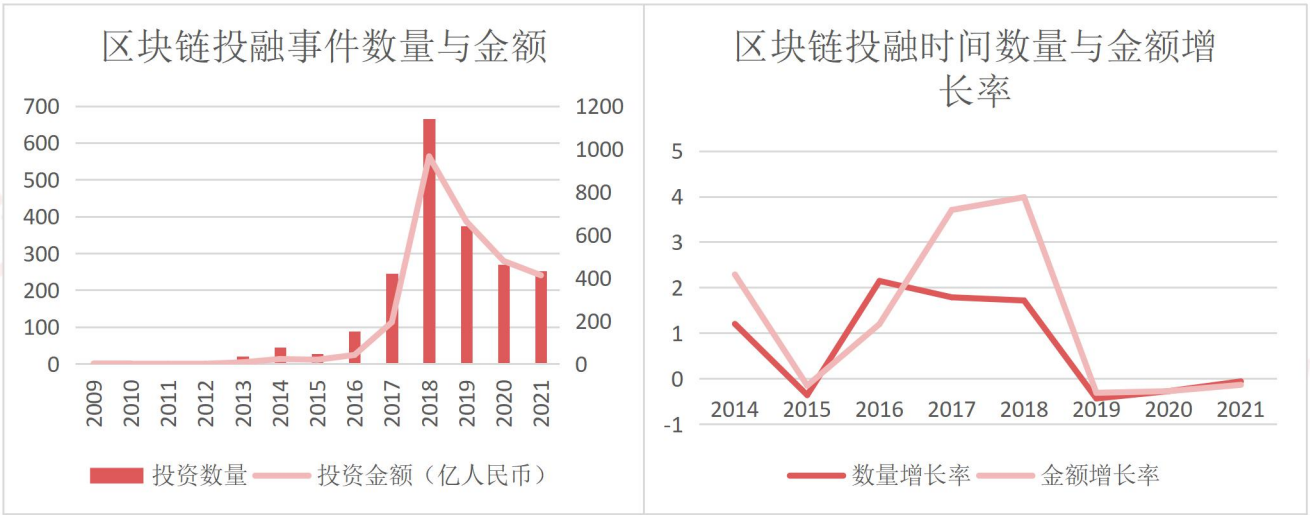
年下半年开始，解锁流动性比率从 20%左右攀升至 40%，而今年最高已超过 60%。DeFi 的成功不光在于代币经济的运作与创新，还在于其与整个加密资产体系有价值相互促进的作用。




*来源：QKL123，图片：Gate.io 研究院*

### 3.4.1.2 应用技术的成功源于对技术突破一直存在需求

其次，在技术创新上，从几乎每个国家都对区块链技术大力支持与发展的情况来看，国家与传统企业对于区块链应用技术上革新迭代的需求是一直存在的。




*来源：IT 橘子，图片：Gate.io 研究院*

区块链应用领域发展很快，“从无到有”只经历了数年的过程，到 17-18 年达到应用领域增长的顶峰，尔后渐渐步入正轨开始稳步发展。论最广为人知的外部因素，2017 年 ICO 爆发虽然存在乱想但无疑为区块链应用领域带来充足的资本以此为技术发展的前提，也让更多投资者关注到该市场；2018 年的中美贸易战再到 2020 年的全球芯片荒，互联网引领了过去 20 年的科技发展，而此时中美双方对彼此科技公司的限制一方面是中方科技的突破已经有可能动摇美方科技主导的地位，另一方面互联网引领的科技发展或已遇到瓶颈，再到后来全球芯片短缺。上述都反映出对技术的革新和迭代的需求，而区块链应用领域可谓应运而生，作为新兴行业，该领域技术上的突破还存在巨大空间，而且区块链应用目前业主要被用于弥补传统行业系统中的各项不足。

