# 未来可期：详解 Rollup 技术、应用与数据

**摘 要：**

2020 年爆发的 DeFi 热潮将链上活跃度推至新高度，也将公链面临的性能问题直接放在了大众眼前。作为目前拥有最大生态的以太坊 Gas Price 飙升，在相当长的时期内维持在 100 Gwei 以上，让以太坊获得了“贵族链”的戏称。虽然近期以太坊 Gas Price 有所下降，但也无法改变冗余存储和冗余计算带来的效率下降的问题。在诞生的各类效率提升的技术中，Layer2 赛道下的 Rollup 技术无疑是当前解决方案中最为亮眼的。

Rollup 的技术方案承袭了其他 Layer2 前辈们，如闪电网络、Plasma 等解决方案的思路。但最为关键的还是其将二层数据再反存到一层的思路。这一思路与以前所有的 Layer2 方案都不同，成为了 Rollup 技术解决用户使用二层时可用性、易用性问题以及衍生的安全性问题等的关键。

围绕 Rollup 技术，诞生了不少优秀的解决方案团队，本文着重介绍了其中四个——Matter Labs、Optimism、Offchain Labs 以及 Starkware。他们在 ZK Rollup、Optimistic Rollup 以及混合 Rollup 上做出了诸多尝试，成为 Rollup 技术体系在不同方向上落地的主要推动团队。除了技术解决方案团队之外，也有不少团队在摸索具有 Rollup 特色的应用，如 Layer2 世界的公交车 Layer2.finance、减缓 Layer2 带来的流动性分割问题的 Caspian 以及帮助 Optimistic Rollup 用户实现快速提款的 Dai Bridge 等，本文也将对这些应用方案做探讨。

从数据表现来看，由于 Layer2(数据统计不包括侧链)方案应用场景尚未铺开，目前整体 Layer2 上的锁仓资金不到 Defi 整体锁仓的 3%，而 Rollup 占据了其中的近 1/3。目前，Optimistic Rollup 的落地已经近在咫尺，通用的 ZK Rollup 系方案还需要一段时间。Op 系的技术有望将以太坊 TPS 提升至 500 上下，ZK 系则能有 100 倍左右的提升，也有一些混合 Rollup 方案其理论 TPS 能达到 2 万。

总体而言，Layer2 是公链发展的必由之路，而 Rollup 技术则是目前为止 Layer2 技术中将易用性、安全性、扩展性、通用型等的平衡做的最好的技术。未来几个月，我们也将看到 Rollup 的解决方案和应用大规模落地，值得期待！

## 作 者

【火币研究院】赵文琦，陈晗，袁煜明

## 作者联系方式

火币研究院：huobiresearch@huobi.com

# 目录

# 一、 Rollup 概述

## 1.1 什么是 Rollup？

在链下的世界中，人们习惯了高速的交易、即时的确认、海量的存储，集中和信任带来效率。进入链上，基于代码控制和博弈机制的运转的分布式系统实现了分散和去信任，存储冗余和计算冗余成为保障系统安全性的重要手段。但冗余不可避免地带来成本提升和效率降低，链上应用的体验让用户产生时代倒退的感觉。为此，也诞生了各类提升区块链运转效率的改进方案。

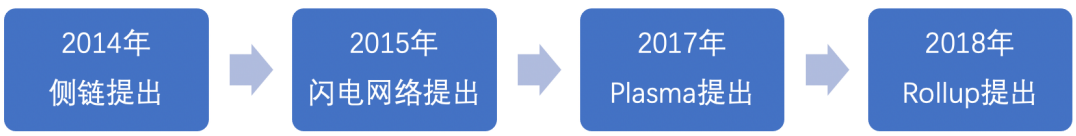
链上改进方案中包括了扩展区块大小、改变共识算法、分片等等。虽然链上的改进方案在当前的区块链技术发展阶段还没有完全展现出在提升效率上的实力(如 ETH2.0 的分片还在开发中)，但其都**无法改变在区块链上为了安全性必须要承受冗余存储和计算的约束的现状**。而这一约束可以被链下的改进方案打破。将存储和计算转移到链下，并设计机制保障链下存储和计算的可信与安全是链下扩展方案的核心。Rollup 就是链下方案中的一类。

那么，Rollup 是什么？国内通常把它翻译成“卷叠”，读起来有点怪但是还是十分形象，打包为卷、压缩为叠，**链下的交易数据打包压缩后传到链上存储**，Rollup 就是对符合这一特征的一类 Layer2 技术的总称。与此相关的一个趣事是 Matter Labs 公开称 ZKSwap 并不是 Rollup，只是一个 Validium[1]，因为当时的 ZKSwap 未满足这一特征。

## 1.2 如何演进出 Rollup？

在 Rollup 之前，Layer2 已经有了几代技术。但是由于**去信任化、安全性、易用性或者通用性方面的问题**，都没有成为被广为接受的方案。Rollup 技术的出现成为打破这一局面的关键。

图1-1 Layer2 技术演进




[1] https://twitter.com/the_matter_labs/status/1364567175864987649

来源：火币研究院[2345]

最早的 Layer2 是**侧链**技术，其发展一直不温不火，最近由于 Polygon 的崛起引来了很多讨论。但，如 Polygon 一类的侧链的运行基础是信任[6]一组验证者，**这类有强信任假设的方案，在没有易用的无信任假设的方案诞生前，可以被作为一种折中方案应用，但绝不是最终的最优方案**。另外，业界对于将侧链归类于 Layer2 是持怀疑甚至是质疑态度的，**原因在于侧链不会保持向主链同步状态变更，更接近一条独立的链，一个新的 Layer1**。

**闪电网络**是最早的尝试无信任假设的 Layer2 解决方案之一。他通过 RSMC 和 HTLC 技术分别解除了对交易对手方的信任依赖和对资金路由节点的信任依赖。即，用户无需假定交易对手方和转发资金的中间节点是不会作恶的。但是这种方案在**安全性、易用性、通用性**上都付出了代价[7]，限制了该项技术的应用推广。

**Plasma** 是闪电网络之后出现的技术。**其模型兼有侧链和闪电网络的特点。**Plasma 与闪电网络的不同在于链下交易的传递、组织和提交形式。闪电网络链下交易的传递基于以状态通道连接而成的网络，交易存储在交易双方的状态通道中，通道中的交易对手方均可自行提交通道中的交易带来的状态变更。但 **Plasma 选择了与侧链更为接近的交易传递和组织形式**，会有 Layer2 的运营者负责接收交易、组织存储(在 Plasma Cash 方案中，需要用户自己存储一部分交易信息)和将状态变更提交上链。然而，侧链是基于信任的模式，用户侧链上的运营者(或者说矿工)不作恶。**在去信任化上，Plasma 沿袭了闪电网络使用欺诈证明的思想**，通过设置挑战期和激励博弈来防止作恶。但是，Plasma 同样存在**安全性、易用性、通用性**上的问题，现今基本是一条已经被放弃作为独立 Layer2 的技术路线。

Rollup 方案仍然**保留了 Plasma 借用二层的运营者来接收、存储和提交状态变更的思想**，但考虑到此前方案中将数据存储在链下的思路衍生出了安全性和易

[2] 侧链：https://blockstream.com/sidechains.pdf
[3] 闪电网络：https://lightning.network/lightning-network-paper.pdf
[4] Plasma：http://plasma.io/plasma.pdf
[5] Rollup：https://github.com/barryWhiteHat/roll_up
[6] 关于信任，可以参考 Vitalik 的文章《Trust Models》，其中提到，”trust is the use of any assumptions about the behavior of other people”, https://vitalik.ca/general/2020/08/20/trust.html
[7] 详情可以参考火币研究院文章《穿云而过的闪电网络》

用性问题，而直接将数据存储在链上无法实现效率提升，因此诞生了将**数据压缩上链的思路。交易数据上链后最直接解决的是用户易用性的问题**，链上的数据是公开透明的，意味不再需要为了防欺诈而要求用户做出一些十分伤害体验的行为，如保持一定的上线频率以及自行保存用于自证清白的数据(闪电网络和 Plasma 都有此要求)。同时，数据上链也间能接解决了一些可能衍生的安全问题，如闪电网络瞭望塔隐私泄露、Plasma 上的批量退出等在 Rollup 的场景下是不需要被考虑的。

图1-2　如何演进出 Rollup

| 侧链 | 闪电网络 | Plasma | Rollup |
| --- | --- | --- | --- |
| • 基于信任 | • 不基于信任 | • 不基于信任 | • 不基于信任 |
| • 不需要向主链同步状态 | • 需要向主链同步状态 | • 需要向主链同步状态 | • 需要向主链同步状态 |
| • 交易发送给运营商 | • 交易发送给对手方 | • 交易发送给运营商 | • 交易发送给运营商 |
| • 运营商存储交易 | • 用户自行存储交易 | • 运营商存储交易，用户存储部分数据 | • 运营商存储交易 |
| • 交易存储在侧链 | • 交易存储在链下 | • 交易存储在链下 | • 交易存储在链下和链上 |

来源：火币研究院

因此，演进至今，Rollup 其实是借鉴吸收了过往众多方案思想并融合了其特有的链上压缩存储思路。在当前来看，Rollup 无疑是 Layer2 方案中最受期待的。在其即将落地之时，希望通过本文梳理 Rollup 当下的技术、应用与数据。

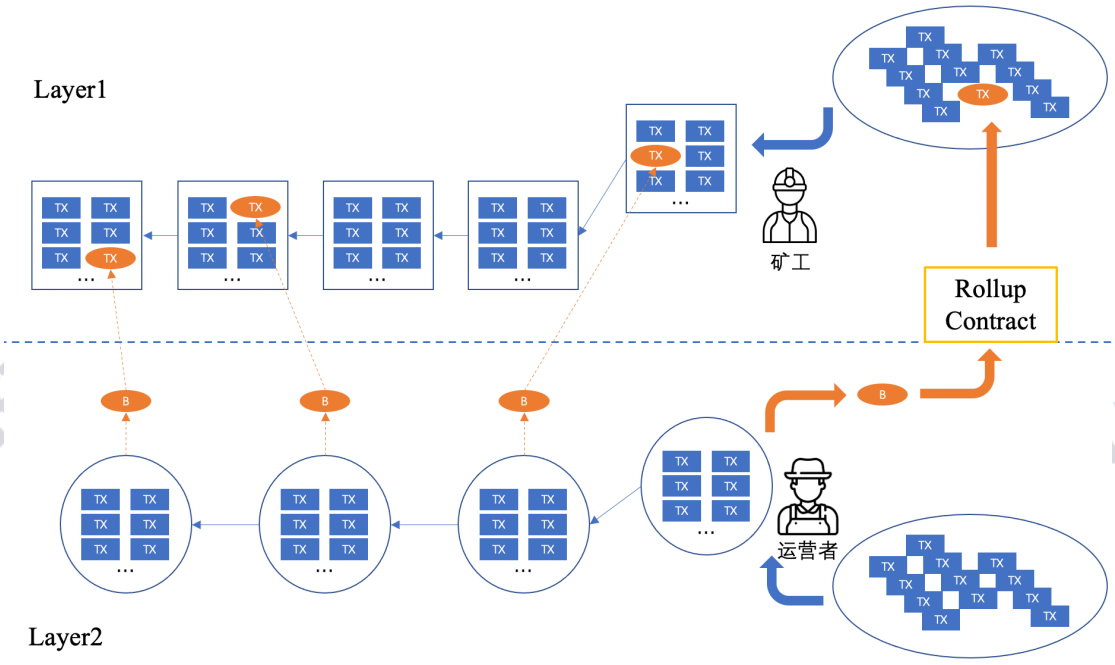
# 二、 Rollup 技术核心要点

在上一章中，我们介绍了什么是 Rollup 以及 Layer2 的思想如何演进传承直至诞生了 Rollup。在本章，我们将深入介绍 Rollup 技术的核心要点。不同 Rollup 技术路线、同一技术路线下的不同团队在将 Rollup 具体落地时会各有差异，因此本小节主要针对 Rollup 共性的思想进行介绍。

