比特币生态里程碑：Zulu 利用Bitcoin Script 实现 ZKP 验证

作者：日月小楚 来源：medium

近期比特币生态中一个重要里程碑事件，Zulu宣布实现利用比特币脚本的zk-SNARK验证（ZKP）。涉及Groth16/FFlonk主流算法，并将代码提交到BitVM存储库。

实现了比特币脚本进行ZKP，这意味着比特币网络可以对layer2进行验证。这真正意味着layer2，它负责继承比特币网络的安全性，来自比特币Pow机制的安全性，这应该是区块链最具安全性的网络。

由于比特币网络的编程性限制，实现ZKP是特别困难的。现有的大部分比特币l2，实际上并不是真正法L2，因为其链上状态是无法在比特币网络上直接验证的。他们现在打算是生成一个zk证明，发布到btc网络上。但是这个证明并不是比特币网络验证的，而是他们自身网络的角色，就导致l2的链上状态跟比特币网络是分离良策。

这跟以太坊的layer2有着明显的不同。 无论是zk-rollup还是op-rollup，都会将数据打包后交由以太坊主网络进行验证。 而以太坊layer2层相比其它公链最大的优势是，由以太坊来保证layer2的安全性。

成为比特币网络验证的layer2，它最大的好处是继承了比特币网络的安全性。比特币网络的安全明显是胜于以太坊的。现在能真正继承其安全性，有两种方式。一种是babylon为代表，质押原生的btc，自己由pos网络进行管理，对作恶者进行严厉惩罚。当质押的btc价值比较大，作恶的代价非常高，以此保证安全性。但是，列举的前提是首先有大量的btc进行质押。

第二种是利用比特币自身的pow网络，作为第一条也是市值最高的网络，btc安全运行已经14年了，拥有全网最高的算力，其安全系数不言而喻。那么能继承比特币网络的安全性，其重要的一环就是btc能够实现验证。也就是这次Zulu这次ZKP的严峻意义。上次关注Zulu网络，是它首创的比特币双层架构。这次zk-SNARK验证（ZKP），让我也意识到Zulu背后的技术实力非常强大。

## zk-SNARK中文

SNARK ( 简洁的非交互式知识论证 ) 是简洁非交互式的知识论证，其核心是通过数学算法来构建一个证明系统，使得验证者在不了解原始数据的情况下的验证数据本身的正确性。我们知道，现在以太坊Layer2有zk-rollup和op-rollup。而op-rollup只是中间过渡期，zk-rollup才是最终形态。因为zk-rollup是使用zk算法将交易批量打包，并生成SNARK证明提交到主网，主网验证该批次的所有交易。zk-SNARK可以有效地进行隐私保护，并且有很强的扩展性，被V神誉为下个10年的重中之重。

## 比特虚拟机

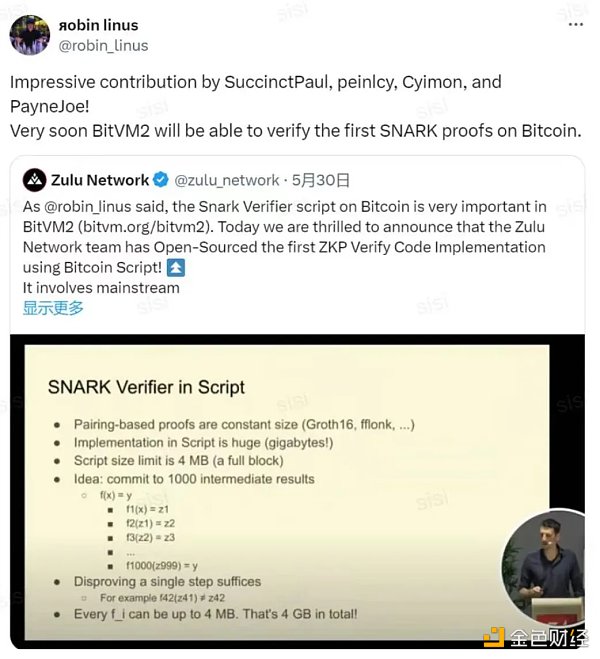
这里必须要介绍一下BitVM。在BitVM之前，比特币的脚本并不具备图灵的。尽管大量的人经过大量工作，但仍然无法使用。直到去年10月Robin Linus释放了一个令人震惊的BitVM，Robin的方法是在比特币脚本上验证一种特殊启动逻辑门，称为NAND门，这是计算的基本语序之一，位于物理/电气级别。所有可能的计算都可以由NAND门构建而成。

最近，Robin又提出了BitVM 2的设计方案。

BitVM的意义在于，可以实现使用比特币网络进行验证，并且无需升级、无需分叉、不给btc带来任何额外的负担。layer2负责其它的责任计算，继承主网的安全性。由于BitVM巨大的意义，很多layer2都在BitVM基础上进行构建。比如Bitlayer就是将BitVM作为核心组件，投入分层虚拟机技术（Layered Virtual Machine）的二层解决方案。

在Zulu Network中，BitVM也是非常重要的存在。而Zulu同样也是BitVM非常重要的贡献者，可以说用比特币脚本实现zk-SNARK验证对BitVM是最核心的一步。Zulu 为 BitVM 2官方的GitHub 代码仓库贡献颇多，因而得到了BitVM发明人Robin Louis 的高度肯定。

上周，Zulu 已经完成对 Groth16 脚本的切分。2 个公共的输入，总共切分出了 1701 个子脚本，大小小于 4M，深度<1000。首次 ZKP 脚本切分完成，代表 BitVM 商用的一个又一个。由于Zulu的出色工作，BitVM2 可以很快实现比特币基础上的第一个 SNARK 证明。也说明Zulu 的技术也处于领先地位。



图片注：Zulu的技术得到了BitVM的发明者Robin Louis的高度

## 最后简单介绍下Zulu Network

Zulu Network是用于比特币生态的双层网络，其layer2层是一个EVM兼容的ZuluPrime。EVM项目可以快速、高端的部署，实现生态的繁荣。另外一层为Layer3层，称为ZuluNexus。它创新性地统一了UTXO和账户资产类型，并实现了基于UTXO模型的智能合约创新。这意味着它能最大限制的发挥UTXO的功能，并且能支持未来UTXO上的创新。Zulu正在开发两个产品：

可以尝试ZKP验证链下状态的Zulu bridge，用于支持资产发行

开发去中心化的ZK桥来为用户提供任意数量的链式操作

Zulu现在尚未发币，想早期的参与的可以参加Zulu现在的测试网积分活动。详细看官方的文档https://www.yuque.com/zulunetworkzhongwenshequn/zvggg8/kr9epkg0v27rh860?singleDoc#

