

# zkdex 产品和工程实践

高性能可扩展zk-rollup网络（应用）

Kevin@stars\_labs

# Why Another ZK-Rollup?

## 我们的出发点

- zk-rollup 具有独特优势-交易最终化速度
- 已有zk-rollup项目，性能与扩展性依然有提升空间（证明生成速度、数据规模）
- zkevm 尚未落地、远未完善（指令集完备、solidity 无缝迁移、性能）
- zkp 技术本身有广阔的应用场景（隐私计算、外包计算等）
- 为先行者致敬：
- Respect: zksync、starknet、aztec、hermez、loopring、zkswap...

# 产品形态

- 完整的 zk-rollup AMM Dex
- 支持二层流动性挖矿(Liquidity Mining)（LP无需提到一层）

兑换

From 余额：100.654321  
33.78904 MAX ETH ▾

To 余额：100.654321  
0.000678936 wBTC ▾

价格 1 wBTC = 33.87954 ETH

该币种流通性不足无法兑换

价格影响 ⓘ <1.0%  
流动资金提供者费用 ⓘ 1.0%  
最低收到 ⓘ 2830.28 wBTC

添加流动性

投入 余额：100.654321  
0.00 MAX ETH ▾

+

投入 余额：100.654321  
0.00 MAX wBTC ▾

确认提供

我当前持有

ETH-wBTC	0.001%
ETH	234,896.89
wBTC	37.89057

添加流动性即挖矿  
获取LS或项目代币

您将获得

64.8636 LS

通过添加特定 LP 交易对流动性 (APY>0) 即可获得LS奖励。

已添加LP数量 145,638.9742704 ETH/wBTC  
流动性占比 0.001245%

确认领取

领取 添加 移除

ETH/wBTC 1068.26 1888.88%  
10,213,256.84 32,450.66 5.6927

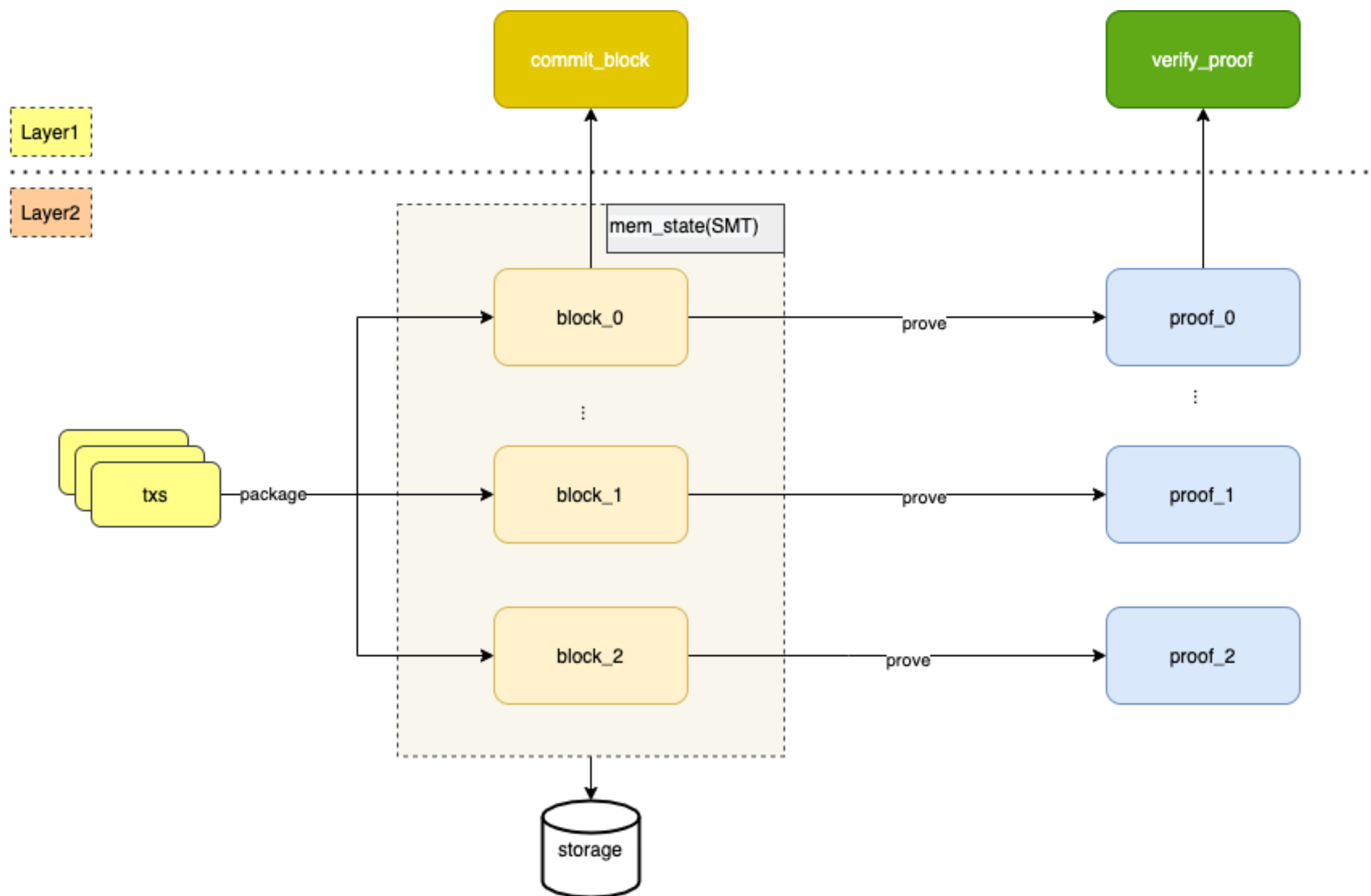
