比特币兴起之路：提升流动性的新机遇

来源：GeekCartel

前赴后继的创业者们并未止步不前，他们不断探索新的解决方案和应用场景。随着技术的进步，比特币的流动性正逐步得到提升。GeekCartel通过梳理一些比特币流动性解决方案，旨在带领大家了解这些项目的发展和技术原理，并从更全面的角度观察最新的发展，帮助用户更好地利用比特币资产和探索更多的应用场景。

### 一、引言

自2009年中本聪发布比特币白皮书以来，比特币一直被誉为“数字黄金”，在加密货币领域占据着不可动摇的地位。其去中心化、稀缺性和安全性，增强了其作为长期价值储存工具的吸引力。

相比之下，以太坊自2015年问世以来，凭借其强大的智能合约平台和灵活的开发环境，迅速成为了区块链行业的另一个重要支柱。以太坊的智能合约功能为去中心化应用程序（dApps）的开发提供了无限可能，使其在去中心化金融（DeFi）和非同质化代币（NFT）领域取得了显著的成就。

尽管比特币在加密世界占据重要地位，但是与以太坊相比，比特币生态系统仍面临一些独特的挑战：

缺乏智能合约平台：比特币生态系统中缺乏强大的智能合约平台，限制了复杂dApps和DeFi的发展。

资产利用不足：对于许多比特币持有者来说，一个重大挑战是他们的资产未得到充分利用，导致错失了在DeFi和NFT等新兴行业中获利的机会。

BTC在各种区块链网络中的碎片化问题：比特币被分散在多个独立的区块链网络和二层解决方案中，这些网络之间可能缺乏有效的互操作性和兼容性，从而限制了比特币的应用和流动性。

尽管比特币的原始设计相对简单，但其社区和开发者不断推动技术创新，以提升其功能和可用性。其中，SegWit更新通过将交易信息和签名信息分离，解决了交易延展性问题并增加了区块容量；Taproot更新引入了Schnorr签名技术，提高了交易的隐私性和效率，为链上智能合约的发展奠定了基础；BRC-20标准则使得比特币网络能够支持代币化资产的创建和交易，扩展了其应用场景并增强了在去中心化金融和其他区块链应用中的竞争力，为比特币的金融应用场景提供了潜力和基础。

前赴后继的创业者们并未止步不前，他们不断探索新的解决方案和应用场景。随着技术的进步，比特币的流动性正逐步得到提升。GeekCartel通过梳理一些比特币流动性解决方案，旨在带领大家了解这些项目的发展和技术原理，并从更全面的角度观察最新的发展，帮助用户更好地利用比特币资产和探索更多的应用场景。注意：本文不构成投资建议。

### 二、比特币流动性探索：提升应用与价值的新路径

#### Babylon: 将比特币安全带入Pos生态

技术实现：

Babylon 是一条基于Cosmos SDK开发的Layer 1 PoS链。Babylon提出了比特币质押协议，该协议被设计为一个模块化插件，用于许多不同的PoS共识算法之上，提供一个可以再质押（Restaking）协议的原语。

Babylon能够将比特币的安全性传递到所有众多 PoS 链（如 Cosmos、Binance Smart Chain、Polkadot、Polygon 和其他已经拥有强大、可互操作生态系统的区块链），创建更强大和统一的生态系统。

Babylon通过比特币时间戳协议和比特币质押协议来实现比特币安全共享。

比特币时间戳协议：Babylon通过将PoS区块的哈希值及其验证者签名发送到比特币区块链，利用比特币的时间戳技术来增强PoS协议的安全性。这一过程包括以下几个关键步骤：

校验点（Checkpointing）：在每个epoch结束时，诚实的验证者会签署该时期最后一个PoS区块的哈希值，并将这个哈希值和他们的签名作为校验点提交到比特币网络。由于比特币区块链具有不可更改性和时间顺序的特性，这些校验点提供了一个不可篡改的时间证明。

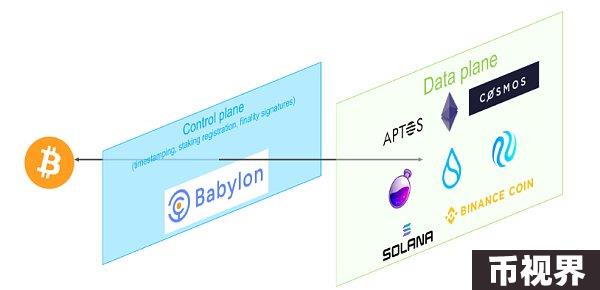
惩罚机制（Slashing）：如果一个验证者的行为被判定为恶意的（例如，签署了冲突的区块），那么他们的质押资金会被削减。比特币区块链上的校验点使得这种削减行为有了一个时间上的证据支持，证明在某个特定时间之前，恶意行为确实已经发生。

比特币时间戳协议还可以解决PoS长距离攻击 。长距离攻击是指利用了PoS链中验证节点解质押后，回到他们还是质押者身份的某个历史区块，启动一条分叉链的可能性。这个问题是PoS系统固有的，无法仅通过改进PoS链的共识机制本身来彻底解决，不论是以太坊还是Cosmos等PoS链都面临着这一挑战。

通过引入比特币时间戳，PoS链的链上数据将会以带有比特币时间戳的形式，存储在比特币链上，即便有人想再造一条PoS链的fork，它对应的比特币时间戳肯定晚于原链，所以此时长距离攻击就会失效。

