

Survey of zero knowledge applications

0. 基础信息

Item	Description
Name	yueawang
Discord Account	Yue#1946
Study Group	Team3
Assignment	Survey of zero knowledge applications
GitHub Rep	https://github.com/yueawang

1. 概述

本文尝试介绍一下ZK相关的应用，尽可能涵盖现有的各种不同种类的应用，然后在每一种中简单介绍一两个代表性的项目。

首先我们知道ZK协议本身主要有两个特点：

- zero-knowledge: 零知识证明，即在不暴露关键隐私的情况下向对方证明一件事情。
- succinct: 简洁性，证据Proof占用的空间很小。

基于这样的特点，目前ZK的主流应用集中在3大类：

- 第一类是扩容，主要理论根据是简洁性，这里扩容主要指以太坊扩容，为了解决以太坊拥堵和高额GAS费问题而来。第2章列举了主流的扩容应用。
- 第二类是隐私保护，理论基础就是零知识证明，理论上说这一类应用才真正叫做ZK，真正的实现了零知识和隐私保护。在第3章对常见的隐私类应用作一个综述。
- 第三类同样利用证明的简洁性，但目的不是扩容，而是用于压缩存储成本，第4章介绍一下代表性项目。

此外，应用的繁荣其实是对应生态的繁荣，在应用背后的ZK生态建设也应该得到关注，特别是开发者工具，开发者教育，社区治理等等，因此在第5章我们梳理一下这个赛道上有代表性的项目的状态。

2. 以太坊扩容类ZK应用

目前，ZK最热门的一个应用类型是扩容，为什么要扩容？主要是因为以太坊的拥堵以及拥堵产生的高额GAS费。因此各个项目方都提供了自己的扩容方案。从[l2beat](#)上可以看到当前主流的扩容方案top10项目方如下。

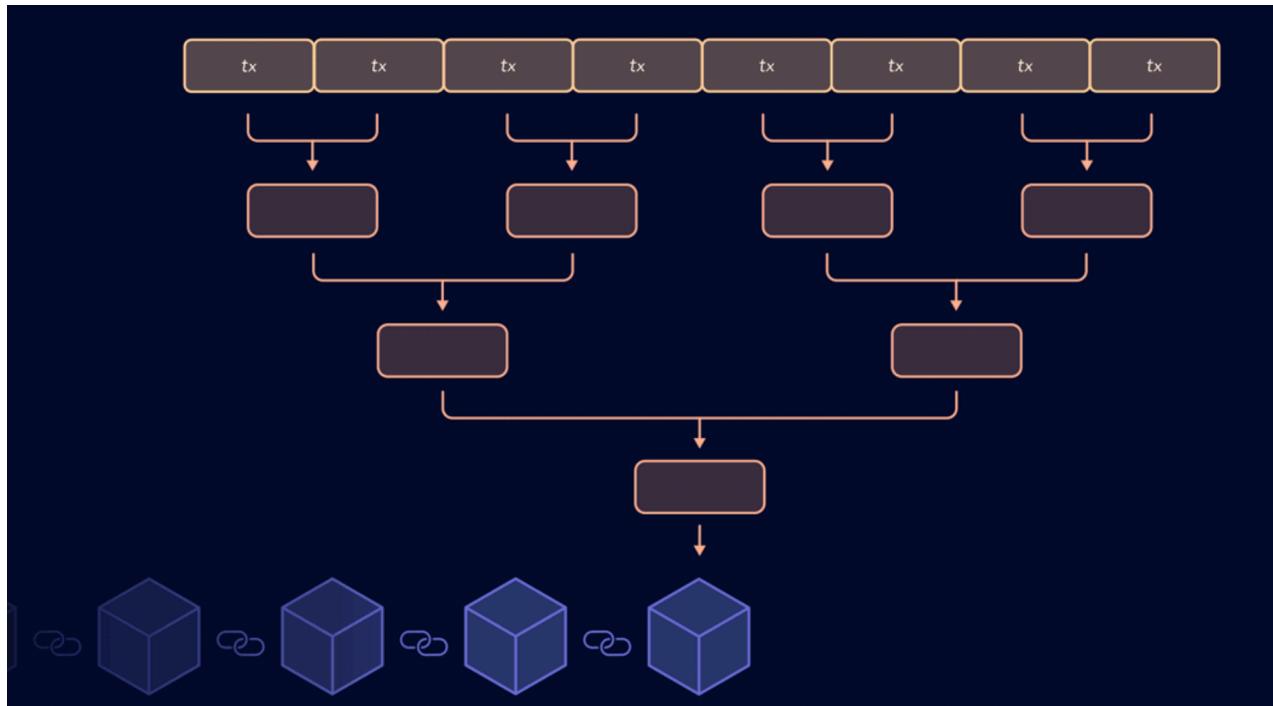
No.	Name	TVL	Breakdown	7d Change	Market share	Purpose	Technology
1.	Arbitrum	\$2.03B		+5.13%	52.62%	Universal	Optimistic Rollup
2.	Optimism <small>OP</small>	\$735M		-0.88%	18.99%	Universal	Optimistic Rollup
3.	dYdX <small>◆</small>	\$578M		-6.59%	14.92%	Exchange	ZK Rollup
4.	Loopring	\$177M		+7.94%	4.57%	Tokens, NFTs, AMM	ZK Rollup
5.	Metis Andromeda <small>OP</small>	\$97.66M		+6.50%	2.52%	Universal	Optimistic Chain
6.	zkSync	\$58.74M		+7.48%	1.52%	Tokens, NFTs	ZK Rollup
7.	Boba Network <small>OP</small>	\$47.67M		+16.81%	1.23%	Universal	Optimistic Rollup
8.	Immutable X <small>◆</small>	\$45.57M		+25.47%	1.18%	NFT, Exchange	Validium
9.	ZKSpace	\$39.95M		+17.03%	1.03%	Tokens, NFTs, AMM	ZK Rollup
10.	DeversiFi <small>◆</small>	\$24.11M		+0.70%	0.62%	Exchange	Validium

扩容方案也可以叫做ZK-rollups，根据dydx上的定义：

Layer 2: ZK-Rollups

Trades are settled in an L2 (layer-2) system, which publishes ZK (zero-knowledge) proofs periodically to an Ethereum smart contract in order to prove that state transitions within L2 are valid. Funds must be deposited to the Ethereum smart contract before they can be used to trade on dYdX.

