对话Zulu Network联创：以比特币的方式创新比特币



作者： Rebbeca Ren（加密厨房 Crypto Kitchen 纽约主厨）

2023 年末，Ordinals 和 BRC-20 的爆炸性增长证明了大家对比特币链上原生新资产的强烈需求。

然而，这股热潮也暴露了比特币网络的固有局限性：高昂的交易费用和缓慢的处理速度严重制约了链上资产的流通效率。

于是，通过将部分交易移至链下处理，以提高交易速度、降低费用、并扩展网络应用能力的比特币的 Layer 2 解决方案被寄予解决障碍的厚望。

时至今日，市面上甚至有上百家 Layer 2（包含侧链）在展开激烈的竞争，而两年前，也就只有闪电网络、Rootstock、Stacks 等老牌协议项目在默默地深耕。

除了链上资产的火爆让开发者们嗅到了机会之外，著名的区块链开发者 Robin Linus 在去年 10 月提出通过 BitVM 为比特币网络引入可编程性，为更多开发者提供了搭建 Layer 2 的技术蓝图。

BitVM 的革命性在于，它能够利用比特币网络进行验证，无需升级或分叉，也不会给比特币网络带来额外负担。Layer 2 负责复杂计算，同时继承主网的安全性。这一创新意义重大，以至于众多 Layer 2 项目纷纷基于 BitVM 展开构建。例如，Bitlayer 就将 BitVM 作为核心组件，采用分层虚拟机技术打造二层解决方案。

加密厨房近期请来了 BitVM 的 GitHub 代码库的核心贡献者之一 Zulu Network 做客 BIT FM Space，联合创始人 Luke 和我们开诚布公的聊了聊打造 Layer2 的心得。



在创立 Zulu 之前，Luke 曾先后就职于 JP Morgan、野村证券和 OKX，凭借在传统金融和加密货币交易所的丰富经验，敏锐地捕捉到了 BitVM 所蕴含的巨大潜力。

在看到 BitVM 白皮书的那一刻，他和团队就认为 BitVM 将彻底改变比特币的性质，使其进化为真正的可编程货币，无需与其他区块链竞争，因为未来所有的去中心化应用都将能够在比特币网络上构建。

「Ordinals、Brc-20、Runes 等等，这些都代表了比特币的发展方向。我们看到了人们的需求，但是比特币原生设计上的限制阻碍了这一点，这就是我们要做的，」Luke 表示。

和其他 Layer2 解决方案不同的是，Zulu 采用了 Dual-Layer（双层架构）和 Trust-Minimized（信任最小化）的 BitVM 桥接：

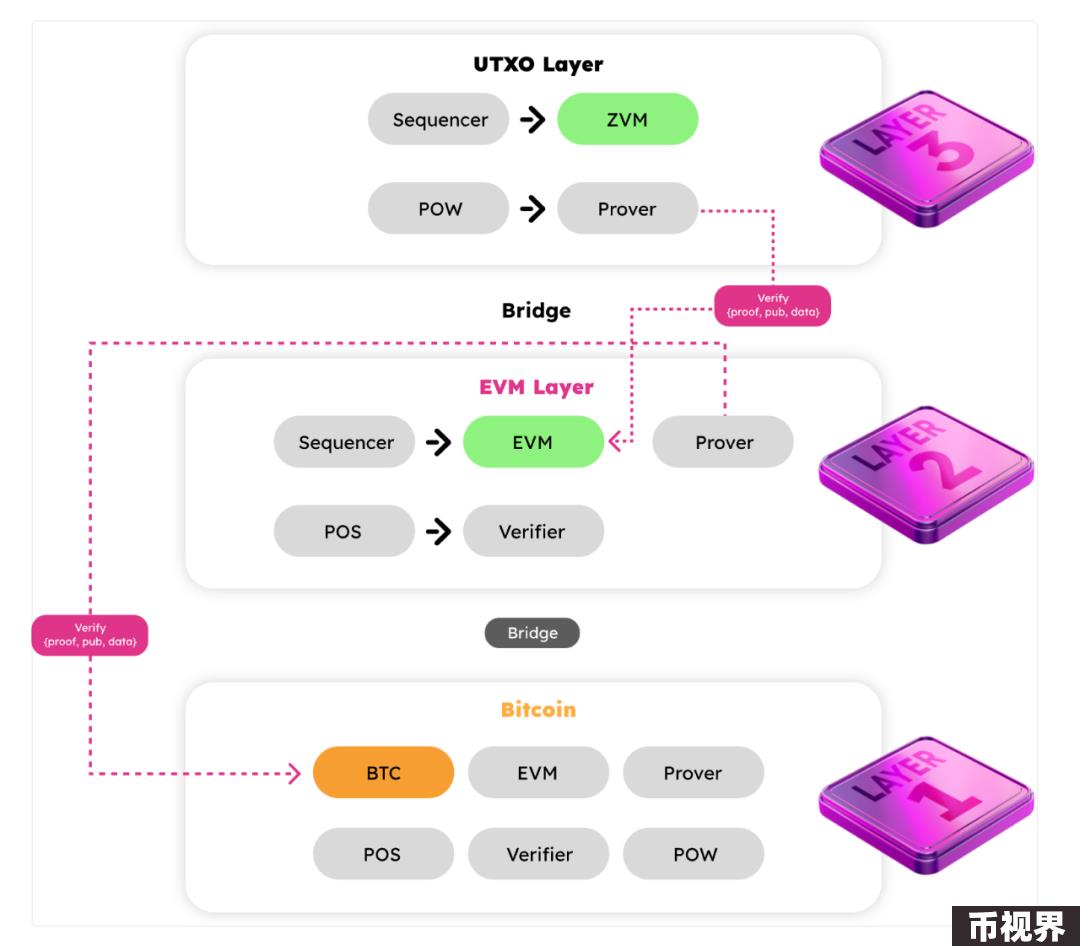
双层架构的第一层（相当于比特币的 Layer 2）名为 ZuluPrime，基于 zkSync 的零知识（ZK）堆栈开发的零知识以太坊虚拟机（zkEVM）构建，专注于提供稳定和成熟的各种去中心化应用（DApps）和金融服务等。

