# Polygon zkrollup 调研

Polygon是一个公链的扩容解决方案

四个扩容方案：Polygon Pos(侧链)，Polygon miden，Polygon nightfall，Polygon Hermez

# Hermez

2021年3月份主网上线

在以太坊上实现payment 和 token transfer 的扩容

技术路线：**zkrollup** :链下生成证明，链上验证　calldata解决数据可用性问题

主网启动时支持的token：ETH、 DAI 、Tether 、wBTC、 Hez

原团队：去中心化身份系统iden3

性能：1. 133倍的吞吐量提升 2. token transfer 费用降低90%

没有提供托管 或者 交易所等服务

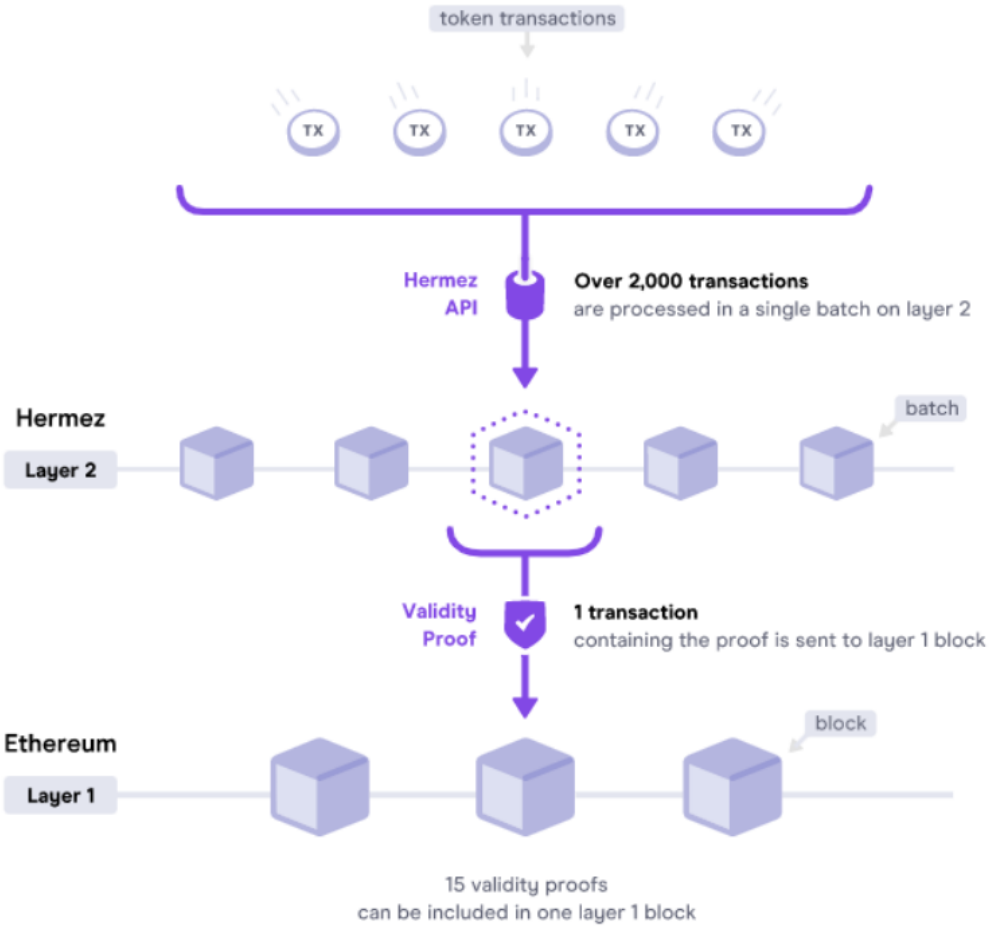
**用户：**

1. 创建账户：通过非托管的个人钱包（metamask）将以太坊L1地址注册到Hermez网络中，获得一个内部地址。
2. 存入资金：将L1的token转入到Hermez地址
3. 发送交易：在Hermez地址之间快速且低费用的交易
4. 取出资金：将资金转回layer1地址

**Coordinator：**

block producers

1. 接受用户交易请求，验证交易有效性
2. 处理交易，更新默克尔树列表
3. 生成零知识证明，保证每一笔transfer交易都是有效的，Coordinator对默克尔树的更新都是正确的。（去掉传统交易中，签名的部分，用zkproof保证正确性）




**Proof of donation:**

Hermez 的 layer 2 链使用 proof of donation 作为共识机制，

其在 coordinator 之中通过**拍卖**过程来选举出进行 rollup 的creator。coordinator 向进行拍卖的合约发送报价，拍卖使用 HEZ 代币进行。后续会使用metics币，时间未定。

拍卖所得的资金主要用于捐赠：

- 30% 直接销毁
- 40% 捐赠给以太坊基金会的一个捐赠账户 Gitcon quadratic funding grants
- 30% 用于激励 Hermez 网络参与方

激励竞拍者获得rollup 权的动力是**打包的交易中包含的手续费。**为了弥补拍卖支付的钱以及操作的花费， coordinator 会尽可能多地收集交易，促进打包效率的提高。

**刚上线时没有人竞拍会怎样?**

A：会有一个固定的 boot coordinator （Hermez自己的节点）负责在没有他人竞拍时担任 rollup 工作。等 Hermez 拍卖参与者变得多且活跃之后由 DAO 投票将 boot coordinator 撤销。

**拍卖过程：**

1. 一个 slot 表示 10 分钟；
2. coordinator 将对某个 slot 的报价发到合约上，由合约收集；可以报价的 slot 范围在未来一个月内；slot 到点的 20 分钟前停止拍卖；
3. 拍卖获胜者将在竞拍的 slot 里负责收集交易，执行 rollup；

**这个拍卖是公开的，可以反复出价。**

**Q：先拍卖然后收集交易，怎么保证有足够多的交易手续费能收回成本弥补拍卖付的钱?**

A：假设 Hermez 链上的交易足够活跃，交易数量足够多，则从中挑选手续费高的交易来收集的话一定可以满足需求。

**Q：收集交易并 rollup 的人已经在 slot 之前选举好，怎样防止他作恶，故意挑选交易来收集?**

A：可能是支持 Hermez rollup 的交易都是转账，基本上只有手续费高低的区别，所以没有做恶动机。

**zksnark:**

Groth16算法+MPC ceremony

# Polygon Miden

**A STARK-Based EVM-compatible Rollup** 11月16日发布的介绍

目前状态: **in develepment**

特色： Miden VM, a STARK-based virtual machine

Miden VM支持任意逻辑和transactions，并且对于在VM上执行的任何程序，都会自动生成基于stark的证明（证明程序被正确执行）

# Polygon Nightfall

与EY合作的项目 **privacy-focused Rollup**

目前状态: **in develepment** 、release the 0.1 version of Miden VM

技术路线：**zk(privacy) + Optimistic Rollups(scalable)**