L1总链上的隐私智能合约：关心隐私的zcash、Horizon、Aleo和铁鱼

龙卷风现金

L2:关心隐私的阿兹特克

。

ZKP的另一个主要用例是在底部L1上生成汇总有效性证书。一般的Rollup分辨率不使用ZKP的隐私特性，这样可以优化吞吐量，也就是可以证明更多的TX。在这种权衡中。ZKP只是用来证明L2交易的准确性。

由于一些通用函数不能被有效证明，所以生成ZKP来证明任意智能合约的准确实现是非常困难的。处理这种效果需要一个特殊的虚拟机。这些虚拟机可以有效地阻止使用底层ZK电路的文本研究。由于这种混乱，ZK-罗博最终只支持取数或单个应用程序序列，例如，它可以在一个混乱中生成ZKP的DEX。。这里的例子包括ZKSync 1.0和Loopring。之后，通用zkEVM完成并投放到通常的市场，包括Starknet、zk Sync2.0、PolygonzkEVM和Scroll。。目前，所有的ZK卷都在以太坊，但有些可以在包括比特币在内的其他链上完成ZK卷。但是，比特币汇总的实现将需要更改比特币操作码和硬分叉链。这在比特币社区普遍不受欢迎。

除了关注隐私的应用序列和汇总，我们还在其他区块链协议中发现了其他应用序列。本节将介绍这些用例。米纳

米娜使用ZKP将区块链的形状缩小到非常小的尺寸(~22KB)。为了做到这一点，米娜使用递归ZKP，也就是其他ZKP的ZKP。当在Mina网络中产生块时ZK-斯纳克被用来生成该块的证明，以确保其有效性。当新块引用前一个块时，新块的ZKP将验证所有前一个块，并坚持大小不变。

档案币

Filecoin使用ZKP来确保存管提供商准确存储他们声称要存储的数据。这个过程被称为复制证明(PoReb)。在此过程中，存储提供商生成ZKP来证明他们存储的是唯一的原始数据。换句话说，由另一个提供者维护的原件不被引用。此外，由于证明的大小远小于存储的数据，使用ZKP会增加存储提供商的带宽要求。CeloPlumo

CeloPlumo使用ZKP创建了一个超轻量级的网络客户端，可以在移动电话和其他资源有限的设备上使用。虽然客户端是轻量级的，但它确保了所访问形状的准确性。黑暗森林

黑暗森林是ZKP游戏中最受欢迎的应用。虽然ZKP的使用适合隐私用例，但ZKP在创建不完整音频游戏中的应用确实很独特，这超越了ZKP在支付网络中的金融应用。

2016年以前，ZKP只是一个研究课题，只在少数学术界讨论。当Zcash发起的团队创造了第一个消耗完成ZKP变种ZK-斯纳克。为了支持Zcash网络中的屏蔽/公开交易，这一切都变了。有了真实的用例，对ZKP的兴趣变得越来越强烈，从而出现了更好的ZKP变种，这也成为第一节讨论的许多手腕的基础。但是需要进一步开发ZKP来完成该技术的主流采用。

为了知道如何进一步完善这项技术，我们可以创造类似的技术，比如野智。在很多方面，ZKP技术与野生智能技术相似，估计也会遵循相似的轨迹。。像ZKP一样，野生智能也是一项有前途的技术，它可以处理许多影响。而原有的野智算法天赋有限，计算复杂度远超现有硬件的天赋。。这使得野生智能应用程序的开发和使用变得很晚而且不现实，并且使得野生智能仅限于研究实验室。在发明了DNN等新架构，应用GPU提高执行速度后，也在逐渐完善。这最终带来了一些突破。比如2012年的AlexNet以巨大的优势赢得了最著名的计算机视觉大赛ImageNet。

AlexNet是人工智能时代的开端，催生了未来的人工智能应用。，如GPT-3、达尔。E2和稳定扩散。[XY002][XY001]明天的ZKP的形态和AI早期的形态很像。人工智能是一项很有前途的技术，目前仍在自动开发中。，但稀疏型的计算导致其研究时间过长。从人工智能的经验来看，我们可以肯定ZKP技术在减少需求处理方面有一些效果。

