



Layer2技术与应用

赵文琦

打 造 最 专 业 的 区 块 链 研 究 机 构

Rebase

北京 | 南京 | 成都 | 上海 | 深圳

ETH HACKATHON

14-16 MAY 2021



用 500 行代码构建下一个
50 亿美金的独角兽

30 天备赛 72 小时Hack

头部投资人一对一Insights

以太坊生态技术大咖点评

以太坊基金会资助

顶级开发者云集

奖金池 20000 DAI

一等奖 1 名：奖金 10000 DAI

二等奖 2 名：每支队伍奖金 3000 DAI

三等奖 2 名：每支队伍奖金 2000 DAI

主办方

Rebase

联合主办



WHITE MATRIX



社区支持

Ethereum Foundation

APRON

D+块+

链茶馆

KUCUN

Plancker

区块链高新区

资本支持

ORDER

PRIMITIVE

SL

VENTURES

ONEBOAT

D

base D. Ventures

合作媒体

链闻

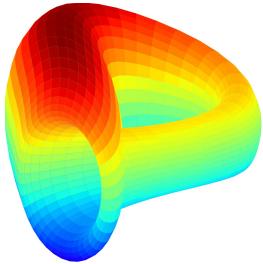
CHAIN

Z 起链网

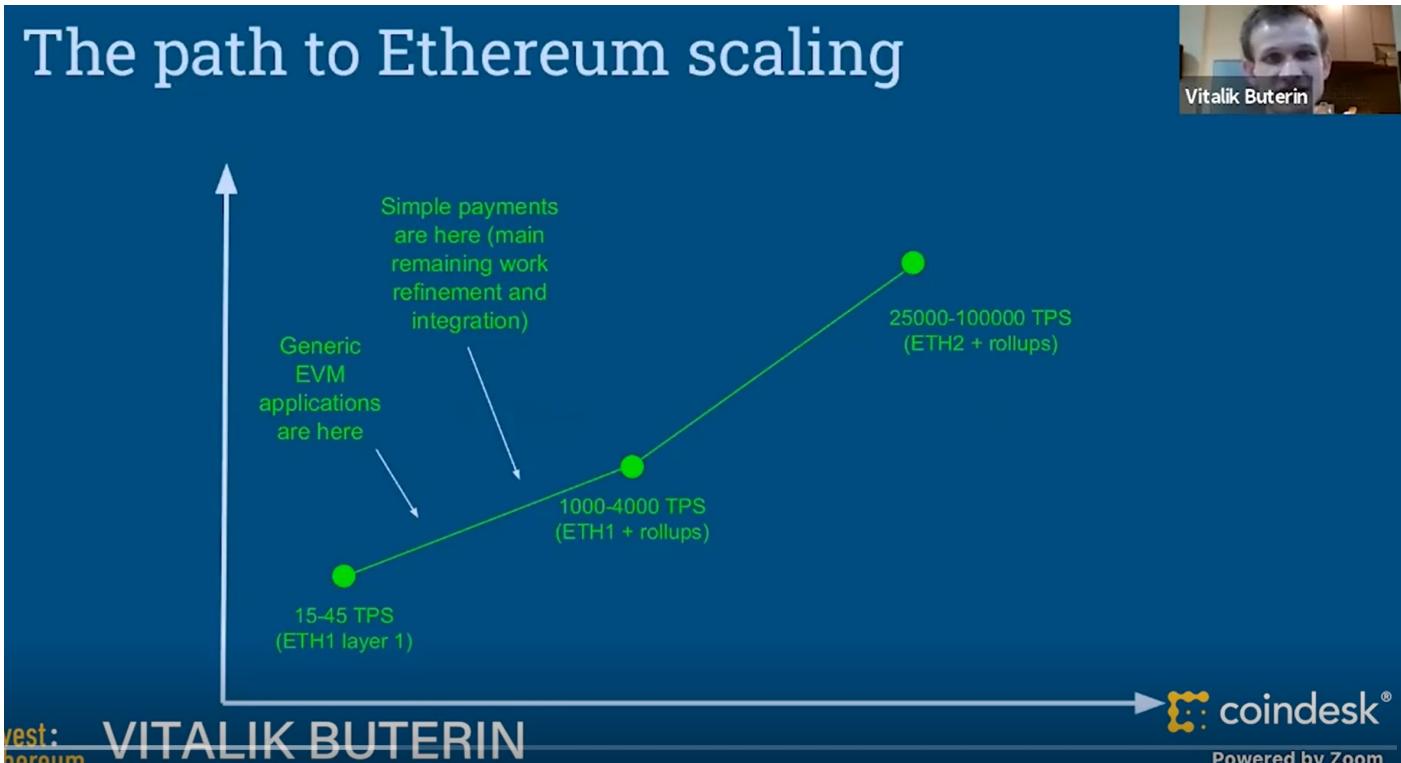
火星财经

巴比特

为什么需要Layer2?