这层设计巧妙地解决了在比特币上直接执行智能合约的复杂性问题，通过引入 ZK 证明的概念，为所有交易的执行生成一个证明，从而保障了交易执行的有效性和网络的安全性。

双层架构的第二层（相当于比特币的 Layer 3）名为 ZuluNexus。这一层不具备 EVM 兼容性，但能同时支持 UTXO 和账户类型，让基于 UTXO 的智能合约开发成为可能。

这种设计既保留了比特币的基本功能，也引入了新特性，为开发者开拓创新提供了空间。

ZuluPrime 和 ZuluNexus 之间通过官方桥相连，实现了资产的快速转移。



在 Luke 看来，ZuluPrime 是他们进入比特币 Layer 2 赛道的入场券，而真正的「杀手锏」则是 ZuluNexus，因为它能够专注于比特币原始生态系统和原生资产的创新 —— 这是大部分 Layer 2 所不具备的。

「以比特币的方式创新比特币，这就是我们想要推进的方向，」他说。

至于 BitVM 桥，它能够确保用户在比特币与 Zulu 网络之间进行跨链资产转移时的安全性和可靠性。这种桥接机制的设计旨在最大程度地减少用户需要信任的第三方，从而提高整个系统的安全性。

在资产跨链转移过程中，BitVM 起到验证者的作用，确保所有操作按预定规则执行。此外，即使 Zulu 网络出现故障或中断，BitVM 仍能够帮助用户安全取回他们的资产。BitVM 类似于一种保护机制，为跨链交易提供了额外的安全保障，提升了系统的稳健性和信任度。

不过，虽然 BitVM 能够实现信任最小化的验证，但它在运作中需要大量的信任或经济激励，以确保各方不会试图欺骗对方。因此它更适合拥有大量比特币的大型流动性提供者，对于小额比特币、BRC-20 代币、Runes 或 Ordinals 提供者不够友好，因为防欺诈成本过高。

所以针对小额资金，Zulu 还推出了一个去中心化的 ZK 桥：值得一提的是，Zulu 是第一个在比特币主网上基于 BitVM 实现 ZK 证明的项目，还得到了 Robin Linus 本人的认可，并将 Zulu 团队的代码合并到 BitVM 的中央存储库中。

通过这样独特的架构，Luke 希望能够帮助开发者以更快的速度、更低的费用来构建 DApp，同时在安全性上也不做妥协。

「如果一个事情不能解决生态系统的关键需求，我就不会去做它。我坚信比特币的第二层解决方案对比特币的未来至关重要。它们解决了比特币网络的一些关键限制，如可扩展性、脚本语言的限制和速度等，」Luke 说道。

2024 年 4 月初，Zulu Network 测试网上线并运行至今，目前已有超过 70 万注册用户，处理了超过 1200 万笔交易。同时，Zulu 在当月完成了 300 万美元的 Pre-Seed 轮融资，投资方包括 Cryptogram Venture 和 D11 Labs 等知名机构。

根据 Defillama 的数据，截至 2024 年 8 月 16 日，以太坊生态 TVL 为 840 亿美元，巅峰时期一度超过 1700 亿美元。而目前比特币生态的 TVL 仅有 6 亿美元，尚不足以太坊 TVL 的 2%，这一数据折射出比特币在 DeFi 领域的巨大发展空间。

随着像 Zulu Network 这样的基础设施建设者不断涌现，比特币正在从单纯的数字黄金，逐步演变为一个功能丰富、可编程的货币网络，让我们持续期待比特币生态的走向。

最后，用我非常喜欢的 Luke 的一句话作为结尾：「我希望看到人们的需求回到比特币上，之前它在某种程度上迷失了，进入了其他网络，现在正在绕一圈回到原点。」