ZK-Rollup示意图如下，即将主链之外的多笔交易聚合成一个状态更新到主链：



出发点虽然都是扩容，但这些项目方解决问题的思路和不尽相同，大方向上有通用和专用两种：

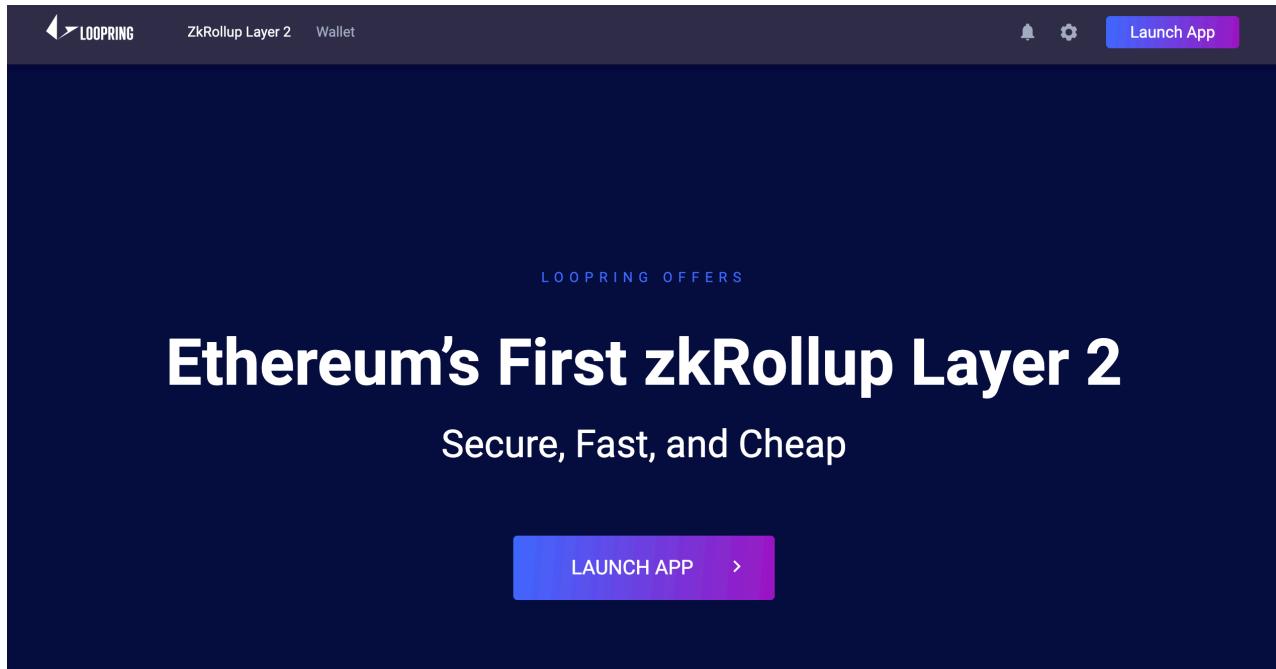
2.1 专用扩容方案

专用扩容方案顾名思义就是指功能比较单一的扩容方案，他们只能解决某一类或者预定义的几类问题，目前常见的有交易所，NFT，Defi等形式。

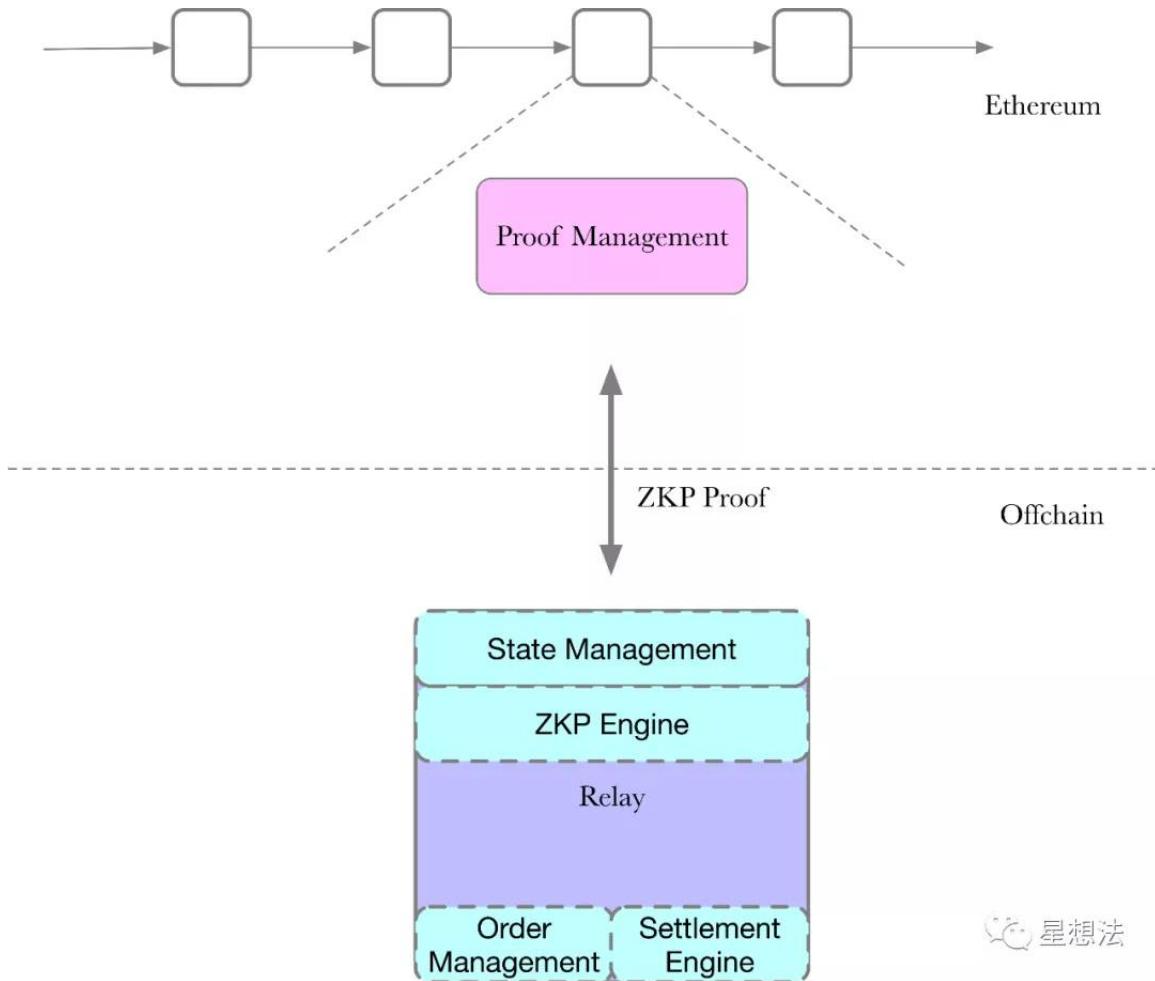
已经有很多基于ZK的交易所，比如[Loopring](#), [Deverisfi](#), 或者NFT交易的[ImmutableX](#), 又或者衍生品交易的[dydx](#)。下面介绍一下各个赛道上的代表性项目：

2.1.1 中心化体验的去中心化交易所--Loopring

路印希望提供一个有中心化体验的去中心化交易所，就体验来说做的还不错。ZK技术上，就像他们主页提到的，是第一个商用的zkRollup Layer 2。路印去中心化交易平台同样基于zkRollup技术，可以在速度，成本和体验上与中心化交易所竞争，同时为用户提供远高于中心化交易所的安全性。



路印的ZK-Rollup采用的是Groth16算法，基于libsnark用c++开发，采用和以太一致的“账户”模型，所有的账户的“状态”（余额）都记录在链下，所有和状态相关的操作，都是在链下更改，提交Proof到链上记录。



总之，路印是传统的zkRollup应用里面非常具有代表性的一个，但是与下文即将提到的其它的Rollups技术方案（比如说Starkware, zkSync, 或Optimism等）有所不同的是，Loopring所开发的zkRollups技术方案主要服务于自己的应用，生态相对较为封闭。

2.1.2 专注于NFT的ImmutableX

ImmutableX相当于基于ZK-Rollup的opensea。

和Loopring自己开发电路不同，ImmutableX是Starkware的合作伙伴，其ZK部分是由starkware提供支持的，参考[imx-starknet](#)，即用Cairo编写的ZK程序，这里顺便提一下Cairo：

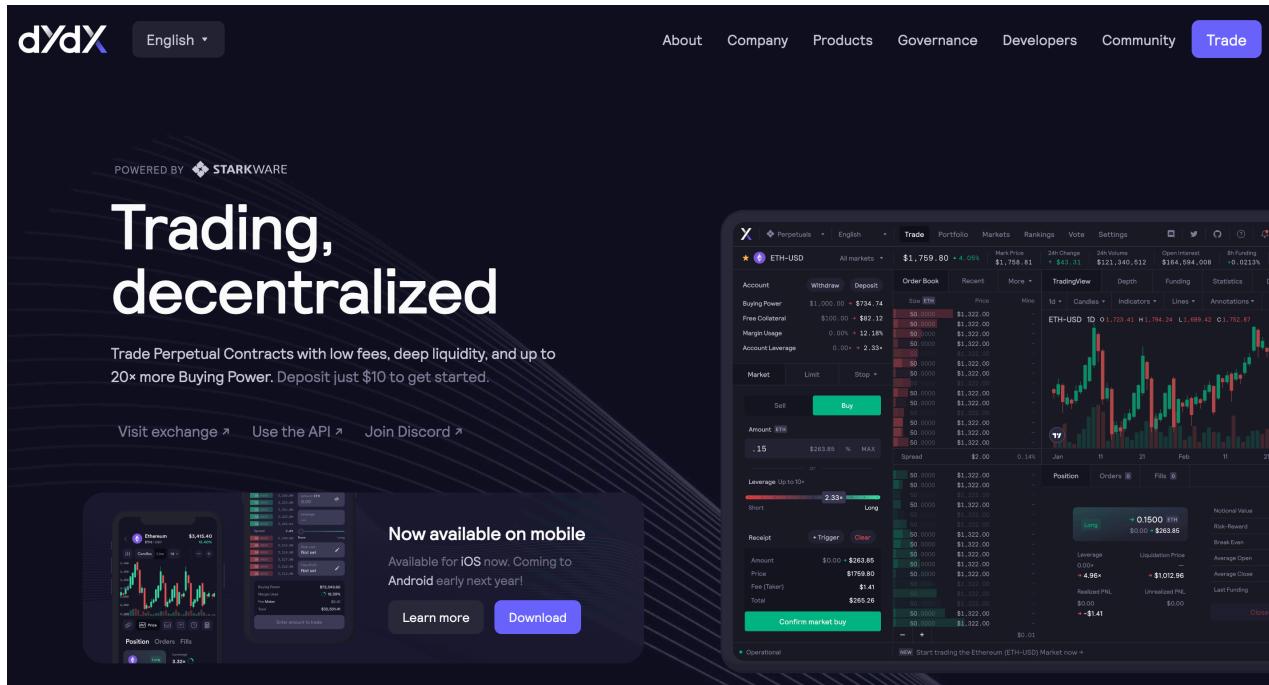
简单来说就是Cairo提供了一个图灵完备的零知识证明语言，任何使用 Cairo 写的程式都能用同一个 Verifier 来验证，每个应用不再需要产生一个专属自己能用的 Verifier 合约。值得一提的是Cairo并不是基于算术电路或者R1CS，而是自己开发的一个称为AIR的多项式约束系统，具体细节可以参考[Cairo官网](#)以及[Cairo白皮书](#)。

The STARK proof system is based on AIRs (Algebraic Intermediate Representation, rather than arithmetic circuits or R1CSs. An AIR can be thought of as a list of polynomial constraints (equations) operating on a (two-dimensional) table of field elements (of some finite field, F) called the "trace" (the witness). A STARK proof proves that there exists a trace satisfying the constraints.