### 3.4.2 未来发展可行性

#### 3.4.2.1 DeFi 与 NFT 的发展可行性

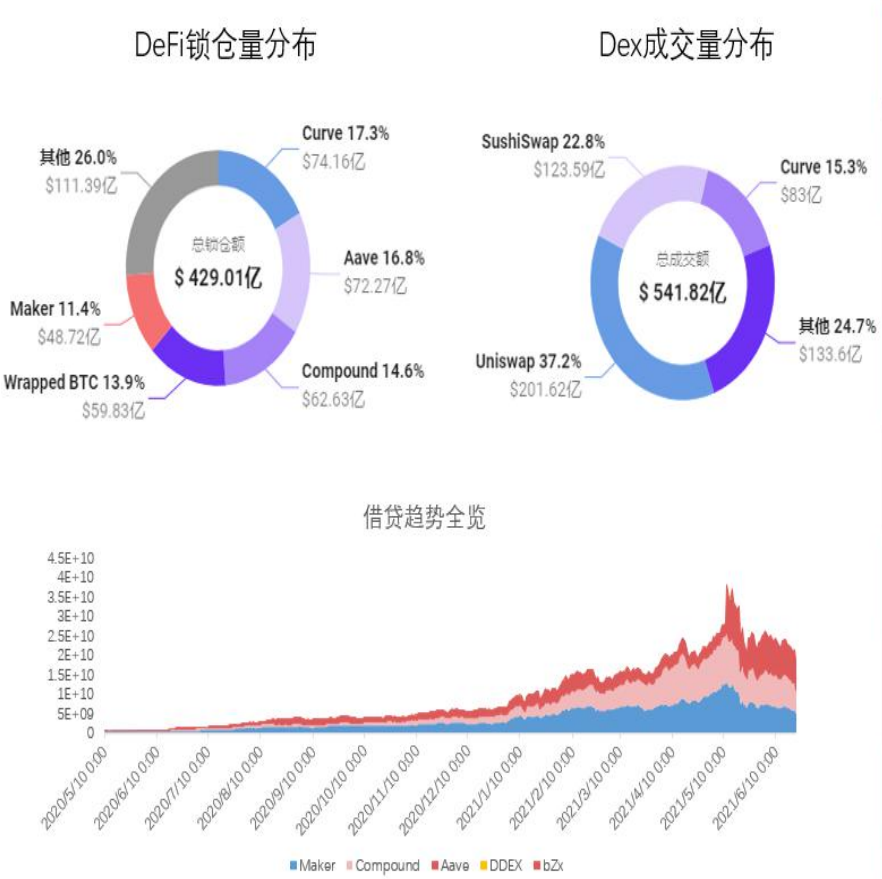
资源与生态

**DeFi**

DeFi 生态资产流主要有四个部分组成：

1. 去中心化交易所项目和借贷为根基的收益源头；
2. 项目代币；
3. 流动性挖矿；
4. DeFi 项目之间互相调用、链成网络，进一步优化市场流动性与效率。

目前，去中心化交易所交易量总共百亿级别，单个项目借贷总量在数亿级别，DeFi 锁仓量在百亿级别，而市场主流的 DeFi 项目总市值占市场百分比 1.305%，单个项目市值不足总市场的 1%。由此观之，DeFi 市场在整个加密资产领域还仅是冰山一角，目前主要为投资者提供额外的投资服务，DeFi 的投资并非加密资产主要投资，其还存在广阔的发展空间。




| 项目 | 市值 | 市场占比 |
|---|---|---|
| Uniswap | 9，503，728，867 | 0.719% |
| Aave | 2，722，264，333 | 0.206% |
| Maker | 2，189，587，495 | 0.166% |
| Compound | 1，235，512，653 | 0.094% |
| Sushiswap | 917，516，958 | 0.069% |
| Curve | 555，960，931 | 0.042% |
| Balancer | 113，179，646 | 0.009% |
| 总计 | | 1.305% |