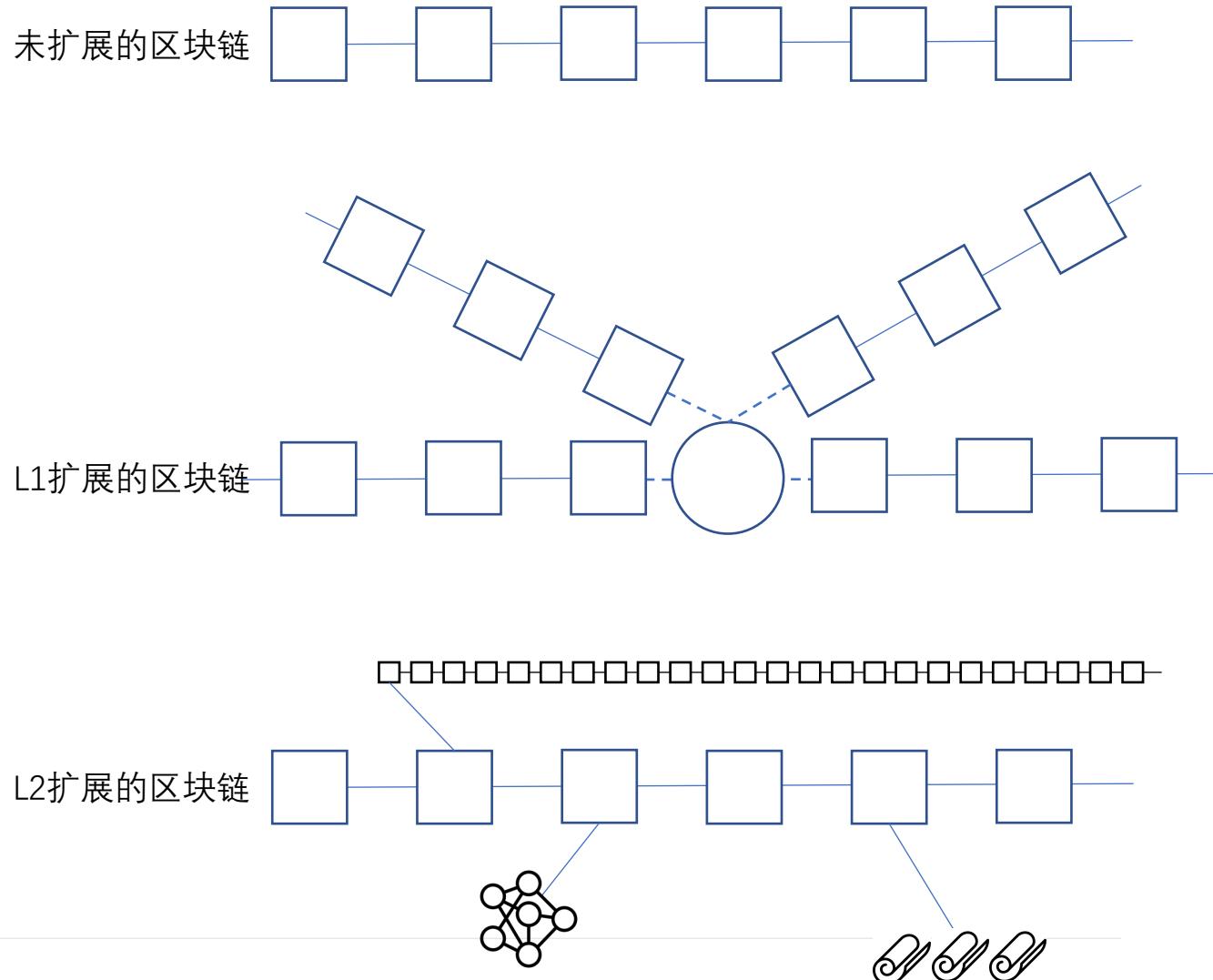
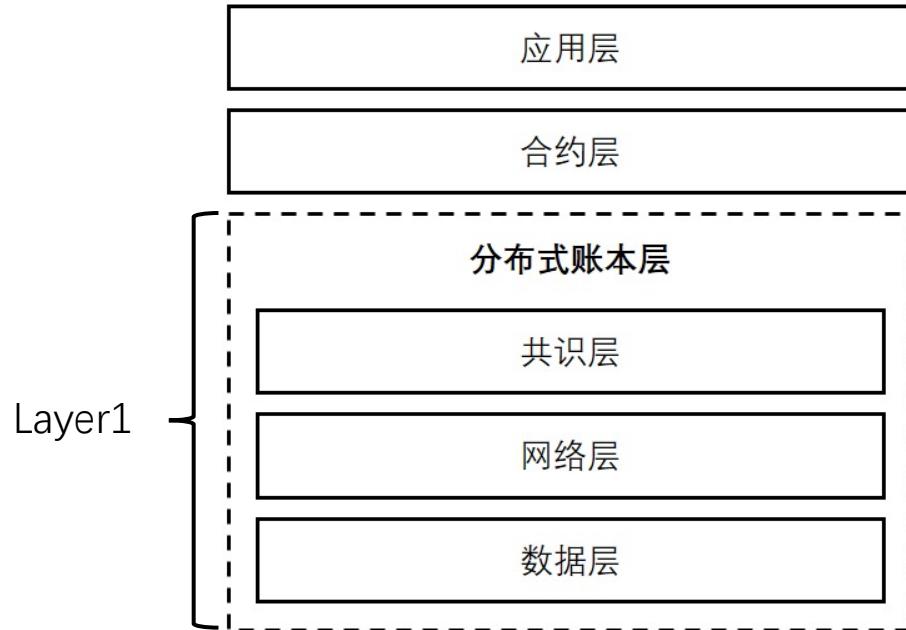