比特币质押协议：该协议允许比特币持有者质押其闲置的比特币，以提高PoS链的安全性，并在此过程中获得收益。

比特币质押协议的核心基础设施是比特币与 PoS 链之间的Control Plane，如下图所示。



Control Plane以链的形式实现，以确保它是去中心化的、安全的、抗审查的和可扩展的，Data Plane代表PoS链，这个控制平面负责各种关键功能，包括：

为 PoS 链提供比特币时间戳服务，以使它们能够与比特币网络同步。

充当市场，匹配比特币权益和PoS链，并跟踪质押和验证信息，如EOTS密钥注册和刷新;

记录 PoS 链的最终性签名；

Babylon使用先进的密码学技术，如一次性提取签名（EOTS），将可削减的PoS攻击转换为可用于销毁的比特币UTXO。

EOTS 是一种特殊的数字签名方案，如果在相同高度对不同的块进行签名会导致密钥泄露。比特币网络使用 UTXO 模型来跟踪交易和账户余额。每个 UTXO 代表比特币网络中某个地址的一定数量的比特币，这些比特币可以被该地址的私钥持有者支配。

当 PoS 验证者质押比特币以参与网络的共识过程时，他们的质押行为被锁定在特定的 UTXO 中。通过使用EOTS，确保验证者违反协议时（如在同一个高度对两个不同的区块进行签名），他们的私钥将被泄露。一旦私钥被泄露，这个私钥可签署一个将原始质押的比特币发送到一个烧毁地址的交易。这样，违规的验证者就会因为自己的不诚实行为而受到经济上的惩罚。

综上所述，Babylon是一个Layer 1 区块链，通过比特币时间戳和比特币质押协议，将比特币的安全性传递到众多 PoS 链上，增强了这些链的安全性，并为比特币持有者提供了收益机会。其独特的质押方案允许比特币持有者质押 BTC 而无需桥接。然而，由于质押 BTC 被锁定在智能合约中，这些 BTC 将在 UTXO 中以未花费状态呈现，随着质押量的增加，可能导致比特币链上交易处理速度下降和交易费用上升，这是 Babylon 面临的主要挑战之一。

项目进度：

Babylon目前还在测试网阶段，官方宣布将与Ankr、Lorenzo协议、B² Network 、Nubit、Yala、Nomic、Automata、Glacier、Solv等一系列站在比特币革命前沿的项目合作。

根据官方数据，Babylon已经通过IBC协议与50条Cosmos链进行了集成，涵盖了DeFi、游戏和基础设施等领域。

投资信息：

2023年12月6日，Babylon获得了由Polychain Capital和Hack VC领投的1800万美元的A轮融资，其他参投机构包括：Framework Venture、Breyer Capital、Symbolic和GeekCartel等。

2024年2月，Binance Labs宣布对Babylon进行投资，投资金额未披露。

2024年5月30日，Babylon宣布完成新一轮融资，融资金额达到7000万，由Paradigm领投。



#### BounceBit：DeFi与CeFi的融合之道

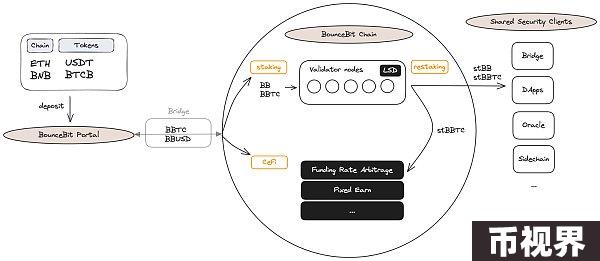
技术实现：

BounceBit 链是一个由验证者质押BTC和其原生代币保障的PoS Layer 1——一种利用原生比特币安全性的双代币系统（原生代币BB和BTC），具有完整的EVM兼容性。

验证者质押BB或BBTC 来记录和验证网络上的交易，获得交易费用作为质押奖励。并且没有最低持有代币数量的要求。这种双代币系统不仅扩大了利益相关者的基础，还为网络的共识机制增加了额外的弹性和安全层。

BounceBit还支持与EVM兼容的链的互操作性，识别和合并如BNB链上的BTCB和ERC20代币WBTC等权益资产。这使得BTC的用例多样化，提升了用户的参与度。

BounceBit引入了一项独特功能——从CeFi和DeFi中并行产生收益。用户可以在获得原始CeFi收益的同时，利用流动性质押衍生品（LSD）进行BTC质押和链上挖矿，这一过程称为比特币的Restaking。该生态系统为比特币持有者提供三种类型的收益：CeFi收益、在BounceBit链上质押BTC的节点运营奖励，以及参与链上应用和Bounce Launchpad的机会收益。



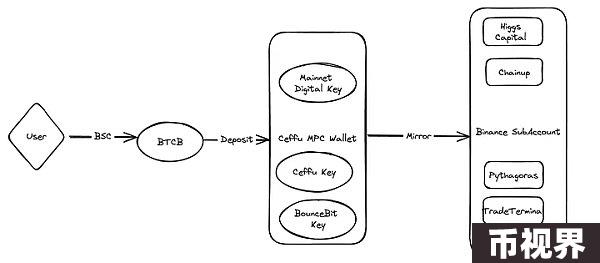
如图3所示，用户将多种Token存入BounceBit Portal转换成LCT（BBTC或BBUSD）。通过桥接将这些LCTs（流动托管代币）跨到BounceBit链上参与 CeFi 收益，也可以将BB或BBTC 质押到验证节点中，并获得作为LSD的stBB或stBBTC，这些代币可以进行再质押，增强网络安全性。