Starkware是ZK领域的重量级选手之一，初创团队加入Cairo生态意味着开发者可以直接利用Starkware的资源，比如Cairo提供的高级的逻辑表达，统一的AIR验证器和底层的ZK软件算法优化，而不用从0开始构造整个ZK协议。

2.1.3 衍生品赛道上的dydx

如果说路印属于基于ZK的现货交易，ImmutableX是ZK上的NFT交易（顺便提一下：路印也有自己的NFT子系统），那么dydx则是为数不多的基于ZK的衍生品交易平台。



和ImmutableX一样，dydx一开始选择了和Starkware合作开发，目前的版本基于ZK，由于期货交易比现货交易更加注重吞吐量，因此dydx依赖于ZK强大的扩容能力，而同Starkware合作则能够在短期内开发出成熟的ZK交易系统，正如其[官方帮助文档](#)所说：

- dydx为何迁移到Layer 2？

以太坊每秒可以处理大约15笔交易（TPS），这不足以支持DeFi、NFT等的高速增长。虽然以太坊2.0理论上会将网络速度提高到100,000TPS，但基础层的扩展仍有一段距离。与此同时，Layer 2扩展解决方案——以Rollup的形式——通过卸载执行来释放以太坊的基础层，从而在不增加网络负载的情况下降低gas成本并增加吞吐量。StarkWare的dydx集成将用于数据完整性的STARK证明与链上数据可用性相结合，确保完全非保管协议。

- dydx为何选择StarkWare作为交叉保证金永续合约的Layer 2解决方案？

为了解决即时扩展问题，dydx的工程团队对各种Layer 2解决方案和其他主网进行了广泛的尽职调查。总的来说，StarkWare能够在最短的时间内为我们的用户提供迄今为止最好的交易体验。

和一般的Rollup不同，而dydx采用的则是被称为 StarkEx 的扩容方案。根据 Vitalik 的提议，这种方案被归类为 Validium。



vitalik.eth ✅
@VitalikButerin



@EliBenSasson suggests "validium" as a clearer name for plasma-with-snarks (aka zk rollup but with offchain data). That is:
[twitter.com/EliBenSasson/s...](https://twitter.com/EliBenSasson/status/126811111111111111)

	SNARKs/ STARKs	Fraud proofs
Data on-chain	ZK rollup	Optimistic rollup
Data off-chain	Validium	Plasma

Eli Ben-Sasson @EliBenSasson
Replying to @avihu28 and 5 others

Suggest *Validia* for this class of protocols, like plasma in having data offchain, like zk-rollups in being validity proofs. (Thanks, @VitalikButerin for Latin spelling help :-)

100 9:58 PM - Jun 1, 2020



30 people are talking about this



Validium 与 Rollup 最大的不同，便是扩容后交易数据的存储位置。Rollup 虽然包含了比主网更多的交易，但是所有交易的信息却以 Calldata 的方式保存在以太坊主网上，因此 Rollup 上的交易信息是可以通过以太坊被验证和恢复的。而 StarkEx 所采用的 Validium 机制，却选择将这些数据保存在链下。数据的链下存储和计算，给了 Validium 机制明显的成本与效率优势。既然不需要数据上链，自然就不会有 gas 成本，而链下计算又可以利用早已成熟的中心化服务器架构，这使得 Validium 可以为上层应用提供近乎于中心化交易平台的流畅使用体验。这便是使得 dYdX 的交易体验可以比肩中心化平台的关键原因。

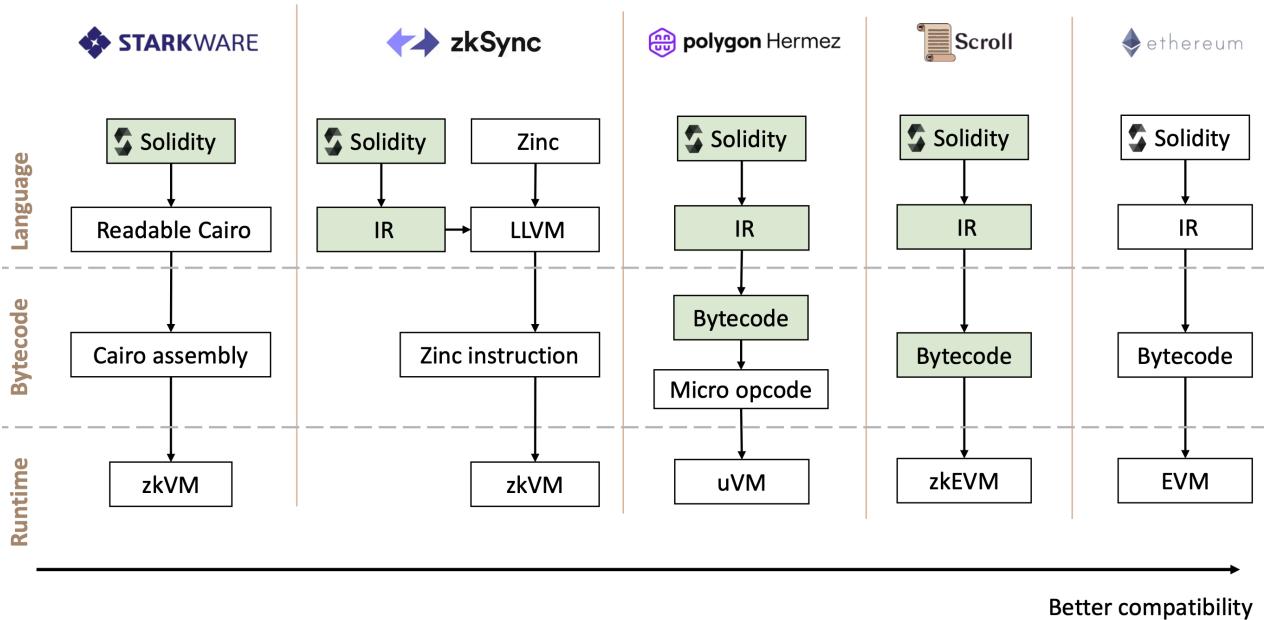
虽然目前dydx在去中心化衍生品赛道上一枝独秀，也基于ZK扩容尽力做到了高性能，但和那几家龙头CEX相比还有不少差距，这一切还是归因于性能不足。然后饿台风扩容方案存在一个天生的缺陷，就是如果扩容的项目方越来越多，以太坊主链还是会拥堵起来，其高额的GAS费最终还是会转嫁给这些扩容项目方的用户。这可能是dydx在其新版本中考虑抛弃ZK二层方案，离开以太坊转投Cosmos的一个重要原因。

总体来说，专用扩容方案特别适合将逻辑简单的合约证明化，为以太坊生态提供用户体验更好的二层应用，但同时缺点也比较明显：功能单一，可组合性不强，（至少目前）扩容始终存在理论上限等。此外，以目前的算力水平，证明生成延时比较大，不适用于某些特定应用场景。即便如此，我认为也不会被淘汰，而是成为下面的通用型的一种补充。

2.2 通用扩容方案

对比专用方案，通用型显然有更大的愿景，理论上来说，只要技术成熟，当前整个以太坊的内容都可以搬到通用二层上（不一定是某一个），而使得目前的以太坊一层只保留zk验证和共识。实际上以太坊基金会也确实在推动相关的进展。通用扩容方案的最佳代表应用是zkvm以及zkevm，即用ZK证明vm/evm的执行过程，从而实现一次编写，无缝迁移（至任意二层）。

和专用型扩容应用百花齐放一样，zkvm/evm应用也存在不同的技术方案：



Cairo和Stakware我们已经提过，这里看看另外两个重量级选手zkSync和Scroll。

2.2.1 zkSync的zkevm

zkSync FAQ Docs zkTools We're hiring M 📱 ⚡ 🌐 🌐

Rely on math, not validators

zkSync solves Ethereum scalability with zero security compromises

zkSync的 VM不是以太坊EVM1:1全兼容版本，而是旨在能够运行 99% 的用 Solidity 编写的合约并保持其相同的行为，例如在恢复和异常期间。同时，编写 zkEVM 以便在电路中高效地产生零知识证明。

zkSync将 PLONK 与自定义门和查找表（通常称为 UltraPLONK）和以太坊的 BN-254 曲线一起使用。自 2020 年 6 月以来，该证明系统已在 zkSync 1.0 以及使用相同证明系统的其他项目中进行了实战测试。

这里有一个重要的区别：电路和执行环境中的实现是分开的，用于不同的目的。生成执行跟踪的证明并提供见证是电路的工作，但这非常慢。另一方面，执行环境是 rust 中 zkEVM 的直接实现，高效且快速。如果我们要依靠电路来生成和执行证明，那么交易的最终确定性将需要数小时。证明生成和执行的分离使 zkSync 上的交易能够即时结算。

