总而言之：

1、随着铭文的兴起，比特币网络现有的应用层无法支撑市场活动，是当前比特币生态发展的主要焦点。

2、比特币主流的Layer2解决方案有闪电网络、侧链、Rollup三种

闪电网络通过建立链下支付通道来实现点对点支付，通道关闭后在主网上进行结算。侧链通过特定地址或者多重签名地址将BTC资产锁定在主网上，同时在侧链上铸造等值的BTC资产。Merlin Chain能够支持全链多种类型的铭文资产，以Bitmap生态系统为后盾，其TVL已达到近40亿美元。BTC Rollup基于Taproot电路，可以模拟链上智能合约，并在比特币主网络之外执行打包和计算操作。B2 Network 处于这一实施的最前沿，拥有超过 2 亿美元的链上 TVL。

3. 专门为比特币构建的跨链桥并不常见。还有更多与主流区块链集成的多链和全链桥接器，其中之一就是 Meson.Fi，它已经与多个比特币 Layer2 建立了关系。

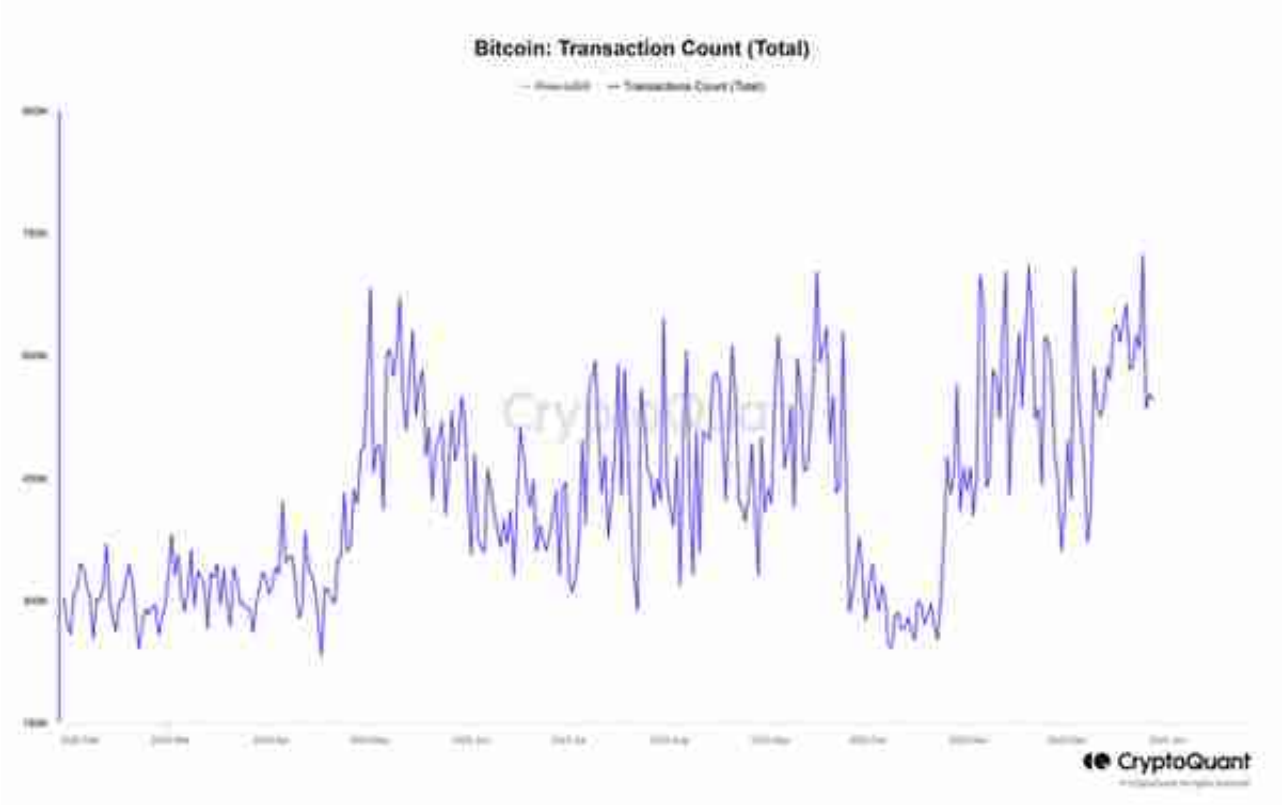
4. 比特币网络上的稳定币协议大多以超额抵押的形式实现，并支持其他 DeFi 协议，为用户带来更多收益。

5. 比特币生态系统中有各种各样的 DeFi 项目，从从其他链迁移而来的，到当前发展热潮期间建立在原生比特币网络上的，以及上一次牛市期间建立并部署为 DeFi 的项目。侧链。总体来说Alex提供了最丰富的交易产品和最流畅的交易体验，但Orders Exchange的成长上限较高。

6. 比特币将成为本轮牛市周期的重要叙事。有必要密切关注比特币生态系统各个垂直领域的顶级项目。

一、背景

随着Ordinals协议导致铭文资产泛滥，曾经缺乏智能合约、开发效率低下、缺乏基础设施和扩容能力的比特币网络正在经历链上数据热潮（参考Kernel之前的文章）研究文章：Can RGB Replicate The Ordinals Hype了解更多详情）。与以太坊网络首次建立时发生的情况类似，格式化的文本、图像甚至视频都被打乱为 4MB Tapscript 脚本，而这些脚本永远不会被执行。虽然链上活动的激增促进了比特币生态系统和基础设施的增长和发展，但它也造成了交易量的激增和网络的巨大存储负担。此外，对于种类繁多的铭文，简单的转账已经不能满足用户的交易需求，用户期待比特币能够推出丰富的衍生品交易服务。因此，比特币应用层的开发现在就变得比较紧迫。



来源：CryptoQuant

2. 比特币 Layer2

与以太坊上以 Rollup 为主的 Layer2 不同，比特币的 Layer2 解决方案仍然很模糊。比特币无法用自己的脚本语言编写智能合约，智能合约的发布必须依赖第三方协议，因此将类似的解决方案应用于比特币并不能保证与以太坊 Rollup 相同级别的安全性。因此，比特币存在多种 Layer2 解决方案，包括闪电网络、侧链、基于 TapScript 的 Rollup 等。

2.1 闪电网络

闪电网络是最早的比特币Layer2解决方案，由Gregory Maxwell于2015年12月首次提出。闪电网络堆栈，称为BOLT，由Lightning Labs于2017年1月发布。此后，它经历了升级和改进。闪电网络允许用户进行任意规模和数量的点对点、链下支付通道转账，无需支付任何费用，直到闪电网络关闭。届时，所有先前的交易均通过单笔交易进行结算。由于使用链下通道，闪电网络有潜力实现高达 1000 万次 TPS（每秒交易量）。但链下渠道存在中心化风险。为了在两个地址之间成功进行交易，必须直接或通过第三方建立链下通道。此外，交易期间双方必须在线才能安全执行。

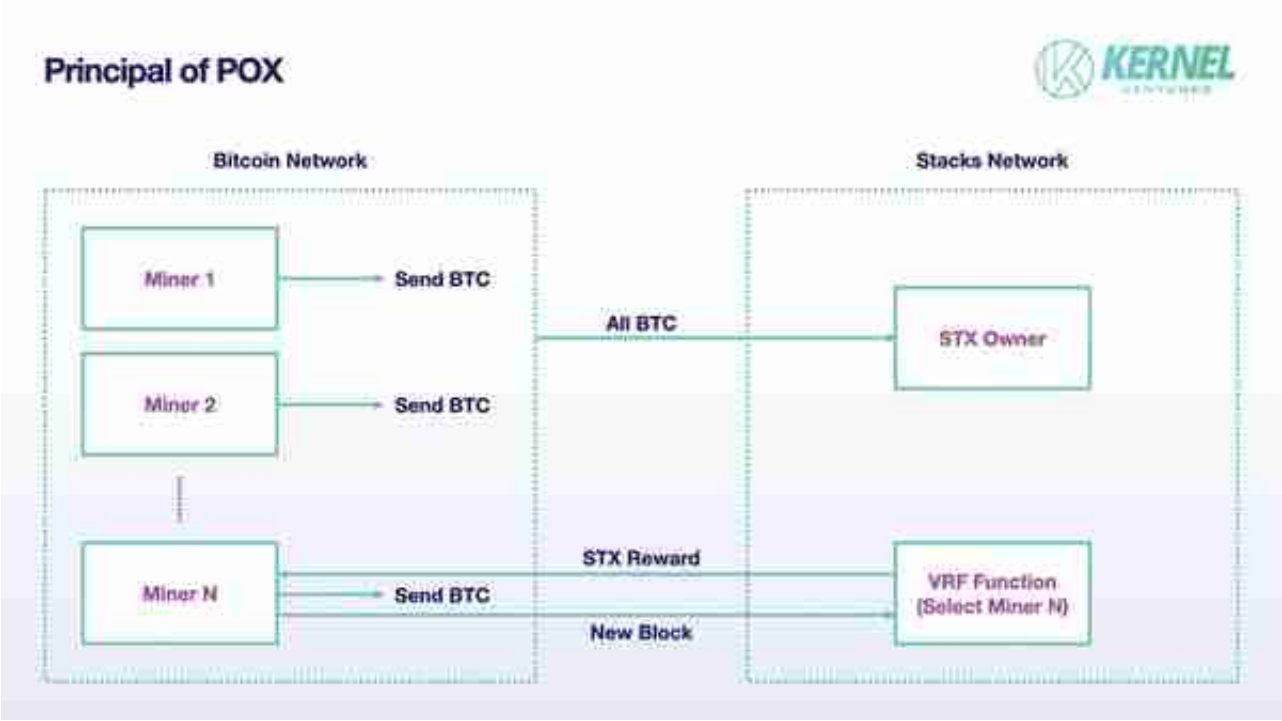
资料来源：Kernel Ventures

2.2 侧链

比特币的侧链解决方案与以太坊类似，在新链上发行与比特币 1:1 挂钩的新代币。这条新链将不受比特币网络的交易速度和发展瓶颈的限制，允许以更快的速度和更低的成本转移与比特币挂钩的代币。侧链方案想必继承了主网的资产价值，但不继承主网的安全性，所有交易都在侧链上记录和确认。