## 2.1. Rollup 如何运转？

如下图 2-1 所示，是 Rollup 运转原理的示意图。在 Layer2 上，用户的各种交易会被发送给二层的运营者。运营者会将一批交易进行压缩。压缩成为一笔交易后，调用链上的处理合约进行处理。这笔调用交易就会像其他的 Layer1 的交易一样进入交易内存池。在 Layer1 上，矿工会接收一层网络中所有的交易并打包成区块发布，这其中就会包含由二层打包上来的交易。

图2-1 Rollup 运转原理




来源：火币研究院

虽然不同 Rollup 的具体实现会不一样，但均需要解决三个共性的问题：**如何实现交易压缩、如何将二层的状态转换同步到一层以及如何保证二层运营者如实提交了二层的所有状态转换**。我们将在下面三个小节分别讨论。

## 2.2. 如何实现交易压缩？

关于为什么要将数据上链，在上一章中已经有阐述。**上链后，二层交易数据在链上的数据可用性(或者说数据有效性、数据可获得性)能得到保障**。但数据如果原样上链，是难以达到通过二层提升效率的目的的，所以会进行压缩。讲到压缩，大家通常的理解是对占用字节数的压缩，也就是体积上的压缩，其实不然。**压缩主要是对交易消耗 Gas 数的压缩，因为以太坊上的区块限制是以 Gas 为限制而不是字节数**，更小的字节数对应着更小的存储占用，但不等同于更小的 Gas 消耗。Rollup 中的压缩，**一方面确实压缩了交易占用的字节数，另一方面也会减少交易执行的计算量以降低 Gas 消耗**。

交易字节数的压缩的方式主要包括使用效率更高的编码方式、缩减交易占用字节数、减少需要上传的数据等。

图2-2　交易压缩

| Parameter | Ethereum | Rollup |
|---|---|---|
| Nonce | ~3 | 0 |
| Gasprice | ~8 | 0-0.5 |
| Gas | 3 | 0-0.5 |
| To | 21 | 4 |
| Value | ~9 | ~3 |
| Signature | ~68 (2 + 33 + 33) | ~0.5 |
| From | 0 (recovered from sig) | 4 |
| Total | ~112 | ~12 |

来源：Vitalik 博客，https://vitalik.ca/general/2021/01/05/rollup.html

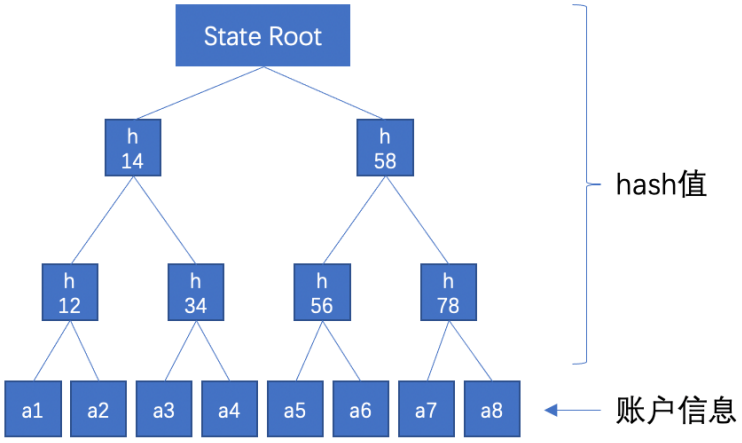
图 2-2 是 Vitalik 归纳的交易在以太坊一层和在 Rollup 上占用的字节数。虽然各团队在最终实现时与 Vitalik 归纳的并不完全相同，但思路是一致的，因此我们在本文中仍然引用 Vitalik 的归纳。

首先，在二层的交易中，Nonce 可以在交易中被省略；Gas 相关的 Gasprice 和 Gas 也不必出现在每笔二层交易中；To 和 From 地址不需要使用以太坊的地址，而是使用其在状态树中的索引(如图 2-3 所示，二层的账户可以由一棵 Merkle 树来组织)；Value 可以使用科学技术法存储节省位数；对于签名，可以将一个批

次中的交易签名进行聚合，降低每个交易的签名存储消耗。同时，这些交易数据会被存储在链上 gas 成本比较低的字段 Calldata 中。

值得说明的是，上传的一层的数据**不仅仅是上述的交易内容**，还会包含**批次交易发生前后的状态根**(图 2-3 中的 State Root)，以及**用于证明(或用于备查)状态转换合法性的数据**。ZK Rollup 系的技术能比 Optimistic Rollup 系技术取得更好的压缩效果，一个重要的原因就是 ZK 需要上传的交易数据比 Op 少，Op 为了方便验证者挑战需要上传一些中间状态信息，但 ZK 只需要针对批次的交易上传证明信息。

图2-3 状态树




来源：火币研究院

除了压缩交易占用字节数以外，Rollup 中交易的计算量也会比直接在一层上执行要少，因为交易不必在一层上重新执行，只需要验证二层运营者提交的状态转换是否正确。对于 ZK 来说，主要来自于验证状态转换证明(零知识证明)是否合法；而对于 Op 来说，主要来自于欺诈交易的挑战消耗。

目前，经过压缩后，在理论上，ZK 系技术能带来的吞吐量提升在 100 倍上下，而 Op 在 30 倍左右。

### 2.3. 如何将二层的状态转换同步到一层？

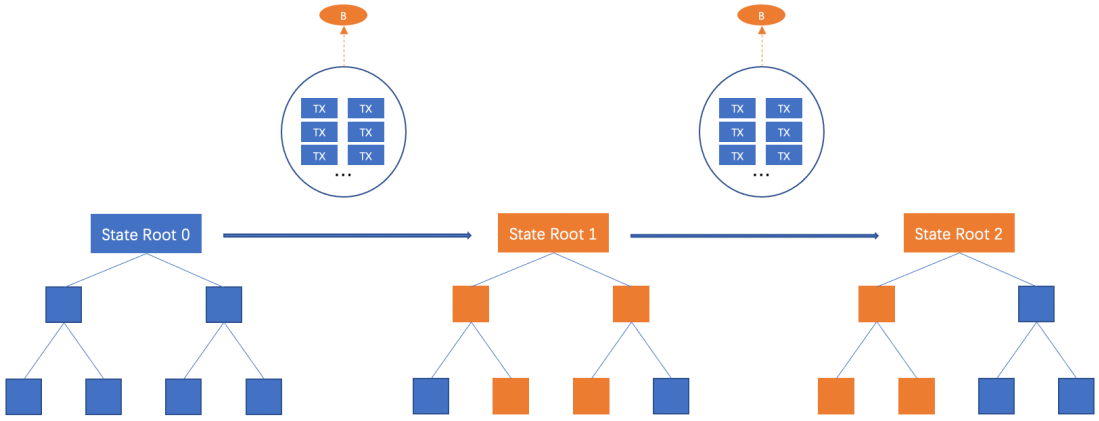
上一小节在讲交易压缩时提到二层运营者除了提交交易信息外，还会提交批次交易发生前后的状态根。这个状态根与以太坊一层的状态树的状态根类似，是

账户状态的归集。

如图 2-3 所示，Rollup 的状态可以用 Merkle 树来组织，叶子节点为账户状态，中间节点存放层层向上进行哈希计算的信息，根节点是最终的哈希值，是二层所有账户状态的摘要。

如图 2-4 所示，是批次交易发生前后的状态转移示意图。二层的交易会改变交易相关的账户的状态，引起叶子节点的信息变动，最终导致根哈希值的变动。二层的运营者会在本地维护二层账户的状态树，记录批次交易发生前后的根哈希值，在上传批次交易时将此二哈希值一并上传。

图2-4 Rollup 的状态转移




来源：火币研究院

## 2.4. 如何防止二层运营者欺诈？

既然，交易信息、状态转换信息都由二层运营者上传，如何阻止运营者上传虚假信息呢？这个问题对于所有要和主链进行状态同步的 Layer2 来说都存在。

Rollup 诞生之前的闪电网络和 Plasma 采用的均是**欺诈证明**的方式，而 Op 系技术承袭二者思想同样使用了该方式。即，在运营者提交信息时不做关于状态转换合法性的校验，但是会为该批次的交易的提交预留挑战期。如果在挑战期内，无人对其合法性做出挑战则交易被确认；若有，则挑战者需提供欺诈证明，证明运营者作恶。

**欺诈证明是相对容易的实现方式(相比后面要提到的有效性证明)，但带来的**

**代价是用户体验和资金效率的牺牲。**在没有保证链上数据有效性的闪电网络和 Plasma 的方案中，需要用户保证一定的在线频率(也叫做用户活性)来防止欺诈，同时，用户资金无法及时取出需要等待挑战期结束。**在 Optimistic Rollup 下，虽然也是使用欺诈证明，但对用户体验和资金效率伤害的情况有所改善。**由于数据上链，挑战者可以由除用户外的第三方提交，降低了对用户活性的假设大幅改善体验。另外，Op 方案下，虽然仍然存在挑战期，但是对于非欺诈的交易，交易的最终性是可以预期的，Op 的使用者可以自行搭建验证节点快速验证交易合法性而不必等到挑战期结束，虽然交易仍然要等到挑战期结束后才能被主链确认，但其最终性可以被快速确认，利用这一点流动性提供商可以提前为用户释放资金流动性。不过，这种解决方案并不是内嵌在 Op 之中，需要依赖应用解决方案。