BounceBit 引入了 "流动托管"（Liquid Custody）的概念，理论上可以确保资产安全存放，使抵押资产保持流动性，并提供更多获取收益的机会。如上述流程中，当用户将资产存入 BounceBit 时，他们将收到一个（LCT）- BB或BBTC，该代币代表他们的资产在安全托管的同时可以桥接到 BounceBit 并在支持的场景下使用，以获取更多收益。

BounceBit允许质押验证者（Staking Validators）参与网络的安全和共识机制，帮助保障网络的稳定性和安全。

共享安全和共识：受Restaking的共享安全模式启发，BounceBit 的BTC桥实施了一种系统，验证者共同维护和保护跨链桥。这种合作方式分配了安全责任，增强了跨链交易的可靠性。

超过50%批准交易：为了验证和执行任何跨链交易，需要超过50%的验证者批准。这种共识机制确保每笔交易都经过了全网验证者的认真审查和认可，为桥接过程增加了额外的安全性和信任层级。



通过创新的CeFi + DeFi框架，BounceBit赋予BTC持有者在多个网络上获得收益的能力。与很多强调去中心化的协议不同，当比特币存放在多签钱包中时，无法产生收益（去中心化协议通常内置了复杂的收益生成机制，这些机制需要资产在智能合约中运行，而比特币的智能合约能力有限）。BounceBit通过整合CeFi模型解决了这个问题，利用Mainnet Digital的托管服务，辅以Ceffu的MirrorX技术，使BTC既可以在链上活动也可以在CEX子账户中以授信进行交易。

如图4所示，用户与BSC（BNB Smart Chain）交互，将BTCB存入Ceffu 多方计算（MPC）钱包 。在 MPC 中，给定数量的参与者各自持有一段私有数据。参与者可以一起计算该私有数据上的公共函数的值，同时使自己的数据保密。这个钱包使用多个密钥来保障交易的安全，包括：主网数字密钥，Ceffu密钥和BounceBit密钥。最后映射到币安子账户，这部分的组件（Higgs Capital，Chainup，Pythagoras，TradeTerminal）支持子账户的不同需求。

综上所述，BounceBit是一个支持比特币再质押的PoS Layer 1网络，整合了CeFi和DeFi模型，提供拍卖、DEX和其他金融服务，允许比特币持有者在多个网络上获得收益。它完全兼容EVM，支持与其他EVM链的互操作性，并通过其桥接系统安全地转移和映射BTC。BounceBit还但是这种结合CeFi和DeFi的方法可能面临安全挑战，特别是在跨链桥的安全机制和多签钱包的管理方面，这要求维护高度的安全性和稳定性，确保资金和交易的安全。

项目进度：

根据官方最新报告：5月13日的Mainnet launch，其链上TVL已达8.82亿，近40万早期贡献者。截止撰稿前，据官方资料，通过BounceBit桥接的BBTC代币总量为1,482，持有BBTC的用户量为155,583，质押量(LSD)达到5,099 BBTC。

BounceBit最近宣布和Ethena建立合作伙伴关系，用户可以通过质押$BBUSD参与BounceBit和Ethena的活动激励。与Nubit合作，以提升数据完整性和数据容量；此外，官方还与LayerZero Labs、USDX、zkLink Nova、Pell Network、Free等达成合作。

投资信息：

BounceBit 在今年二月通过种子轮募集了 6百万美元，由 Breyer Capital 和Blockchain Capital 共同领投。并在三月和四月， 分别获得了来自OKX Ventures 和Binance Labs的战略融资。



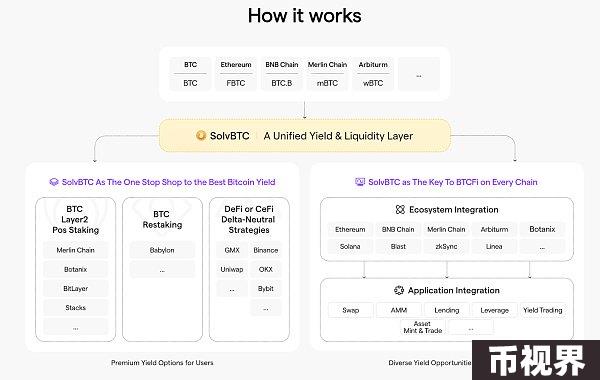
#### Solv：释放SolvBTC力量，开启BTCFi之门

技术实现：

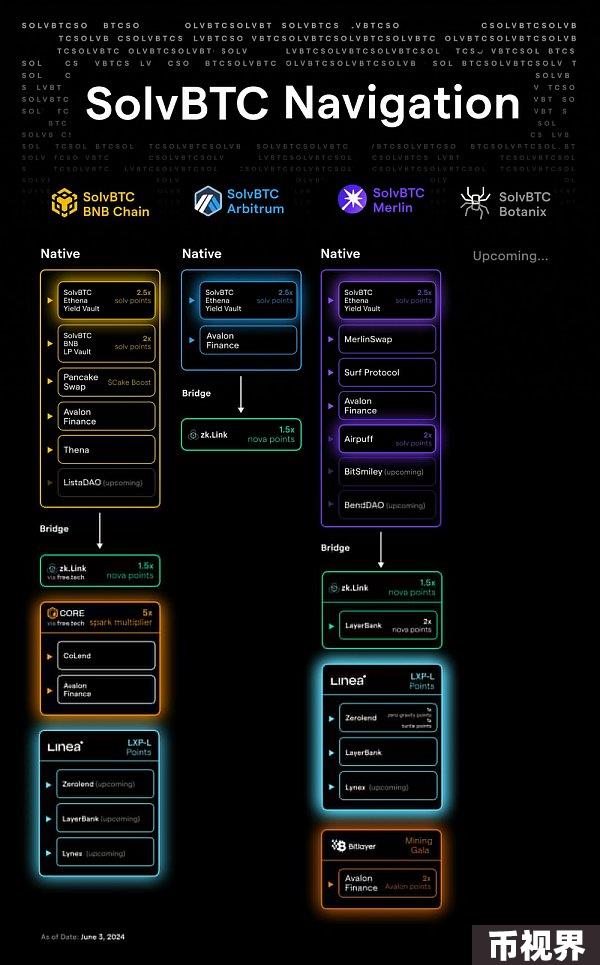
Solv Protocol 推出了SolvBTC，这是一种开创性的全链收益比特币资产。SolvBTC在安全的资产管理框架内开发，为比特币持有者解锁了新的可能性和机会，同时创造了一个高效的BTCFi生态系统。