2.2.1 堆栈

Stacks 2.0于2021年发布，用户可以在比特币主网上锁定BTC并在Stacks上获得等值的SBTC资产，但他们在侧链上的交易需要支付Stacks原生代币STX作为gas。与以太坊不同，比特币网络不允许使用可以有效管理锁定的 BTC
的智能合约地址。因此，锁定的 BTC
会被发送到特定的多重签名地址。释放过程相对简单，需要向 Stacks 上的 Burn-Unlock 合约请求销毁 Stacks 上的 SBTC，并将锁定的 BTC 发送回原始地址，因为 Stacks 网络允许使用 Clarity 语言进行智能合约开发。Stacks网络的区块释放过程采用POX共识机制。比特币矿工向区块机会发送 BTC 出价，出价越高，矿工的权重就越高。最终，通过特定的可验证随机函数选出获胜者，将区块打包到Stacks网络上，并获得相应STX形式的奖励。同时，这部分竞价BTC将以SBTC的形式分发给STX代币持有者作为奖励。



资料来源：Kernel Ventures

此外，Stacks预计将在4月份推动中本聪升级，其中将包括对其开发语言Clarity的优化，以降低开发者的门槛。其次，Stacks优化了网络的安全级别，确认Stacks上的交易在比特币主网上进行结算，将Stacks的安全性从侧链升级到与比特币主网相同的Layer2。最后，Stacks 还对其出块率进行了重大改进，在测试阶段达到每个块 5 秒（而当前阶段每个块 10-30 分钟）。如果中本聪升级成功，Stacks可以缩小甚至消除以太坊上Layer2的差距，这应该会引起很多关注并刺激生态系统的发展。

2.2.2 RSK

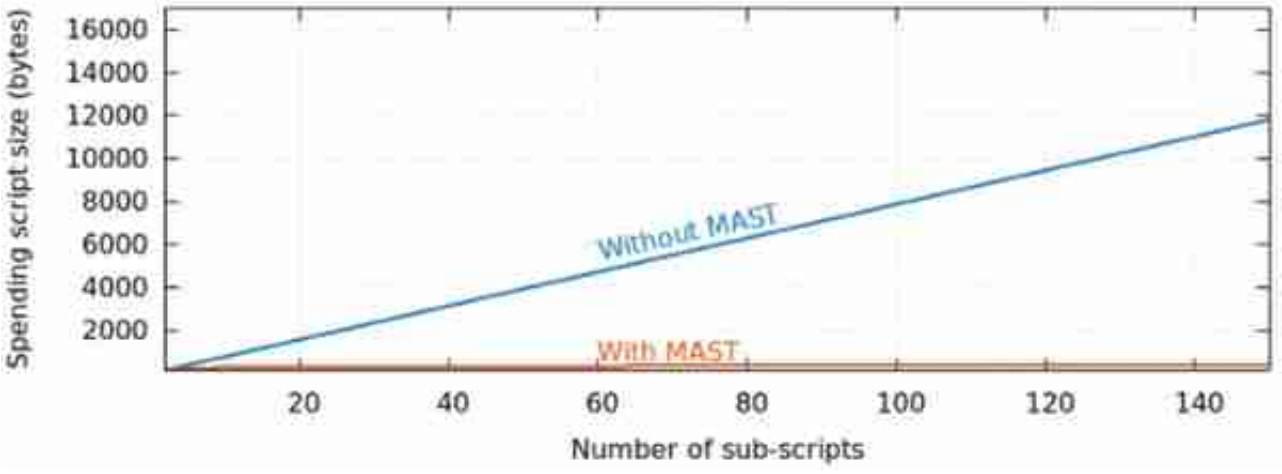
RSK（RootStock）是一条没有原生代币的比特币侧链，侧链上的交易目前在比特币上处理。用户可以通过内置的 PowPeg 协议在 RSK 上以 1:1 的比例将主网上的 BTC 兑换为 RBTC。RSK 也是一条 POW
链，但随着合并挖矿机制的引入，比特币矿工的基础设施和设置可以完全应用到 RSK 挖矿过程中，从而降低了比特币矿工参与 RSK
挖矿的成本。到目前为止，RSK 上的交易速度是主网上的三倍，成本是主网上的 1/20。

Parameter	Bitcoin	RSK
Average block confirmation time	10 minutes	30 seconds (miners can lower it to 15 seconds)
Suggested confirmation time for exchanges	30 minutes (3 blocks)	60 minutes (120 blocks) with current merge-mining hash rate (40%).
Max. transactions per second	3.3 tps (assuming an average size tx)	10 tps (external transactions, as of January 2019) 20 tps (internal transactions)
Current average transaction cost	24 ¢	0.46 ¢

资料来源：RSK 白皮书

2.2.3 BEVM

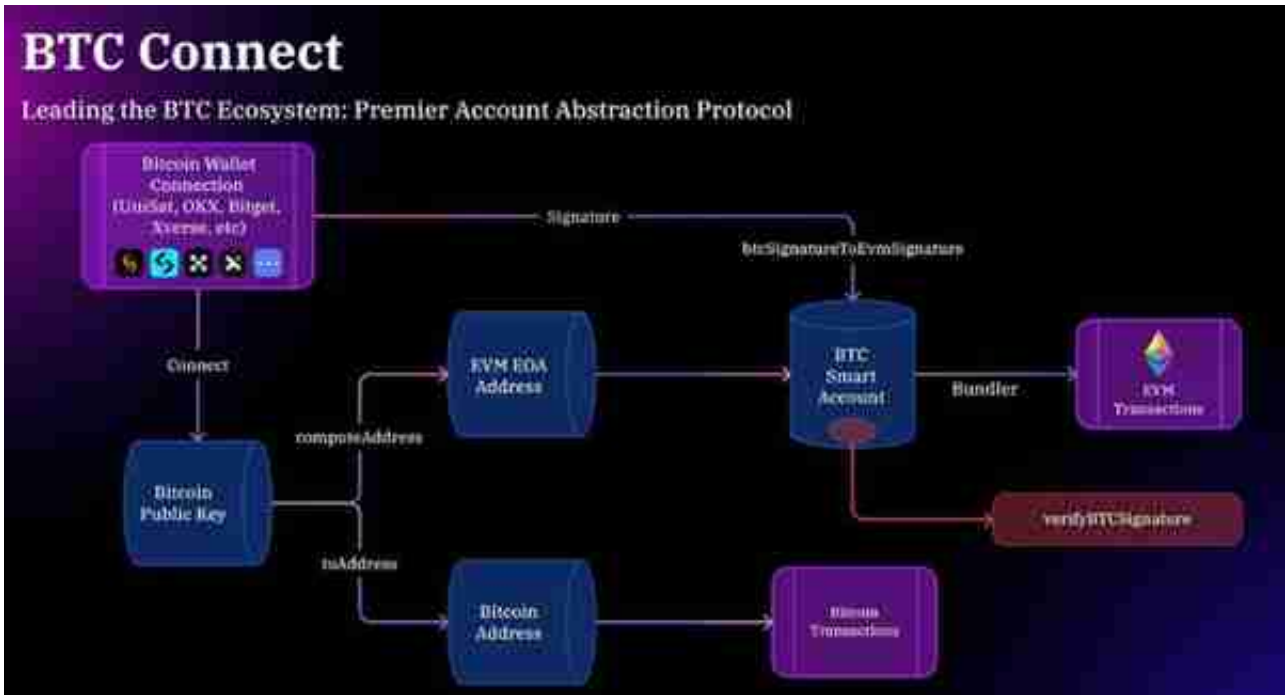
BEVM 是一个兼容 EVM 的 POS
侧链，尚未发行自己的原生代币。它在比特币网络上使用 Schnorr
的多重签名算法，将传入的资产存储在由 1,000
个地址控制的多重签名脚本地址中，这对应于 BEVM 上的 1,000 个 POS
验证者。通过在TapScript区域编写MAST（Merkelized Abstract Syntax Tree）脚本可以实现资产的自动化控制，其中程序被描述为多个独立的块，每个块对应一部分代码逻辑，不需要脚本中存储大量逻辑，仅存储每个块的哈希结果。这大大减少了需要存储在区块链上的代码量。当用户将BTC转移到BEVM时，这部分BTC会被脚本程序锁定，锁定的BTC只有经过超过2/3的验证者签名才能解锁并发送回相应地址。BEVM 与 EVM 兼容，因此可以对最初构建在以太坊上的 dApp
进行经济高效的迁移，与上述与 BTC 挂钩的资产进行交易，同时将其用于支付
Gas 费用。