相比于欺诈证明，更有技术挑战性的防欺诈方式是要求二层运营者提供**有效性证明，即，二层运营者直接证明其提交的状态转换是有效的(正确的)，自证清白。**这也是 ZK Rollup 系方案使用的方式。在该种方式下，提交即正确，用户不必担心欺诈，提取资金也不会有冻结期。方案近乎完美，美中不足是太难，以致于在很长一段时间内，ZK 系解决方案只能针对一些特定的操作生成证明，无法通用。但随着密码学技术理论和实践的突破(PLONK、多项式承诺等)，通用的 ZK 解决方案已经近在眼前了。

# 三、 主要技术团队分析

上一章我们介绍了 Rollup 技术的核心要点，这一章，我们将对数个代表性的 Rollup 团队及他们的解决方案进行梳理。同时，对于每一个方案，我们也将从 Rollup 所关注的**安全性、退出时间、用户活性假设、通用性、计算量、复杂度、吞吐量提升**等方面进行分析，以进一步理解 Rollup 技术。

## 3.1 MatterLabs

Matter Labs 的二层解决方案 zkSync 是 ZK Rollup 技术路线的头部项目。当前的主网版本承载的资金量超过 9 百万美元，二层的单笔交易手续费可以低至 $0.001(但目前在$0.1 级别)。不过虽然其理论吞吐量可达数千，由于需求不足，实际运行的 TPS 小于 0.1。同时，提现时间现在仍在小时级别。

这些数据一定程度上反映了 ZK 系解决方案在当前表现并不良好，但这种不良好更多是由于当前整个二层的发展阶段和 ZK 系技术尚有瓶颈待突破造成的。Matter Labs 在 ZK Rollup 技术路线上处于绝对领先的地位，其兼容 EVM 的虚拟机也将是 ZK 系技术迈向下一个阶段的里程碑。

### 3.1.1. 项目进展

Matter Labs 基于密码学证明开发出 zkSync 解决方案，该方案于 2020 年 7 月上线主网，2021 年 5 月份将上线 zkSync1.x 版本，并且将在 2021 年 5 月份上线 2.0 版本的公开测试网，8 月份上线主网。

1.0 版本支持资产转账，不支持通用智能合约；1.x 版本支持 NFT 原子交换和铸造等功能；2.0 版本将使用 ZK Rollup 和 zkPorter 混合账户架构，该架构支持两种账户的完全互操作，支持图灵完备的 ZincVM，可移植现有的 Solidity 源代码，原生支持所有以太坊钱包，并且其开发中的 zkPorter，通过放弃链上数据可用性，带来 TPS 的大幅提升，远超 ZK Rollup 2000 的理论值，可达到 20,000 笔以上。

### 3.1.2. 技术方案

当前 zkSync 的主网版本是以 ZK Rollup 技术为核心的，其解决方案思路和

前两章介绍的 ZK Rollup 的思路基本一致我们不再赘述。但 Matter Labs 官方在四月中旬发文再次着重介绍的 zkPorter 的解决方案值得关注。

纯 Rollup 的技术解决方案最重要的特点是保证了链上的数据可用性，而链上数据可用性能免除对用户活性的要求，大幅提升用户体验和可用性，但随之带来的是有限的扩展性。因为链上每个区块有 gas 上限，**所以理论上，所有保证链上数据可用性的技术方案都会有扩展性的上限，只能带来线性的提升**。

为了同时免除对用户活性的假设并大幅提升扩展性，**zkPorter 将数据存放在链下以绕开 gas limit 导致的十分有限的吞吐量的上限，同时，对于所有交易，其状态转换的证明仍旧会提交到链上，由链下的守护者进行验证**。zkPorter 中还有一个重要的点是**引进了分片**，ZK Rollup 所在的分片是基础分片，其余所有的分片可以由用户自行决定数据可用性方案，这些分片的可用性可以由 zkSync 的守护者来维护，也可以由该分片上的协议自行维护。**在该种架构下，TPS 可以提升至 2w，手续费也可再降低十倍**(如图 3-1)。

图3-1　zkPorter 数据表现

| Shard | Throughput | Security | Transaction costs |
|---|---|---|---|
| zkRollup shard | 3k TPS | L1-level security via zkRollup | ~USD $0.01 (at 100 Gwei gas price) |
| Guardians shard | 10k-20k TPS | Bond of 2/3 of the zkSync Guardians stake | ~USD $0.001 |
| Protocol X shard | Depends on protocol complexity | Secured by the validators of protocol X | Low |

来源：Matter Labs 官方文档

### 3.1.3.　特点

- **安全性高，没有资金体量上限**。Rollup 部分具备与 Layer1 同等的安全性，同

时二层的承载资金量的增加不会降低二层的安全性。Layer1 上的数据有效性和零知识证明是 zkSync 解决方案的关键。智能合约可基于 Layer1 上的状态、数据和证明自动化验证交易的有效性，没有其他安全性假设。

- **退出时间相对较短。**当前 zkSync 实际退出时间最长需要数小时，但理论退出时间是在 15 分钟左右的。主要原因是当前二层的交易数量不多，延长推出时间可以降低每笔交易需要平摊的手续费。即便如此，相比使用欺诈证明类型的技术方案(如 Op Rollup、Plasma、闪电网络等)数周的推出时间，仍然是相对较短的。
- **无用户活性假设。**由于该技术方案保证了 Layer1 上的数据可用性，并且所有交易都有有效性证明，因此不需要用户保证一定的上线频率来防欺诈。
- **通用性差，暂不支持通用的智能合约。**当前版本的 zkSync 仅支持充提和转账，能力过于有限导致当前 zkSync 没有太多应用场景，整体的锁仓量在 zk 系的方案中表现并不亮眼。这是整个 ZK Rollup 技术路线当前面临的共性问题，即仅支持专用型的操作。但是，zkSync 团队当前正在研究 EVM 兼容以及实现通用的智能合约，并且团队预计在今年即可上线支持通用智能合约和 EVM 的 2.0 版本。
- **计算量大。**对每笔交易，除了要计算每笔交易本身带来的状态转换之外，还需要生成相应的状态转换证明，生成证明的过程需要消耗大量的计算资源。相较而言，其他如闪电网络、Plasma、Op Rollup 省去了这部分的计算资源消耗。同样的交易，zksync 的二层运营商成本会高于 op 系列解决方案的成本，但在当前二层利用率并不高的情况下该资源消耗并未成为 zksync 发展的重要挑战。如果基于 ZK Rollup 的二层应用场景增长，专用的证明器或者定制化的硬件也可以缓解该问题对资源消耗和用户体验带来的影响。另外，zkPorter 的方案也为低计算量和更高的 tps 提供了解决方案。
- **复杂度高。**由于零知识证明技术的复杂性，普通的应用开发团队几乎不能应用 ZK Rollup 的方案去迁移和开发应用。兼容 EVM 的 ZK Rollup 方案会大大改善这一问题，但是其代码的复杂度也会大幅上升，代码的审计会比 OVM 的难度高很多，对该 ZincVM 的安全性和鲁棒性的验证可能需要经数年的考验。

- **Rollup 部分吞吐量提升有限，但 zkPorter 部分吞吐量有望巨幅提升。**由于一层区块 gas limit 的上限限制，Rollup 技术的吞吐量提升无法与其他不保证链上数据有效性的 Layer2 方案相比。但 Matter Labs 团队也意识到了这个问题，提出了新的 zkPorter 的方案以巨幅提升 TPS。

#### 3.1.4. 应用

目前，zkSync 作为 ZK Rollup 技术的头部解决方案受到许多生态应用方的关注，如 Curve 已经在以太坊测试网上集成 zkSync，imToken 与 zkSync 达成深度合作并将在钱包中支持 zkSync，SushiSwap 和 Argent 已选择将 zkSync 作为最终落地的扩容方案。但由于当前 zkSync 支持的操作有限，实际完成集成和应用的还很少，主要集中在支付领域。如 Gitcoin、Storj、Golem 等均集成 zkSync 作为支付方式之一。这些应用场景相比繁荣的一层的生态在实用性和资金回报上都相去甚远，也这就导致了 zkSync 实际的吞吐量仅在 0.05 tx/s 左右。

### 3.2 Optimism

如同 Matter Labs 是 ZK Rollup 技术的头部团队，Optimism 是 Optimistic Rollup 技术路线的头部团队。该团队脱胎于原本研究 Plasma 技术的 Plasma Group 团队，后放弃 Plasma 转向 Optimistic Rollup。

**其提出的 OVM 为降低一层到二层的代码迁移成本提供了重要的思路，便捷的代码迁移是生态快速融合的基础。**虽然其主网还未上线，但是 Synthetix 已经在其基础上运行，目前承载资金量超过 1 亿美金，单笔交易的费用可以低至 $0.07 左右。吞吐量方面，Optimistic Rollup 技术方案的理论值在 500 左右。

数据表现尚不强劲的主要原因是 Optimism 目前还处于有限访问的阶段，只针对部分已授权的应用开放少许功能测试，但其对于通用智能合约较好的兼容性仍然受众多项目方的青睐。从短期看，它的应用场景会更加广阔。

#### 3.2.1 项目进展

Optimism 基于 Optimistic Rollup 的技术提出了 OVM 并且构建了 Optimistic

Ethereum。其在 2021 年 1 月开启 Optimistic Ethereum 主网的软启动（试运行）。随后在 3 月份，Synthetix 开始了向 OE 的迁移，目前已经能在 Synthetix 上进行 Layer2 上的 staking，但其更核心的合成资产和交易的业务尚未部署到主网上。预计在 2021 年 7 月，OE 会上线公共主网。

### 3.2.2 技术方案

Optimism 的 Optimistic Ethereum 是对 Optimistic Rollup 的代表性实现，其技术核心思想在前两章有过深入讨论这里不再重复，但需要针对其 OVM 做特别说明。

**Optimism 支持在二层扩容网络上使用 OVM，一方面兼容以太坊虚拟机最大程度保障通用性，另一方面做了一些适应性调整保障 OVM 可以实现 Optimistic Rollup 的机制。**这些调整主要包括三个方面，第一方面是调整虚拟机中的一些操作码，来保证程序在一层和二层执行的时能得到相同的结果，例如对 TIMESTAMP、ADDRESS 等操作码的调整；第二方面是调整了编译器，保证 Solidity 编写的程序能被正确编译成 OVM 支持的操作码；第三方面是修改 Geth 客户端，让其兼容 OVM 对交易的处理方式。