Solv作为一个统一的流动性入口，将各种流动性资源和投资机会整合到一个平台上。用户不需要访问多个不同的平台或协议，就可以在Solv Protocol上找到和管理他们的投资。通过将闲置的基础资产转化成生息资产和促进跨协议、跨生态的乐高组合，Solv 将刺激整个网络的流动性活力，打造高效的流动性分配层。

以 SolvBTC 为例，如图6所示，用户端可以将BTC和BTC相关资产（如wBTC、BTBC、MBTC等）通过应用层的DeFi协议（如DEX-去中心化交易所、稳定币、借贷等）将质押、再质押和DeFi交易收益代币化。Merlin、Stacks、Botanix、Bitlayer等，这些都是支持SolvBTC运作的基础设施平台和链。它们为SolvBTC提供了必要的技术支持和生态系统连接，确保SolvBTC可以在多种区块链和协议上顺利运行。



此外，SolvBTC与各个生态上的DeFi和CeFi项目充分集成，使用户能够探索新的增长途径并最大化他们的收益潜力。这种整合将比特币的流动性带入各种 DeFi 协议，以促进 BTCFi 的繁荣。SolvBTC也成为了BTCFi统一的流动性门户。



Solv 实现了一个去中心化的资产管理架构，其中还包括内置的Solv 守卫（Guard）和预言机(Oracle)。通过利用智能合约，Solv 建立了一个无需信任的流程标准，优先考虑资产的安全性，为用户提供优质的收入来源。

Solv Guard是根据各个Vault的交易策略，定制设计的具有独特操作机制和专门权限范围的系统。其中定义了关于转移目的地和DeFi协议操作的规则，

仅允许安全钱包多重签名在指定范围内操作。

智能合约的升级需要通过与信誉良好的合作伙伴使用多重签名地址和时间锁定机制（TimeLock）共同控制。此外，如果策略涉及在中心化交易所操作，Solv将与Ceffu和Copper等链上托管机构合作，以确保交易所外资金结算的安全。

通过在安全钱包多重签名的使用权基础上授予治理权限，实现了治理权与用户权限的分离。这种分离使得未来能够通过改变治理结构来配置参数和升级合约。

交易策略Vault: 储存资金和提供流动性，并执行资金配置。其核心设计理念是在确保资金运作效率的同时，消除交易对手风险（交易对手风险是指在交易过程中，对方未能履行其财务义务的风险，这里通过智能合约自动执行交易，无需依赖单一的中介或对方履约，从而降低了交易对手风险）。

在这个Vault中，投资和还款操作是通过保持投资组合中的Delta中性策略（Delta-Netural Strategies）来实现的。

Vault使用Solv Guard维护和实时价格预言机来确保操作的安全性和依赖于当前市场数据的决策。

综上所述，Solv推出了SolvBTC，这是一种创新的全链收益比特币资产，旨在为比特币持有者提供新的机会和可能性，同时创建一个高效的BTCFi生态系统。SolvBTC通过统一的流动性入口，将各种流动性资源和投资机会整合到一个平台上，使用户能够在Solv Protocol上轻松找到和管理投资。Solv架构包含Solv Guard、预言机等去中心化资产管理机制，并与多家基础设施供应商合作，确保资产安全和系统高效运行。除了SolvBTC，官方还提供多种资产和投资策略。尽管Solv使用多重签名和其他机制等安全措施，但智能合约本身的漏洞或被攻击的风险依然存在，可能会导致资产丢失或被盗。为此，Solv积极与知名审计公司合作，以最大限度地减少这种风险。

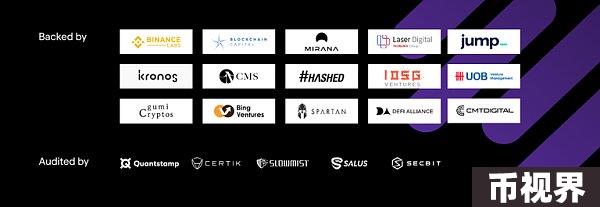
项目进度：

SolvBTC已支持 BNB Chain、Merlin、Arbitrum和比特币主网的比特币资产，即将支持以太坊主网。官方宣布将通过与 Ethena 团队合作，把 sUSDe 稳健的策略收益整合到 SolvBTC.ena 中，还将与Babylon、BotanixLabs合作。6月6日，Binance Web3推出了Solv质押奖励活动，用户可以通过质押BTCB兑换SolvBTC来赚取奖励。