来源：BTCStudy

2.2.4 梅林链

Merlin Chain 是一条兼容 EVM 的比特币侧链，允许通过 Particle 网络生成的比特币地址直接连接到网络，并生成唯一的以太坊地址。它还可以直接连接到具有以太坊帐户的 RPC 节点。Merlin Chain目前支持BTC、Bitmap、BRC-4??20和BRC-20资产的跨链转移。BRC420协议是Bitmap资产社区基于Merlin Chain等递归铭文开发的，整个社区还提出了RCSV的递归铭文矩阵、基于递归铭文的Bitmap Game元宇宙平台等项目。



来源：Merlin 文档

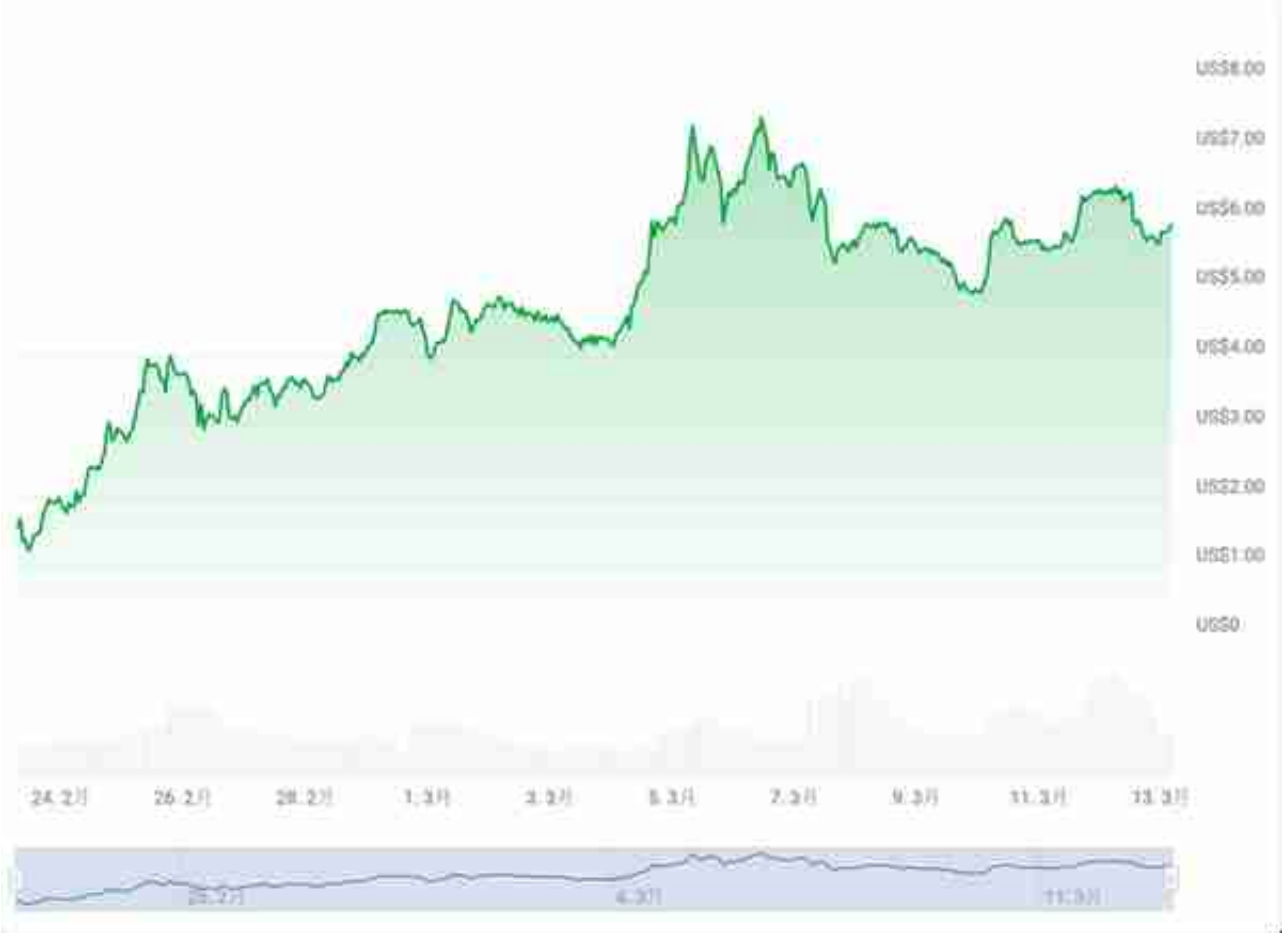
Merlin Chain 于 2 月 5 日上线，随后进行了一轮 IDO 和质押奖励，分配了 21% 的治理代币 MERL。直接且大规模的空投吸引了大量参与者，Merlin Chain 的 TVL 目前已超过 30 亿美元，比特币的链上 TVL 超过
Polygon，在所有区块链中排名第六。

Name	Category	TVL	1d Change	7d Change	1m Change
1 Merlins Seal 4 chains	Farm	$2.182b	-0.10%	+16.75%	+273%
2 B2 Buzz 4 chains	Farm	$359.97m	+12.09%	+31.44%	
3 Lightning Network 1 chain	Payments	$327.12m	+0.28%	+14.07%	+38.32%
4 Thorchain 9 chains	Dexes	$102.34m	+5.00%	+50.40%	+61.71%
5 BiFi 6 chains	Lending	$26.36m	+0.27%	+13.94%	+45.11%
6 ckBTC 1 chain	Cross Chain	$13.85m	-2.63%	+14.56%	+16.27%
7 Maya Protocol 6 chains	Cross Chain	$10.59m	+2.15%	+37.95%	+55.91%
8 BoringDAO 20 chains	Cross Chain	$3.02m	+0.54%	+14.41%	+45.24%
9 HOPE Collateral 2 chains	Cross Chain	$1.46m	-0.35%	+14.28%	+45.25%
10 BitStable Finance 3 chains	CDP	$208,085	-2.60%	+61.26%	+167%

来源：DefiLlama

在People's Launchpad的IDO期间，用户可以质押Ally或超过0.00025 BTC来获得奖励积分，可以兑换MERL，累积奖励质押限额为0.02 BTC，相当于460个MERL代币。本轮分配规模较小，仅占MERL总量的1%。然而，考虑到今天的场外交易价格为 2.90 美元 MERL，它已经创造了超过 100% 的回报率。在第二轮质押激励中，Merlin分配了其总代币的20%，允许用户通过Merlin的印章将BTC、Bitmap、USDT、USDC以及部分BRC-20和BRC-4??20资产质押到Merlin Chain上。用户在Merlin上的资产将以美元为单位进行每小时快照，最终的日均价乘以10,000就是用户获得的积分数量。第二轮质押基于Blast的团队模式，用户可以选择成为领导者或团队成员。领导者将收到邀请码并与团队成员分享。

Merlin在当前比特币Layer2生态中相对成熟，解放了Layer1资产的流动性，并允许比特币以更低的成本在Layer2上转账。Merlin背后的Bitmap生态系统非常庞大，技术也比较完善，从长远来看很可能会有良好的发展。梅林的股份回报率很高。除了MERL的预期回报外，还有机会获得相应的Meme或项目空投的其他代币，例如官方空投的Voya代币。质押超过0.01 BTC即可获得90个Voya代币空投，自项目上线以来，Voya代币价格不断上涨，最高达到发行价的514%。Voya目前报价为5.89美元，按照质押时比特币均价5万美元计算，收益率高达106%。



来源：CoinGecko

2.3 汇总

2.3.1 比特虚拟机

BitVM 基于比特币 Layer2 的 Optimistic Rollup。与以太坊上的 Optimistic Rollup 类似，交易者首先将交易发送到比特币网络上的 Layer2，在那里进行计算和打包，然后将结果发送到 Layer1 上的智能合约进行验证，同时给验证者时间来挑战证明人的陈述。然而，比特币不支持原生智能合约，因此实现起来并不像以太坊的 Optimistic Rollup 那么简单。整个过程涉及到比特值承诺、逻辑门承诺和二进制电路承诺，下面可以概括为BVC、LGC和BCC。

BVC（Bit Value Commitment）：BVC本质上是一个电平结果，只有两种可能，0和1，类似于其他编程语言中的Bool类型变量。比特币是一种基于堆栈的脚本语言，不存在 bool 类型，因此在 BitVM 中使用字节码组合来模拟它。在BVC中，用户需要先提交一个输入，只有当哈希结果等于HASH1或HASH0（其中HASH1的输出为1，HASH2的输出为0）时，比特币网络才会对输入进行哈希并解锁脚本。在下