### 3.2.3 特点

- **安全性弱于一层。**欺诈证明路线的方案，依赖于一层的抗审查性。如果二层交易的资金量很大，可能会诱使一层的矿工发起 51%攻击，审查挑战交易，导致二层作恶的排序者提交的虚假交易无法被成功挑战。
- **退出期长，资金效率低。**Op Rollup 基于经济激励的博弈模型使得交易在挑战期结束以前不具有确定性，并且无法运行全节点的终端用户无法提前验证交易的确定性。因此 Op Rollup 相较 ZK Rollup 的验证时间长，PoW 共识机制下的挑战窗口期约为 2 周，PoS 共识机制下的挑战窗口期为 1 周。
- **无用户活性假设，但需要验证者。**Optimism 团队的解决方案保一层上数据的可用性，虽然仍然需要监控一二层状态防止欺诈，但不需要用户自行监测，可由第三方的验证者代替。
- **灵活性高，支持通用智能合约。**Optimistic Ethereum 是第一个无需大规模重

写智能合约即具有完整跨层移植功能的 Rollup 解决方案，即以太坊上的应用的合约代码迁移成本非常低。因此，在短期成为了众多应用团队关注和选择的解决方案。

- **计算开销较低、一层 gas 消耗较低。**该解决方案中的的状态转换的有效性不需要在一层主动验证，相比于 ZK 系的解决方案能节省大量的验证的 gas 消耗。并且省去了在二层生成证明的计算开销。
- **吞吐量提升十分有限。**纯 Rollup 系的技术，对吞吐量的提升由于受限于一层区块的 gas limit，本身就十分有限，加之 Op 需要提供更多的中间状态数据便于挑战，所以只能带来几十倍的吞吐量提升，是各类二层技术中提升最为有限的方案。

### 3.2.4 应用

虽然基于 Optimistic Rollup 的 Optimistic Ethereum 在安全性和资金效率上都不如 ZK 系的技术，但由于其兼容 EVM 的解决方案有望成为 Rollup 系技术中最先落地的，许多团队采用其作为下一个阶段的扩容解决方案。当前，Synthetix 已在 Optimistic Ethereum 上实现质押服务，Uniswap 也一直在与其合作推进二层的落地，在近期也宣布了将在其上推出 alpha 版本。。Volmex 在 Optimism 本地测试网上开发应用并进行 OVM 部署，IDEX 上线低延迟、高 TPS 的 2.0 版本，MakerDAO 为 Optimism 提供二层 DAI 快速提款方案以缩短提款时间至几分钟，Compound 预计选择 Optimistic Rollup，Saddle 未来将智能合约迁移至 Optimism 上。

## 3.3 Offchain Labs

Arbitrum 方案是由 Offchain Labs 提出并创建的，最早是一个纯粹的研究型学术项目，后经过不断优化和改进，逐渐转入实践。

该方案也是基于 Optimistic Rollup 的解决方案，通过经济激励的博弈模型维护安全性并通过欺诈证明来维护交易有效性，**主要区别在于挑战机制和实现形式。**目前，Arbitrum 主网还未上线，但已经在以太坊的主要测试网中运行了一段时间，性能表现良好。测试案例的数据显示，其最优吞吐量在几百左右，挑战期只有数

十分钟。只不过，挑战时间设置的较短可能会带来一些安全问题，还有待技术团队来进一步解决和完善。

### 3.3.1. 项目进展

截至目前，Arbitrum 测试网已经平稳运行了约六个月。2021 年 3 月，Offchain Labs 团队更新了第四个测试网版本，并将其选定为主网的候选版本。5 月 28 日，其主网测试版 Arbitrum One 已经向开发者开放。如果不出意外，其公共主网将于 2021 年内上线。根据 Arbitrum 的路线图，团队下一步的工作是主网的正式上线。为此，团队正在和多个项目方积极合作，共同进行网络的集成、审计和压力测试。

按照目前的进展来看，**Arbitrum 有可能反超 Optimistic Ethereum 成为以太坊上第一个落地的通用型 Rollup，这对于整个以太坊生态和 Rollup 来说都是重大的突破。**

### 3.3.2. 技术方案

Arbitrum 技术方案的设计与 Optimism 类似，与可兼容以太坊智能合约，并可通过欺诈证明和经济博弈的方式维护交易有效性，二者的主要区别在于挑战机制。Optimism 只需要排序者和验证者执行一次欺诈证明交互即可判断出结果，**而 Arbitrum 认为一次交互可能导致欺诈证明需要包含大量的交易从而超出 gas 限制，并且提出欺诈证明是由于单条指令执行异常导致，无需执行全部的指令。**因此，Arbitrum 将欺诈证明分为多轮步骤，只需要证明排序者在执行某条指令时出现异常，即可证明排序者作恶，节省成本。

### 3.3.3. 特点

Arbitrum 的方案与 Optimism Rollup 的主要特点是一致的，我们不再赘述，主要可以关注欺诈证明机制的变化带来的改变。

- **多轮欺诈证明交互。**Arbitrum 采用多轮欺诈证明验证交易的有效性，降低单次挑战需要消耗的 gas，不必担心 gas 费用超出限制。
- **对 EVM 的兼容性更强。**虽然 Optimism 团队的 OVM 对 EVM 兼容，但其实不是 100%兼容，已有的项目从一层迁移过来仍然需要修改代码，Arbitrun 团

队的方案则是几乎 100%兼容。

- **多步交易可能存在安全性问题。**Arbitrum 交易的有效性验证需要多轮交互，内置虚拟机需要支持异步机制，该机制更加复杂，代码量更大，可能存在安全问题。

#### 3.3.4. 应用

由于 Arbitrum 落地预期强烈，当前已经有众多应用都宣布支持 Arbitrum 的生态。包括 Uniswap、Sushiswap、MCDEX、Bancor、ImToken 等。其中，Uniswap 社区已经投票通过将 V3 部署在 Arbitrum 上；去中心化永续合约交易所 MCDEX 推出的无需许可即可创建合约 V3 版本已登录 Arbitrum 测试网中，与开发团队协同推进方案的测试和应用；同时，MCDEX V3 也计划在 Arbitrum 主网上线后立刻完成部署，并对用户开放；另外， OKEX 也宣布将支持 Arbitrum 网络的充值和提现。用户无需再与以太坊一层交互，降低交易手续费。

### 3.4 Starkware

StarkWare 是一个来自以色列的零知识证明研发机构，专注于研究以太坊二层扩容技术。该团队在二层的技术积淀也非常深厚，二层技术路线、二层网络网络、零知识证明协议、编程语言、二层应用均有涉猎。几乎覆盖了二层所有的技术核心点。

其提出的 Layer2 底层的技术为 Validium，后又进一步推出了 Volition。StarkWare 团队推出了一个去中心化的二层扩容网络 StarkNet，支持以太坊上的通用计算，具备一定的免许可性和抗审查性。根据 StarkWare 在今年 1 月底公布的 StarkNet 路线图来看，该方案分为四个阶段，以逐步实现去中心化和生态集成。目前，团队已完成阶段 0 的构建，主要完善了三个重要组件，即证明协议 zk-STARK、编程语言 Cairo 和交易所扩容方案 StarkEx。

#### 3.4.1. 项目进展

StarkWare 对目前流行的 SNARK 算法做了改进，自主研发出新一代零知识

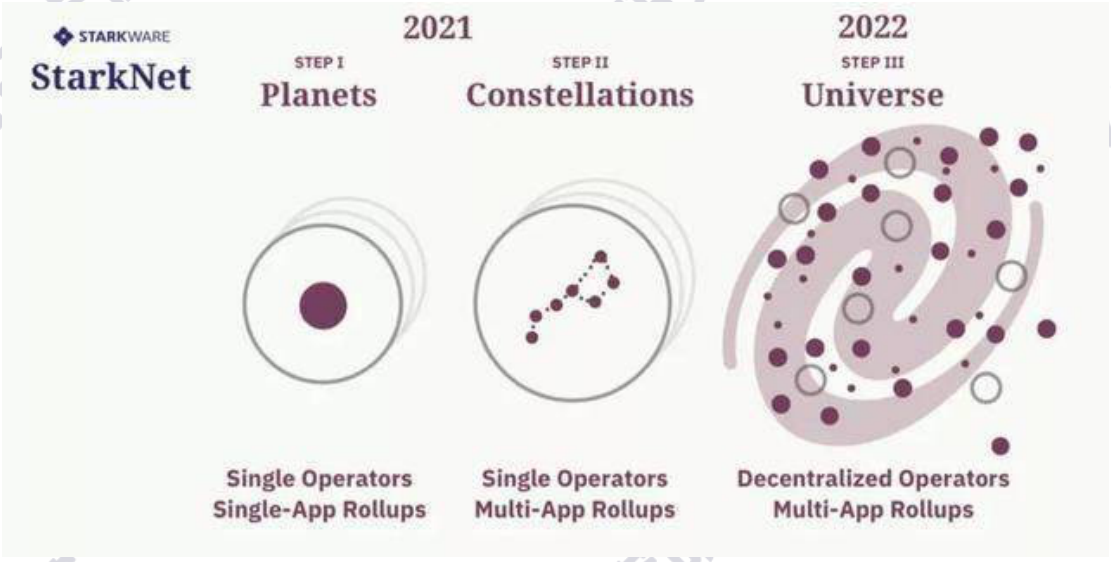
证明协议 STARK。该协议于 2020 年 6 月上线主网，能够大幅提高运行效率，并可以提供抗量子计算的零知识签名，是整个 StarkNet 去中心化证明层的基石。

另外，StarkWare 还创造了独有的编程框架 Cairo，以生成通用计算的 STARK 证明。Cairo 于 2020 年 10 月在主网上线，面向所有开发者。该框架不仅是图灵完备的，还能避免零知识证明中复杂的电路设计，将证明的生成与验证分开进行。StarkWare 团队不断改进 Cairo，为其引入了众多新的功能、语法和内部插件，最近正在探索投票场景下的应用。

StarkWare 也在阶段 0 中推出了第一个基于 STARK 的 ZK Rollup 应用 StarkEx。StarkEx 既是 StarkNet 第一批具体应用，也是专注于交易所场景的二层扩容引擎。StarkEx 最早于 2020 年 6 月上线以太坊主网，随后在 2020 年 12 月上线了 2.0 版本。2.0 版本是完全建立在 Cairo 框架上，支持一二层交互以及 ERC721、链下铸币、智能合约密钥恢复等功能。目前，StarkEx 仍处于迭代更新的状态，团队计划于 2021 年 5 月推出 StarkEx 3.0,该版本将包含 L1 限价单和批量长效的闪电贷功能。

按照团队计划，后续三个阶段分别对应单运营者单应用 Rollup、单运营者多应用 Rollup 以及去中心化运营多应用 Rollup，最终将在 2022 年底前逐步完成部署(图 3-2)。