*来源：QKL123，coinmarketcap（数据截止 2021 年 6 月 22 日），图片：Gate.io 研究院*

## NFT

NFT 商品在加密领域主要集中在艺术品、球星和游戏三个方面。头部市场拥有百万级别交易量，多数市场处于数十万级别。根据市场不同，商品不同，投资者不同，单个商品价值浮动区间巨

大，不可一概而论，而高价艺术品多在单件百万级别，今年 2 月 25 日成交天价艺术品《Everydays: The First 5000 Days》最终以 6025 万美元落槌。

| 收藏品 | 交易量$ | 交易数 | 销售 |
|---|---|---|---|
| NBA Top Shot | 611,850,000 | 402,900 | 6,488,522 |
| CryptoPinks | 360,890,000 | 3,249 | 13,895 |
| Axie Infinity | 133,240,000 | 81,359 | 546,502 |
| Rarible | 116,060,000 | 55,621 | 165,669 |
| Sorare | 85,130,000 | 25,273 | 440,660 |
| Meebits | 68,890,000 | 2,563 | 4,463 |
| Veefrends | 62,310,000 | 4,579 | 9,628 |
| Bored Ape Yacht Club | 53,200,000 | 5,150 | 13,580 |
| Hashmasks | 51,800,000 | 4,753 | 12,024 |
| Foundation | 45,980,000 | 10,447 | 15,647 |
| Decentraland | 45,460,000 | 4,603 | 14,529 |

| NFT | 价格$ |
|---|---|
| CryptoPunk#7804 | 7,560,000 |
| CryptoPunk#3100 | 7,510,000 |
| Stay Free (Edward Snowden, 2021) | 5, 270, 000 |
| Save Thousands of Lives | 5, 110, 000 |
| Mona Money Matrix | 3, 020, 000 |

| 市场 | 交易次数 | 交易量$ |
|---|---|---|
| NBA Top Shot | 402,900 | 611,850,000 |
| OpenSea | 135, 247 | 610, 770, 000 |
| CryptoPunks | 3, 232 | 356, 660, 000 |
| Rarible | 56, 763 | 159, 380, 000 |
| Axie Infinity | 80, 491 | 131, 800, 000 |

*来源：DappRader（数据截止 2021 年 6 月 22 日）图片：Gate.io 研究院*

该领域既有大众消费品，又有艺术品等小众收藏品，横跨范围极广。发展的空间与传统市场消费品一样，具备延续、扩展性，是一个将会非常多元化并且多跨界的领域。

## 发展限制条件

DeFi 和 NFT 主要是资本运作的结果，其发展限制条件或者说行业主要风险大致可分为市场风险和技术风险。

市场风险在于加密资产的高波动性，币价的涨跌直接关系着 DeFi 和 NFT。比如对于 DeFi 而

言，抵押品跌破临界点，某些资产突然暴跌可能引起连锁反应，并强制平仓，也就是历年都会发生的大规模合约爆仓。而对于 NFT 而言，市场的暴跌可能会影响手中 NFT 的价值认可，造成有价无市的情况。

技术风险一方面在于欺诈者和黑客攻击等安全性问题，另一方面在于预言极喂价问题，黑客攻击或通过来自外界的虚假数据进行操纵，从而影响相关资产。

#### 3.4.2.2 应用技术发展可行性

##### 应用范围内企业发展典型路线图

纵观区块链应用领域区块协作、数据处理、安全与隐私、资产/数据非同质化等主要倚靠技术的项目，其企业的发展路线可归纳为技术完善与生态搭建两方面。项目早期在去中心化、性能和安全性三方面上择其重点进行技术突破与完善，中后期发展企业特色并增进“三方面”的权衡，同时以生态搭建为主扩大商业与扩展经济模式。