面的部分中，我们将把整个代码片段总结为 OP_BITCOMMITMENT 操作码，以简化描述过程。

```
<Input Preimage of HASH>
OP_IF
    OP_HASH160      //对用户的输入进行哈希
    <HASH1>
    OP_EQUALVERIFY      //输出 1 if Hash (input) == HASH1
     < 1 >
OP_ELSE
    OP_HASH160      //对用户的输入进行哈希
    <HASH2>
    OP_EQUALVERIFY      //输出如果Hash (输入) == HASH2
     < 0 >则为0
```

LGC（Logic Gate Commitment）：计算机中的所有功能本质上都是一系列布尔门的组合，可以简化为一系列与非门。也就是说，如果我们能够通过字节码来模拟比特币网络中的与非门，那么我们本质上就可以实现任何功能。尽管比特币没有直接实现 NAND 操作码，但它确实有一个 AND 门 OP_BOOLAND 和一个 NOT 门 OP_NOT，可以将它们叠加以重现 NAND。对于从 OP_BITCOMMITMENT 获得的两个输出电平，我们可以用 OP_BOOLAND 和 OP_NOT 操作码组成 NAND 输出电路。BCC（Binary Circuit Commitment）：基于LGC电路，我们可以在输入和输出之间构建特定的门关系。在BCC门电路中，这个输入来自TapScript脚本中对应的hash-primary image，不同的Taproot地址对应不同的门，我们称之为TapLeaf，众多的TapLeaf组成一个Taptree，作为输入到 BCC 电路。

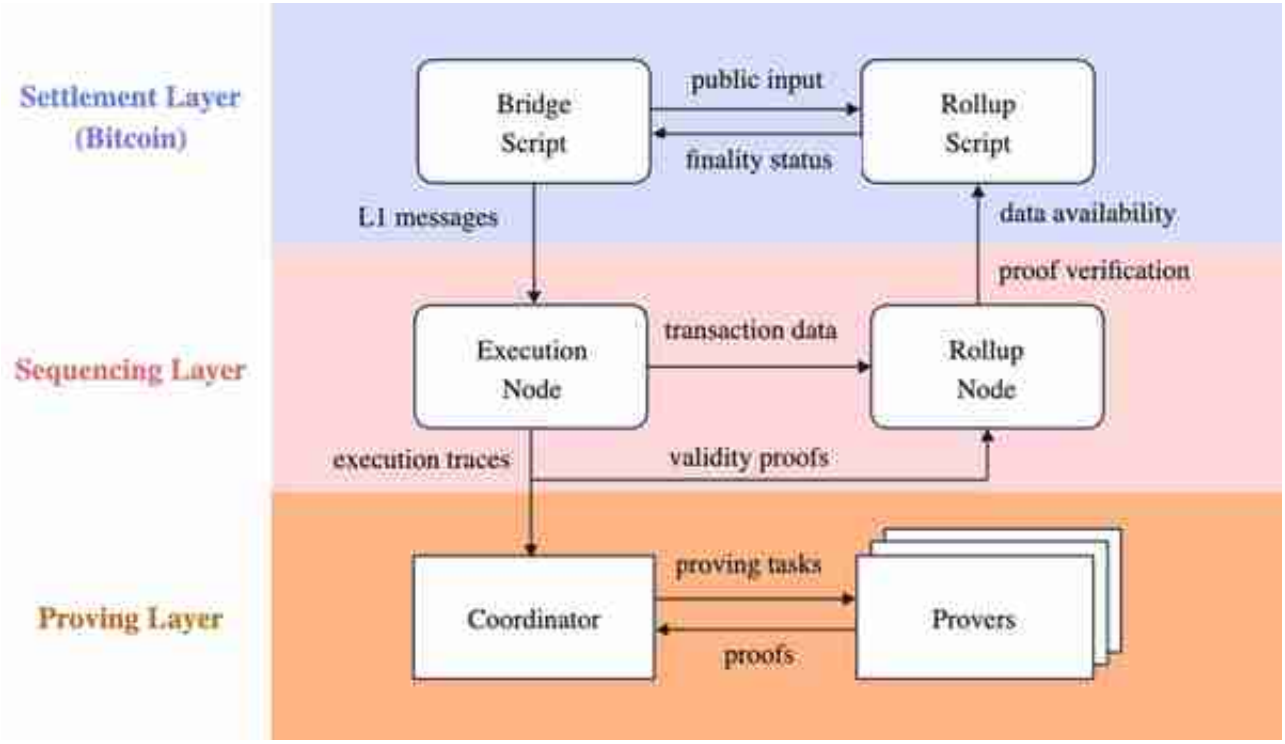
来源：BitVM 白皮书

理想情况下，BitVM 证明者会在链外编译和计算电路，并将结果返回到比特币网络以供执行。然而，由于链下过程不是由智能合约自动化，为了防止证明者进行欺诈交易，BitVm 要求网络上的证明者进行挑战。验证者首先重现某个 TapLeaf 的输出，然后将其与证明者提供的其他 TapLeaf 结果相加，作为驱动电路的输入。如果输出为假，则挑战成功，这意味着证明者提供了欺诈消息，反之亦然。然而，要完成这个过程，挑战者和证明者之间需要预先共享Taproot电路，并且只能实现单个证明者和单个验证者之间的交互。

2.3.2 中本聪虚拟机

SatoshiVM 是适用于比特币的 EVM 兼容 zkRollup Layer2 解决方案。SatoshiVM 上智能合约的实现与 BitVM 上相同，使用 Taproot 电路来模拟复杂的功能。SatoshiVM分为三层，结算层、排序层和证明层。结算层，又称比特币主网，负责提供DA层，存储交易的Merkle Roots和零知识证明，并通过Taproot电路验证Layer2打包交易的正确性来结算交易。排序层负责打包和处理交易，并将交易结果连同零知识证书返回主网，证明层负责为从排序层收到的任务生成

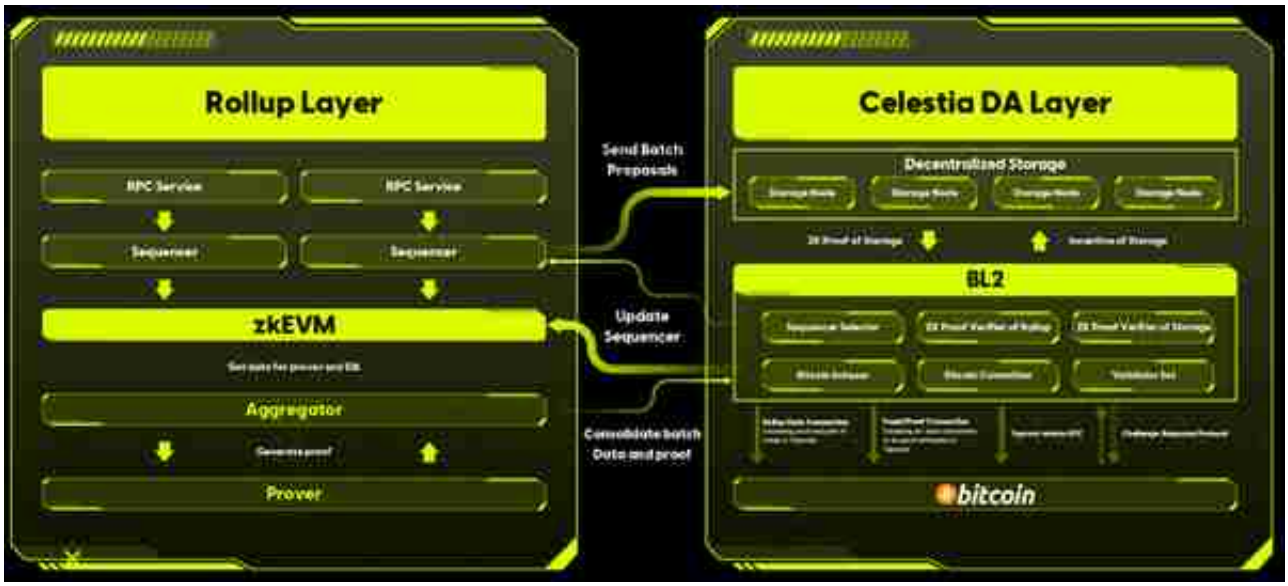
零知识证书并将它们传递回排序层。



来源：SatoshiVM 文档

2.3.3 BL2

BL2 是基于 VM 通用协议（官方预配置的 VM 协议，与所有主要 VM 兼容）的 zkRollup 比特币 Layer2。与其他zkRollup Layer类似，其Rollup Layer主要通过zkEVM打包交易并生成相应的零知识证书。BL2的DA层引入Celestia来存储批量交易数据，仅使用BL2网络来存储零知识证明，最后将零知识证明验证和少量验证数据（包括BVC）返回到主网进行结算。



来源：BL2.io

BL2的官方X账号每日更新，同时也公布了其发展计划和代币计划，将分配20%的代币给OG Mining，并于近期推出测试网。现阶段，与其他比特币 Layer2 相比，该项目相对较新，并且处于早期阶段，X 上只有 33,000 名关注者。值得关注，因为它引入了一些较新的概念，例如 Celestia 和比特币 Layer2。然而，网站上没有实际的技术细节，只有预期内容的演示，也没有该项目的白皮书。同时目标也相当大，比如比特币上账户的抽象、兼容主流虚拟机的VM协议等。团队是否能够实现这个目标还存在疑问，所以我们会考虑采取更加保守的做法。