图3-2　StarkNet 路线图




来源：Starkware 官方文档

### 3.4.2. 技术方案

Starkware 最早提出的二层解决方案是 Validium，**这个方案将数据保存在链下，但同时结合了 ZK 的思想对状态转换做有效性证明。**具体来说，数据在链下的有效性由链下的公证人保证，同时公证人会将链下交易的状态转换生成 SNARK 证明上传到链上。SNARK 证明避免了公证人上传错误的状态转换到链上。但由于数据存储在链下，公证人可以合谋不提交数据，将用户的资产冻结。因此，**其实 Validium 方案并不是 Rollup 系的技术**，但是在 Validium 方案中用户资产也被冻结的问题被讨论之后，**Starkware 推出了一个新的方案，Volition。Volition 其实是 ZK Rollup 方案和 Validium 方案的结合**(图 3-3)，用户可以根据自己的需求选择将数据可用性的保证放在链上还是链下。因此，我们还是将 Starkware 团队的工作放进了本篇 Rollup 的文章中。

图3-3 Volition 和其他 Layer2 技术

<table>
<tr><th></th><th colspan="2">Validity Proofs</th><th>Fault Proofs</th></tr>
<tr><td>Data On-Chain</td><td rowspan="2">Volition</td><td>ZK-Rollup</td><td>Optimistic Rollup</td></tr>
<tr><td>Data Off-Chain</td><td>Validium</td><td>Plasma</td></tr>
</table>

来源：Starkware 官方文档

在前面的章节中**我们介绍过 Matter Labs 的 zkPorter 的方案，这个方案的思想就是源自于 Validium**，但是在 zkPorter 中，链下的守护者无法冻结用户的资产，且在 zkPorter 中有一个分片是 ZK Rollup 的分片，数据可用性由链上保证，用户可以选择将自己的资产放在 ZK Rollup 的分片中或者可用性在链下的其他 zkPorter 的分片中。**所以其实 zkPorter 的方案和 Volition 的方案是更为相似的。**

### 3.4.3. 特点[8]

- **安全性弱于一层，公证人有权冻结资金。**Validium 将数据保存在链下，二层的公证人只会向链上提供状态转换的证明，不会提交细节的交易信息，导致如果二层的公证人不将最新的状态公布给用户，用户无法自行构造证明来证明账户状态。因此存在二层公证人冻结用户资金敲诈的可能。
- **退出时间相对较短。**因为 Validium 方案下公证人为状态转换提供了有效性证明，不需要挑战期，因此退出时间相对较短。
- **无用户活性假设。**虽然该方案没有保证链上数据的有效性，存在欺诈的可能，但是 SNARK 证明能避免公证人提交虚假交易，因此不需要用户保持在线频率来防欺诈。另外，即便发生前述的公证人冻结资金的情况，也不能通过用户保持在线解决。
- **通用性强于 zkSync，但不兼容 EVM。**Starkware 团队开发了 Cairo 语言，应用团队使用该语言开发应用可以省去自行编写生成证明的工作。但是由于不兼容 EVM，现有以太坊的生态应用迁移过来需要额外的开发工作，这也是 Starkware 团队的方案没有获得广泛采纳的重要原因之一。
- **吞吐量大幅提升。**由于数据放在了链下，Validium 的吞吐量提升比 ZK Rollup 还要再高一个数量级。

### 3.4.4. 应用

当前已有多个应用宣布集成 StarkWare 的二层扩容方案。去中心化自治组织 BadgerDAO 于 2 月份在 StarkNet 上启动；Celer 也计划利用 Cairo 编程语言，为自身扩容方案 Layer2.finance 开发基于零知识证明的版本；现货交易所 dYdX、衍生品交易所 DeversiFi 和 NFT 交易市场 Immutable 均上线支持了 StarkEx 方案，截至目前共产生超过 10 亿美元的交易量。其中，DeversiFi 最早采用 StarkEx 扩容引擎，提供代币兑换功能，用户从 Layer 1 进入该网络无需支付任何 Gas 费；dYdX 的二层网络版本于 4 月正式上线以太坊主网，提供十种代币的永续合约交易；而 Immutable 交易市场则与 StarkEx 在 NFT 领域开展合作，发布了二层解决

[8] 本小节的特点主要针对 Validium 技术。

方案 ImmutableX 的 Alpha 版本，支持区块链卡牌游戏玩家进行交易。

# 四、 应用方案解读

在前面的章节中，绝大部分的内容都围绕 Rollup 技术的思想和其主要技术团队的落地情况进行了分析，但除此之外，应用也是 Rollup 生态中不可忽视的一环。**除了一些本身已经在以太坊一层上长期运行的项目会落地到 Rollup 上，还有一些针对 Rollup 的特点或者说是缺点(如，带来流动性割裂、有挑战期等)而特别设计的应用。**本节也将针对其中 3 个代表性的应用方案进行解读，带读者一窥 Rollup 特色的应用是如何设计的。

## 4.1. Celer：Layer2.finance

Celer Network 于 2021 年 2 月发布最新的解决方案 Layer2.finance，以降低 DeFi 的使用门槛，通过聚合需求来分摊单个用户承担的交易手续费。2021 年 4 月底，Layer2.finance v0.1 主网正式上线，目前支持 AAVE，Compound 和 Curve 三种 DeFi 协议。根据团队披露的数据来看，该方案上线一周后锁仓总量已超过 140 万美元，为 900 多笔交易节省了近 3.4 万美元的 Gas 手续费，性能表现良好。

### 4.1.1. 解决的问题

当前在谈 Layer2 时，大家更多想到的是把 Layer1 上的应用搬到 Layer2 上去，以实现把计算和存储部分转移到 Layer2 降低主链的负荷。但这种方案在落地时，往往涉及到代码、资金、生态的迁移，在当前的 Layer2 的发展阶段下，这些迁移都并非易事。Celer 的 layer2.finance 反其道而行之，**不转移链上原本的应用，将交易的指令在 Layer2 上聚合，然后在 Layer1 上统一执行**，绕过前述问题，实现交易成本的降低。

### 4.1.2. 方案

Celer 提出基于原地扩容的全新 Layer2 解决方案 Layer2.finance。该方案包含以下几个部分：

首先，用户要将以太坊链上的资金存入到 Layer2.finance 的一层 Rollup 基金池合约中，这些资金会划分为闲置、已承诺和已分配三种不同的状态。其中，已承诺资金代表了交易从提交到实际执行的中间状态；已分配资金代表了交易执行

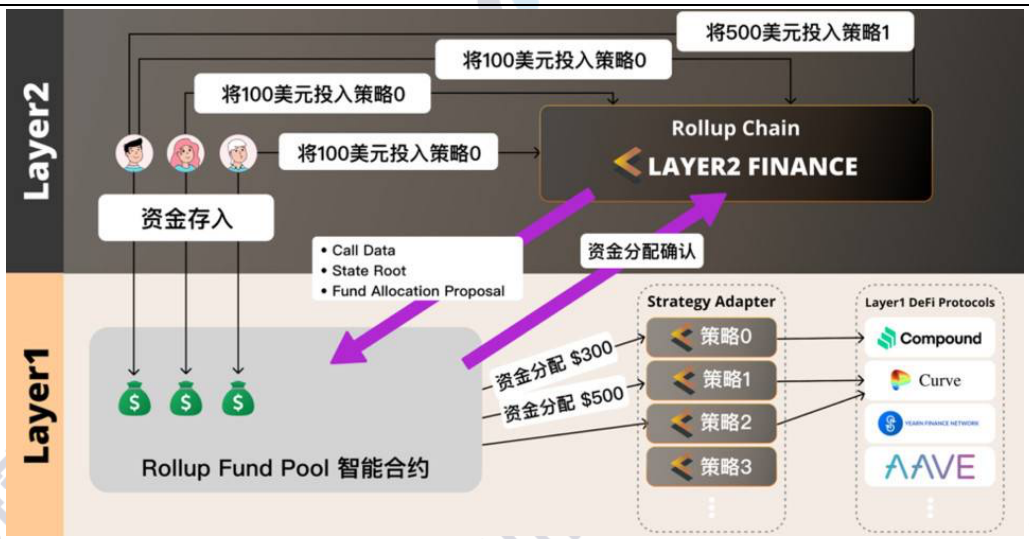
完成后，用户收到的流动性凭证 stToken，未来可用于赎回流动性，并将收益转换为闲置资金。

然后，用户就可以在 layer.finance 的二层网络中进行资金分配，即将资金投入不同 DeFi 协议以获取收益或从协议中撤出。

随后，Layer2.finance 的出块节点会在 Rollup 链上收集交易并根据目的 DeFi 协议地址进行聚合分类。当汇总了足够多的交易或固定时段结束后，出块节点会把这些交易打包成块，向主链提供每个用户的状态根以及资金分配的具体方案。

最后，Layer2.finance 的链上合约根据接收到的指令执行相应的资金分配操作。同时，出块节点也会根据一层交易结果更新二层用户的资金状态，确认资金分配无误后，返回用户相应的流动性凭证。

图5-1　Layer2.finance 运行流程




来源：Celer.Network 官方文档

由于 Layer2.finance 目前使用的是 Optimistic Rollup 框架，所以 Rollup 区块在与一层交互时会存在挑战期。在该挑战期内，如果 Layer2.finance 协议进行了错误的资金分配，任何人都可以提交欺诈证明来回滚交易。未来，Layer2.finance 将采用 ZK Rollup 路线来适配高并发聚合交易场景，不再需要设置挑战期来保证状态转换的有效性。

#### 4.1.3. 优势

- **低成本。**如果把 DeFi 比作地铁站，那 Layer 2.finance 就是穿梭在各个 DeFi 协议中的地铁。用户一改以往高消费的“专车”，只需购买便宜的“地铁票”，通过“多人拼单”的形式，来降低个体与 DeFi 的交互成本。
- **无需迁移 DeFi 协议。**对于用户来说，自身持有的资金仍可以像之前一样在链上的多个 DeFi 协议中使用，降低 Layer2 带来的流动性割裂的问题；对于各个 DeFi 协议来说，不仅可以省去开发专用二层网络版本的工作，还可以通过连接 Layer2.finance 实现自身二层用户的积累。
- **可叠加的可扩展性。**从短期看，单条 Layer 2.finance 受限于链上容量，可能会随着交易规模的增大而无法维护；但长期来看，一旦 ETH2.0 落地，系统可以增加多条 Layer 2.finance Rollup 链到对应的流动性系统中，打破扩展性的上限。