Layer2已经被纳入以太坊的扩容路线图

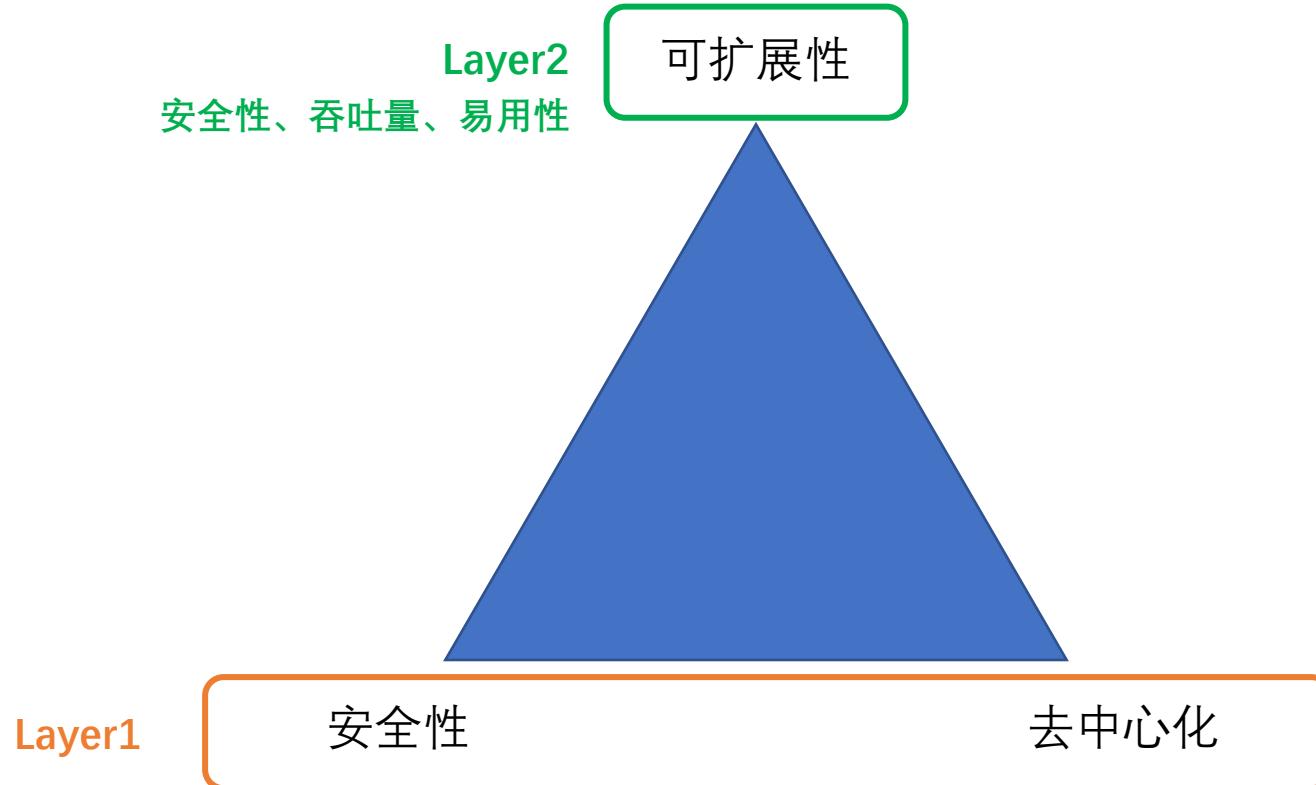


Layer2是一系列链下扩展性解决方案的统称，该种扩展**不涉及对区块链本身的改造**，通过其他方式来实现可扩展性的提升，即**链下改进**

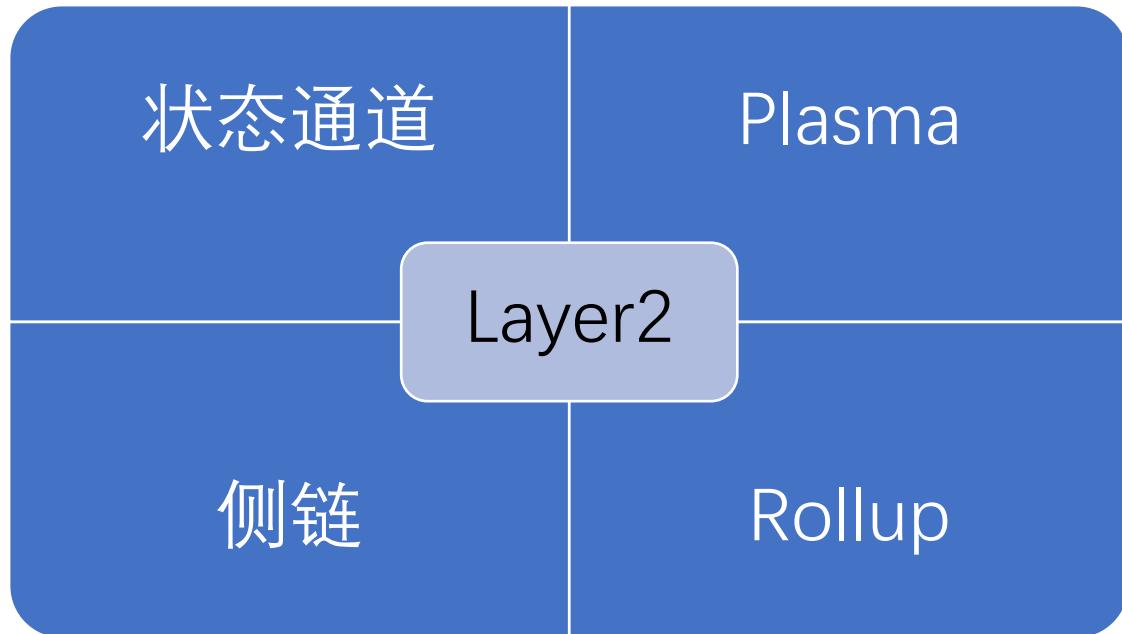
什么是Layer2?