首页 兑换 挖矿 L2钱包 浏览器

# zk-rollup 的技术痛点

从生产系统角度来考量

- 理论与实际系统tps
- 证明验证 gas 消耗大
- 系统扩展性弱
- 资金安全性
- 多 rollups 互通
- EVM&solidity 兼容性

# zk-rollup 交易生命周期



# 理论系统tps

- 理论值：
- 以太坊区块  $\text{gaslimit} / \text{每笔交易calldata消耗的 gas} / \text{区块间隔}$
- 例如 2k、3k
- 问题：
- 1) 未考虑实际证明生成时间
- 2) 未考虑区块信息和证明验证所消耗的 gas
- 3) 未考虑不同交易类型消耗的 gas 差异

# 实际系统tps

- 实际生产值:
- $\text{tps} = \text{Txs\_block} * \text{N\_proof\_parallel} / \text{T\_proof}$
- T\_proof: 单个证明所需时间
- Txs\_block: 2^26门, 所容纳最大交易数(plonk+bn256)
- N\_proof\_parallel: 证明生成并行度
- GPU加速+算法优化: 实现了 3-4X 速度提升
- 大规模证明集群调度: 分布式证明任务调度实现 100-200证明组
- plookup+customgate: 减少电路门数(working on)

# 证明速度优化：GPU 加速+算法优化

2^26 门，plonk+bn256 曲线，加速效果，3.3X

环境	配置	FFT			Multi-Exp			时间 /s
		单个 时间	总 时间	总 占比	单个 时间	总 时间	总 占比	
CPU	Xeon(R) Platinum 8163, 2.5GHz, 366GB memory	2.5s	160s	23%	32s	346s	49%	700s
GPU	Xeon(R) Platinum 8163, 2.5GHz, 366GB memory, Tesla T4 x2	0.75s	38s	18%	10s	115s	55%	210s
加速		X3.3	X4.3		X3.2	X3.0		X3.3