此外，zkSync计划将 zkEVM 和编译器结合在一起，并和递归证明结合起来：块之间的递归证明为N个块发布一个证明，块内的递归聚合块的不同逻辑部分的子证明。

2.2.2 Scroll

官网：<https://scroll.io/>

项目简介：Scroll Tech 旨在通过强壮的证明网络从而构建 EVM 兼容的 zk-Rollup。



A native zkEVM Layer 2 Solution for Ethereum

Scaling Ethereum with cutting-edge research and technology

项目目标：

1、Scroll 将构建一个完全兼容 EVM 的 zk-Rollup

通过一个简洁的证明来支持对以太坊区块的直接验证。基本思想是验证 EVM 执行跟踪中每个操作码的一致性和完整性。这样，L1 智能合约就可以无缝迁移到 Scroll。我们将反向构建，而不是使用新的 zk 友好原语——我们将使用自定义优化来支持原生 EVM。这给我们带来了巨大的优势，无需任何修改即可与所有现有的以太坊基础设施兼容！

2、Scroll 将启用和标准化第 2 层证明外包

我们设计了一个强大的外包机制，可以激励 Rollup 的 rollers 为 Scroll 生成零知识证明。Scroll 将对此类方案进行标准化，以适应更广泛的一般链下计算。这将打开一个新的证明市场。对开发者的另一个直接影响是他们可以在 Scroll 中部署复杂的合约，而无需考虑 gas 限制。许多新应用程序可以通过链上提交的证明在链下启用。Scroll 团队还构建了世界上最快的 GPU 和 ASIC 证明器来支持这一点。从长远来看，Scroll 计划实现完全去中心化并减少 MEV 的影响。

3、Scroll 将升级到新的证明系统

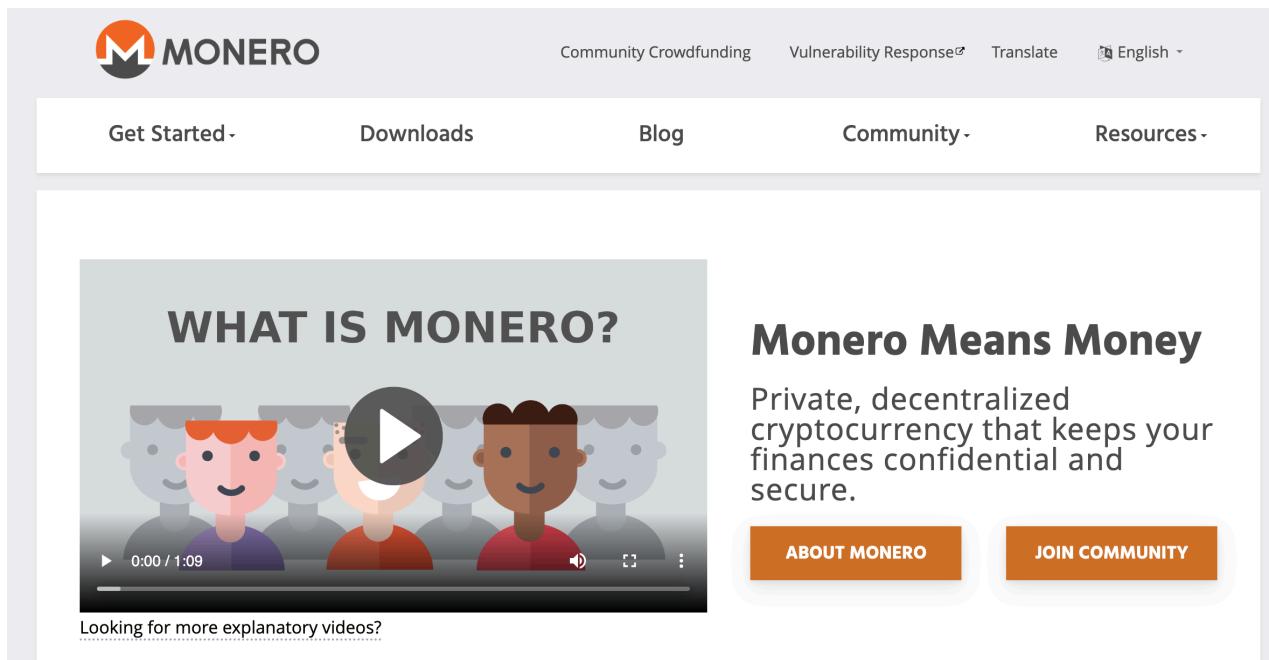
Scroll 将采用新的分层零知识证明系统。第一层将证明高效（定制电路优化和硬件高效证明算法）。第二层将是验证者高效的（简洁的证明和 EVM 友好的验证算法）。与所有现有解决方案相比，它有可能支持比 EVM 更大的程序和更多功能，如隐私。

总体来说，基于ZKEVM的通用型方案是未来ZK应用的一个热门方向，优点很多，但缺点也很明显，通用性必然带来工程上的复杂性，无论是实现，调试，还是审计都是难点，目前zkEVM还没有一个广泛应用的版本。

3. 隐私类ZK应用

目前，ZK发展的另外一个热门方向是隐私保护，提到隐私保护就不得不提到下面几个重量级的应用。

3.1 monero



The screenshot shows the official Monero website. At the top, there's a navigation bar with links for 'Community Crowdfunding', 'Vulnerability Response', 'Translate', and language selection ('English'). Below the navigation is a main menu with 'Get Started', 'Downloads', 'Blog', 'Community', and 'Resources'. The central feature is a large video player titled 'WHAT IS MONERO?'. The video thumbnail shows four stylized human figures. Below the video player is the text 'Looking for more explanatory videos?'. To the right of the video, the tagline 'Monero Means Money' is displayed, followed by the description 'Private, decentralized cryptocurrency that keeps your finances confidential and secure.' There are two orange buttons: 'ABOUT MONERO' and 'JOIN COMMUNITY'.

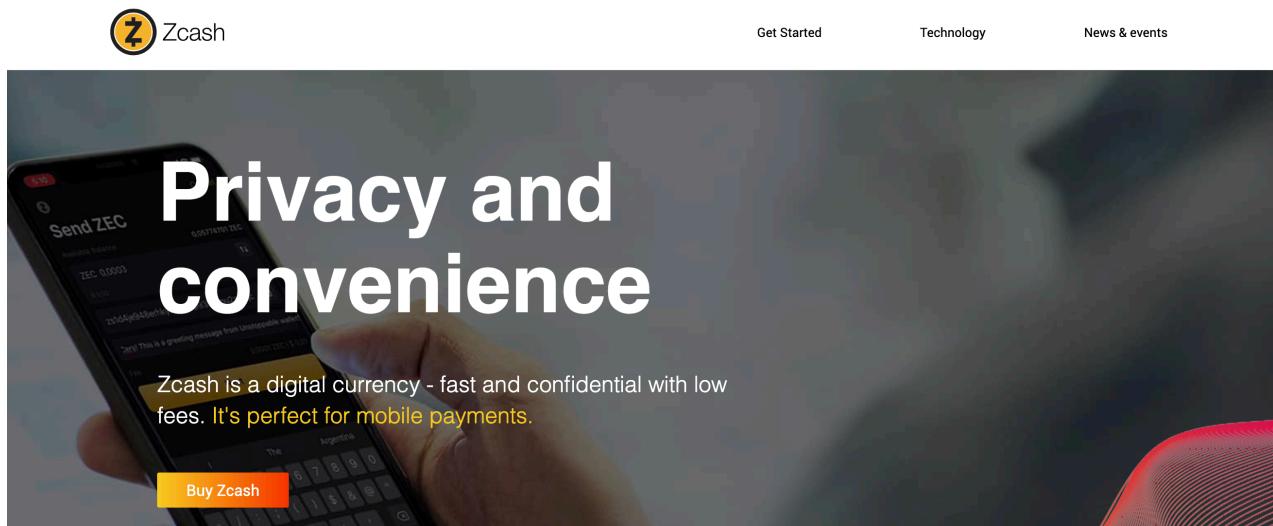
门罗的创立早在ZK概念成为热门话题之前。门罗币使用加密技术来隐藏发送和接收地址以及交易金额，正如门罗官网所宣称的那样：

- 门罗币是加密货币匿名和抗审查领域中的先锋。当下存在的大多数加密货币都拥有透明可查询的区块链，包括比特币和以太坊，这意味着世界上的任何人都可以查看任何一笔交易。而币的地址可以和实体世界的个人关联起来。
- 门罗币的交易是保密且无法被追踪的。每个门罗币的交易都默认必须是混淆交易地址和金额的。让所有人必须保持匿名意味着每一个门罗币用户的活动都会增强其他所有人的隐私。这和其他可选匿名的加密货币在匿名效果上有着本质上的不同（比如ZEC）。门罗币具有可互换性。因为交易互相混淆且保密，任何特定的几个门罗币不会因为过去的历史记录而受到针对性的追踪。这也意味着门罗始终具有抗审查性。

