BOB：Hybrid L2（混合 L2）

Vision Paper，2024 年 10 月

Alexei Zamyatin 与 Dominik Harz
research@gobob.xyz

摘要

BOB 是一种由比特币确保安全的新型混合 L2 区块链。作为最安全的分散型网络，混合 L2 继承了比特币的安全性。它还采用比特币的安全性，打造与比特币、以太坊和其他 L1 区块链之间的信任最小化跨链桥。因此，混合 L2 不依赖于第三方跨链桥实现互操作性，并解决了分散的比特币多链的流动性问题。

1 引言

最初设计的比特币，是一种分散型、透明和抗审查的支付系统。经过十余年的发展，智能合约链使得打造分散型金融应用和其他创新产品成为可能，这其中包括 NFT、社交媒体和游戏代币化，以及 DAO 和其他信任最小化的治理结构。比特币虽仍然是全球加密货币领域的核心，但在创新和开发者活动等方面已经处于落后态势。

作为网络，比特币稍显缓慢而僵化，然而，就市值、交易量和活跃用户数而言，比特币仍然比所有其他加密货币加起来都要高。比特币在全球拥有 3 亿用户、1 万亿美元市值和无与伦比的品牌认知度，一如既往地占据主导地位。然而，它的 DeFi 活性最低。以太坊的 DeFi 总锁定价值 (TVL) 约占市值的 30%，相较之下，比特币的 DeFi TVL 仅占其市场规模的 0.1%，二者相差 300 倍。

过去数年，比特币多次尝试通过协议变更和分叉的方式引入智能合约和 DeFi，但均以失败告终。比特币反对包括智能合约在内的所有协议升级，因为这可能会大大改变其功能性或增加其复杂性。可以预料的是，未来不管多久，比特币都不可能具有像以太坊那样的天然可编程性。因此，所有的努力最终都会导致比特币 L2 成为比特币 DeFi 的首选方案。

混合 L2。本文介绍了混合 L2 这种旨在应对在比特币平台创建和扩展 DeFi 的关键挑战的新型比特币二层解决方案。混合 L2 具有三种关键特性：

- 利用 BitVM2[4] 对比特币进行乐观验证和错误证明，实现**比特币的安全性**。
- **信任最小化的比特币跨链桥。**利用 BitVM 支持的跨链桥设计，只要比特币安全，且网络中至少有一个诚实的节点（如用户自己）来处理链上争议，用户就可以在 BOB 上进行比特币的存取。这种新的安全模型被称为存在性诚实（1/n），并严格优于现有的依赖诚实多数假设（t/n）的比特币多重签名。
- 由比特币确保安全的**连接以太坊的信任最小化跨链桥**。BOB 将 L1/L2 以太坊乐观卷叠的桥设计与编码为 L1 智能合约的比特币轻客户端相结合，以比特币的最终确定性为条件确定 L2 取款的正确性。这种设计可以扩展到大多数拥有智能合约的 L1 链。

作为第一个混合 L2，BOB 为去信任化互操作性问题提供了实用的解决方案：作为最受信任的单一网络，比特币确保了 L2 及其所有跨链桥的安全。BOB 进一步解决了比特币在数十条链间流动性分散的挑战。用户无需将比特币包装成支持 DeFi 的区块链，即可将来自各区块链的资产存入 BOB 网络，从而利用比特币固有的流动性确保安全的提款。最后，通过向比特币缴纳费用，BOB 又可以反哺比特币的长期可持续安全预算。

2 比特币 L2 的现状：机会与挑战

比特币 L2 有望在不改变比特币核心原则的前提下，让比特币重焕创新活力。在不需要集中交易所的情况下解锁比特币万亿美元市场的交易、借贷和质押等 DeFi 用例的承诺吸引了成千上万的开发者：已有数十个区块链表示拥有“比特币 L2”的称号。

然而，构建比特币 L2 并非易事，之前的尝试一直在努力实现与以太坊相同的吸引力。我们认为，成功推出比特币 L2 仍然面临以下三个核心挑战：

- **比特币安全性和信任最小化的比特币跨链桥。**这是比特币 L2 与所有其他链的区别所在。来自最强大、最分散的网络的安全性，以及在不信任任何第三方的情况下存取比特币的方式。到目前为止，这一点还不可能实现：几乎所有的比特币跨链桥都是可信的多重签名。如今，比特币的历史上终于第一次出现了用 BitVM2 实现这一目标的蓝图。
- **构建竞争生态系统。**L2 的成功取决于它的 dApp 生态系统。创建成功产品的基石是一流开发工具和 DeFi 基础设施的可用性（如：钱包、机构托管和预言机）。这也意味着亚秒级交易速度和 Gas 代币的提取等需要与时俱进。比特币应用无法提供有竞争力的构建器环境，因此，这使得其几乎不可能在以太坊和其他网络上与竞争对手竞争。在撰写本文时，即使针对某些用例进行了优化，非 EVM 智能合约环境的优势也通常被缺乏基础设施以及由此对应用上市时间表产生的负面影响所掩盖。
- **引入蓝筹流动性（冷启动问题）。**稳定币、出入金、集中交易所接入、与其他网络连接的跨链桥以及超级用户的流动性是 DeFi 生态系统成功的关键。网络效应已被证明是新产品成功的决定性因素，因此，在孤立的区块链上闭门造车会给应用开发人员带来重大风险。