来源：BL2的X账户

2.3.4 B2网络

B2网络是以比特币为结算层和DA层的zkRollup Layer2，其结构为Rollup Layer和DA Layer。用户交易首先在 Rollup Layer 中提交和处理，该 Rollup Layer 使用 zkEVM 方案执行用户交易并输出相关证明，然后将用户状态存储在 zkRollup Layer 中。批量交易和生成的零知识证明被转发到DA层进行存储和验证。DA层可以细分为三个部分：去中心化存储节点、B2节点和比特币主网。去中心化存储节点接收 Rollup 数据，并根据 Rollup
数据定期生成时空零知识证明，并将生成的零知识证明发送给 B2 节点，B2 节点负责数据的链下验证，然后验证完成后，将交易数据和相应的零知识证明记录在比特币主网上的TapScript中。B2节点负责确认ZKP的真实性并最终完成结算。

来源：B2网络白皮书

B2 Network 在 BTC Layer2 各大程序中影响力不错，X 上有 30 万关注者，超过了 BEVM 的 14 万和 SatoshiVM 的 16.6 万，这也是 Zk Rollup Layer2 的一个。同时，该项目已获得 OKX 和 HashKey 的种子轮融资，备受关注，链上 TVL 已超过 6 亿美元。

来源：bsquared.network

B2 Network 已推出 B2 Buzz，为了使用 B2 Network，您需要邀请链接。B2 Network采用与Blast相同的沟通模式，为新人和已经加入网络的人提供了强大的双向利益绑定，让他们有足够的动力来推广项目。完成关注官方X账号等简单任务后，即可进入质押界面，支持使用BTC、以太坊、BSC、Polygon四种链上的资产。除了比特币之外，铭文、ORDI 和 SATS 也可以在比特币网络上质押。如果你质押BTC，可以直接转移资产，而如果你质押铭文，则需要铭文和转让，需要注意的是，由于比特币网络上没有智能合约，资产本质上是多重签名的。锁定到特定的 BTC 地址。B2网络上质押的资产至少要到今年4月份才会释放，这期间质押获得的积分可以兑换用于虚拟挖矿的挖矿组件，其中BASIC矿机只需要10个组件即可激活，而ADVANCED矿机需要80多个组件。

官方公布了部分代币计划，代币总量的5%将用于奖励虚拟挖矿，另外5%将分配给B2网络上的生态项目进行空投。在通证经济公平性备受关注的当下，通证总量的10%很难充分调动社区的积极性。预计B2网络未来还会有其他质押激励或LaunchPad计划。

2.4 综合比较

在BTC Layer2的三种类型中，闪电网络的交易速度最快、交易成本最低，在实时支付和线下购买方面应用较多。然而，要实现比特币上应用生态的发展，在闪电网络上构建各种 DeFi 或跨链协议在稳定性和安全性方面存在一定难度，因此应用层市场的竞争主要集中在双方之间链和 Rollup。侧链方案不需要在主网上确认交易，并且有更成熟的技术方案和实施难度，因而拥有三者中最高的TVL。由于比特币主网缺乏智能合约，Rollup数据的确认方案仍在开发中，实际使用可能还需要一段时间。

资料来源：Kernel Ventures

3. 比特币跨链桥3.1 多位

Multibit是专门为比特币网络上的BRC20资产设计的跨链桥，目前支持BRC20资产迁移到以太坊、BSC、Solana和Polygon。在跨链桥接的过程中，用户首先需要将资产发送到Multibit指定的BRC20地址，并等待Multibit在主网上确认资产转移，然后用户才有权铸造该资产。其他链上对应的资产，要完成跨链桥接过程，用户需

要支付gas在其他链上铸币。在跨链桥中，Multibit 的互操作性最好，BRC20 资产数量最多，包括 ORDI 等十多种 BRC20 资产。此外，Multibit还积极拓展BRC20以外的资产跨链桥接，目前支持BTC原生稳定币协议Bitstable的治理代币和稳定币的Farming和跨链桥接。Multibit 处于 BTC 衍生资产跨链桥的最前沿。

Multibit支持的跨链资产，来源：Multibit的X账户

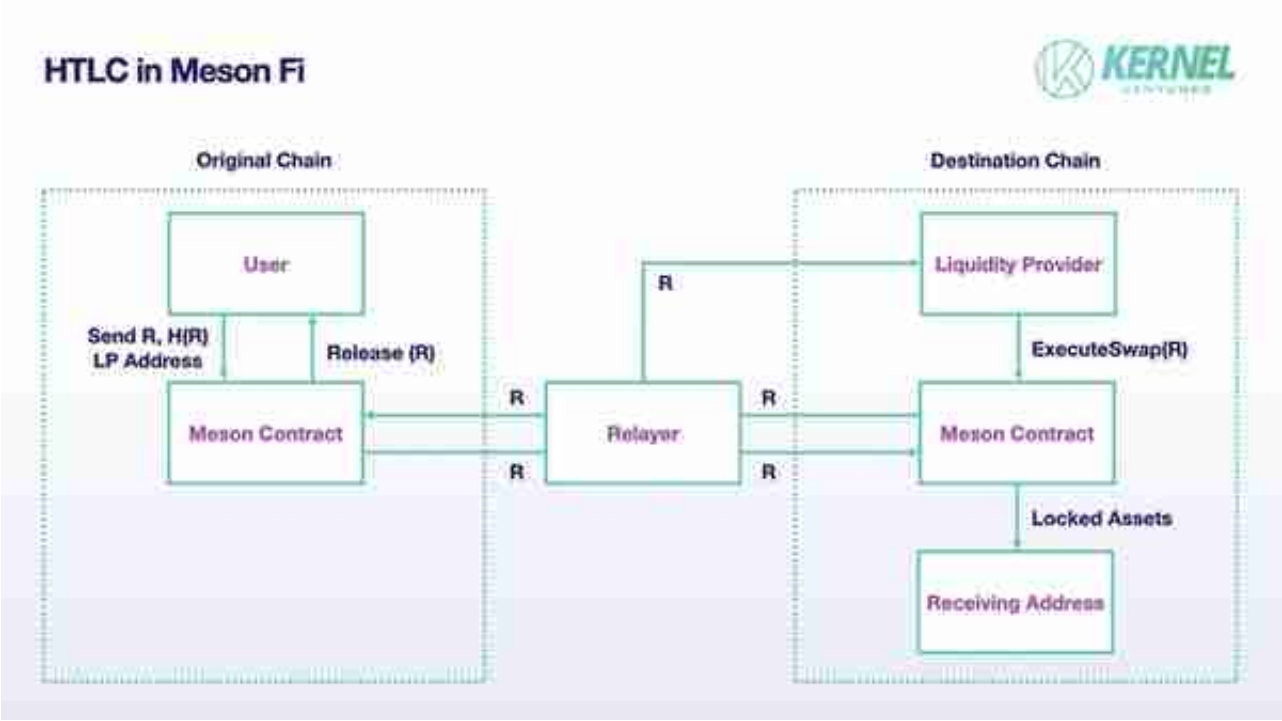
3.2 索比特

Sobit 是 Solana 和比特币网络之间的跨链协议。跨链资产主要是BRC20代币和Sobit的原生代币。用户将比特币主网上的BRC20资产抵押到指定的Sobit地址，并等待Sobit的验证网络验证用户可以在Solana网络上的指定地址铸造映射的资产。SoBit 验证网络的核心是一个基于验证器的框架，该框架需要多个可信验证器来批准跨链交易，从而提供针对未经授权传输的额外安全性。Sobit的原生代币为Sobb，可用于支付Sobit跨链桥的跨链费用，总计10亿枚。Sobb 在公平启动中分配了 74% 的资产。与目前比特币上的其他 DeFi 和跨链代币呈现上涨趋势不同，Sobb 的价格在短暂上涨之后就进入了下行周期，跌幅超过 90%，并没有随着 BTC 的上涨趋势而出现明显的上涨势头，这使得可能是索布选择垂直造成的。Sobit和Multibit的市场定位非常相似。但现阶段Sobit只能支持Solana的跨链，只有三种BRC20资产可以跨链桥接。与同样提供BRC20资产跨链桥接的Multibit相比，Sobit在生态系统和跨链资产的完整性方面都远远落后，因此在与Multibit的竞争中很难取得任何优势。