门罗和其他系统的主要区别在于ZK协议的选择，和常见的zkSNARK或者zkSTARK不同，门罗采用的是bulletproof。其不需要可行设置。如下图所示：

Comparing Proof Systems				
Proof System	Σ -Protocol	SNARKs	STARKs/CS-Proofs	Bulletproofs
Proof Size	Long	Short	Shortish	Short
Prover	Linear	FFT	FFT (Big memory req.)	Linear
Verifier	Linear	Efficient	Efficient	Linear
Trusted Setup	No	Required	No	No
Practical	Yes	Yes	Not Quite	Yes
Assumptions	Discrete-Log	Non-falsifiable	OWF (Quantum secure)	Discrete-Log

3.2 Zcash



Zcash可能是最著名的隐私项目，其在挖矿记帐以及产生交易上的机制与比特币类似，不同的是在Zcash上有公开(Unshielded)或是私人(Shielded)两种帐户类型，公开帐户跟私人帐户可以互相交易，但私人帐户的付款、收款的金额地址都不会揭露在区块链上，通过zk-SNARKs (Non-interactive zero-knowledge proof – 非交互式零知识证明)，Zcash让矿工在验证记帐的当下可以确认用户没有凭空伪造代币。

The top screenshot shows a BTC transaction details page. The transaction ID is dbf8355dade08bac60b6c3b20736ee8d182b7e9c8e4a6828ca6e9deb71b8ea2c. It has 1 Satoshi/vByte, 0.00001204 BTC, and was created on 2018-10-30 08:12:15. There are five outputs listed, each with a different address and value (10.00000000). The bottom part of this screenshot shows the 'BTC' logo.

The bottom screenshot shows a ZEC transaction details page. The transaction ID is f0c3d0382f... and it was created on Tue 30 Oct 2018 11:15:19 HKT. It is categorized under 'Value Transfer'. The transaction shows a 'JoinSplits' process where two inputs (Transparent 20.01421649 ZEC + Shielded ? ZEC) are combined into one output (Transparent 0 ZEC + Shielded ? ZEC). The inputs are listed as t1RwbKka1CnktvAJ1cSqdn7c6PXWG4tZqgd (10.00000001 ZEC) and t1RwbKka1CnktvAJ1cSqdn7c6PXWG4tZqgd (10.01431648 ZEC). The output is listed as Outputs (0). A red box highlights the 'Outputs (0)' section. At the bottom right, there is a watermark for '知乎 @忘川百科'.

由于ZEC继承了BTC的UTXO数据结构，因此两者交易展现方式非常接近。上图是一笔BTC转账的典型过程，付款地址，收款地址，转账金额被展现的一清二楚。而下图中采用了匿名转账的ZEC转账过程，却什么信息都没有，金额，收款人都是空白。这笔交易已经被确认有效，但外界永远无法得知其中的细节，这就是采用了“零知识证明”的匿名交易。

由于私人帐户交易细节都被隐藏，这时收款人需要借助于查询私钥(View Key)才能查看到交易细节。转出帐户的持有者可以分享查询私钥给收款人，收款人就可以使用查询私钥看到特定交易，借此确认代币真的来自于付款方。

Zcash不仅仅是一个重量级的隐私转账项目，同时还有一个对密码学开发者社区非常有意义的贡献：Zcash开发并且开源了了一套可用的ZK密码学库--Halo/Halo2。如同Zcash的官方博客所宣称的那样：“两个月后，我们宣布了一个名为Halo的密码学库。自从向世界宣布以来，Halo已被公认为是一项突破，不仅适用于加密货币，而且适用于整个应用密码学领域。它是在后续科学工作的基础上建立和扩展的：[BCMS2020] [BDFG2020] [BCLMS2020]。”

“我认为Halo之所以有价值有两个原因。首先，它有一些重要的直接好处。它消除了可信设置，彻底消除了许多人对ZK-SNARK技术的疑虑的根源。

“但其次，更重要的是，它将Zcash转移到了一个从根本上更具适应性和对未来友好的密码学堆栈，这将在未来几年甚至几十年内受益。其他项目已经在探索或迁移到PLONK、Halo或其他基于多项式的技术，以避免需要特定于应用程序的可信设置，Zcash将受益于能够利用该生态系统而不是停留在越来越过时的技术中。

“Halo的‘增量可验证计算’性质为未来的升级奠定了基础，这些升级使用Halo的聚合功能来组合块内甚至块之间的证明，从而大大降低验证成本并为Zcash拥有Mina的长期理想铺平道路-类似“自我验证”的属性。Halo的适应性也为Zcash与以太坊和其他区块链接口打开了大门，允许第2层协议轻松地在它们之间移动。所以我认为Zcash结合Halo有很多优势，这是一个很好的升级，可以与其他出色的工作并行进行，以便更容易在UX层使用隐私保护交易。”

Vitalik Buterin, 以太坊联合创始人和Zcash社区成员

“Halo是Zcash向前迈出的一大步。没有可信设置的零知识系统将确保每个人都可以使用隐私和未来的可扩展性！”

Zaki Manian, Cosmos联合创始人和Zcash社区成员

目前很多正在开发的ZK项目都受益于Halo2，比如刚刚提到的zkEVM。

3.3 Aleo

The screenshot shows the Aleo homepage. At the top, there's a dark header with the Aleo logo, navigation links for 'For Developers', 'Blog', and 'Opportunities', and social media icons for Twitter, GitHub, and LinkedIn, along with a 'Subscribe' button. Below the header is a blue banner with the text 'Welcome to Aleo. Discover the first platform for private applications.' and a 'Learn More' button. The main content area has a black background with white text. It features the tagline 'Zero-Knowledge is Finally Here.' followed by a large, bold, white text block: 'Where Applications Become Private.'. Below this, there's a smaller white text block: 'Modular and compliant. The ultimate toolkit for building private applications is finally here.'

Aleo正在构建一个集成零知识证明的网络，这是一种让平台变得可扩展、私有和可互操作的加密技术。Aleo区块链——基于一种新颖的共识协议——旨在通过利用零知识(ZK)证明比传统模型更快、更高效。ZK是一种加密技术，可让两方在不共享基础数据的情况下相互验证信息。结果是隐私以及链下计算的独特可扩展性优势。

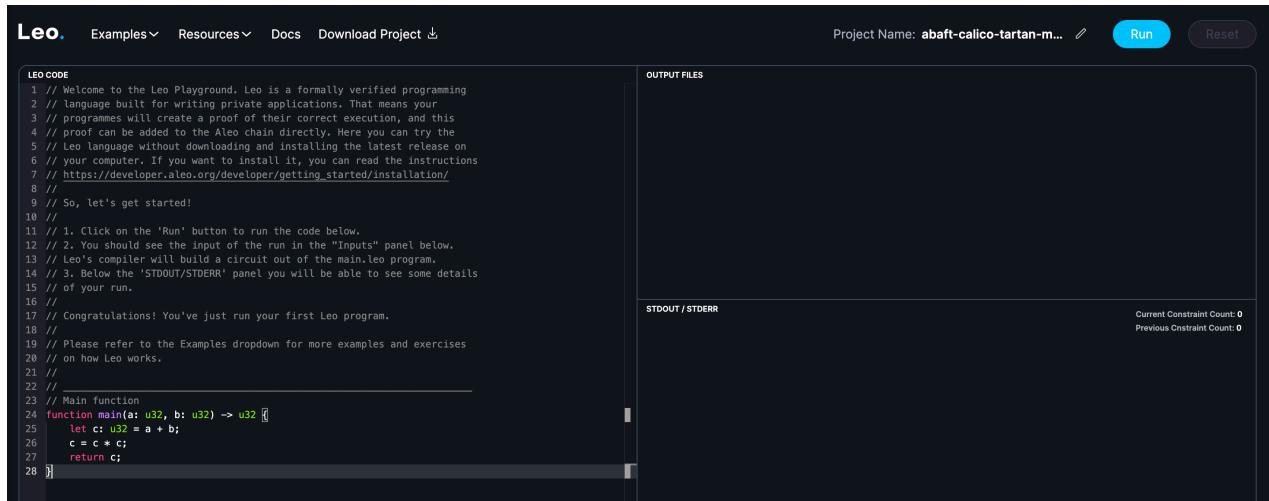
完全透明和对可扩展性的限制阻碍了区块链应用程序的发展，并强调了对统一、无许可和私有解决方案的需求。

Aleo 解决方案的基石是 zkCloud，其中包括 snarkOS 区块链和 snarkVM，这是一个用于大规模处理交易的链下私有环境。Aleo 区块链 snarkOS 是一个去中心化网络，由运行新颖的简洁工作证明共识协议的节点组成。

snarkOS 的目的是维护状态——保护分散网络中的数据——并验证代表状态转换/交易的证明。去中心化网络使任何人都可以以无需许可的方式部署部署在 snarkOS 上的应用程序或智能合约或与之交互。

