BTC、Solana、Restaking，一级市场角度如何看待这三个赛道？

撰文：Lao Bai

很喜欢的公众号《橙皮书》前段时间发布了一篇文，标题叫做「Crypto 阳痿」。

「一种可怕的无聊在 Crypto 世界蔓延，像黑死病一样，没人知道从哪开始的，但是不知不觉的，你发现这种病已然无处不在了」。

想想也是，最近的圈子，技术上的热点确实没什么值得拿来大书特书的，唯一有热度的话题集中在 Pepe，Trump，Jenner 等 Meme 上，上一次偏技术向的热点可能还是图币二象性的「Pandora」?

一级市场也同样受到影响，好在创新总还是在发生，虽然依旧没有看到什么真正 0 到 1 的东西，但 1 到 10 的东西各个赛道 Still Happening。

上期研报主要集中在 ETH 上 Modular 叙事下各个层的新思路，这期我们来看看 BTC，Solana，以及 Restaking 这三个赛道上的「1 到 10」都有哪些

### 一.BTC

很多人期待的 Rune 并没有带来想象的热度，如果说 BRC20 或者说 Ordi 是一场「手忙脚乱」的惊喜的话，Runes 则是一场从 Cex 到 Dex 到 Infra 集体「万事俱备，只欠东（上）风（线）」的迎接仪式，然而应了那句「大热必死」的老话，至少短期内是这样。长线来看，Runes，Atomical，RGB&RGB++ 等协议还是有望给 BTC 的资产发行注入新的活力，BRC20 两个月前的升级也明显朝着功能性更加灵活的路线在努力，别的不说，基于 BRC20 的原生稳定币目前实现起来就容易许多了。

BTC 生态最近两个月最值得拿来说道说道的，除了之前我写过的 UTXO Stack，应该是 Unisat 推出的 Fractal -@fractal\_bitcoin，Arch Network -@ArchNtwrk，以及 Quarry -@QuarryBTC 这三个项目。

Fractal - 有着非常「奇特的」设计理念，本质上你可以把他看作是一条 BTC 的 100% Fork，但出块时间降低到了 30 秒

你可能会想 - 这啥玩意啊，这不就是个 BTC 测试网么？莱特币，BCH，BSV 啥的好歹还有些自己的东西，你这就是个 99% 镜像链，有什么意义呢？安全性怎么保证呢？

其实意义不少

1. Fractal 正儿八经的跟 BTC 一样的 POW，SHA256，有市值，有激励，比 BTC 测试网稳定很多（用过 BTC 测试网的都懂），且快很多（30 秒一个块）

2. 跟 BTC 主网 1/3 联合挖矿（主网矿工每 90 秒可以挖一个 Fractal 区块），理论上可以做到 80-90% 级别的 BTC 主网安全性

3. 因为与 BTC 100% 保持一致，所以先有 BTC 上的各类 XXRC20 资产和基础设施都可以无缝迁移过来，不需要改一行代码

4. 会比 BTC 主网更快实施 OP\_CAT，ZK 原生验证 OPCode 等具备「争议性」的操作码提案

5. 因为 4，未来可以通过脚本实现基于铭文的合约

6. 这事儿别人做你会觉得很奇怪，但 Unisat 来做，感觉再适合不过了

Arch - 相较于各类「审美疲劳」BTC EVM L2/ 侧链，Arch 通过一个索引器 + 带去中心化 Prover 的 ZKVM，把可编程性带入了 BTC，类似一个 1.5 层 - 交易通过 L1 来触发，在 Arch 的 ZKVM 里执行各种资产转换的逻辑，最终生成 ZK 证明并把结果广播回 BTC 主网

给我的感觉和 RGB++ 有些异曲同工之妙，都是依靠 BTC 主网交易来触发，不同的是 RGB++ 用的是基于 CKB Cell 的同构绑定，而 Arch 则是依赖索引器 +ZKVM 来实现

Quarry - 把基于 BTC 的联合挖矿做成了 Infra 形式，相当于做了一套矿工或者说算力版本的「OP Stack」+ 「Eigen Layer」

简单来说，你可以通过他们 Quarry 快速 Launch 一条 POW 链，这条链可以与 BTC 矿工进行联合挖矿，通过 BTC 矿工的 hashrate 来保证自身的安全。而代币奖励则给到参与的矿工，类似 EigenLayer 的 AVS 奖励。相较于 EigenLayer 或是 Babylon 争取的是 BTC 与 ETH 的持币用户的 POS 安全，Quarry 争取的是矿工的哈希算力安全。只是在 POS 大行其道的市场，POW Appchain 能够啃下多少份额，还值得观察下

### 二. Solana

Solana 这段时间最有意思的应该是「模块化」这个概念

众所周知，ETH 这边走的是模块化这个概念，而 Solana 一直是单片链那边阵营的代表

而过去几个月，确实聊过数个在 Solana 上做模块化的项目

比如 MagicBlock -@magicblock，Sonic -@SonicSVM，Solforge，Mantis -@mantis 等等

Magicblock 主打的是一个 Ephemeral （临时）Rollup - 主打一个「用完就删，阅后即焚」，话说这概念最早应该是 AltLayer22 还不 23 年最早提出的，但现在应该不是 Alt Layer 的主要卖点。MagicBlock 作为主打 Solana 全链游戏引擎的项目，这个 Ephemeral Rollup 应该会是他们解决方案的一部分