# Gas消耗优化：聚合证明+GPU加速

聚合 18 个区块，验证消耗节省 X15，证明加速 X2.2

聚合证明

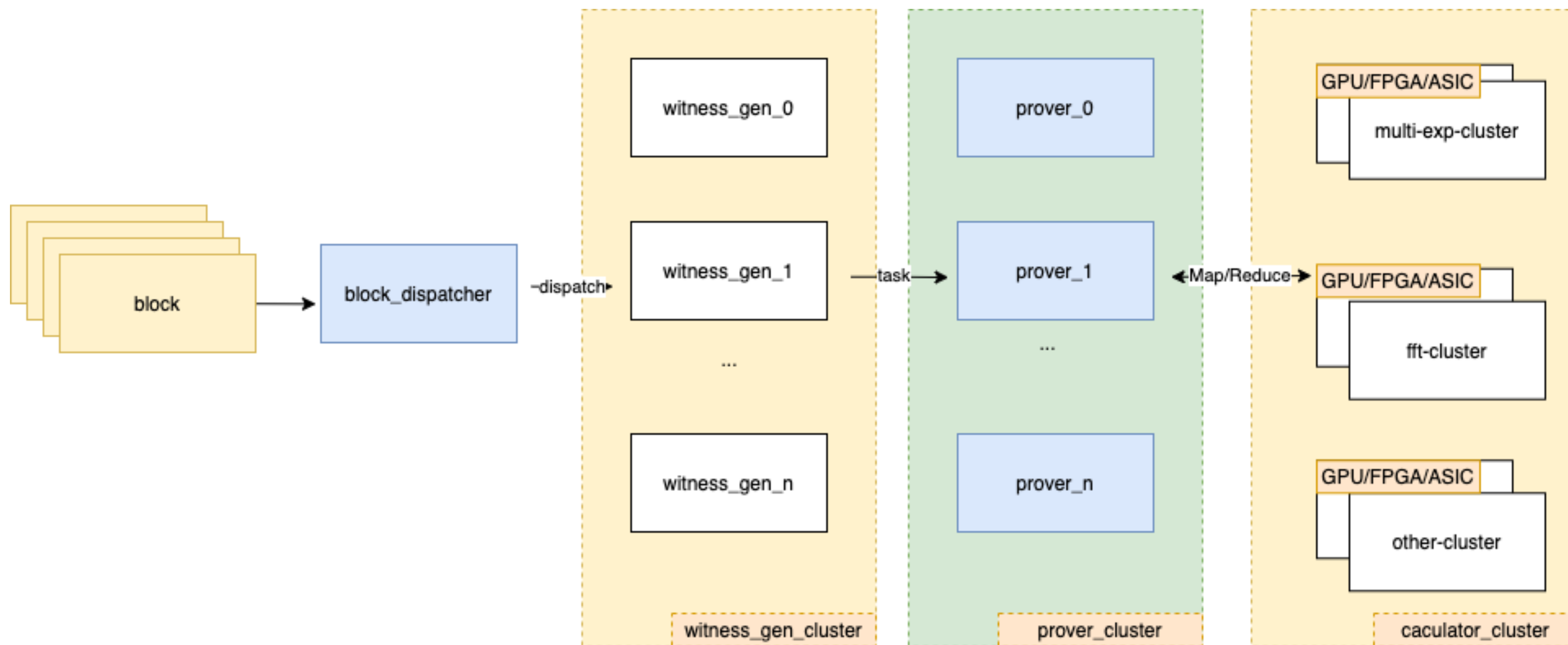
环境	proofsize[18 个区块 ](bytes)	验证消耗 gas
无聚合证明	1056*18	0.5m*18
聚合证明	1088	0.6m
节省		X15

GPU 加速

环境	配置	证明时间[18个区块]
CPU	CPU: Xeon(R) Platinum 8163 CPU 2.50GHz 366GB memory	564s
GPU	GPU: Xeon(R) Platinum 8163 CPU 2.50GHz 366GB memory, Tesla T4x2	256s
加速		X2.2

# 大规模证明集群调度

## 分布式任务调度系统



# 系统扩展性

如何支撑5-10M日交易量：服务拆分、内存计算、数据

- 服务拆分：api、core、prove cluster、eth\_pub/eth\_sub
- 核心系统内存计算模型
- 状态(SMT)数据快照与回滚
- 分库分表与聚合查询
- 冷热数据分离

# 资金安全性

## 实际运营与服务承诺

- 状态校验与紧急恢复机制
- 紧急撤离模式（合约、电路、链下系统、前端）
- 前端代码安全托管
- 代码开源

# 开放的 Rollup

- 市场价格参考（兑换）：引入 chainlink price feed 作为价格评估因素
- 二层数据索引：借助thegraph基础设施，定制subgraph进行标准化数据展示
- 钱包与CEX接入 SDK
- 跨 rollup 资金互通（跨链桥）

# Working On

- plookup+customgate: 优化电路门
- EVM&Solidity 兼容性: 让开发者专注业务

# 产品演示

- <https://zkdex.oss-cn-hangzhou.aliyuncs.com/demo/zkdex-demo-o.mov>

# 实验室介绍

@stars\_labs

- Stars-Labs（星辰实验室）专注于区块链前沿技术研究、产品研发、基础设施建设等领域。团队人员来自国内外顶尖名校，博士团5人。团队在以太坊生态、Layer2、零知识证明、隐私计算、跨链桥等方面有较强积累，致力于在最具挑战的技术领域取得引领性的行业成果。
- 星辰实验室目前产品包含：高性能公链，Layer2 扩容网络，跨链桥等。



# Thanks

@stars\_labs

- 源自社区，回馈社区
- Let's rollup!
- 欢迎交流: @kvh\_kevin