区块链行业相较传统市场募资难度更低，产业更新，市场关注度更高，相关项目较容易完成早期发展，本报告认为未来发展的重点将在中后期如何将发展延续与将企业存续下去。

以 ADA 和蚂蚁链为例：

**Cardano**

Cardano 从开发模型重构区块链开始，首先实现网络的平稳将系统核心更加去中心化，然后

开始将开发的重点放在生态/DAPP 的搭建上，允许技术和非技术用户都在网络上创建并执行智能合约，开展大规模 DAPP 平台生态的营造。

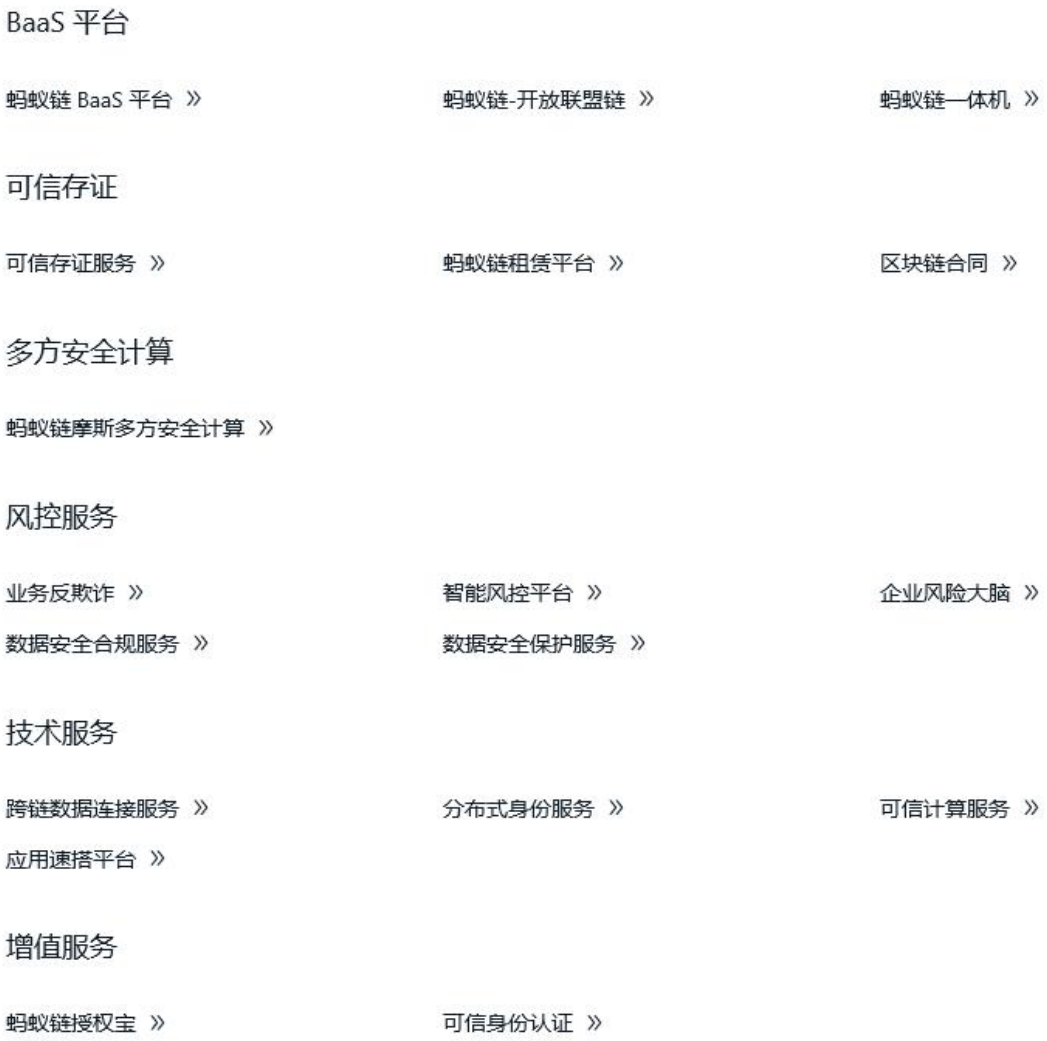

*来源：ADA 官网，图片：Gate.io 研究院*

Cardano 规划的未来是在生态大规模搭建成功之后，踏入“Basho”和“Voltaire”时期，即同以太坊一样具备生态之后开始继续需求“三方面”权衡上的突破，Cardano 的第一步在性能上的优化——提高扩展性和互操作性（重点发展在侧链技术），第二步将回归去中心化——让系统的运营更加社区自治更加去中心化。从路线图上来看，Cardano 未来的规划与以太坊类似，并未突破以太坊的进度，其技术上发展的重点按去中心化→性能→性能→去中心化的顺序在进行。