进一步看Layer1与Layer2



Layer2的主要技术方案

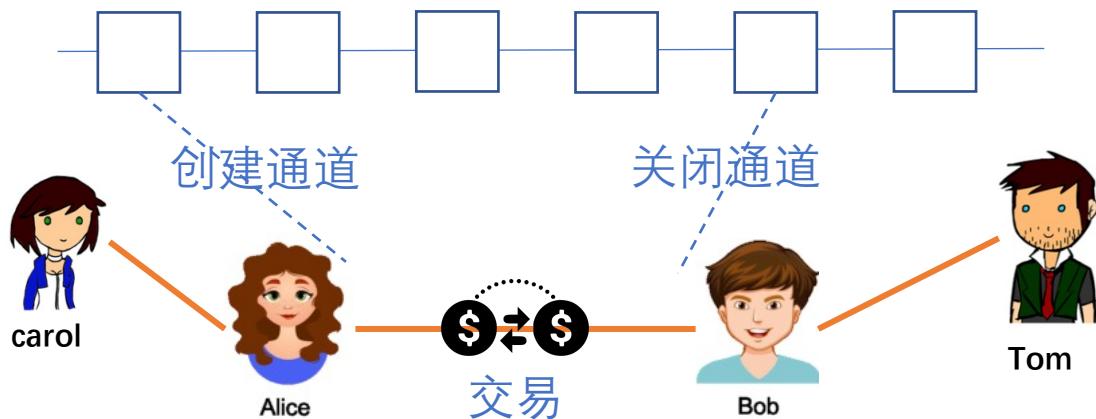


如何进入和退出？
如何提高扩展性？牺牲了什么？

状态通道

核心原理

- 一个通道可以实现用户两两之间的资金转移
- 大量通道共存时可以构成一个二层的通道网络
- 未建立直连通道的用户可以通过网络路由实现资金转移



代表团队

闪电网络、雷电网络、Celer等

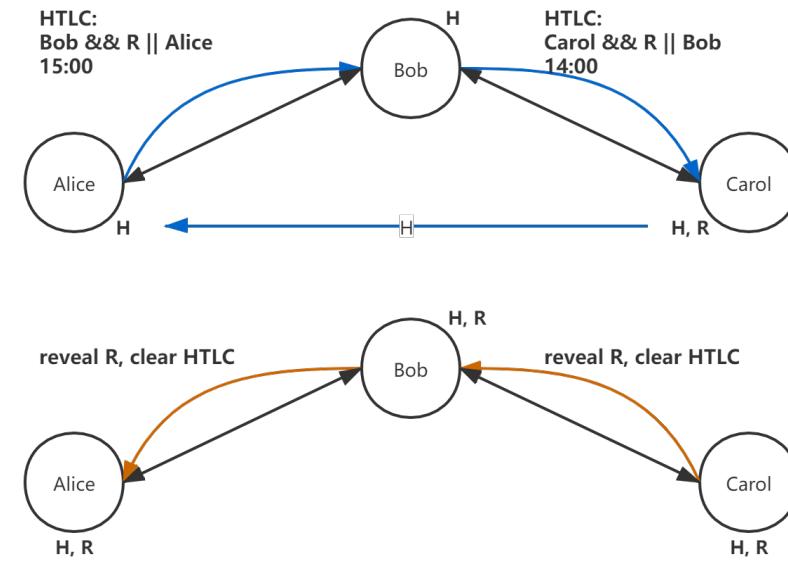
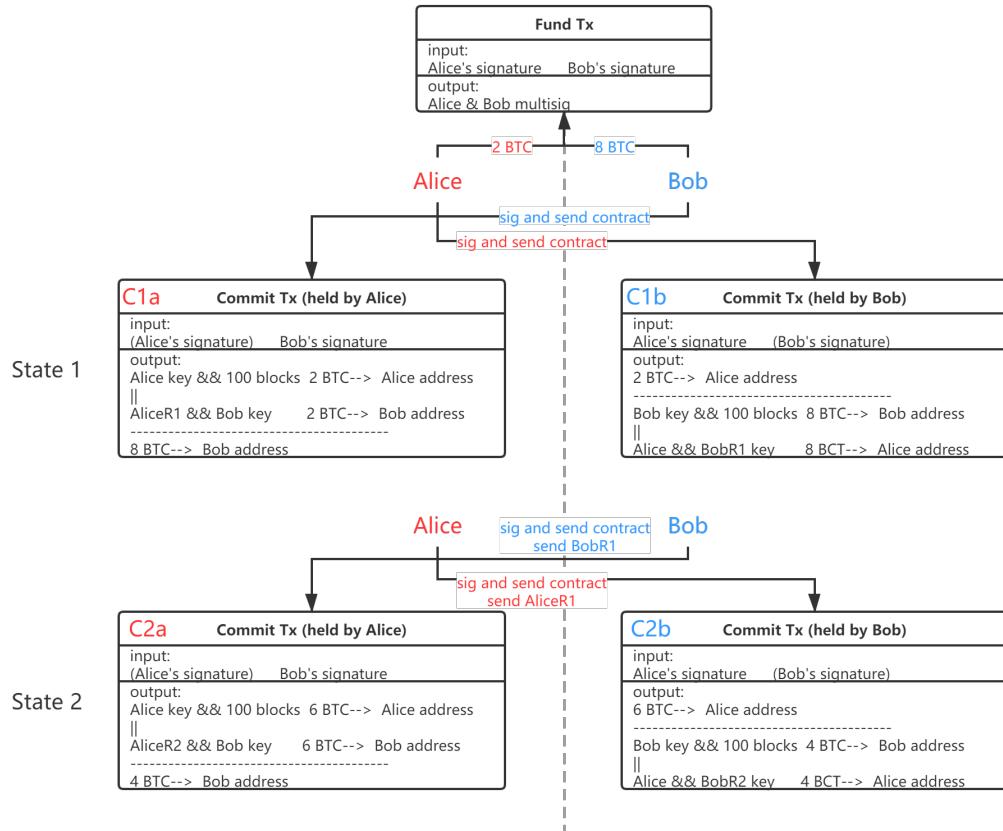
优势与问题