截止撰稿前，Solv 已实现超过 12亿 美元的 TVL，为超过 10万名用户提供高质量的收益；已经有17,490 BTC 在Sovl上质押。

投资信息：

Solv 已经获得了包括 Binance Labs、Blockchain Capital、Mirana 在内的投资。



#### Lorenzo：比特币流动性金融层

技术实现：

Lorenzo为比特币持有者提供了一个高效的市场，使他们能够轻松找到最佳的投资机会。

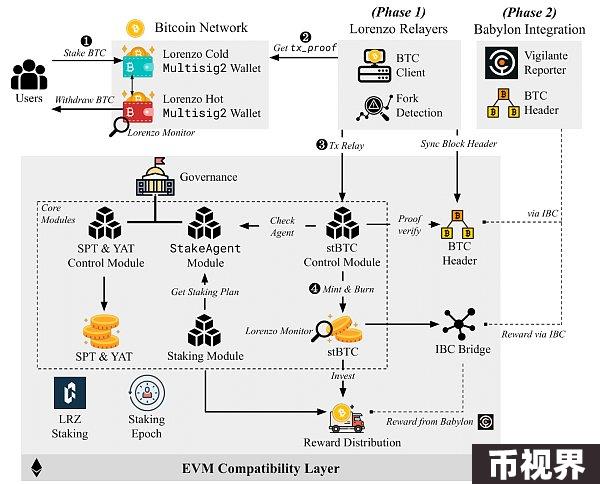
Lorenzo通过将质押的比特币代币化为流动性本金Token (Liquid Principal Tokens - LPTs)和收益累积Token (Yield Accruing Tokens - YATs)，激励用户参与质押并提供收益。此外，Lorenzo还提供了LPT和YAT的交易基础设施，确保用户可以方便地管理和交换其代币，从而最大化他们的投资收益。

流动性本金Token (LPTs)：LPTs是代表质押的比特币本金Token。以图9中的Babylon为例，例如，Babylon-Lorenzo-01 是一个 比特币流动性再质押计划（BLRP），用户将比特币质押当质押到 Babylon-Lorenzo-01 时，将获得1:1兑换的stBTC作为LPT, 用户可以在Lorenzo平台上买卖或管理这些LPTs，从而使质押的比特币变得更具流动性和可操作性。

收益累积Token(YATs)：YATs是代表从再质押交易中累积收益的Token。同样以Babylon-Lorenzo-01 为例，YAT 将在到期时从 Babylon 和 Lorenzo 获得收益，YATs也可以在Lorenzo平台上进行买卖或管理，使得用户能够将收益变现或再投资。

在 Babylon 出现之前，BTC 资产分布在各条公链上。而 Babylon 的出现将这些 BTC 资产集中进行质押，并释放出 stBTC 作为流动性质押代币进入各个生态系统。各个生态系统对 stBTC 的支持将影响新的 BTC 分布格局。 Lorenzo 将成为 BTC 的流量分发入口，本金stBTC作为流动性层，而YAT承担了金融的部分，用来构建类似 Pendle 的利息率市场，为用户提供投资回报。

BLRP是Lorenzo平台上用于获取比特币流动性的计划。通过BLRP，项目方可以利用质押的比特币流动性，而质押者之后将获得收益奖励。每个BLRP的创建者需要明确说明质押的比特币流动性将如何使用、比特币再质押代币的发行规则以及质押者将如何获得奖励。



根据图9我们可以看出，Lorenzo协议架构中主要有以下设置：

用户质押和取回比特币

质押BTC：用户将比特币质押到Lorenzo的多签冷钱包。

取回BTC：用户可以通过Lorenzo 多签热钱包取回他们的比特币。

Lorenzo中继器（Relayers）

获取交易证明：Lorenzo Relayers获取比特币网络中的交易证明（tx\_proof）。

分叉检测（Fork Detection）：中继器还负责检测比特币区块链的分叉情况，确保数据的一致性和可靠性。

stBTC Control Module

负责stBTC的铸造和销毁，并进行证明验证（Proof Verify）。

核心模块（Core Modules）

质押代理模块：管理质押计划（Staking Plan）并检查代理（Check Agent）。

stBTC 控制模块：负责stBTC的铸造和销毁，并进行证明验证。

SPT & YAT 控制模块：管理和控制LPTs和YATs的发行和交易。

质押模块(Staking Module)：获取和管理质押计划，协调质押操作。

当用户将比特币质押到Lorenzo平台上的一个标的（比如一个特定的投资计划或项目））时，质押代理需要完成以下流程：

完成再质押：质押代理需要及时将用户的比特币质押到指定的项目中。

上传再质押证明：质押代理需要将再质押操作的证明上传到Lorenzo平台，以确保交易的透明和可信。

发行代币：质押代理根据标的定义的规则，为每个再质押交易在Lorenzo平台上发行LPTs和YATs。

转移代币：质押代理将生成的LPTs和YATs转移到质押用户的地址，使用户能够管理和交易这些代币。

Lorenzo不仅可以作为质押代理处理用户的比特币质押，还负责监督其他质押代理的行为。如果质押代理有任何违规行为，Lorenzo将介入并采取措施，确保质押代理的行为符合规定。

通过以上内容，我们可以看到Lorenzo将部分功能设计为模块化架构，以实现可扩展性。跟据官方资料，Lorenzo支持Babylon，通过IBC桥和证明验证机制，Lorenzo将比特币流动性带入多个区块链生态系统（未来还会接入其他链），增强了比特币质押的灵活性和应用场景。Lorenzo还兼容EVM，使其能够运行以太坊智能合约，提供LPT和YAT的交易基础设施（如提供交易对，借贷协议和不同结构的比特币收益产品），促进多样化的DeFi应用开发。作为创新的比特币LPT和YAT市场，Lorenzo若遇到流动性不足或市场波动过大的情况，需尽力提高平台用户参与度和交易量，以增强整体市场流动性。