**蚂蚁链**

蚂蚁链是个典型的区块链技术产品开发企业案例，目前开发的产品除了前文提及的区块协作方面的联盟链，还涵盖了本文所探讨的其他三个方面——数据处理、安全与隐私、资产/数据非

同质化，是一个全方位的区块链产品平台。




*来源：antchain*

根据蚂蚁链的商业路线图表明，其打造全方位的技术产品的同时，逐步搭建中国境内与国际接轨的大规模生态。其发展路线印证了生态搭建对于区块链技术发展的重要性。


*来源：antchain*

## 发展限制条件

综合 3.3 与 4.2.2 中的调研，区块链应用技术层面的发展存在两方面的限制：

首先是在去中心化、性能和安全性上的权衡。目前公链龙头以太坊完成网络稳定环境之后，开始试图在不降低安全性的同时寻求性能上的突破——扩容。而 ADA 经历和以太坊类似的发展之后，发展的重点在利用侧链技术实现互操作性同时更加提升性能，而其最终的路线将再度回归去中心化的议题。技术在这三方面上的权衡将继续是未来的一个重要攻克难题。

其次是生态搭建。项目完成自有技术后，生态的大小将决定项目发展潜力的大小。2.1 中数据显示，同时期起步、同样是技术发展重点在跨链的项目 DOT 和 CKB，搭建出生态大小的不同让二者的市值排名目前分别在第 8 位和第 111 位（根据 coinmarketcap 统计）。而如何公链赛道一样，项目越来越多，技术形成一定的模板，技术突破要求越来越高，新进项目进入市场的难度加大，生态搭建或将成为主要的限制条件。

## 4 总结

比特币本身的技术特点和缺陷，再加上以太坊为主的公链生态，打造出了现有的区块链应用领域。所以现有区块链价值的体现，一方面在于对比特币技术的延续，另一方面在弥补比特币技术的缺陷。另外，公链围绕比特币已形成多元化的发展，公链系统的发展趋势，其一是围绕去中心化、性能和安全性三方面的进行权衡，并辅以对任意区块链和任意资产间的跨链技术；其二是特色化的技术开发道路。而特色化的公链技术发展道路又可分为三个方面：一是充足资本，扩大规模与市场运营，在去中心化、性能和安全性中发展重点技术，提供供应，寻找需求，进而抢夺市场；二是开创自有领域，创立特色的企业愿景；三是将区块链与其他高新技术结合，创建其他新进企业难以实现的技术。

本文认为，区块链应用延续比特币技术和公链技术之后，资金层面运作的重点在 DeFi 和 NFT，技术发展的重点在区块协作、数据处理、安全与隐私、数据或资产非同质化四个方面。在未来加密货币和区块链价值共识的增强将提高 DeFi 和 NFT 生态的参与率和使用率，layer2 的技术改进将进一步降低二者的交易成本，DeFi 项目中支付和资产上链具有更好的前景，NFT 在短

期价格泡沫后的资产价值发现回归理性。在技术层面，区块协作可以将跨域协作的概念延升到行业的可重构开放式商业模式，未来经济发展的核心将可能从“资本”转移到“资本+数据”的模式；数据处理的发展将主要在泛金融应用和产业供应链两个领域，前者发展的关键在性能高 TPS 和跨链交互上，后者发展的关键在数据处理的及时与高效性上；安全与隐私的完善可以结合其他行业技术比如人工智能，或者将需求性能和安全性的链或者项目分开处理；资产/数据非同质化还需将价值锚定机制完善，并可以将通证资产实际价值落地且缩小地域间的价值差异。