Sonic 主打的则是 Solana 上的 Gaming Appchain，最近也是刚刚官宣完了融资, 用了一套 HyperGrid Framework 的架构可以让游戏轻松的发一条 SVM Appchain 出来，Sonic 作为第一个打样的 L2 应该可以理解成 Arb 上的 XAI？

Solforge 则是一个偏通用型 Appchain Stack，打算定位成 SVM 版的 OP Stack 或者 Arbitrum Orbit

Mantis 则是一个 Intent 结算层的 SVM Rollup，并不局限于服务 Solana 生态，跟 EVM 相关的 OrderBook Flow 一样可以来 Mantis 这边结算，毕竟 Solver 这东西天生自带部分链抽象属性

这里有几个有意思值得观察的点

1. Solana 虽然主打单片高性能，但据说上半年一个游戏火了之后，这游戏的 TX 占到了全链的 20% 之多，这还是日活只有 4,5 位数的情况，不敢想如果日活再上一个台阶，或是出现数个类似游戏链会承受怎样的负荷，这可能也是 Solana 生态起了「模块化」念头的重要催化剂

2. Toly 本人从去年的反对模块化，到今年似乎对这个方向偏中性态度了，从他今年的 Twi 便能看出不少端倪

3. Solana Foundation 的不少人是偏向支持模块化的，不少开发者也认为 Solana 的模块化势在必行

4. Multicoin 的 Kyle 一直是 Solana 与单片链的布道者，他本人据说依旧反对这个概念

未来 6-12 个月 Solana 的基建应该会是个有意思的观察，除了模块化叙事的升温，FireDancer 年底前的精简版和明年的完全版上线会给 Solana TPS 和稳定性带来的提升，也非常值得期待

### 三. Restaking

Restaking 应该是近半年最火的一个赛道，没有之一

然而发现很多人对于当前两大龙头 Babylon 于 EigenLayer 的区别并没有很了解，甚至一些聊过的项目方也对此有些疑惑，所以值得拿出来单独说说

简单来说，Eigen 因为天生具备智能合约的能力，所以可以设置相对复杂的 Slashing 机制，比如第一个打样的 AVS EigenDA 就是这么来的，如果你想用 Babylon 来做一个类似「BabylonDA」之类的东西，是实现不了的，因为 BTC 原链的脚本支持不了这么复杂的东西

但同样，Babylon 的黑科技 EOTS（可提取的一次性签名）以及 BTC 时间戳协议也是 Eigen 没有的，这也是 Babylon 可以在 BTC 生态做独一份 Restaking 的底气，主打一个「原生 BTC Restaking」，这也是 Eigen 实现不了的

当然，这种原生 BTC Restaking 能实现的功能有限，基本上覆盖的就两点，一是帮助 POS 链通过 BTC 时间戳协议防止 Long Range Attack，二是帮助 POS 链实现或者说冷启动他的 POS 安全共识。一言以蔽之，发链可以找我，做 DAPP 请出门左转去隔壁 Eigen

如果你就是非要想拿 Babylon 去做一个 AVS，来实现一个类似 EigenDA 或者 Oracle 之类的东西行不行呢？答案是「可以」，但你需要「扩展包」。比如 Chakra -@ChakraChain或是 SatLayer -@satlayer，在 Babylon 之上「套一层娃」，用这两个项目内置的智能合约来实现更加复杂的 Slashing 机制，你就可以基于此去开发类似 DA，存储，预言机之类的 DAPP 流派 AVS 了

抽象一点来说，单就功能性来讲: Babylon+Chakra/SatLayer = Eigenlayer

Babylon 这边，生态项目除了像是上述两个致力于把 Babylon 变得像 Eigen 一样「复杂」，还有像是 Solv Protocol,Lorenzo 等对标 EtherFi，Renzo 这样的 LRT 生态位。Eigen 这边，因为天生就「足够复杂」，所以 Stack 或者说「扩展包」已经堆到一个更高的 Level，比如 Ethos -@EthosStake 做的是 AVS 的 Coordination/Interoperability Layer, Aethos -@aethosnetwork 做的是 AVS 的 Programmable Policy（策略编辑）Layer 等等。感觉随着 Eigen 这边的 Stack 越来越丰富，基建越来越完善，Eigen 可能也越来越像一个 AWS，最终各种点点点 + 拖拽就能实现你想要买的一个「安全等级 + 基建套件」，在此之上你是要起一个链还是做一个存储或是 Oracle 之类的 DAPP，完全是你的自由

P.S 最近跟一个 FA 聊天，他说近期聊了至少五六十家 VC，有看 Infra 的，有看游戏的，有看比特币的，只有一个赛道是所有 VC 都在看的，一个不拉！你们猜是哪个？

答案是：Ton……

然而 Ton 上面投资，难度比 ETH 或者 Solana 上高得多……你就想下如果半年前 Notcoin 拿着 Deck 或者 Demo 来找 VC，会有几个 VC 看到这玩意会决定梭哈呢……

下次研报如果有机会，我再来写写 Ton