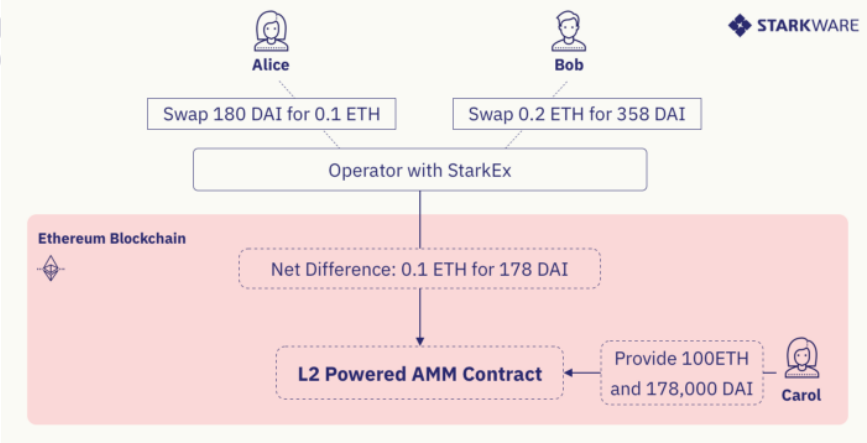
#### 4.1.4. 局限

Layer2.finance 目前同样存在一定的局限性。首先是**打包聚合交易导致的延迟问题**，用户在表达资金分配的意图到实际的资金分配中存在固定延迟，需要在成本和时效性上做出抉择；其次，**该方案存在高级操作的局限性**，用户无法执行多个 DeFi 协议的高级定制化组合；最后，**用户在该方案上的可选择性是有限的**。目前 Layer2.finance 只上线了三个 DeFi 协议，虽然未来会慢慢整合更多的策略协议，相对稳定且收益率较保守的项目可能是会被优先考虑的。

### 4.2. Starkware：Caspian

StarkWare 于 2021 年 4 月发布 L2 AMM 流动性聚合方案 Caspian，**可以有效应对 Layer 1 流动性被分流到二层导致的流动性碎片化问题**。根据团队预估，该方案在 6 月即将上线的 StarkEx3.0 升级中有望得以实现，但目前看来有所推迟。

图5-2 Caspian 方案总览




来源：StarkWare 官方文档

### 4.2.1. 解决的问题

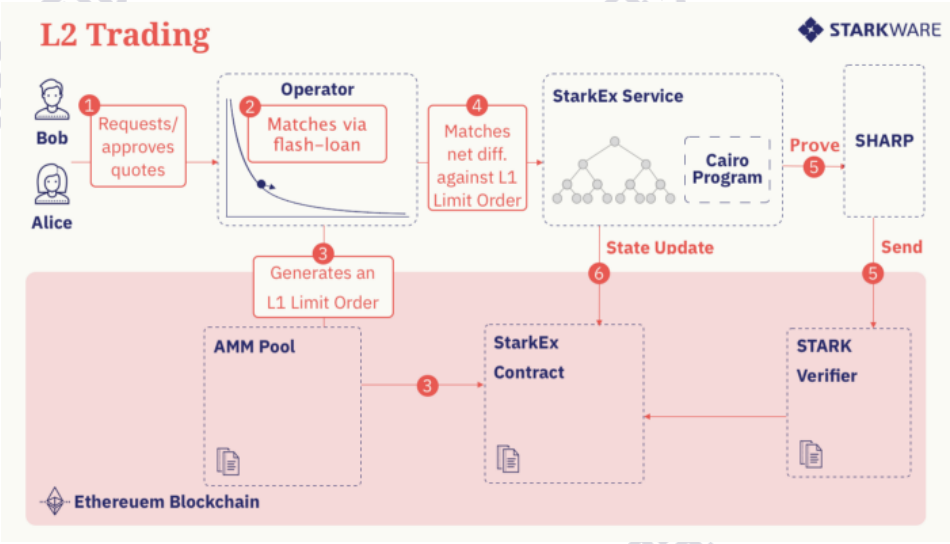
随着链下扩容逐渐成为以太坊网络 2021 年发展建设的主旋律，Layer2 上会诞生新的 AMM 项目，已有的一层的 AMM 项目也会迁移部分流动性到二层，导致一层流动性被分流，加重资金碎片化问题。对于 AMM 应用来说，它们的资金聚集效应十分显著，往往需要较大的资金体量才能提供好的交易体验。所以，妥善解决流动性碎片化问题并提高资金效率，是十分有必要的。

### 4.2.2. 方案

StarkWare 提出由二层驱动的 AMM 设计方案 Caspian，**把交易放在二层进行，再从一层的 AMM 池中向各个交易地址调配资金**。Caspian 分为链下和链上两部分，链下包含运营商、交易者和流动性提供者，其中，运营商是一个可以处理二层网络交易的做市商，它可以按批次处理多笔交易，当一个批次交易结束时，会生成 STARK 有效性证明，并且根据状态变更来结算批次里的交易；交易者指的是各个二层应用上的用户；而流动性提供者则是以太坊链上的各个流动性提供者。链上是一个由 Layer 2 驱动的 AMM 智能合约以及 StarkEx 合约，前者是一个标准的 AMM 合约，但稍有不同的是，它的唯一对手方是链下的运营者且提款要等待前一批次的交易处理完成才能进行；后者即为支撑运营者服务的 StarkEx 系统。该方案的具体过程如下：

首先，运营商聚合起一批二层用户发来的交易，并自行撮合接受到的报价订单；然后，运营商可以在链上的 AMM 合约中生成一个限价单，并将该批次里产生的交易净差额与该订单撮合，完成用户剩余的资金分配；最后，运营商将该批次的交易发送给 StarkEx 系统，生成批量 STARK 证明，在经过 verifier 验证后完成该批次交易的结算以及状态的更新。在整个过程中，AMM 合约池中的代币流动性是通过一层流动性提供者提供的，其本质还是保持代币的流动性在 L1，根据 L2 交易指令来进行资金调配。

图5-3　Caspian 运行流程




来源：StarkWare 官方文档

另外，在 Caspian 的设计中，还新增了闪电贷的功能。通过将贷款期限延长至整个交易批次的流程，运营者可以提前在链下铸币发送给交易者，但前提是必须在该批交易结束时销毁它们。这样一来，可以大大提高运营商作为中间方撮合订单的效率。

### 4.2.3.　优势

目前众多应用只能靠多个做市商实现在不同网络中部署资金，执行做市策略。Caspian 方案可以实现在二层进行指令调配以及交易的聚合，在一层的流动性池中将资金发送到用户地址，完成跨 L1 和 L2 的 AMM，**缓解二层分流一层资金带**

**来的流动性碎片化问题。**

#### 4.2.4. 局限

从该方案的设计机制上看，Caspian 是**存在中心化风险的**。因为运营商既是 AMM 智能合约的对手方，也是与一层交互的唯一对象，可以决定部分交易需求的去留，一旦出现作恶行为，很可能导致用户资金的损失；另外，该方案还处于概念性阶段，**还有一些组件待补充**，例如 L1 限价单和批量闪电贷，这些功能的具体实现要等到 6 月 StarkEx3.0 网络升级后才有可能；最后，Caspian 的设计思路与 Celer 的 Layer2.finance 类似，后者已于 4 月上线，占据一定的先发优势。

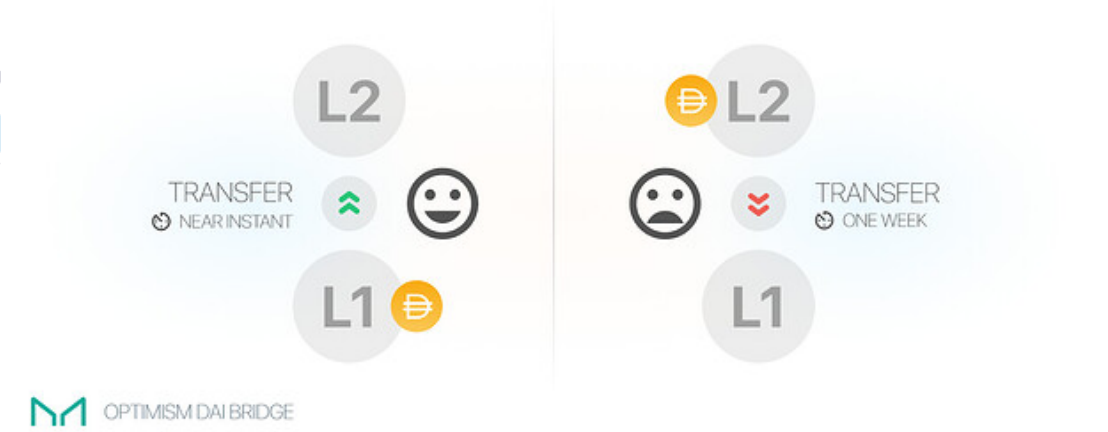
### 4.3. MakerDAO：Dai Bridge

3 月初，MakerDao 智能合约团队在其官方论坛上发布了一种新的解决方案 Optimism Dai Bridge 来支持快速提款，用于解决 Optimistic Rollup 需要一周提款时间的问题。据团队表示，该功能将在今年第三或第四季度正式上线。

#### 4.3.1. 解决的问题

由于 Optimism 在设计中借鉴了 Plasma 的欺诈证明机制，从一层到二层网络的代币转移可以很快完成，但反向移动则需要用户等待一周左右的争议期，用于验证状态是否正确更新。Maker 团队认为，资金提取时间过长会成为制约 Optimistic Rollup 发展和影响用户体验的重要因素。

图5-4 Optimism 存款和取款时间对比




来源：MakerDAO 官方文档

### 4.3.2. 方案

**Optimism Dai Bridge 引入预言机快速验证排序者提交的交易**，验证无误后，提前将用户在二层要提取的 DAI 借由中间代币 fdai 的桥接铸造出等量的一层上的 DAI，**避免了漫长的等待带来的资金利用率和可组合性下降的问题。**

该方案的具体过程如下：首先，二层上所有有关 oDai(二层上的 DAI 在该方案中被称作 oDAI)的交易请求会被链上的 CTC(Canonical Transaction Chain，是 Optimism 团队的解决方案中的一个组成部分)合约记录下来；然后，交易提款请求会经过 Maker 的预言机验证，确认交易的有效性和金额；通过验证的提款交易会映射到一层上铸造出相应数量的 fDai，这些 fDai 可以看作是用户对原先锁定在一层上 DAI 的取款凭证；最后，用户将手中的 fDai 质押可以在一层铸造出新的 DAI 给用户提走。等到该交易的挑战期结束，抵押的 fDai 和锁在一层合约中的 DAI 会被清算，用户只需要支付一定的利息即可。这样一来，用户无需等待 DAI 的一周锁定期，近乎即刻就能实现提款。