本报告在最后也试图回溯目前区块链应用的关键成功因素，佐证发展趋势的可行性和归纳发展即将面临的限制条件。然而区块链作为新兴行业，资本运作模式和技术更新迭代都在以极其迅猛的速度发生，对于区块链应用的想象和发展空间或许也在时刻发生着变化，所以本文只能以现有主要应用进展和发展现状展开想象，无法做到全景复盘与深度预测。

## 5 参考资料

1. Dominic Williams（2019）. DFINITY In A Nutshell — A Non Technical Introduction. DfinityFun. Available at：https://www.chainnews.com/articles/957331367088.htm

2. DfinityBase （2021）。从“不可能三角”谈 DFINITY 和以太坊。Available at：https://www.bishijie.com/shendu/196596.html

3. 于戈，聂铁铮，李晓华，张岩峰，申德荣，鲍玉斌（2019）。区块链系统中的分布式数据管理技术-挑战与 展望。计算机学报 （CHINESE JOURNAL OF COMPUTERS）。Available at：

http://cjc.ict.ac.cn/online/cre/yge7-20191030123019.pdf

4. 孟小峰，刘立新（2020）。区块链与数据治理。《中国科学基金》2020 年第 34 卷第 1 期。

5. 张奥，白晓颖（2020）。区块链隐私保护研究与实践综述。软件学报。Available at：http://www.jos.org.cn/html/2020/5/5967.htm#outline_anchor_56

6. Cardano 白皮书。Available at：https://docs.cardano.org/introduction/

7. Polkadot 白皮书。Available at：https://polkadot.network/PolkaDotPaper.pdf

8. Solana 白皮书。Available at：https://solana.com/solana-whitepaper.pdf

9. The internet Computer 白皮书。Available at：https://sdk.dfinity.org/docs/interface-spec/index.html

10. Matic Network 白皮书。Available at：https://github.com/maticnetwork/whitepaper

11. Algorand 白皮书。Available at：https://www.algorand.com/technology/white-papers

12. 任万盛（2020）。2020 年全球区块链专利排行榜 TOP100，中国 52 家公司上榜。零壹智库。Available at：https://www.01caijing.com/article/266206.htm

13. 前瞻产业研究院（2021）。2021 年中国区块链行业市场现状、竞争格局及发展趋势。Avalaible at：https://bg.qianzhan.com/trends/detail/506/210319-1035cd0b.html

14. Stefan Grasmann（2020）. Yield Farming-large holders' chartered? Avalaible at：https://www.ccvalue.cn/article/451558.html

15. Modesta Jurgelevičienė，Ian Kane（2020）. 2020 Dapp Industry Report. DappRader. Available at：https://dappradar.com/blog/2020-dapp-industry-report