Sobb 的价格，来源：Coinmarketcap

3.3 介子Fi

Meson Fi是一个基于HTLC（哈希时间锁定合约）原理的跨链桥。支持BTC、ETH、SOL等17条主流链之间的跨链交互。在跨链过程中，用户在链下对交易进行签名，然后提交给 Meson Contract 进行确认，并锁定原链中相应的资产。Meson Contract 确认消息后，通过 Relayer 将消息广播到目标链。Relayer 共有三种类型：P2P 节点、中心化节点和无节点，P2P 节点安全性较好，中心化节点效率和可用性较高，无节点则要求用户在两条链上都持有一定的资产，用户可以根据实际情况选择情况。目标链上的LP也通过Meson合约的postSwap检查交易后，调用Meson合约上的Lock方法锁定对应的资产，然后将地址暴露给Meson Fi。接下来的操作是HTLC过程，用户在原链上指定LP的地址并创建哈希锁，通过在目标链上暴露哈希锁原始图像来删除资产。接下来是HTLC流程，用户指定LP地址并在原链创建哈希锁，暴露目标链中的哈希锁镜像来检索资产，然后LP检索用户锁定的资产通过原始图像在原始链中。



资料来源：Kernel Ventures

Meson Fi并不是专门为比特币资产设计的跨链桥，而是像LayerZero一样的全链桥。然而，主要的BTC Layer2如B2 Network、Merlin Chain和BEVM都已与Meson Fi建立了合作伙伴关系，并建议在质押过程中使用它来跨链桥接其资产。据官方报道，Meson Fi 在为期三天的 Merlin Chain 质押活动中处理了超过 20
万笔交易，以及约 2000 笔 BTC
资产的跨链质押交易，包括跨所有主要链到比特币的交易。随着比特币上 Layer2 不断发布和引入质押激励，Meson
Fi’ 更有可能吸引资产进行跨链，并看到协议收入的增加。

3.4 综合比较

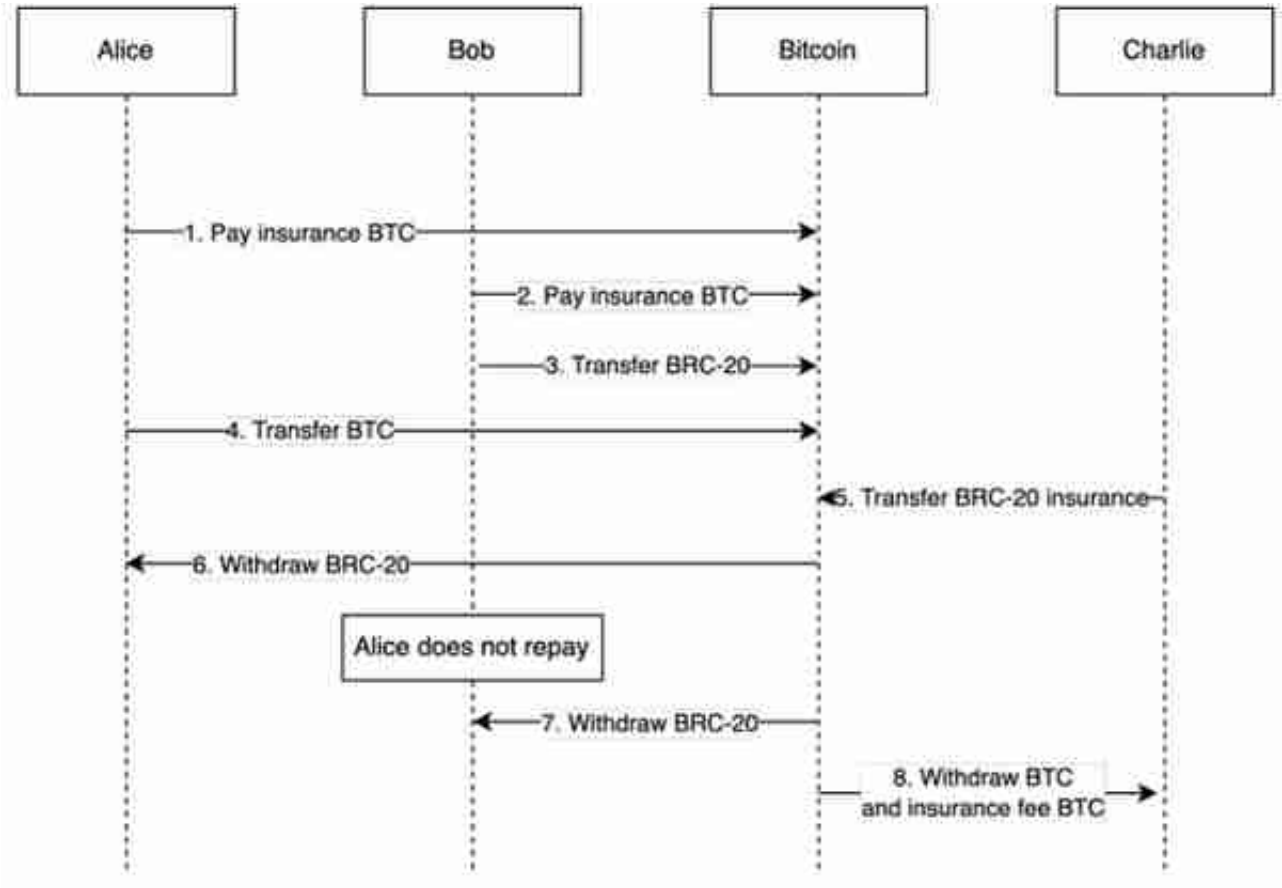
总体而言，Meson Fi 和另外两种跨链桥是两种不同类型的跨链桥。Meson Fi
本质上是一个全链跨链桥，但恰好与比特币的许多 Layer2
配合，帮助其桥接来自其他网络的资产。另一方面，Sobit 和 Multibit
是为比特币原生资产设计的跨链桥，服务于 BRC20 资产以及比特币上的其他 DeFi 和稳定币协议资产。相比之下，Multibit提供的BRC20资产种类更加丰富，包括ORDI、SATS等数十种资产，而Sobit目前仅支持三种BRC20资产。此外，Multibit还与一些比特币稳定币协议合作，提供跨链服务和权益收益活动，提供更全面的服务。最后，Multibit还提供了更好的跨链流动性，为以太坊、Solana、Polygon等五大链提供跨链服务。

4. 比特币稳定币4.1 比特笑脸

BitSmiley是比特币网络上基于Fintegra框架的一系列协议，包括稳定币协议、借贷协议和衍生品协议。用户可以在BitSmliey的稳定币协议中通过超额抵押BTC来铸造bitUSD，当他们想要提取抵押的BTC时，需要将bitUSD发送回Vault钱包进行销毁并支付费用。当抵押物价值低于一定阈值时，BItSmiley将对抵押资产进入自动清算流程，清算价格计算公式如下：

?????????????????????? ?????????? = (?????????????????????????????? ?? * ??????????????????????????????) / (?????????????????????? ??????????????????)

具体的强平价格与用户抵押品的实时价值以及bitUSD的铸造量有关，其中强平比率是一个固定的常数。在强平过程中，为了防止价格波动给被强平者造成损失，BItSmily 中设计了强平罚金来对此进行补偿，强平时间越长，补偿金额就越大。资产清算由荷兰式拍卖完成，以求在最短的时间内完成资产清算。同时，BitSmiley协议的盈余将存储在指定账户中，并定期进行拍卖，以BTC竞价的英国拍卖形式进行，可以最大化盈余资产的价值。BitSmiley项目将使用剩余资产的90%来补贴链上抵押品，其余10%将分配给BitSmiley团队用于日常维护费用。BitSmiley 的借贷协议还为比特币网络的结算机制引入了多项创新。由于比特币主网的10分钟出块率，无法像以太坊那样引入预测机来实时判断价格波动，因此BitSmiley引入了一种机制来保证第三方免受对方失败的影响按时交付，即用户可以选择提前向第三方支付一定数量的BTC来保证交易（双方均需支付），当一方未能按时完成交易时，该交易将由第三方投保。当一方未能按时完成交易时，担保人将赔偿另一方的损失。

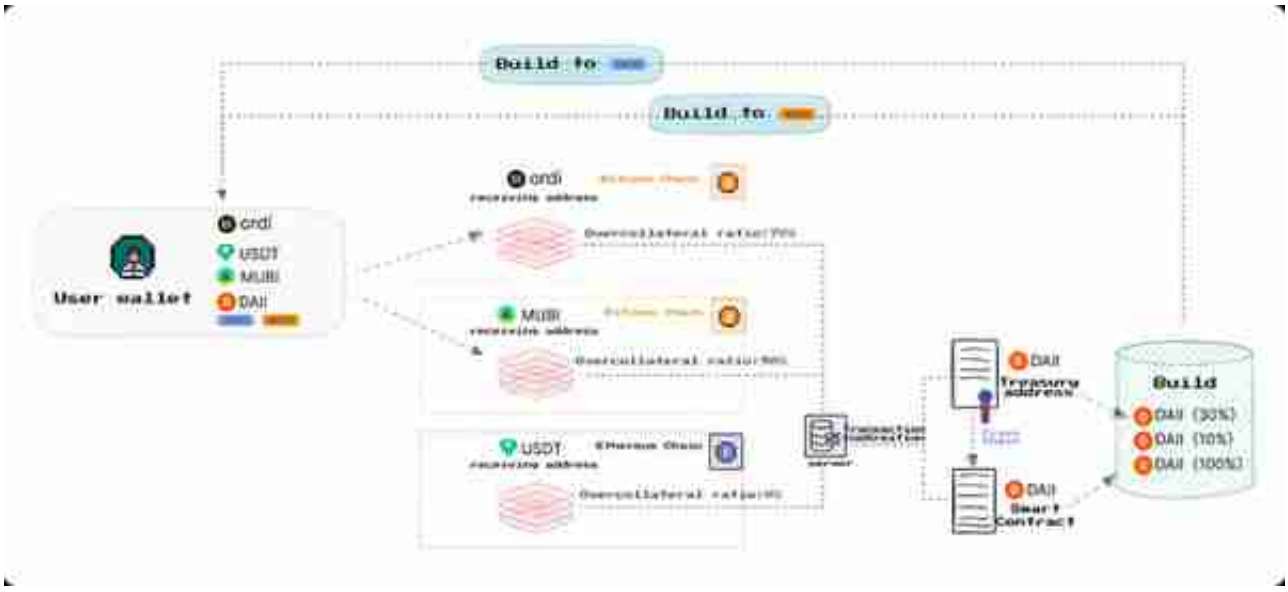


来源：BitSmliey 白皮书

BitSmiley 提供了广泛的 DeFi 和稳定币功能，并在结算机制上进行了多项创新，以更好地保护用户并提高其与比特币网络的兼容性。无论是在结算还是抵押机制方面，BitSmiley 都是一种优秀的稳定币和 DeFi
模式，在比特币生态系统仍处于起步阶段的情况下，BitSmiley
应该能够在稳定币竞争中占据重要份额。