不仅如此，Maker 团队还提出可以将这项服务扩展到任何二层代币的快速兑换。除了稳定币 DAI 之外，用户可以首先在二层上将资产兑换成 oDAI，再利用 Optimism Dai Bridge 交换 oDAI 为 DAI，最后按照比率兑换回原先的资产。这个过程需要集成 L2 上的 AMM 以及与 L1 上 AMM 的协作，如果成功实现，可以很大程度提高二层资产到一层的快速流动。

**整个方案的核心是相信了预言机对交易状态的提前验证，因此相信了提款交易的最终性，提前将资金释放给用户。**

图5-5　Optimism Dai Bridge 运行流程


来源：MakerDAO 官方文档

### 4.3.3.　优势

- **提款时间快。**解决了 Optimism 的用户痛点，将提款时间由一周缩短至几分钟。
- **无需对手方。**Maker 本身具有 Dai 的发行能力，这里只是利用 fDai 作为连接桥梁，实现 Dai 的发行。并且，该方案与现有抵押借贷的协议逻辑衔接，提供资产保障，用户只需要和 Maker 协议本身交互，无需对手方参与交易过程。
- **灵活性强、流动性高。**系统设立了 Maker 协议的 fDAI 库，用户不仅可以按照上述方案获取 fDAI，也能从其它用户手中交易 fDAI 从而铸造出 DAI，完成提款。
- **保证二层用户利益。**即便预言机失灵，造成了 DAI 的超发，但并不会影响二层用户的利益。原因是，增加的 DAI 相当于 Maker 协议的负债，这时会触发 Maker 里的债务拍卖机制，系统增加流通中的 MKR 量，用于清偿债务，将损失转移给了 MRK 持有者。锁定在一层合约中的 DAI 和二层中的 oDAI 价值仍然是相等的。

#### 4.3.4. 局限

在该方案中，**假定了预言机是正常运行、可以信任的**，但原方案中未阐述这种预言机更细致的工作原理，不排除出现预言机与二层排序者串谋的机攻击或者预言机宕机等情况。

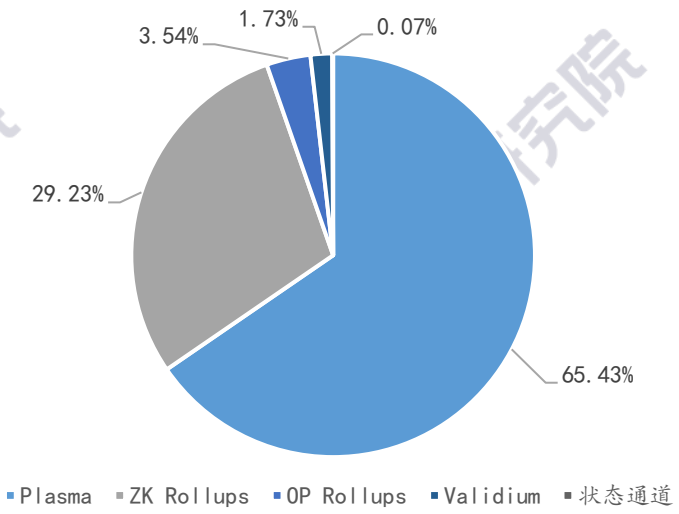
# 五、 数据表现

上文详细介绍了目前主流的 Rollup 代表项目及应用方向，尽管目前其中多数仍处于刚上线或上线前期，但已有一些数据值得关注。本章将从**资金承载、开发进度和实际性能**上对主流项目进行对比分析。

截止 6 月 25 日，超 11.8 亿美元的价值由以太坊 Layer2(本小节统计的 Layer2 数据不包含侧链)项目承载，约占以太坊 DeFi 近 459 亿美元总锁仓量的 2.57%。其中，Rollup 占据 Layer2 方案 32.77%的资金量。各个方案中头部项目的承载资金量数据显示，其中 ZK Rollup 占比 29.23%，其次分别是 Optimistic Rollup（3.54%）和 Validium（1.73%）。

由于 Rollup 系落地速度不快，项目迁入也存在一定开发难度，因此整体资金承载量自先锋项目如 ZKSwap 和 Loopring 上线后尚未出现第二个爆发点。同时，随着近 2 个月 Polygon 生态的崛起，打乱了整个 Layer 2 赛道的格局，让 Rollup 分支资金承载占比自 4 月末超 50%下降，近 2 个月占比下降超 17 个百分点。

图5-1 截止 6 月 25 日 Layer 2 各分支资金承载情况




来源：The Block，火币研究院整理

ZK 系凭借着 ZK Swap 和 Loopring 对以太坊二层交易所的早期快速布局，目前仍承载着 Rollup 方向下近 85%的资金；OP 系基于头部项目 Synthetix 的早期布局承载着分支近 10%资金；Validium 以 StarkWare 为代表，上线较晚且应用场景限定在几个去中心化交易所上，仅承载了近 5%的分支资金。

图5-2　Layer2 各分支项目进度

| 技术路线 | 项目/团队 | 开发进度 | 应用情况 | TVL (百万美元) | 实际性能 |
|---|---|---|---|---|---|
| ZK Rollup | Loopring | 上线 3.6 版本，代码已审计，交易所已公测 | 路印 DEX/钱包 | 139.79 | tps(目前)：0.6<br>退出时间：2h |
| | zksync | 1.x 版本已上线；不完全兼容 EVM 的 2.0 版本上线测试网，主网 8 月正式上线 | Curve、imToken、Sushi、Argnet 将接入；Gitcoin、Storj、Golem 等集成 | 7.74 | tps(目前)：0.05<br>退出时间：5h |
| | Hermez | 主网已上线 | Hermez 钱包 | 30.72 | tps(目前)：0.00092<br>退出时间：20min |
| | zkSwap | 主网已上线，交易所已运行 | DEX | 122.85 | tps(目前)：0.0843<br>退出时间：20-40min |
| OP Rollup | Optimism | 软启动中，主网延期至 7 月上线，近期集成 Etherscan 支持查询 | Synthetix 质押服务；*Uniswap v3、MakerDAO、Compound 等已布局 | 41.74(Synthetix) | tps(目前)：14-34(测试)<br>退出时间：7D |
| | FuelLabs | 上线 1.0 版本 | *UI 开发中，钱包集成中 | - | tps(目前)：-<br>退出时间：10min(HTLC)或 7-14D |
| Arbitrum | OffchainLabs | 已向开发者开放主网测试版 | MCDEX、Bancor、Uniswap v3、集成中 | 0.07 | tps(目前)：0.1141(测试)<br>退出时间： 7-14D |

| | | | | | |
|---|---|---|---|---|---|
| Validium | StarkWare | 已完成阶段 0 的构建，StarkEx 2.0 上线；结合了 ZK 技术的 StarkNet 已上线测试网 | DeversiFi 和 Immutable X；*dYdX (StarkWare+ZK) | 20.48(DeversiF+ImmutableXi) | tps(目前)：-<br>退出时间： 10min |

来源：火币研究院整理

### 5.1 开发进度

开发进度上看，**ZK 系**最受瞩目的项目 **zkSync** 目前已上线 1.x 版本主网，目前已接入了 Curve、Sushiswap 等头部应用；而其 2.0 版本也于月初上线测试网，预计 8 月正式发布。值得一提的是，公测中的 2.0 版本已开放 zkPorter，支持链下数据可用性；同时正在加速开发 zkEVM 以为项目方提供更好的智能合约兼容性。另一方面，**ZKSwap 和 Loopring** 则分别于去年 12 月和今年 2 月末基于 ZK Rollup 技术上线其去中心化交易所，但后续在技术开发上并未持续寻求突破，而是转向生态的探索。而 **Aztec 和 Hermez** 两个专注转账的应用也纷纷上线主网，但目前生态应用落地较少。

Optimistic Rollup 技术研发行列中最主流的团队是 Optimism 和 Fuel labs。**Optimism** 团队目前仍处于启动状态中，主网延期至 7 月上线，但 Synthetix 已于 4 月兼容其技术，率先上线了 SNX 质押功能。**Fuel labs** 在 2021 年 1 月宣布了其 1.0 版本的上线，但目前应用侧仍处于钱包集成、UI 开发等阶段。

Validium 方案是由以色列研发机构 StarkWare 主导开发，目前已完成阶段 0 的部署并上线其交易所扩容方案 StarkEx 2.0 版本。应用方面，目前 dYdX、DeversiFi 和 Immutable X 正基于其技术进行开发，但整体生态及参与者仍较少。

**Arbitrum** 的第一个版本最早出现于 2014 年，目前已向开发者开放主网测试版 Arbitrum One。应用方面，早期推进开发的团队包括 MCDEX、Bancor 等；而在其主网测试版上线后，Uniswap v3、Sushiswap、DODO 等知名项目也纷纷进行了部署，目前已有超 250 个项目申请接入。

### 5.2 资金数据

从承载资金方面看，截止 6 月 25 日，部分具备 Rollup 功能的主流项目承载

资金量如下：

图5-3 承载资金量

| Rollup 种类 | 项目/团队 | 承载资金量（百万美元） | 分支内占比 |
|---|---|---|---|
| ZK Rollup | ZKSwap | 122.85 | 35.54% |
| | Loopring | 139.79 | 40.44% |
| | dYdX | 43.95 | 12.71% |
| | ZKSync | 7.74 | 2.24% |
| | Aztec | 0.63 | 0.18% |
| | Hermez | 30.72 | 8.89% |
| | **合计** | **345.67** | **100%** |
| OP Rollup | Optimism (Synthetix) | 41.74 | 99.83% |
| | Arbitrum | 0.07 | 0.17% |
| | **合计** | **41.81** | **100%** |
| Validium | DeversiFi | 20.04 | 97.85% |
| | ImmutableX | 0.44 | 2.15% |
| | **合计** | **20.48** | **100%** |

来源：The Block，火币研究院整理

整体看，ZKSwap 和 Loopring 作为 ZK 系先锋先行落地，分别承载了约 1.23 亿美元和 1.40 亿美元的资金，目前在本文研究的四个技术路线中独占鳌头。值得一提的是，作为新萌生的 L2 DEX，ZKSwap 近两个月自超 13 亿美元大幅缩水超 90%至目前的 1.23 亿美元，**这或许是独立研发 ZK Rollup 路径的 DEX 共同面临的困境：在早期挖矿红利消失后，不支持 EVM 的技术如何突破 L2 资产孤岛的封锁。**从解决思路上，我们看到 ZKSwap 作出了 2 类尝试：通过加码挖矿、回购销毁生态通证 ZKS 以持续刺激用户进入；通过开发 NFT 协议试图增加玩法，此功能尚未上线。在现阶段，前者是针对存量用户的策略，后者则可能打开新的增量市场。此外，作为早期项目的 dYdX 虽然也采用了 StarkEx 的方案，但使用