优势：极大提升吞吐量、降低交易成本、支持跨链
问题：集中化、网络稳定性、网络本身的扩展性、
用户友好性、智能合约支持的不好

现状

状态通道类型的layer2解决方案进展并不顺利

闪电网络：RSMC+HTLC



欺诈证明
链下的数据有效性

Plasma

由闪电网络提出人Joseph Poon和以太坊创始人Vitalik共同提出

核心原理

将主链计算转移到Plasma链上，通过欺诈证明的方式防止作恶

代表团队

Matic(Polygon)、OMG等

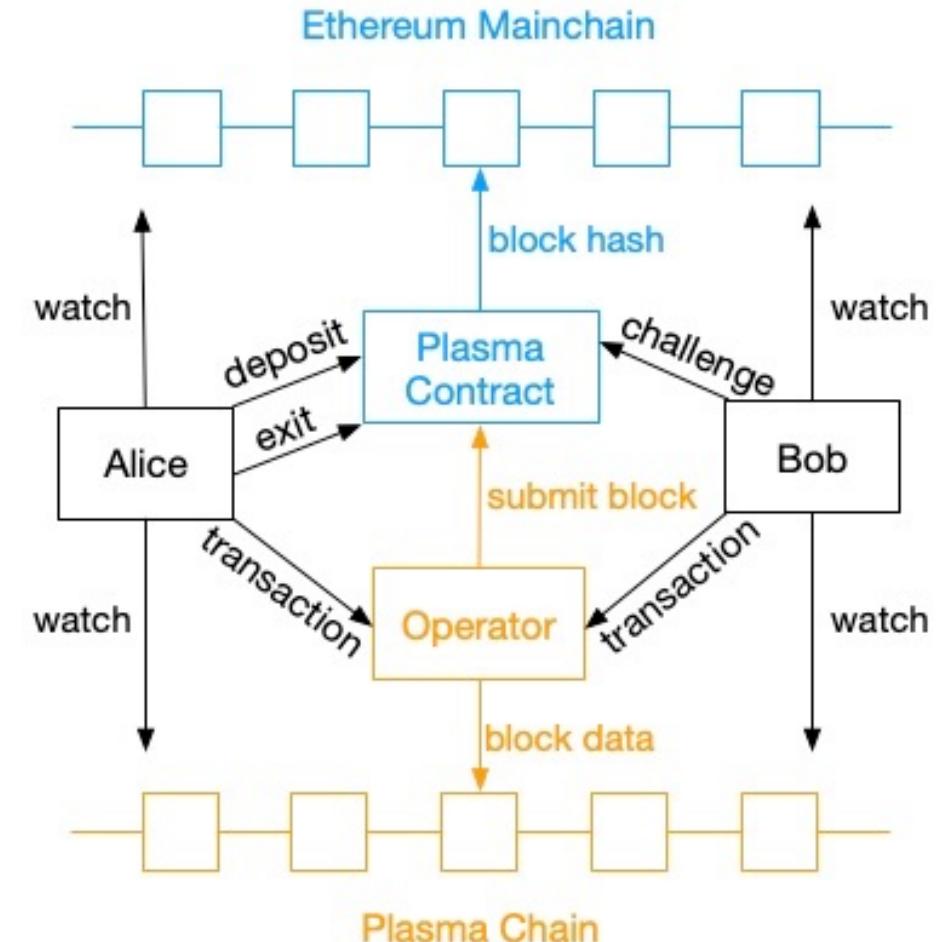
有Plasma MVP和Plasma Cash等方案

优势与问题

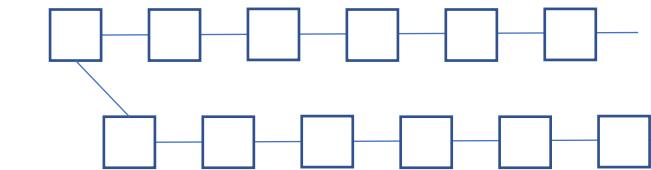
- 优势：交易成本低、比一般侧链安全性高
- 问题：对用户存储要求高、退出机制复杂有争议期

现状

多数Plasma项目已经停止或换方向，少数团队还在坚持，活力不强



侧链



The diagram illustrates a side chain architecture. It features two parallel horizontal chains of six square nodes each. The top chain is connected by blue lines, and the bottom chain is also connected by blue lines. A single blue line connects the second node of the top chain to the second node of the bottom chain, representing a cross-chain interaction.

xDai chain
Balance: 0.96 xDai
Show More

1 XDAI Request

ETH Mainnet
Balance: 411.93 DAI
Show More

Haven't received your tokens?



ETHDenver大会，4450笔点餐订单，交易费只有0.2\$

什么是rollup?