# 6 附录

| | ADA | DOT | SOL | MATIC | ICP | ALGO | GateChain |
|---|---|---|---|---|---|---|---|
| 独立技术 | Ouroboros 权益证明共识协议：该 PoS 协议的核心是权益池，即由权益池运营商运行的可靠服务器节点，ada 持有者可以将他们的权益委托给这些节点。权益池用于确保每个人都可以参与协议，无论技术经验或可用性如何以保持节点运行。这些权益池专注于维护并在一个实体中持有各种利益相关者的联合权益。 | NPOS：减少寡头效应，从较小的集合中选择验证人，从而使较小的持有者可以提名验证人来运行基础结构，同时仍然可以获得系统的收益，而无需运行自己的节点。 | POH：所有的链上操作，都不需要特意等到出块时间再来进行验证而可以直接去证明链上操作的历史记录，验证者节点始终保持满负荷运行，所以在处理交易的效率上会高出很多。 | Polygon chains：两种以太坊兼容网络，”安全即服务“网络与独立网络。安全链提供高水平的安全性，但要牺牲部分独立性和灵活性。独立链提供了最高水平的独立性和灵活性，但有时需要权衡验证者池的建立。 | Threshold Relay Technology：阈值签名接力可以让任何一个能建立「虚拟计算机」的安全抗攻击网络中，让大量客户端节点共同协作的唯一方法，是借助密码学来生成随机数。阈值签名接力使用加密技术来创建随机性，按照几乎不可摧毁、不可操纵、不可预测的方式，按需选择相应的网络参与者。DFINITY 网络的参与者通过阈值签名接力会生成一个确定性的可验证随机函数（VRF），为整个区块链网络上的协作、运算提供支持。 | ASA：Algorand 标准资产，用于发币，用于替代金融资产。 | Vault Account：首创新账户模型，具备资金被盗找回、私钥丢失可恢复等功能，高安全性的资金存储功能账户 |
| | Haskell：函数式编程语言不易出现歧义和人为错误，从数学角度来看，更易于测试和验证。 | Wasm 元协议：首创无需硬分叉就可以施行链升级。 | Turbine：区块广播技术，一个区块传输时，它会分成很多个小数据包，然后广播到大量的随机节点。 | 可组合的四层技术：Ethereum layer，Security layer，Polygon networks layer，Execution layer，并可自由组合。 | USCIDs ：对跨节点的状态存储进行分区(切分)，要求每一个客户端，维护分配给他们的唯一的状态数据的副本。 | 原子交易：用于在没有中间人的情况下实现代币的交换。 | RTM（Revokable Transaction Model）：使保险账户（Vault Account）支持转出资金可撤回功能 |
| | RINA，递归网络架构（Recursive InterNetwork Architecture）：解决每个节点支撑通信的网络带宽问题。 | 平行链：将分片做到极致，变成一条链，不同的链之间互通形成波卡特有的跨链系统。 | Gulf Stream：每个验证者都知道未来领导者的顺序，验证者会提前将交易转发给预期的领导者，让验证者提前执行交 | | NNS：区块链神经系统可以访问虚拟机中的特殊操作码。这允许 BNS 冻结、解冻和修改其他独立的软件对象（智能合约），并且可以配置用户运 | 无状态合约和有状态智能合约：如果仅仅需要简单的逻辑判断功能，那么无状态合约 | EVM 模块：用户无需跨链迁移资产即可使用智能合约，兼容“ETH”虚拟机智能合约代码，任何在以太坊 |

| | | | | |
|---|---|---|---|---|
| | 易，减少确认时间，减少对验证者的内存压力。 | 行的 DFINITY 客户端软件。 | 的能够快速低成本的完成这一过程；而如果需要在链上存储一些数据，那么就需要使用有状态智能合约来实现。 | 上正常运行的智能合约，都可以无缝迁移到“GateChain”上运行 |
| | sealevel：构建横向扩展的技术方案，是并行交易处理的引擎。<br><br>Pipelining：在内核级别进行数据获取、在 GPU 级别进行签名验证，在 CPU 级别进行存储，在内核空间进行写入，将 TPS 提高到 5 万。 | | | Vault Account：首创新账户模型，具备资金被盗找回、私钥丢失可恢复等功能，高安全性的资金存储功能账户<br>RTM（Revokable Transaction Model）：使保险账户（Vault Account）支持转出资金可撤回功能 |

声明

因出具该研究报告，特做出如下声明：

- 本研究报告是内部成员通过尽职调查和客观分析得出的结论，旨在对区块链应用价值进行总结，并不能完全以此来预测相关项目代币的价格影响。
- 本研究报告非衡量研究对象本身价值、以及其相关项目发行代币价值的工具，不构成投资者做出最终投资决策的全部依据。
- 本研究报告引用的项目资料来源自内部认为可靠、准确的渠道，因为存在认为或机械错误，信息均以获取时态为准、内部成员对研究报告中所依据的相关资料的真实性、准确度、完整性以及及时性进行了必要的核查和验证，但对其不做任何明示或暗示的陈述或担保。