就像AI从LeNet-5部署到AlexNet部署到Resnet-50部署到Transformer一样，ZKP算法也会经历发展阶段，在功能上会带来明显的进步。。事实上，我们已经看到了这方面的停顿。自2011年引入ZK-斯纳克以来，我们开发了一种更激进的算法。2018年，STARKware的创始人开创了Stark，这是一种ZKP方法。不需要信任设置，证明生成时间更短。这项技术是Starkware包括StarkNet在内的几个产品的基础。

随着2019年PLONK的推出，ZKP实现了持续发展。，这是一个SNARK完成，允许许多应用程序使用单个可疑设置，而无需中止重复设置。PLONK缓和了多个实现的开发。这些实现被各种Web3协议使用，比如Aztec、Mina和Celo。

ZKP的一个主要限制是计算复杂，导致证明时间过长。例如最近Polygon发表的zkEVM在64核效应器上实现了5分钟生成500kgas计算的证明。提高ZKP的研究时间是ZKP技术主流化的关键。类似于AI优化软件执行引擎和使用通用硬件是实现这种手段的必要条件。

优化软件

很多ZKP生成运算都是大规模并行的，也就是说并行处理，比如GPU，可以减缓ZKP的计算速度。。常用的GPU库(如CUDA)可以用来减缓NvidiaGPU上ZKP的计算。由于每个项目使用不同的ZKP算法，几个项目正试图从外部开发这种算法。。这里一个明显的例子就是Filecoin对Groth16算法的实现，使用GPU来减缓证明过程。再比如Edgeswap用GPU缩短PLONK&#039证明时间缩短了75%。

常用硬件

由于GPU一般会使得ZKP验证时间的提升受到限制，在这种情况下，我们的另一种选择就是使用常用硬件，比如FPGA或者ASIC。。在制造通用芯片(ASIC)之前，FPGA一般被视为硬件原型平台。FPGA，大致区分了GPU和FPGA的混合处置方案，中短期可以使用。它在加速集中式网络和以隐私为中心的网络的ZKP方面起着次要作用。但是，假设ZKP技术发展到我们预期的水平，ASIC最终会赢得这个市场。目前，ZKP的硬件加速还没有完全实现。这可能是由于ZKP算法的多样性和碎片化。然而，我们认为，通过准确的商业方法，一些初创公司可以专注于开发和货币化这部分技术堆栈。

为了释放ZKP的潜力，需要建立几个通用层和工具。。这些共性对于简化ZKP应用程序的开发过程是必要的，每组开发人员都应该专注于他们的最佳职责。例如，应用程序开发人员不应该担心ZK电路及其义务的底层细节。再次使用人工智能的类比创建多个通用层后，AI可以大大提高。使用这些概括，AI应用程序开发人员不需要担心硬件资源分配。TensorFlow和PyTorch等框架概括了所有这些底层细节。

ZK开发栈没有AI开发栈完善。然而，建立这些抽象需要一些艰苦的工作。底层有低级别的ZKP库，比如PLONK和STARK。在这一层之上像Noir这样的初级语言试图抽象底层的ZK加密技术，并帮助应用程序开发人员专注于应用程序逻辑。Circom是另一种流行的ZKP语言，它位于这两层之间。因为它可以用来创建复杂的ZK后端，所以也可以用来开发基于ZKP的应用程序。Web3中ZKP抽象的另一个例子是StarkWare的开罗演讲。它允许开发人员实际使用STARK在底层证明的通用智能契约。为了提供进一步的抽象虚空思维&#039；的Warp工具允许Solidity开发者直接将他们的Solidity代码转换成Cairo。使用Warp，您可以将UniswapV3代码转换为Cairo。只需要停止对原始实体代码的最小改变。

基于对ZKP发展道路的讨论，我们肯定了一些与ZKP有关的想法。好的想法可以分为两组：工具和应用。

初级开发框架

类似于AI中的Tensorflow和PyTorch，初级ZKP开发框架关于解锁应用层面的创新非常重要。这些框架需要：

ZK-rollupSDK

ZK-rollup越来越受欢迎，它可以为游戏或高吞吐量DeFi协议启用应用特定的L2。在这种情况下，ZK累计停止执行和结算。L1将处理共识和数据可用性。然而，启动特定于应用程序的ZK汇总仍然非常复杂。我们相信，提供开发人员友好的SDK来发布自定义ZK汇总的初创公司将处理真正的业务需求。并能通过提供开发工具箱、开发者效力、定序器服务、配套基础设备，成为有价值的企业。