链上数据可用性

数据上链者作恶

有效性证明——ZK Rollup

欺诈证明——Optimistic Rollup

ZK Rollup

zkRollup引入了零知识证明技术，将数百个交易捆绑为一个交易。链上验证一次交易中持有的所有转移，退出的等待时间很短。

核心：

rollup+零知识证明

压缩方式：字段压缩和删除

怎么防谁来负责压缩：relayer（运营商）

止作弊：有效性证明

代表团队：

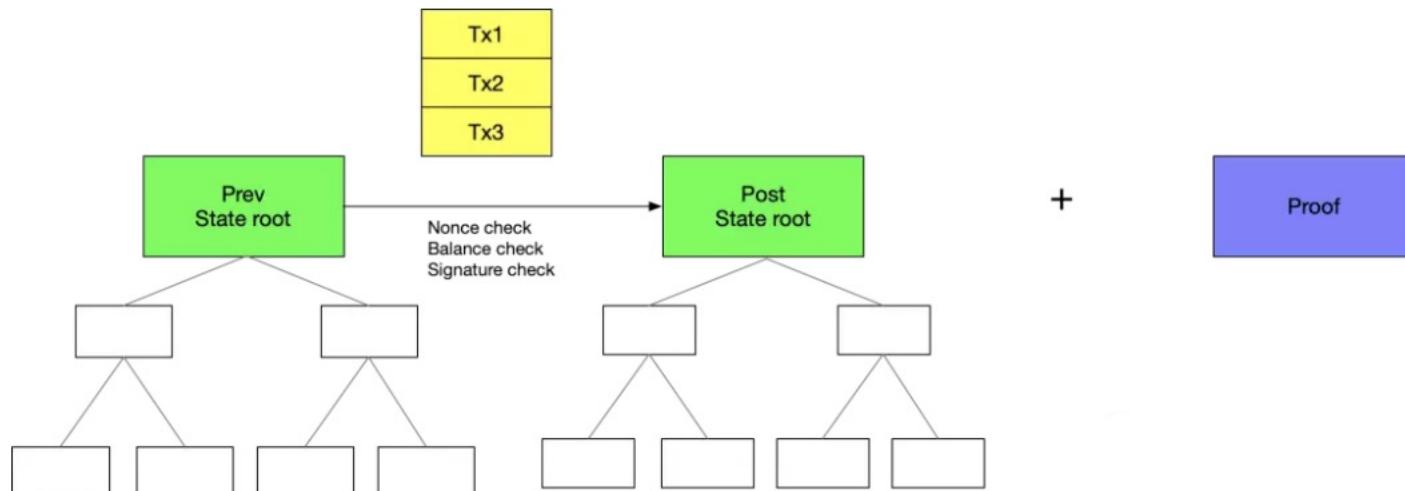
Matter Labs、Loopring等

实现的效果：

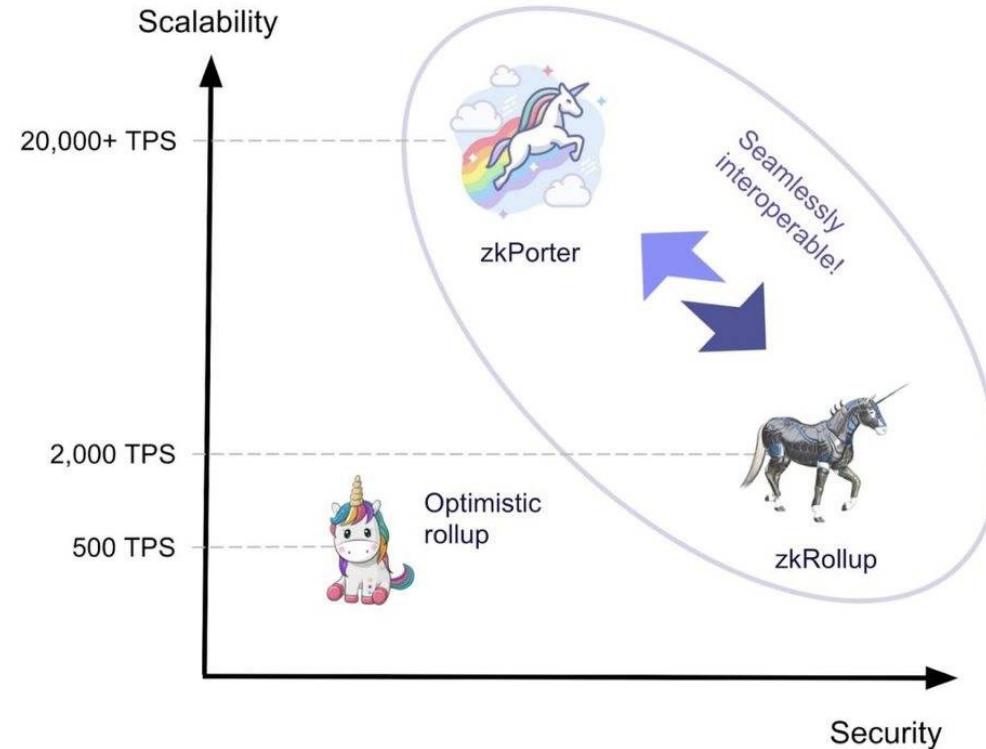