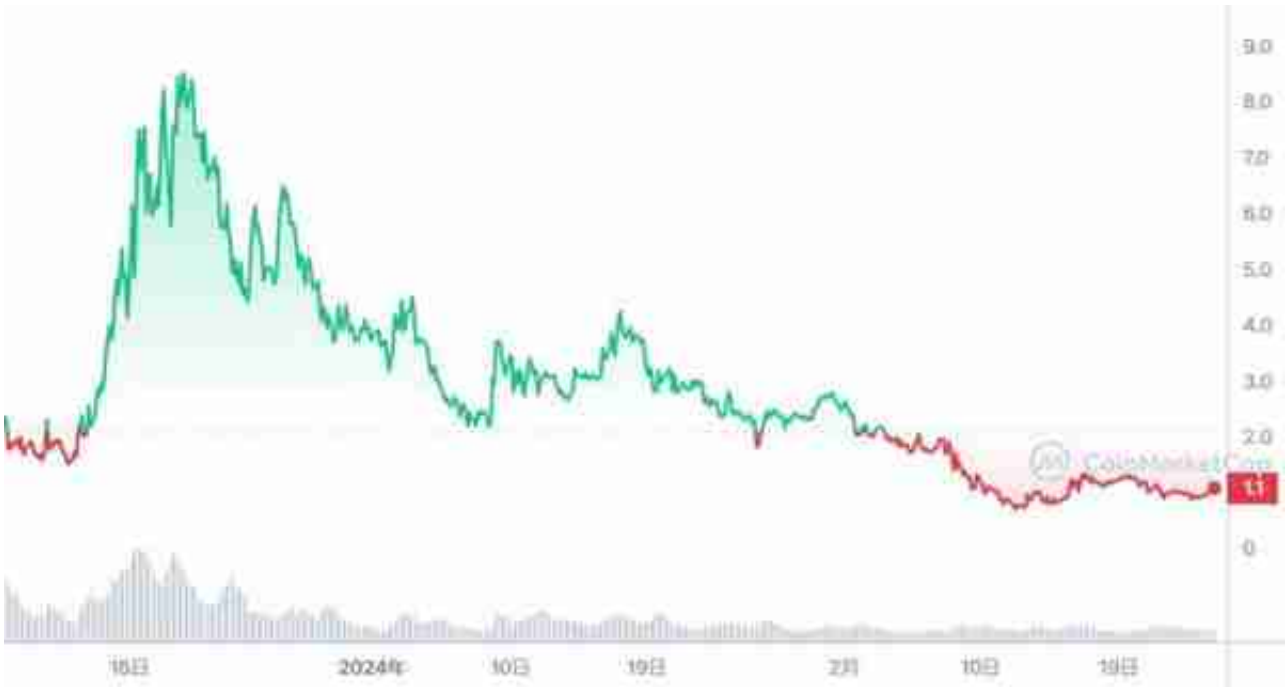
4.2 位稳定

BitStable是基于超额抵押的比特币稳定币协议，目前支持比特币主网的ORDI和MUBI资产以及以太坊的USDT抵押。根据三种资产的波动性，BitStable
设置了不同的超额抵押比例，USDT 为 0%，ORDI 为 70%，MUBI 为 90%。



资料来源：Bitstable.finance

BitStable也在以太坊上部署了相应的智能合约，通过质押获得的DALL稳定币可以在以太坊上1:1兑换成USDT和USDC。同时，BitStable采用了双通证机制，除了稳定币DALL之外，还采用了BSSB作为自己的治理通证，通过BSSB持有者可以参与社区的治理并分享网络的收益。BSSB 总数为 2100
万个，分为两种方式分配。第一种是通过在比特币网络上质押 DALL
代币来赚取相应的 BSSB 治理代币，项目通过质押奖励分配 50% 的 BSSB
代币。第二种方式是去年11月底Bounce Finance上的两轮LaunchPad，其中30%和20%的BSSB通过质押拍卖和固定价格拍卖来分配。然而，在质押拍卖期间发生了黑客攻击，导致超过 300 万个 BBSB 代币被销毁。



资料来源：coinmarketcap

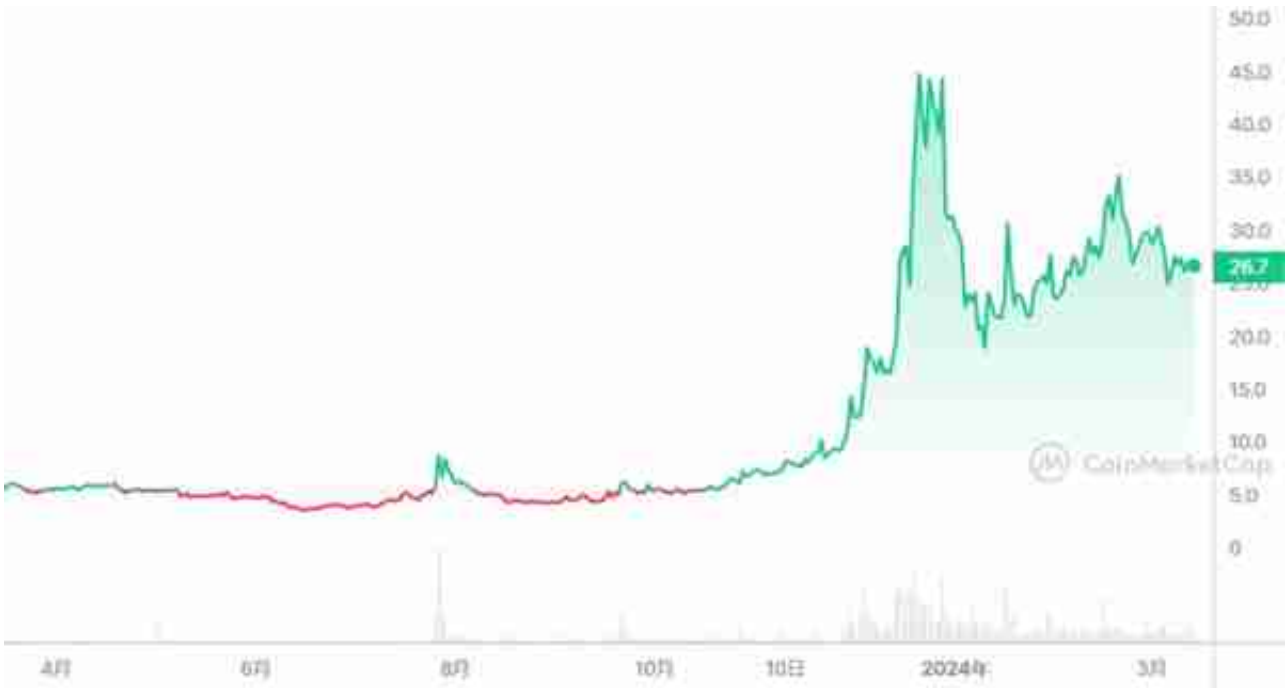
黑客攻击期间，项目组及时响应。剩下的25%未受到黑客攻击影响的代币仍然被发行，虽然成本较高，但这一措施较好地恢复了社区的信心，最终避免了价格冲突。

5. 比特币 DeFi5.1 反弹金融

Bounce Finance 由一系列 DeFi 生态项目组成，包括 BounceBit、BounceBox 和 Bounce Auction。值得注意的是，Bounce Finance最初并不是一个服务于BTC生态系统的项目，而是为以太坊和BSC设立的拍卖协议，去年5月它转变了方向，以利用比特币发展热潮。BounceBit 是一个与 EVM 兼容的比特币 POS 侧链，并将根据谁从比特币主网质押比特币来选择验证者。BounceBit还引入了混合收益机制，用户可以将BTC资产质押在BounceBit上，通过POS验证和相关的DeFi协议在链上赚取收益，也可以通过镜像链上资产和从CEX安全地转移资产和从CEX转移资产。在 CEX 上赚取收入。BounceBox 类似于 Web2
中的应用商店，发布者可以自定义设计一个 dApp，即盒子，然后通过 BounceBox 进行分发，然后用户可以选择自己喜欢的盒子参与 DeFi
活动。Bounce Auction 是 Ether 项目的主要部分，是对各种资产的拍卖，并提供多种拍卖选项，包括固定价格拍卖、英国拍卖和荷兰拍卖。