的是其 ZK Rollup 版本，依托其一层 TVL 转化也为 ZK 系承载资金提供了加成。

OP 方案受限于 Optimism 团队的延期发布，目前承载资金基本靠 Synthetix 的质押功能支撑。未来随着 Synthetix 核心的合成资产铸造、Uniswap V3 的二层版本接入，以及其他头部 Defi 应用的迁移，其承载资金或可大幅提升。与目前的 ZK 路径不同，OP 天然对 EVM 及智能合约开发友好，或更易复制、创造生态热度；**但同时，OP 在机制上较长的退出周期会在另一维度上加剧资产孤岛的问题**，用户在进入生态前或需反复思考，**这对每个项目的在安全和收益上的稳定性提出了更高的要求**，推测早期或只有足够成熟的项目可吸引到大量资金。

最后，Validium 由于接入的项目如 DeversiFi、ImmutableX 等则本身生态较小，因此整体承载资金较少。而 Arbitrum 刚进入开发者测试阶段，出现一定规模的资金量仍待其主网正式上线、接入用户后观察。

### 5.3 实际性能

实际性能方面，我们主要观察**吞吐量（tps）、提现/退出至一层的时间**以及**整体费率**较以太坊的提升和变化。

我们在图 5-2 中已列出统计范围内各项目近期实际吞吐量（tps）的对比。可以看到，虽然各项目理论 tps 均较以太坊 15 tx/s 的数值有了较大增长。ZK 系支持以太坊 100 倍以上的理论吞吐量峰值，OP 系则在以太坊 33 倍（500 tps）左右，但**由于各项目整体还都在上线之初，交易活跃度仍不高，且功能尚未完全开放，因此实测的吞吐量数值仍很低。**

从提取资金至一层的时间来看，Rollup 方案目前整体仍较慢。尽管理论上 ZK Rollup 在一二层之间的资金转移可以实现数分钟内提取资金，但**由于交易活跃度仍不够高，出于降低单笔交易费用的考量，目前提款时间还只能做到数小时内级别**；最快的如 ZKSwap 和 Hermez 也需要 20 分钟。而 Optimistic Rollup 由于设置了欺诈证明机制，**资金提取时间常需要 1 周左右**。

图5-4　资金提取速度

| | ZK Rollup | | | | | Optimistic Rollup | | Validium | Arbitrum |
|---|---|---|---|---|---|---|---|---|---|
| | ZKSync | Loopring | Aztec | ZKSwap | Hermez | Optimism | Fuel | StarkEx | OffChainLabs |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **取款时间** | 5 小时 | 2 小时 | 4 小时 | 20-40 分钟 | 20 分钟 | 7 天 | 7-14 天 | 10 分钟 | 7-14 天 |

来源：火币研究院整理

从费用上看，目前已上线或测试中的项目，在二层内执行基本功能如转账、清算等的费用已大幅降低，折美元计价均低于 1 美元；交易行为则取决于各项目的盈利模型有较大差异。而在一二层充值、提现中，由于涉及到和以太坊一层的合约的交互，**仍需基于以太坊费率进行收费，整体小于等于以太坊普通交易费用。**其中，充值部分费用因交易自动执行，因此一般将取决于项目代码复杂程度。根据调研，目前项目整体充值费用约为以太坊一笔普通转账费用的 0.5-1 倍。提现方面项目方则略有不同，如 ZKSwap 固定收取价值 5 美元的 L1 网络费用；测试中的 Optimism 团队决定在前期减免费用；路印实际提取费用约为以太坊交易的 1/4，前期进行减免；zkSync 则基本等同于以太坊转账交易。

**结合资金数据和性能看，目前 Layer 2 方案下的生态还在相当早期，尚待头部 DeFi 项目汇聚在同一二层项目下，靠可组合性吸引大量用户迁移，带领浪潮。**目前的难点主要在获得大量 DeFi 头部项目站台的 zkSync 和 Optimism 成熟度较低，支持全部功能的正式版本分别拟于 8 月和 7 月上线。头部项目包括 Curve、Sushi、Uniswap、Compound 等也均未推出可让用户测试的版本。

未来，随着两个项目顺利落地，而上述头部项目也纷纷推出二层版本，**用户可以在一个 Layer 2 生态内体验较完整的链上活动，且速度和费用均可以“多快好省”，则将逐渐形成良性的循环。**同时，Uniswap v3 上线至今，尽管资金效率大幅提升，但对应的费用也持续上升，这在二层版本中可以得到极大缓解，或将获得更多中小流动性提供者的支持，进而衍生出基于其 NFT 开发的新项目，这也令人期待。

整体看，各 Rollup 项目 2020 年以来进度加速，**开发进度及承载资金量均由较明显进步，但仍处于较早期的状态；ZK 系因 ZKSwap、Loopring 的早期入局落地较快，而 OP 系呼之欲出。**性能上看，由于生态及活跃度尚不成熟，各项目

的实测性能仍据其理论峰值有较大差距，但已基本实现对高昂费用的降低。**但由于技术研发及实现的难度、项目方基于安全性及生态的考虑、用户基于习惯的选择等因素，整体仍处于早期，生态尚不完整。**

# 六、 总结与展望

Rollup 作为以太坊二层新一代技术，相比闪电网络、Plasma、侧链等等被寄托了更高的期待。目前 Rollup 还主要在前期的技术积累和难点攻克的阶段，尚未大面积铺开应用生态。

从技术落地上，可以预见的是，**Optimistic Rollup 路线的方案因为可以率先实现兼容 EVM 的通用二层网络，通用方案会先于 ZK 系技术落地**。而对于 Layer 2，不管是何种类型的 Rollup，对 EVM 的兼容会是决定生态能否快速成长的重要因素，这一点不仅表现在 Rollup 上，在侧链领域，我们也能看到兼容 EVM 的 Polygon 和不兼容的 xDai 在发展上的巨大差异。同时，**由于技术本身的限制，预计 ZK 系和 OP 系将在此后分别针对 EVM 兼容和退出时间缩短上努力**，以克服由此带来的障碍。此外，**跨 Layer 2 的交互会是长期来看另一各重要的问题**，该领域的解决方案大概率是基于场景的基于信任的解决方案会先诞生。

从生态上看，**Rollup 方向下各分支目前均处于早期，生态不完善**，尽管我们观察到各头部项目在 ZK、OP 和 Arbitrum 上已在部署中，但**整体仍是以 DEX 类为主**。而随着 Rollup 技术在去年下半年至今的推进，今年下半年我们将会看到 Rollup 各个头部团队的重要更新和落地。由此，我们也推测，**第一批落地的仍将是头部 DEX、钱包、预言机和一些数据类中间件项目**；随着第一批基础设施的不断完善、各 Rollup 项目在技术上持续优化，**头部 defi 应用将开始大规模推进在 Layer2 上的落地**；随着吞吐量的提升和交易手续费的数量级级别的下降会解开束缚在一层应用身上的枷锁，跨 Layer 2 交互及跨以太坊交互的技术同步跟进，**新的 defi 场景定会诞生**。

Rollup 未来是否已来，我们共同期待。

# 参考文献

[1] https://zksync.io/faq/

[2] https://community.optimism.io/docs/

[3] https://offchainlabs.com/Arbitrum-USENIX.pdf

[4] https://www.chainnews.com/articles/996131059338.htm

[5] https://ethfans.org/posts/the-why-s-of-optimistic-rollup

[6] https://ethfans.org/posts/whats-up-with-rollup

[7] https://medium.com/offchainlabs/whats-up-with-rollup-db8cd93b314e

[8] https://blog.godsunchained.com/2021/04/07/immutable-x-marketplace-early-access/

[9] https://www.theblockcrypto.com/linked/100653/dydxs-layer-2-live-ethereum-scaling-solution-starkware

[10] https://medium.com/starkware/starks-over-mainnet-b83e63db04c0

[11] https://mp.weixin.qq.com/s/fGX1vZ9ylp3QAzBK0GIjVw

[12] https://mp.weixin.qq.com/s/oRSnb0EyCGfUdj5f3GlpUQ

[13] https://mp.weixin.qq.com/s/ogqwq4oSa2D9SVKaF1w1sg

[14] https://www.sohu.com/a/445659790_100217347

[15] https://medium.com/starkware/caspian-an-l2-powered-amm-f20e93b5421

[16] https://www.youtube.com/watch?v=vDiMYP8vc60&list=PLcIyXLwiPilUFGw7r2uyWerOkbx4GFMXq&index=18&t=1s

[17] https://www.chainnews.com/articles/908635230658.htm

[18] https://www.chainnews.com/articles/021738991995.htm

# 关于火币研究院

火币区块链应用研究院（简称“火币研究院”）成立于 2016 年 4 月，于 2018 年 3 月起致力于全面拓展区块链各领域的研究与探索，以泛区块链领域为研究对象，以加速区块链技术研究开发、推动区块链行业应用落地、促进区块链行业生态优化为研究目标，主要研究内容包括区块链领域的行业趋势、技术路径、应用创新、模式探索等。本着公益、严谨、创新的原则，火币研究院将通过多种形式与政府、企业、高校等机构开展广泛而深入的合作，搭建涵盖区块链完整产业链的研究平台，为区块链产业人士提供坚实的理论基础与趋势判断，推动整个区块链行业的健康、可持续发展。

**联系我们：**

咨询邮箱：huobiresearch@huobi.com
官方网站：http://www.huobiresearch.com/
微信公众号：HuobiCN
新浪微博：火币区块链研究院
https://www.weibo.com/u/6690456123
Twitter：Huobi_Research
https://twitter.com/Huobi_Research
Medium：Huobi Research
https://medium.com/@huobiresearch

欢迎加入研究院学习交流小组

扫码添加学习小助手微信

# 免责声明

1. 火币区块链研究院与本报告中所涉及的项目或其他第三方不存在任何影响报告客观性、独立性、公正性的关联关系。
2. 本报告所引用的资料及数据均来自合规渠道，资料及数据的出处皆被火币区块链研究院认为可靠，且已对其真实性、准确性及完整性进行了必要的核查，但火币区块链研究院不对其真实性、准确性或完整性做出任何保证。
3. 报告的内容仅供参考，报告中的结论和观点不构成相关数字资产的任何投资建议。火币区块链研究院不对因使用本报告内容而导致的损失承担任何责任，除非法律法规有明确规定。读者不应仅依据本报告作出投资决策，也不应依据本报告丧失独立判断的能力。
4. 本报告所载资料、意见及推测仅反映研究人员于定稿本报告当日的判断，未来基于行业变化和数据信息的更新，存在观点与判断更新的可能性。
5. 本报告版权仅为火币区块链研究院所有，如需引用本报告内容，请注明出处。如需大幅引用请事先告知，并在允许的范围内使用。在任何情况下不得对本报告进行任何有悖原意的引用、删节和修改。