Aleo 执行模型的加密核心是 snarkVM。与以太坊虚拟机不同，snarkVM 使客户端能够在链下运行计算，仅发布链上计算的证明。此模型可实现更高的可扩展性和无限的应用程序运行时间。

为了帮助开发人员编写私有应用程序，Aleo 创建了一种名为 Leo 的编程语言。它的外观和感觉就像一门传统的编程语言，其语法抽象了低级密码学，使在 ZK 中表达逻辑变得简单直观。Leo 编译器是第一个经过正式验证的 ZK 证明编译器。此外，Leo 语言受到 JavaScript、Scala 和 Rust 等编程语言的影响，非常强调可读性和易用性。可以去 leo-playground](<https://play.leo-lang.org/>)体验一下。



The screenshot shows the Leo playground interface. On the left, there is a code editor window titled "LEO CODE" containing the following Leo code:

```
// Welcome to the Leo Playground. Leo is a formally verified programming
// language built for writing private applications. That means your
// programmes will create a proof of their correct execution, and this
// proof can be added to the Aleo chain directly. Here you can try the
// Leo language without downloading and installing the latest release on
// your computer. If you want to install it, you can read the instructions
// at https://developer.aleo.org/developer/getting_started/installation/
//
// So, let's get started!
//
// 1. Click on the 'Run' button to run the code below.
// 2. You should see the input of the run in the "Inputs" panel below.
// 3. Leo's compiler will build a circuit out of the main.leo program.
// 4. Below the "STDOUT/STDERR" panel you will be able to see some details
// of your run.
//
// Congratulations! You've just run your first Leo program.
//
// Please refer to the Examples dropdown for more examples and exercises
// on how Leo works.
//
// Main function
function main(a: u32, b: u32) -> u32 {
    let c: u32 = a + b;
    c = c * c;
    return c;
}
```

On the right, there is an "OUTPUT FILES" panel and a "STDOUT / STDERR" panel. The "STDOUT / STDERR" panel shows the output of the run, which is currently empty.

3.4 非公链应用tornadoCash/zk.money

因为他们都没有自己的公链，严格来说他们更接近上面的专用扩容方案，其专用领域是隐私转账，而不像前面提到的扩容项目大多应用于透明非隐私的交易或者支付。

3.4.1 tornado.cash

Tornado.Cash 使用零知识简洁的非互动知识论证(也称为zk-SNARK)，以验证和允许交易。

每处理一笔存款，Tornado Cash生成一个随机的字节区域，通过Pederson哈希（因为它与zk-SNARK更友好）计算，然后将代币和20 mimc哈希发送到智能合约。然后合同将把它插入到Merkle树中。

为了处理提款，相同区域的字节被分成两个独立的部分：一边是**secret**，另一边是**nullifier**。这个 nullifier 是链上发送的公共输入，用于用智能合约和 Merkle 树数据进行检查，所以避免了双重支付。

基于zk-SNARK，可以在不透露任何信息的情况下证明20 mimc哈希的初始承诺和nullifier。即使nullifier是公开的，隐私性也会得到维护，因为没有办法将散列的nullifier关联到初始承诺。此外，即使交易的信息存在于Merkle根中，关于确切的Merkle路径的信息，即交易的位置，仍然是保密的。

3.4.2 zk.money

zk.money是基于Aztec网络构建的第2层隐私应用程序。以太坊用户可以使用它来屏蔽Token信息并保护其交易数据不受公众的攻击。屏蔽Token意味着将其置于zkSNARK（零知识证明密码学）外壳下，以保护用户的隐私。发送和接收Token是匿名的，不会公开发布任何交易数据。



zk-money由Aztec提供支持。当前版本的Aztec L2 Rollup技术由Aztec作为中心化汇总服务商运行，后续将有更多的汇总服务商加入。届时系统将被分散成去中心化模式。当前，用户依靠Aztec来将汇总交易中继到链中。万一Aztec突然消失，有一种紧急模式允许用户直接从合同中从系统中提取资金。

值得一提的是Aztec也是ZK领域的一位重量级选手，目前非常流行的Plonk框架最初就是来自Aztec。

3.5 隐私计算类ZK应用Rosetta

目前实现隐私计算的途径可以分为密码学、联邦学习和硬件可信执行环境（TEE）等几大类。而其中以密码学理论为基础的 MPC（Multi-Party Computation，安全多方计算）是最有安全保障的技术路线，其秉持的基本理念是信任计算复杂度理论、代码，而不是信任人、硬件，而联邦学习和 TEE 目前还很难讲清楚安全性，经常被发现新的安全漏洞。并且，联邦学习中核心部分也往往需要使用同态加密等密码学手段进行强安全性的保障。从工程技术的角度上看，联邦学习是分布式机器学习技术的延伸，主要的挑战是训练过程中如何进行多异构终端的同步更新等 [1]，很多传统分布式系统开发经验仍然适用。而以 MPC 为代表的密码学途径则带来了一些全新的挑战。

其中最核心的困难是，密码学属于计算机理论领域，很多概念、算法协议都需要有长期的专业知识积累才能理解，而业务落地中的典型 AI 方向，无论是计算机视觉、文本挖掘还是用户行为建模等都更加面向实际场景。**如何打通以密码学为典型代表的隐私保护技术与 AI 技术之间的壁垒？**这是开发者在实际构建一个通用的、易用的隐私计算框架时需要解决的核心问题。围绕着这个核心问题，又有一系列具体的工程技术挑战：

- **如何实现系统的易用性？**AI 开发者不会愿意，也不应该为了在业务中引入数据隐私保护能力而费时耗力地学习各种复杂、抽象的密码算法。一个好的隐私 AI 框架应该是易上手的，便于 AI 开发者使用自己熟悉的方式快速解决自己的数据隐私问题。
- **如何实现系统的高效执行？**这包括单机和多机两个层面。密码学的计算大部分都是在大随机数的密文上进行，为此常常需要使用专用的硬件指令、SIMD（Single Instruction/Multiple Data）等技术来进行单机并行化的加速，这些优化实现需要对于密码学基础库有深入的了解，并往往需要根据协议算法做进一步的并行优化。而在多机层面上，则需要考虑如何和很多 AI 框架自身的并行优化技术兼容。
- **如何实现 MPC 多方之间的高效通信？**在 MPC 中，多方之间需要进行大量的同步通信，而且信道上的内容大都是无规律的、不可压缩的一次性使用的随机数，这就需要在保证安全性的同时，根据具体的计算逻辑进行很多工程优化以减少通信量和通信次数。
- **如何保障隐私保护技术的可扩展性？**MPC 等隐私计算技术还在不断发展之中，也是学术研究上的热点问题，所以一个好的隐私 AI 框架，需要能够支持研究者简单快速地将新的算法协议集成进

来。

针对这些问题，业界已经有一些探索，比如[Rosetta](#)。



Rosetta 是一个基于[TensorFlow](#)开发的隐私计算框架，它将陆续集成密码学、联邦学习和可信执行环境等主流的隐私计算技术。Rosetta 旨在为人工智能快速提供隐私保护技术解决方案，不需要用户掌握任何密码学、联邦学习和硬件安全执行环境领域的专业知识。Rosetta 在用户接口层复用了 TensorFlow 的对外 API 从而使得用户可以以最低的改造成本将隐私保护功能集成到现有的 TensorFlow 程序中。在简单场景下，只需添加如下一行代码就可以完成这样的转换：

```
import latticex.rosetta
```

当前版本集成了3方参与的安全多方计算（MPC）协议。当前使用的默认底层协议是[SecureNN](#) 和自研的 Helix 协议。这些协议可以在诚实者占多数的半诚实安全模型假设下保障数据安全。

Rosetta 还集成了一个高效的零知识证明协议 [Mystique] (<https://eprint.iacr.org/2021/730>)，用于复杂机器学习模型预测阶段的相关安全证明，例如 ResNet。关于其使用请参考 [示例说明](#).

3.6 其他隐私项目

比如隐私身份等，Oxparc 和 polygon 似乎有这方面的尝试，比如这片[blog](#)文章提到的

ZK Identity: Why and How (Part 1)

Last month, we kicked off the OxFARC ZK-Identity Working Group: a working group experimenting with zkSNARKs to build digital identity tools. This post is the first in a series on why advances in cryptography will be important for enabling new identity primitives. This first post covers the “Why”; future posts will cover the “How.”

以及[polygon-id](#)这篇文章提到的一种web3 身份识别方案：

A look at Polygon ID, a new zk-proof based Web3 identity solution

Polygon's unique identity service is tailored to address KYC concerns in the Web3 space.