Bounce 的原生代币 Auction 于 2021 年发布，并在 Bounce Finance 的多轮 Token LaunchPad 中被用作赚取积分的指定 Stake 代币，这推动了近期 Auction 代币价格的上涨。更值得关注的是，Bounce改用比特币后打造的新质押链Bounce Bit现已开放链上质押获取积分并测试网络交互积分，并且该项目的X账户明确表明

积分可以兑换代币，代币发行将于今年 5 月进行。



资料来源：Coinmarketcap

5.2 订单交换

Orders Exchange 是一个完全建立在比特币网络上的 DeFi 项目，目前支持数十种 BRC20 资产的限价和市价挂单，并计划在未来引入 BRC20 资产之间的互换。Orders Exchange的底层技术由Ordinals Protocol、PSBT和Nostr Protocol组成。有关 Ordinals 协议的更多信息请参阅 Kernel 之前的研究文章 Kernel Ventures: Can RGB Replicate The Ordinals Hype。PSBT 是比特币的一个关键功能，用户通过 SIGHASH_SINGLE 签署由输入和输出组成的 PSBT 类型签名 | 任何人都可以支付。PSBT是一种比特币签名技术，允许用户签署由输入和输出组成的PSBT-X格式，输入包含用户将执行的交易，输出包含用户交易的先决条件，这需要另一个用户执行Output内容并在Input内容最终生效之前对网络公式执行SIGHASH_ALL签名。在交易所的挂单交易中，用户通过PSBT签名的方式完成挂单，并等待对方完成交易。

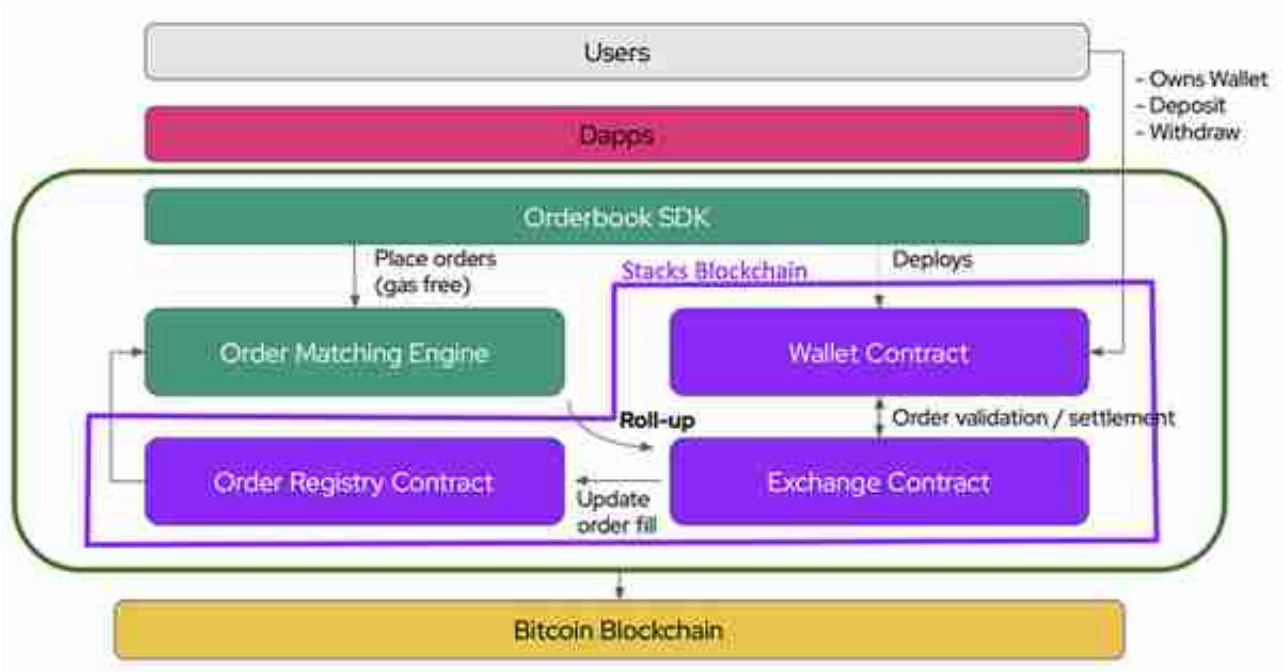
来源：orders-exchange.gitbook.io

Nostr是使用NIP-100建立的资产转移协议，提高了不同DEX之间资产的互操作性。Orders Exchange 1亿枚代币已全部释放。而尽管在白皮书中强调ttokens只是实验性的，没有任何价值，但该项目精心设计的空投计划仍然显示出明显的通证经济意图。初始代币分配主要有3个方向，45%的代币分配给Orders Exchange上的交易者，40%的代币空投给早期用户和推广者，10%分配给开发者。不过，无论是官网还是官方推文，都没有对 40% 的掉落进行详细描述，官方公布掉落后，在 X 上或 Discord 的 Orders 社区中也没有任何讨论，因此实际掉落的分配情况仍然是可疑的。总体来说，Orders Exchange的买单页面直观清晰，可以清楚地看到所有买单和卖单的价格，在提供BRC20交易的平台中属于较高水平。随后在 Orders Exchange 上推出 BRC20 代币兑换服务也应该有助于协议的价值获取。

5.3 亚历克斯

Alex 是一个建立在比特币侧链堆栈之上的 DeFi 协议，目前支持互换、借贷、借入和其他一些交易类型。同时，Alex对传统的DeFi交易模式进行了一些创新。第一个是Swap，传统的Swap定价模型可以分为两种：普通货币对的x*y=k和稳定币的x+y=k，但是在Alex上，你可以设置货币对的交易规则，并设置是将两次计算的结果按照一定比例x*y=k和x+y=k的线性组合。Alex还推出了OrderBook，这是一种链上和链下相结合的订单细化模型，允许用户以零成本快速取消待处理交易。最后，

Alex提供固定利率借贷活动，并为借贷服务建立了多元化的抵押品池，而不是传统的单一抵押品，由风险资产和无风险资产组成，降低了贷款风险。



来源：Alexgo 文档

与 BTC 生态中的其他 DeFi 项目在 Ordinals 协议炸毁 BTC 生态后进入市场不同，Alex 早在上一次牛市时就开始致力于 BTC DeFi 生态，并已筹集了种子轮资金。Alex 在性能和交易类型方面也很出色，即使是以太坊上的很多 DeFi 项目也比 Alex 的交易体验没有太大的竞争优势。Alex的原生代币Alex Lab的总供应量为10亿，其中60%已经释放，仍然可以通过在Alex上质押或作为流动性提供者来获得。然而，收入很难达到早期发布时的水平。作为比特币上最成熟的 DeFi 项目之一，Alex 的市值被认为并不算高，比特币生态系统可能是本次牛市的重要引擎。此外，Alex部署的侧链Stacks将进行重要的中本聪升级，其中Stacks将在交易速度和交易成本方面进行大幅优化，并且其安全性将得到比特币主网的支持，使其成为真正的Layer 2。此次升级也将大大降低Alex的运营成本，并提高其交易体验和安全性。Stacks链也将为Alex提供更大的市场和交易需求，为协议带来更多的收入。

6. 结论

Ordinals协议的应用改变了比特币网络无法实现复杂逻辑和发行资产的缺陷，比特币网络上陆续引入了各类资产协议，对Ordinals的思想进行了改进。但应用层还没有做好提供服务的准备，在铭文资产激增的情况下，比特币应用所能实现的功能就显得不合时宜，比特币网络上的应用开发成为了热点。各方夺取。Layer 2

在各类应用中优先级最高，因为所有其他 DeFi 协议，无论开发如何，如果不提高比特币主网的交易速度、降低交易成本，都将很难释放流动性，并且链上将充斥着出于投机目的的新交易。在提高了比特币主网的交易速度和成本之后，下一步就是提高交易的体验和多样性。各种 DeFi 或稳定币协议为交易者提供了广泛的金融衍生品。最后，跨链协议允许比特币主网上的资产流入和流出其他网络。比特币的跨链协议相对成熟，但并非完全是自比特币主网发展以来，因为许多多链桥和主流跨链桥都是为了向比特币网络提供跨链服务而设计的。对于像SocialFi和GameFi这样的dApp来说，由于比特币主网络的高gas和延迟限制，目前还没有出现优秀的项目，但随着Layer2网络的提速和扩容，它们很可能会在Layer2上出现比特币网络的。可以肯定的是，比特币生态系统至少将成为本次牛市的热门话题之一。热情充沛，市场巨大，虽然比特币上的各个生态系统还处于发展初期，但这次我们很可能会在牛市中看到各个垂直领域优秀项目的涌现。