项目进度：

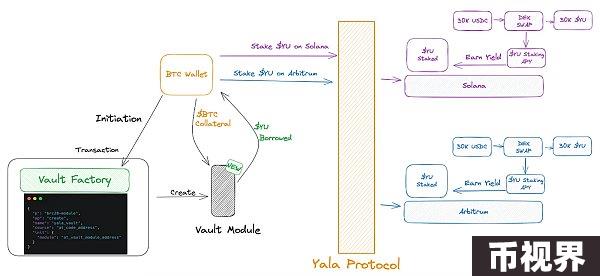
Lorenzo测试版主网在5月26日上线，用户可以尝试使用Lorenzo将stBTC桥接至Bitlayer生态。

根据官方信息，第一季度宣布的合作和集成项目包括：Babylon、Cosmos Hub、BounceBit、Flash Protocol、Nubit；最近还与Bitlayer、Portal Finance、enzo、BitSmiley等达成合作。

#### Yala ：实现多链稳定币的比特币原生DeFi协议

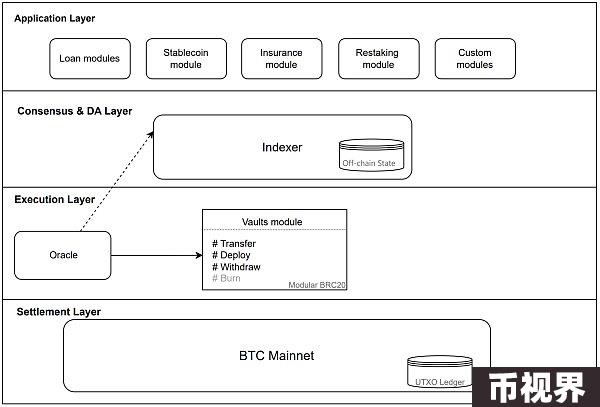
技术实现：

Yala的创新在于将比特币的流动性带到各个生态，让BTC用户可以通过稳定币得到收益。，该协议旨在利用比特币固有的安全性和流动性。利用Yala模块化基础设施提供贷款协议，使用户能够通过存入BTC或UTXO资产来借出超额抵押的稳定币($YU)。用户可以利用$YU稳定币通过在生态系统的各种DeFi协议来产生收益。Yala Finance 系统具有Vaults、清算算法、自动稳定器和保险模块等基本组件，可为 BTC 资产提供全面的 DeFi 生态系统。



如图10所示，Yala 通过混合使用不同的 DeFi 协议和多个区块链（Solana、Arbitrum、以及BTC L2，比如Botanix），使投资更加灵活和活跃。用户可以选择将他们的投资分散到不同的活动中，例如质押、流动性挖矿和借贷，跨越各种生态系统。这种以用户为导向的方法允许利用每个活动和区块链的独特优势，帮助用户建立多元化和强大的投资组合。

Yala架构包括应用层、共识与数据可用性（DA）层、执行层和结算层。基于这一设计，开发者可以使用Yala的SDK实现定制模块以开发BTC生态应用。



应用层：应用层是应用程序运行的地方，其上的模块定义了状态更改的逻辑。模块可以是目的区块链虚拟机上的智能合约 ，比如EVM中的智能合约，也可以是Inscrption Assets中的Tapscript。通过这个模块实现最终Yala的稳定币原生态可以跨多个生态系统的各种DeFi协议以及区块链来产生额外的收益。Yala的应用层包括贷款模块、再质押模块、保险模块、稳定币模块以及自定义模块。

稳定币模块构成了Yala金融系统的基础，稳定币是多链的，并且在每个目标链上都是原生的。比如由于BRC-20代币无法直接铸造，系统维护了一个稳定币储备池，即稳定币模块。用户通过转移和提取铭文到稳定币发行模块，来模拟传统稳定币的铸造/销毁过程（在初始阶段，Yala基金会作为一个受社区监督的中央实体，负责确保$YU的稳定性；治理基金会将转变为去中心化自治组织（DAO），以确保可持续发展和更广泛的社区参与）。

共识和数据可用性层：在 Yala 系统中，DeFi交易是在目标链上进行，数据通过索引器（Indexer）节点实现状态更新和共识，最终的状态变化会通过UTXO交易反映在比特币主链上，以确保数据的安全性和一致性。

数据可用性是指区块链网络中存储的数据能够被所有参与节点有效访问和使用的能力。与其他区块链中的数据可用性不同，BTC资产采用UTXO格式，包含两次状态变化（输入和输出），并且BTC的区块间隔较长，大约10分钟。

而Yala中数据可用性的实现只需要针对见证脚本格式的链外状态变化，由索引器维护。索引器以见证脚本（Witness Script）的形式捕获全局状态和平衡， 见证脚本是隔离见证（SegWit）中引入的扩展脚本（SegWit通过将签名数据与交易数据分离，目的是提高比特币交易的效率和安全性 ）。链外状态的变化最终将反映在链上的UTXO转移交易中，BTC的共识机制和安全性验证了这些链上UTXO交易，从而间接确保了链外状态变化的可靠性和一致性。另外，Yala和DA提供商Nubit合作，Nubit提供bitcoin indexer的状态验证。基于以上设计，Yala的挑战是实现Indexer的可信度和链外状态的安全实时更新。对此，Yala提出了一些未来的发展方向和解决方案：

实现Indexer的可信度：

数据可采样：在DA层中，直接使用数据可用性采样（DAS）来降低验证成本；验证者只需随机下载部分数据块以验证所有数据的可用性。还将使用纠删编码和KZG多项式承诺来实现Yala DA层中的DAS。