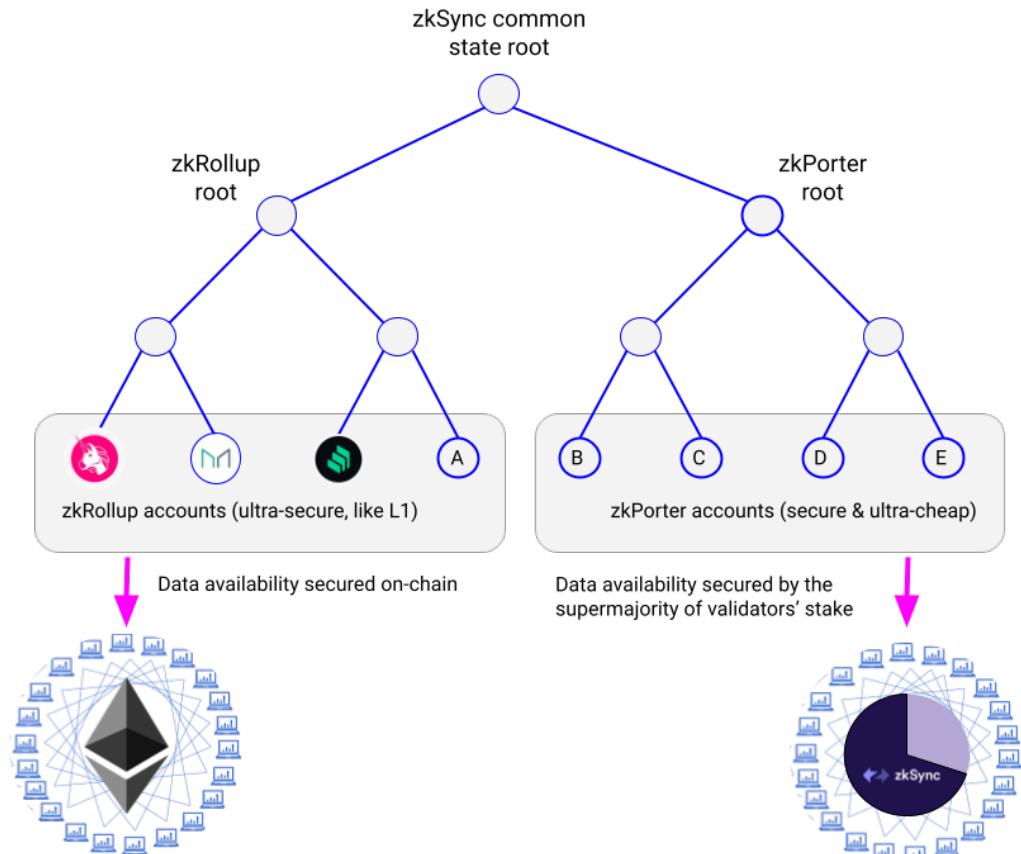
1. 安全性高，等同于layer1的安全性
2. 2000-2500 TPS
3. 仅有数分钟的退出等待
4. 没有用户活性假设

问题：

1. 暂未支持通用的智能合约
2. 复杂度高
3. 吞吐量提升有限



zkSync: zkRollup+zkPorter+ZincVM



OP Rollup

Optimistic Rollup 的构造大量借鉴了 Plasma 和 ZK Rollup 设计。但某种程度的在扩展性上进行了权衡，以允许在受 Layer 1 保护的 Layer 2 中运行完全通用的智能合约。