ZKP硬件加速器

瞄准特定用例，在早期市场建立先发制人地位的专业硬件公司，已经被证明是非常有价值的公司。当英伟达专攻人工智能硬件，成为北美最有价值的半导体公司时，人工智能领域就是如此。比特币挖矿也是如此。、比特大陆、迦南和Whatsminer通过专攻ASIC采矿成为独角兽。想象并制造高效ZKP硬件加速器的公司也可能遵循一条非常轨迹。

ZK桥和互操作性

ZKP可用于创建跨链音频传输协议的有效性证书，其中跨链消息可在手段链上快速验证。这类似于在底部L1上验证ZK卷的方式。然而，关于跨链消息传递因为要验证的签名方案和加密函数在源链和手段链之间可能不同，所以复杂性更高。

ZK离线游戏引擎

黑暗森林证明了ZKP可以让消息不完整的离线游戏成为可能。。这对于更具互动性的游戏想象非常重要，因为在这些游戏中，玩家&#039；行为是保密的，直到他们决定公开。凭借离线游戏的技能，我们希望ZKP成为游戏执行引擎的一部分。。对于成功将隐私功能集成到高通量离线游戏引擎中的创业公司来说，机会是巨大的。

身份处理方案

ZKP在身份领域有很多机会。。它们可用于声誉或链接Web2和Web3身份。目前我们的Web2和Web3身份是合并的。Clique和其他项目通过使用预测机器将这些身份联系起来。。通过启用Web2和Web3身份的匿名链接，ZKP可以进一步发展这种方法。这为那些使用Web2或Web3数据来证明他们在特定领域的专业知识的人提供了匿名DAO成员的用例。。另一个用例是基于借款人的无担保Web3借贷。

sWeb2社交位置(比如Twitter关注者的数量)。

ZKP合规部

Web3支持匿名在线账户自动加入金融系统。从这个意义上说，Web3实现了极大的财务自由和通融。随着Web3法规的增加，ZKP可用于符合要求但不破坏匿名性的活动。。ZKP还可用于证明投资者身份或任何其他KYC/反洗钱请求。

NativeWeb3公共债务融资

TradeFi债务融资一般用于支持成长型创业公司。在不筹集额外风险资本的情况下加速增长或推出新的业务线。Web3DAO和匿名公司的兴起为Web3&#039原始债务融资。例如通过使用、道或匿名公司，可以根据其增加用途的证明，以合作利率获得无担保贷款，而不会泄露借款人&#039；这对贷方来说是个新闻。公共定义

金融机构一般不披露其交易历史的微观风险敞口。由于链分析时不时的进步，在使用链协议(如DeFi协议)时很难令人满意。。一个可能的解决方案是开发一个以隐私为中心的DeFi产品来维护协议参与者的隐私。一个试图实现这一愿景的协议是半影&#039；szkSwap。此外Aztec的Zk.money通过用户参与模糊的DeFi协议，为公共DeFi提供了一些赔钱的机会。一般来说，一个有效的、面向隐私的DeFi产品协议的成功实施可以从机构参与者那里获得可观的费用。

ZKP

web3广告推动了让用户拥有自己数据的趋势，比如阅读历史、私人钱包活动等等。为了用户的利益，Web3也支持这些数据的货币化。。由于数据货币化可能与隐私冲突，ZKP可以掌握哪些方面的群体数据被允许泄露给广告商和数据聚合者。

私有数据的共享和货币化

假设与正确的实体共享。我们的很多私人数据都会产生很大的影响。群体福祉数据可以帮助研究人员通过众包开发新药。私人财务记录可以与监管机构和监督机构共享，以发现和惩罚不当行为。ZKP可以实现这些数据的私人共享和货币化。

私人管理

道和链管理正在完善，未来管理方式的一个次要缺陷是参与的非隐私性。ZKP是解决这一效应的基础。管理层参与者可以停止投票，而无需透露投票方式。此外ZKP可以将管理提案的可见性限制在“道”成员范围内，从而使“道”能够建立协作优

势。

ZKP技术是Web3领域最具创新的技术之一。它为突破性的协议和公司提供了一些机会。