Andjela Radmilac [Twitter](#) [LinkedIn](#) [Email](#)

Mar. 31, 2022 at 8:30 am UTC

3 min read

Updated: March 31, 2022 at 4:04 am

4. 其他类

扩容和隐私以外的其他类别，

4.1 数据压缩公链代表Mina

Mina是什么：使用zk-SNARK技术，将区块大小压缩在kb级别的轻量化区块链。

The screenshot shows the Mina Foundation website. At the top, there is a navigation bar with links to Docs, About, Tech, Get Started, Community, and Blog. To the right of the navigation is a red button with the text "SIGN UP FOR NEWSLETTER" and a white "M" icon. Below the navigation, there is a large, colorful background image with a rainbow gradient and a central sunburst effect. On the left side of the image, the word "LEARN" is written in white capital letters. In the bottom-left corner of the image, there is a white rectangular overlay containing the text "2021-03-12 / MINA FOUNDATION" at the top, followed by "22kB-Sized Blockchain – A Technical Reference" in a large, bold, black font. At the bottom right of the image, the word "TAGS" is followed by "/ ZERO KNOWLEDGE".

对传统区块链来说，整个账本中的历史交易记录数据量非常大，因为每个区块中都存了当时发生的某些交易，再进行堆叠数据量可想而知。使用zk-SNARK,只需要把每个区块中的交易做一次证明：“这些交易是正确的”，然后在区块中仅存入这个证明即可。

传统区块链：存入所有的交易记录



压缩区块链：存入“所有交易记录都是对的”的证明

这样就实现了一种效果：区块链上储存的全都是交易正确性的证明，而非交易本身。因为前面说到的这种证明占用空间很小，因此区块的大小得以被压缩。

Mina的创新：递归使用zk-SNARK，将区块的总大小保持在恒定的kb量级

如果按照上述做法，为每个区块创建一个SNARK，每个区块的确实是变小了。但是随着时间的推移，SNARK也会堆积起来，100个包含SNARK的区块，会导致区块链整体又变大了100倍。因此单纯的压缩一个区块的大小还是治标不治本的，为了从根源上压缩整个区块链的大小，Mina创新性的对zk-SNARK进行了“递归”使用，即对于当前任意一个最新的区块来说，只需要一个最新的证明即可验证过往信息全部的正确性，而这个最新的证明仅仅需要21kb左右：1kb的SNARK证明 + 20kb的过往交易路径摘要，这就保证了对于任意时间点来说，Mina区块链上只保存了当前正确状态的更新，而没有像比特币和以太坊的区块链那样保存大量的交易原始数据。由此看出，Mina通过递归使用zk-SNARK,达到了一举两得的效果。

整体来看，Mina主打轻量化和隐私计算，作为一个底层区块链来说，这2点足够有差异化，其背后也有过硬的技术团队和强劲的资方支撑。因此Mina会有自己的发展赛道，短时间来看还没有其他能与其功能类似的公链。但目前功能比较单一，据我所知目前只有转账功能，如何真正的拓展更多的应用场景，将与其他公链合作的特性真正落地，是目前摆在Mina面前的重要问题。

4.2 数据存储代表Filecon

Filecoin使用ZK验证存储过程，利用的还是ZK简洁性的特点。

对于要在Filecoin上验证的存储，涉及两个证明：**复制证明(PoRep)**和**时空证明(PoSt)**。

在 PoRep 中，存储提供商证明他们正在存储一段数据或信息的唯一副本。PoRep 只发生一次，即客户端和提供者之间的初始存储交易发生、并且数据首次由矿工存储时。每个上链的 PoRep 都包含 10 个单独的 SNARK，它们共同证明该过程是通过概率挑战正确完成的。

另一方面，PoSt 用于证明存储提供商会随着时间的推移继续存储原始数据，在这期间没有被操纵或损坏。当存储提供商首次同意为客户存储数据时，他们必须以 FIL 作为抵押品。如果在协议期间的任何时候，提供者未能证明 PoSt，他们将受到处罚，并且可能会失去所有或部分 FIL 抵押品。

如果没有使这些证明变得小而高效的解决方案，它们将占用大量的网络带宽，并为存储提供商和矿工带来高昂的运营成本。现在，存储提供商使用zk-SNARKs生成证明来降低成本，它生成的证明数据包很小，验证过程也非常快。

通常需要数百KB来验证的证明可以使用zk-SNARK压缩到仅192字节。如上所述，每个PoRep 包含10个SNARK，即每个1920字节（ 10×192 字节）。这样一来，就能保证Filecoin一直维持30秒的出块时间。

zk-SNARKs是在Filecoin主网上线以来就在使用的的重要工具，它已经构成了Filecoin网络的一部分，并对未来高效、经济、安全的网络发展起着至关重要的作用。它改变了Filecoin网络的游戏规则，将验证过程大幅减少，同时保证了用户对Filecoin网络的信任。

5. ZK生态相关应用

这一类本质上并不是ZK应用，而是属于整个ZK生态的一部分，包括开发者社区，各种开发工具，以及教育，他们并不直接应用ZK，但是有了他们，ZK的未来才更加丰富多彩。

5.1 ZK领域特定语言

除了前面提到的Cairo, leo，常见的ZK相关的DSL领域特定语言还有Circom, Zinc等。

5.1.1 Circom

[Circom](#)是一种新颖的特定领域语言，用于定义可用于生成零知识证明的算术电路。[Circom compiler](#)是一个用 Rust 编写的 circom 语言编译器，可用于生成具有一组关联约束的 R1CS 文件和一个程序（用 C++ 或 WebAssembly 编写），以有效地计算对电路所有线路的有效分配。其主要特点之一 [circom](#) 是其模块化，允许程序员定义称为模板的可参数化电路，可以将其实例化以形成更大的电路。从小的单个组件构建电路的想法使得测试、审查、审计或正式验证大型复杂 [circom](#) 电路变得更加容易。在这方面，[circom](#) 用户可以创建自己的自定义模板或从[circomLib](#)实例化模板，circomLib是一个公开可用的库，包含数百个电路，例如比较器、散列函数、数字签名、二进制和十进制转换器等等。Circomlib 对从业人员和开发人员公开可用。

证明系统的实现也可以在我们的库中找到，包括[snarkjs](#)，用 Javascript 和 Pure Web Assembly 编写，[wamsnark](#)用原生 Web Assembly 编写，[rapidSnark](#)用 C++ 和 Intel Assembly 编写。

Circom 旨在为开发人员提供一个整体框架，通过易于使用的接口和抽象证明机制的复杂性来构建算术电路。

5.1.2 Zinc

来自Matter-lab的[zinc](#)是在 zkSync 平台上开发智能合约和 SNARK 电路的新兴框架。

现有的 ZKP 框架缺乏特定于智能合约的功能。由于智能合约处理有价值的金融资产，因此安全性和安全性至关重要。这就是为什么现代智能合约语言（如 Simplicity 或 Libra's Move）的设计者更倾向于代码的安全性和形式可验证性而不是表达性。

Zinc 旨在通过提供一种简单、可靠的智能合约语言来填补这两个世界之间的空白，该语言针对 ZKP 电路进行了优化，并且易于开发人员学习。

该框架包括一个简单的、图灵完备的、以安全为中心的通用语言，专为开发智能合约和零知识证明电路而设计，学习曲线平坦。语法和语义紧跟Rust.

Zinc 编译器使用 LLVM 作为其中端和后端，为代码优化提供了一套强大的解决方案。

目前matter-lab由于路线图调整暂时暂停了zinc的工作，但未来会恢复，正如官方文档提到的那样：

We are currently fully focused on a [Solidity-first approach](#). We will resume work on Zinc after Solidity is released!

5.2 竞赛及教育方向

5.2.1 竞赛类：zprize.io, zkhacks, etc

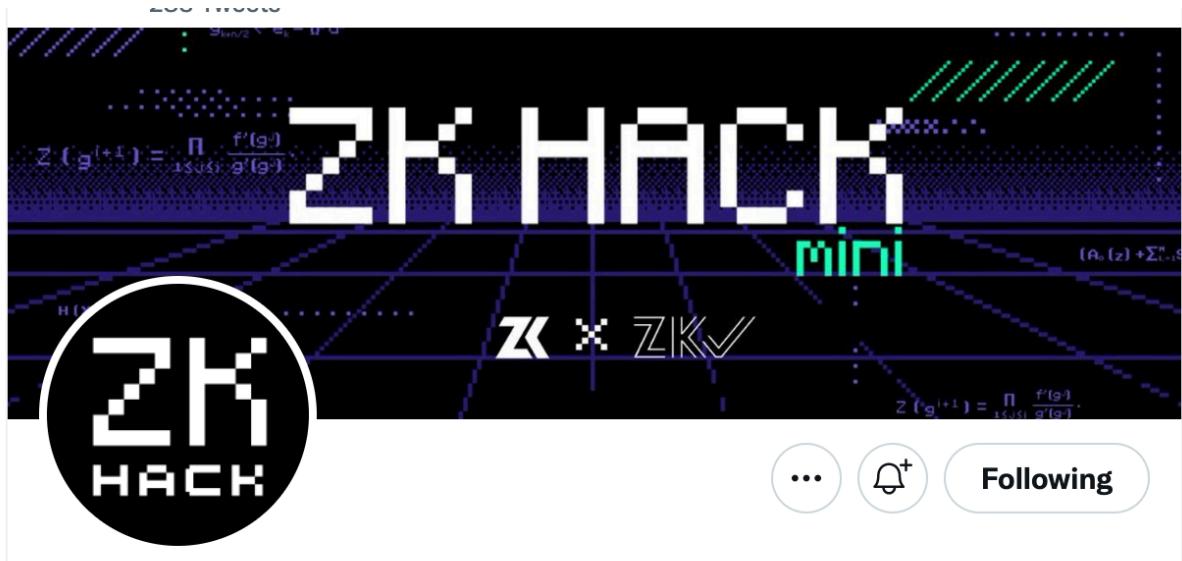
- [zprize.io](#)