核心：

rollup+欺诈证明

压缩方式：参考zk，但由于支持通用智能合约，压缩效果减弱

谁来负责压缩：Aggregator（运营商）

怎么防止作弊：欺诈证明，只要运营商中有1个节点是诚实的
(诚实运营商可以拿出攻击者无可反驳的证据)

代表团队：

Optimism、Fuel Labs等

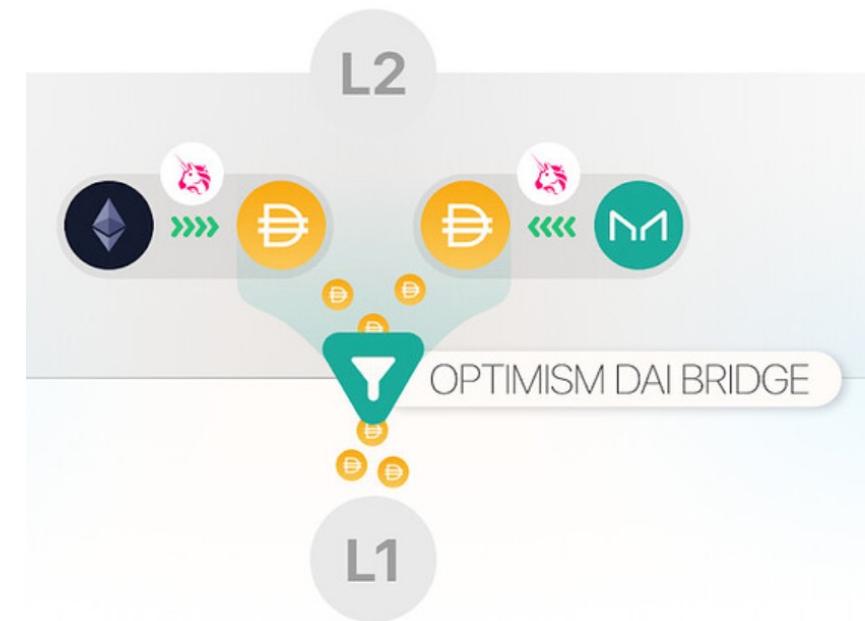
实现的效果：

- 1.数百 TPS
- 2.完全兼容智能合约

问题：

- 1.TPS提升十分有限
- 2.退出期长，资金效率降低
- 3.潜在的安全性问题

Maker DAO的DAI Bridge



	状态通道	侧链	Plasma	Optimistic Rollup	zkRollup
示例	Pisa、Celer	Skale、PoA	OMG、Matic	OVM、Fuel	zkSync、Loopring
安全性					
在线假设（例如瞭望塔）	有	有限	有	有限	无
大量退出能力假设	无	无	有	无	无
验证者可联手冻结资金	不可	可	不可	不可	不可
验证者可联手盗取资金	不可	可	不可	不可	不可
运营者密钥暴露风险	高	高	一般	一般	低
加密经济学攻击风险	一般	高	一般	一般	低
密码学原语	标准	标准	标准	标准	新
性能/经济性					
在 Eth1 上的最大吞吐量	1~无限	10 K+	1~9 K+	0.5 K	2 K
在 Eth2 上的最大吞吐量	1~无限	10 K+	1~9 K+	5 K+	20 K+
资金利用的效率性	无	有	有	有	有
需要额外的链上交易来开启一个新账户	是	否	否	否	否(依赖于具体实现)
交易手续费	极低	低	极低	低	低
便利性					
取款时间	1 笔交易	1 笔交易	1 周	1 周	1~10 分钟
即时的交易确认	满足	部分满足	部分满足	部分满足	部分满足
其它维度					
智能合约灵活度	有限	灵活	有限	灵活	灵活
EVM 字节码可移植性	不可	可	不可	可	不可
原生隐私支持	有限	无	无	无	有

来源 : Matter Labs



谢谢观看

关注微信公众号 [HuobiCN](#)

打 造 最 专 业 的 区 块 链 研 究 机 构

Rebase

北京 | 南京 | 成都 | 上海 | 深圳
ETH HACKATHON
14-16 MAY 2021



用 500 行代码构建下一个
50 亿美金的独角兽

30 天备赛 72 小时Hack
头部投资人一对一Insights
以太坊生态技术大咖点评
以太坊基金会资助
顶级开发者云集

奖金池 20000 DAI
一等奖 1 名：奖金 10000 DAI
二等奖 2 名：每支队伍奖金 3000 DAI
三等奖 2 名：每支队伍奖金 2000 DAI

主办方 **Rebase** 联合主办 **ETHPlanet** **WHITE MATRIX**
社区支持 **Ethereum Foundation** **APRON** **一块+** **链茶馆** **KUCIN** **DoraHacks**
Mask **XDEFI** **Acala** **Ploncker** **区块链高校联盟**
资本支持 **ORDER** **PRIMITIVE** **SC VENTURES** **ONEBOAT** **D**
HECO **FIDA** **LANCER**
合作媒体 **链闻 CHAIN NEWS** **Z 起链网** **火星财经** **巴比特**

扫码报名