内容验证：Yala 的DA层需要验证的内容包括交易数据、交易数据的Merkle树和承诺（Commitments）。交易数据将由Indexer直接验证，同时Indexer也将生成Merkle树。当前，承诺也可以由Indexer生成，官方称未来可能会考虑增加专门的验证者。验证内容将以分布式方式存储，并在一段时间内（参考ETH上的blob存储时间，设为一个月）公开，在此期间任何人都可以验证验证内容。

使用Nubit的DA层解决方案：Nubit是一个具有即时最终性的比特币原生数据可用性层。Yala 正在与数据可用性 （DA） 层 Nubit 合作构建索引器。借助 Nubit 的数据可用性层，Yala 的索引器能够对 Inscription Assets事件进行更深入、更可靠的验证。

执行层：

执行层包括BTC Vaults和Oracle模块模块。

Oracle模块：借贷协议需要实时获取抵押资产的市场价格，以确定何时触发条件执行。Yala基金会负责维护Oracle模块和Oracle安全模块（OSM）。Oracle模块从链外来源获取价格输入。链外Oracle节点通过链外数据API检索所需数据，将其格式化后返回给Oracle模块。为了防止攻击者试图控制大多数Oracle，Yala协议使用OSM接收价格输入，而不是直接从Oracle接收。OSM作为Oracle和协议之间的防御层，发布价格时有30分钟的延迟，以便在Oracle受损时进行紧急防御。Yala基金会负责决策紧急Oracle和价格延迟的持续时间。

BTC Defi模块：Yala中的所有DeFi交易操作通过Indexer（共识层）- 根据Oracle的价格信息引导Defi模块的状态变化。

Yala 创新地设计了模块化架构，实现比特币的原生 DeFi 协议。Yala 的稳定币支持多链且在目标链上是原生的，使用户可以通过 $YU 在多个生态系统中的各种 DeFi 协议上获得额外收益。此外，通过共识层的 Indexer 来维护链外交易状态，并将其反映到链上的 UTXO，同时借助比特币的共识机制来验证交易。然而Yala 的 Indexer 可信度和链外数据的安全实时更新仍然面临挑战，Yala积极探索具体的推进方案。目前，利用Polyhedra的zkbridge的信息验证，帮助Yala在bitcoin和EVM的生态做多链验证功能，保证DeFi的安全性。加上利用Nubit DA，帮助Bitcoin生态的inscription信息验证。对于这个从零到一，要到一百一万的创新项目，Yala团队积极探索，怀着对安全技术的热忱追求打造这个defi项目，未来我们有望见证这一系统的进一步完善和优化。

项目进度：

Yala官方宣布与Alchemy Pay、Avail、Babylon、Botanix、Map protocol、Nubit、 Polyhedra和Stacks合作。

根据官方信息，开发团队目前仍在继续改进Yala的基础设施。

### 三、项目对比

本文梳理了几个比特币流动性相关的项目，包括Babylon、BounceBit、Solv、Lorenzo和Yala，旨在帮助大家更好的了解这些项目。接下来，我们将对这些项目进行对比分析，从而为大家提供一个更客观的视角。

名称

Babylon

BounceBit

Solv

Lorenzo

Yala

项目核心

将比特币安全带给PoS链

CeFi+DeFi结合盘活比特币流动性

通过SolvBTC将比特币的流动性带入各种 DeFi 协议

提供比特币的LPTs和YATs交易市场；优化用户收益

实现多链稳定币的比特币原生DeFi协议

技术实现

通过比特币时间戳协议和比特币质押协议共享比特币安全

验证者共同维护跨链桥，Mainnet Digital的托管服务，辅以Ceffu的MirrorX技术

将各种流动性资源和投资机会整合到一个平台上

；交易策略Vaut 执行投资策略

模块化设计，SPT & YAT 控制模块管理和控制LPTs和YATs的发行和交易；质押代理监管机制

模块化设计，通过稳定币模块铸造多链原生稳定币，支持多个DeFi协议

支持的链

比特币、Cosmos，Binance Smart Chain，Polkadot，Polygon等；EVM兼容

比特币，BNB链，以太坊等；EVM兼容

比特币、Merlin、Arbitrum、BNB Chain等; EVM兼容

比特币、Babylon，BitLayer, 未来将支持其他链；EVM兼容

比特币、以太坊、Solana、Arbitrum等；EVM兼容

安全机制

基于比特币时间戳的校验点和惩罚机制；针对PoS攻击的一次性提取签名（EOTS）

验证者批准（>50%）跨链交易；Ceffu 多方签名钱包

Safe Guardian交易规则，多重签名和时间锁控制智能合约升级

多重签名钱包，证明验证，分叉检测；质押代理监督机制

通过Indexer（链外）实现共识和数据可用性，通过UTXO实现链上验证

从表中可以看出，虽然每个项目的侧重的不同，但这些项目都致力于促进比特币的流动性。通过各自独特的技术解决方案，让用户可以将自己的比特币发挥出更大的经济价值。这不仅帮助用户通过不同的方法获取收益，还大大提升了比特币作为数字资产的流动性和应用广度。

### 四. 总结与展望

越来越多为了提升比特币流动性效率的项目出现，它们不仅提升了比特币的流动性，还拓宽了其在去中心化金融技术领域中的应用。这些项目通过提供创新的解决方案和便捷的交易功能，极大地促进了比特币生态系统的发展。