零知识密码学是一项开创性的新技术，可为 Web 3.0 协议和应用程序提供隐私、互操作性和可扩展性。zprize 与其他的 XPrize 一样，选定的团队将争夺跨越一系列类别的金钱奖励。目前已经累积了超过 700 万美元的奖金，以及来自赞助项目的代币赠款。

所有获奖作品都将成为开源库，以造福所有人。zprize希望这个基础能够支持下一代去中心化协议和应用程序，从而为下一代网络提供安全、可互操作和可扩展的应用程序。

- [zkhack](#)



ZK Hack

@_zkhack_

Workshops, puzzles, videos and zero knowledge events, hosted by [@zkvalidator](#) and [@zeroknowledgefm](#) join our discord - discord.gg/tHXyEbEqVN

[🔗](https://zkhack.dev/mini.html) zkhack.dev/mini.html [Joined September 2021](#)

ZK HACK 是一个互联网上专注于ZK进展的社区! 他们举办业界研讨会，高水平竞赛，学术讨论会以及公开课，是一个非常有意思的ZK推动团体。目前ZK Hack已经举办了多届竞赛，但限于水平，我一个都没有参加，只能看看题解：）

5.2.2 教育类：Lattice, OXParc, etc

为了进一步繁荣生态，一些ZK研究机构/项目方同时会举办面向开发者（爱好者）的培训，公开课，讲座等等，类似的项目方有[Lattice Foundation](#), [Oxparc](#)等等。以Oxparc为例：

OxPARC 基金会促进以太坊和其他去中心化平台上的应用级创新。我们主要关注的领域是：

- **研究与开发。**我们支持使用新技术的实验性去中心化应用程序，例如零知识密码学。OxPARC 项目旨在突破区块链应用在技术上的可能性。
- **开源工具和基础设施。**新的应用程序设计模式需要新的工具和基础设施。我们鼓励根据开放的生态系统价值开发这些工具。
- **教育和生态系统发展。**我们的目标是将更多的开发人员、技术人员、作家和思想家带到去中心化应用程序开发的前沿。我们通过教育计划和其他社区倡议来做到这一点。

我们资助、提供运营支持或以其他方式参与的项目包括[Dark Forest](<https://blog.zkga.me/>)、[EthUniversity](<https://www.ethuniversity.org/>)、[Reboot](<https://reboothq.substack.com/>)、[Project Sophon](<https://github.com/projectsophon>)等。

就在刚刚过去的6月份，Oxparc才举办过一次培训班，参见[halo2 learning group](#)。

5.3 ZK硬件加速方案

我们已经看到了很多ZK软件方案，但是目前ZKP还是比较慢，如何让它们变快？采用硬件方案显然是最直接的一种！

事实上，根据不同的ZKP证明系统，证明的生成过程可能有所不同，但瓶颈实际上存在共性，即：

1. 大数向量的乘法，特别是变基和定基多标度乘法（以下简称 MSM）
2. 快速傅里叶变换（以下简称 FFT）和反 FFT（尽管有无 FFT 证明系统的技术）。

简单来说：

1. MSM 的内存访问需求是可预测的，可以实现大量的并行化，但由于原始的计算量和内存需求非常大，其成本仍然很高。
2. FFT 的内存访问是随机的，这一点对硬件并不友好，而且自然很难在分布式基础设施上运行。

问题是能够同时优化 MSM 和 FFT 算法并让 ZKP 生成效率大幅提升的硬件是什么样的呢？此外，各种加速技术可以在多种硬件技术上实现：GPU、FPGA 或 ASIC。但是哪一个是最好的选择？要回答这个问题，我们首先必须承认 ZKP 仍处于早期发展阶段。系统参数（例如 FFT 宽度或元素的位大小）或证明系统的选择仍然很少有标准化。

由于这些因素，FPGA 有两个核心特性使其在 ZK 环境中优于 ASIC：

- “多次写入”与“一次写入”：ASIC 上的业务逻辑是一次写入。如果任何 ZKP 逻辑发生变化，您需要从头开始。FPGA 可以在 1 秒内重新刷新任意次数，这意味着它们可以在具有不兼容证明系统的多个链上重复使用相同的硬件（例如，因为他们想要跨链提取 MEV），并灵活地适应 ZK “元”的变化。
- **更健康的供应链：**ASIC 设计、制造和部署通常需要 12 到 18 个月或更长时间。相反，FPGA 供应链是健康的，像[赛灵思](#)这样的领先供应商允许从网站（即没有任何联系点）在[16周内](#)到达的大量零售订单。这允许以 FPGA 为中心的运营对其产品有更紧密的反馈循环，并通过购买和部署更多 FPGA 来扩大其运营。

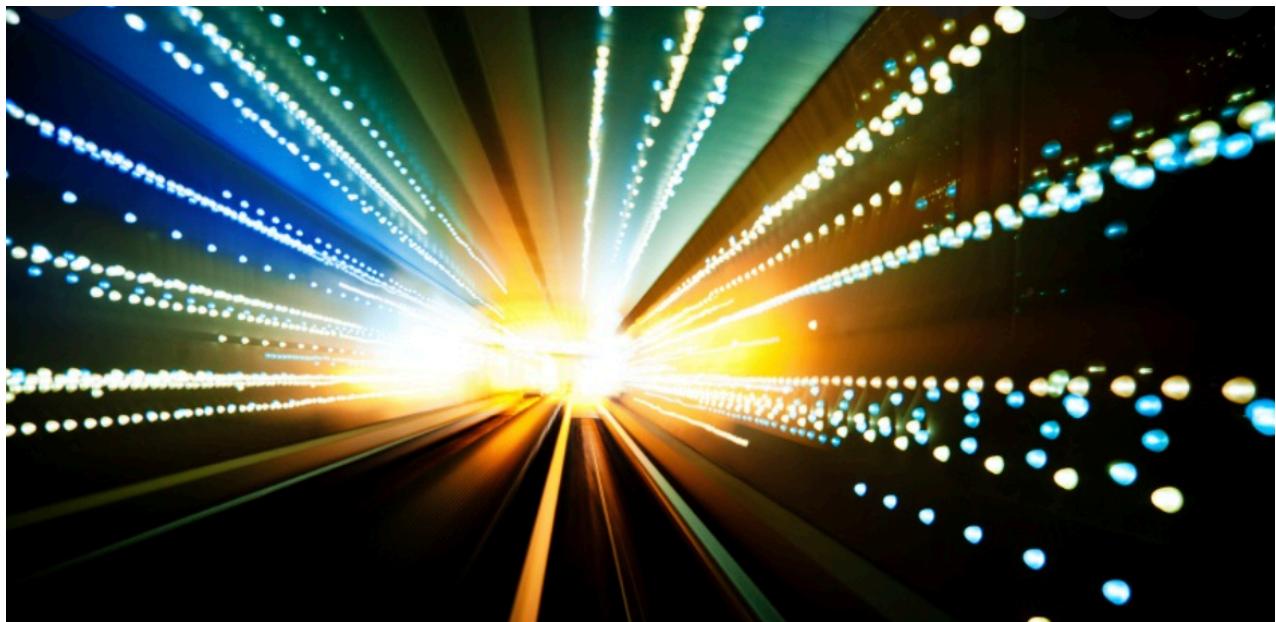
我们还期望 FPGA 的性能优于 GPU，原因与它们在机器学习和计算机视觉领域蓬勃发展的原因类似：

- **硬件成本：**一流的 FPGA（领先的处理节点、时钟速度、能效和内存带宽）比一流的 GPU 便宜约 3 倍。全球对 GPU 的需求进一步加剧了这一问题。
- **电源效率：**FPGA 的能效比 GPU 高[10倍以上](#)，[其中一个重要原因是需要将 GPU 连接到主机设备，这通常会消耗大量电力。](#)

鉴于上述情况，[有些研究人员](#)预计市场上的赢家将是专注于 FPGA 而非 ASIC 或 GPU 的公司。然而，如果只有一个或几个 ZK L1 或 L2 最终实现了主导规模，并且 ZK 证明系统稳定在单个实现附近，那么 ASIC 胜过 FPGA 的可能性可能会更高。但是，如果这种情况真的发生的话，我们可能还需要几年的时间。

6. 总结

ZK是区块链世界的一个重要研究方向，随着ZK技术研究的深入，我们应该会看到更快的硬件，更安全，高效的算法，以及更有想象力的应用方案。



7. 参考文献

本文资料全部来源于网络，主要包括项目方官网，密码学研究人员的博客，技术介绍文章等。