今年比特币ETF的通过，也是加密货币领域的一个重要里程碑。ETF的通过不仅向加密圈外的投资者展示了比特币的潜力，也使得合规资金能够更加便捷和安全地进入这一市场。这对比特币和整个加密货币市场来说，都具有深远的意义。

由于比特币流动性的相关产品与资金直接挂钩，每个项目需要确保其协议或智能合约的安全，尤其是在处理跨链操作和复杂的金融产品时，任何小的漏洞都可能导致重大的资金损失。由于不同的区块链之间存在差异，特别是比特币上缺乏完善的智能合约系统，整合和互操作性成为一大挑战。开发者需要具备广泛的知识和适应能力，结合不同区块链之间的特性实现更有效的数据和资产交换。虽然面临诸多挑战，但随着技术的进步和市场的适应，GeekCartel 相信比特币生态的未来依旧乐观，预期会带来更加丰富和安全的去中心化金融产品和服务。

来源：https://medium.com/@GeekCartel

### 参考资料

图片：

https://docs.babylonchain.io/assets/files/btc\_staking\_litepaper-32bfea0c243773f0bfac63e148387aef.pdf

https://x.com/babylon\_chain/status/1796171723471258091

https://docs.bouncebit.io/cedefi/bouncebit-cefi-+-defi/infrastructure

https://medium.com/@bouncebit/explaining-bouncebits-philosophy-77b4682cf111

https://bouncebit.io/

https://solvprotocol.medium.com/unlocking-the-power-of-solvbtc-your-gateway-to-bitcoin-yield-and-btcfi-4dea1dbddc4a

https://x.com/SolvProtocol/status/1797531248384147663

https://docs.solv.finance/solv-documentation

https://docs.lorenzo-protocol.xyz/introduction/architecture

https://medium.com/yalabtc/bridging-bitcoin-liquidity-how-does-yala-stablecoin-achieve-meta-yield-6ced86cd6e5a

https://docs.yala.org/yala-a-bitcoin-based-asset-protocol/yala-architecture

文本：

https://bitcoin.org/files/bitcoin-paper/bitcoin\_zh\_cn.pdf

https://lorenzo-protocol.notion.site/56688385995649bfa7ea87bdbcc4ebf4

https://www.binance.com/en/square/post/97988

https://www.investopedia.com/bitcoin-taproot-upgrade-5210039

https://www.coinbase.com/en-sg/learn/crypto-glossary/what-are-brc-20-tokens

https://docs.babylonchain.io/assets/files/btc\_staking\_litepaper-32bfea0c243773f0bfac63e148387aef.pdf

https://arxiv.org/pdf/2207.08392

https://docs.babylonchain.io/assets/files/btc\_staking\_litepaper-32bfea0c243773f0bfac63e148387aef.pdf

https://coinmarketcap.com/academy/glossary/timestamp

https://academy.binance.com/en/glossary/unspent-transaction-output-utxo

https://research.web3caff.com/zh/archives/16140?ref=1502

https://blog.nomic.io/stbtc-babylon-4e362d61a3b0

https://blog.ata.network/automata-collaborates-with-babylon-to-advance-tee-research-and-enhance-multi-prover-security-with-5f49d7d38ace

https://babylonscan.io/timestamping

https://docs.bouncebit.io/

https://medium.com/@bouncebit/introducing-liquid-custody-on-bouncebit-78e5923f7687

https://www.ceffu.com/support/announcements/article/bouncebit-partners-with-ceffu-Integrates-mirrorx-for-off-exchange-settlement

https://www.ceffu.com/blog/what-is-multi-party-computation-technology

https://mnd-dev-media-reimp.s3.ap-southeast-1.amazonaws.com/5f3202c0\_139a\_4513\_a66e\_f6f5621cf1bd\_fa058c1996.pdf

https://www.theblock.co/post/279603/bitcoin-restaking-protocol-bouncebit-funding-tvl

https://docs.solv.finance/solv-documentation/getting-started-1/how-it-works/a-decentralized-asset-management-architecture/2.-built-in-safe-guardian

https://docs.solv.finance/solv-documentation/getting-started-1/how-it-works/a-decentralized-asset-management-architecture/3.-price-oracle

https://docs.solv.finance/solv-documentation/getting-started-1/how-it-works/a-decentralized-asset-management-architecture/1.-trading-strategy-vaults

https://www.investopedia.com/terms/d/deltaneutral.asp#:~:text=Delta%20neutral%20is%20a%20portfolio%20strategy%20that%20uses%20multiple%20positions,of%20the%20position%20to%20zero.

https://docs.lorenzo-protocol.xyz/introduction/bitcoin-liquidity-finance

https://docs.lorenzo-protocol.xyz/introduction/bitcoin-restaking-token-issuance-and-settlement

https://docs.lorenzo-protocol.xyz/introduction/financing-bitcoin-retaking-tokens#id-1-exchanges-for-lpts-and-yats

https://news.bitcoin.com/building-on-bitcoin-how-yala-is-transforming-btcs-potential-into-a-reality

https://academy.binance.com/en/glossary/unspent-transaction-output-utxo

https://medium.com/yalabtc/a-deep-dive-into-yalas-collateral-and-insurance-strategies-962da37dd9c1

https://bitcoinops.org/en/topics/tapscript/

https://docs.yala.org/yala-a-bitcoin-based-asset-protocol/native-brc20-based-defi-attempts#primary-tokens

### 致谢

在这个新兴的基础设施范式中，仍有许多研究和工作要做，本文未涉及的领域也很多。如果您对任何相关的研究主题感兴趣，请联系Chloe。

非常感谢Severus和Jiayi对本文提出的有见地的评论和反馈。