3 背景：跨链桥、轻客户端、BitVM

混合 L2 利用了三个主要概念：轻客户端、跨链桥和通过 BitVM 对比特币的乐观验证。

轻客户端：区块链轻客户端协议，在比特币中也称为“简化支付验证”(SPV)，允许资源有限的节点在不下载底层区块链全部数据的情况下有效地验证支付的执行情况。取而代之的是，只需要包含验证共识最终确定性所需足够数据的区块头和选定交易即可。轻客户端协议的复杂性和安全性由各自区块链的共识机制决定。比特币的轻客户端经证实是安全的，可以很容易地被其他具有智能合约功能的链验证，例如，Threshold 已经在以太坊上运行这样的轻客户端数年之久。[1]另一方面，存储和跟踪超过一百万个验证器的公钥的过程较为复杂，因此，以太坊还不具备安全的轻客户端。[2]

跨链桥：事实证明，要在两个不同的区块链之间安全地桥接或“包装”资产 (i) 需要两个链都正常运行，且 (ii) 不能没有可信的第三方[5]。然而，在实践中，我们可以让任何网络参与者承担这个角色，减少对该第三方的信任依赖。这可以通过所谓的“轻客户端桥”来实现，其中 *A* 和 *B* 两条链能够验证彼此作为链上智能合约一部分的共识协议。当把资产 a 存放到 *A* 链上的跨链桥中时， *B* 链上的智能合约在创建包装的表示 *b (a)* 之前验证该事项已经在 *A* 链的共识下完成。反之亦然，当我们销毁 *B* 链上的 *b (a)*，接收 *A* 链上的基础资产 *a* 时，我们首先验证该事项确实已经作为 *A* 链共识的一部分在 *B* 链上最终确定。因此，除了两条链的安全操作之外，我们唯一需要的信任是至少有一个节点将在两个网络之间起到中继作用，传递验证所必需的数据。遗憾的是，轻客户端较为复杂，因此这种设计很少在实践中成功实现。就比特币而言，其脚本语言的表达能力限制加上区块和堆栈大小限制，截至目前，任何形式的链上轻客户端仍然无法实现。

BitVM：BitVM 是一种以乐观方式在比特币上执行任意程序的机制：执行发生在链外，但在失败的情况下，争议会在链上解决和执行[3]。两个主要的用例是比特币乐观卷叠（类似于 Arbitrum [2]）和信任最小化跨链桥。在这两种情况下，BitVM 都允许用户在 L2 中存入和提取比特币，这样，只要网络中有一个由轻客户端验证启用的诚实在线节点，存币就不会被窃取。

欲了解 BitVM2 协议的完整协议规范，以及使用 BitVM2 为连接链实现轻客户端的信任最小化比特币跨链桥[4]，请参考我们最新的论文。

该设计可概括如下：

(1) 用比特币脚本将程序压缩成 SNARK 验证器（如，Groth16[1]）。
(2) 将验证器分成子程序块，每个子程序块最大 4MB，可以在比特币交易中执行。
(3) BitVM2 操作者在设置期间使用 Taproot 树[3]和交易预签名提交程序。
(4) 用户将一些资金存入 BitVM2（如：跨链桥存款）。
(5) 当试图从 BitVM2 提取资金时，任何人都可以对操作者提出质疑（如：如果操作者试图从跨链桥中盗用资金）。
(6) 操作者如果受到质疑，则必须披露所有中间子程序结果，以展示其如何得出最终计算结果。
(7) 如果操作者存在作弊行为的，所披露的子程序结果中将会有一个错误结果。随后，任何人都可以在比特币交易中执行特定的子程序，得出正确的结果作为错误证明，反驳操作者。
(8) 错误操作者被踢出，且不能再接触存在 BitVM2 中的资金。

4 BOB 混合 L2

混合 L2 的设计建立在对比特币安全性的信任以及共识验证的简便性之上。

4.1 比特币安全性

BOB 混合 L2 将使用比特币进行结算和安全保障。人们普遍认为，比特币 L2 的理想设计是零知识卷叠（ZK 卷叠），其中状态变化采用离线计算，再使用零知识证明在链上证明其有效性。截至目前，比特币系统尚无法实现 ZK 卷叠：比特币脚本中 ZK 验证器的高效实现需要通过共识分叉额外引入操作码。

因此，BitVM2 支持的乐观验证是目前实现比特币安全的实际途径。这意味着要实现 zkVM，它为每次状态转换生成有效性证明，并定期将这些证明与状态差值一起发布到比特币主链。当与 BitVM2 配对时，任何网络参与者均可通过错误证明来提出质疑和反驳。与以太坊 L2 类似，在质疑期（如 7 天）内没有错误证明的，可认为状态是最终状态。安全性*几乎*等同于比特币安全性：只要网络中有一个在线节点触发一个错误证明即可。

在 BitVM 设计空间内的各种乐观卷叠方法之间存在许多平衡安全性与效率和实用性的技术折衷，包括围绕数据可用性的考虑、无权限挑战逻辑和轻客户端模型等。BOB 混合 L2 的实施细节将在即将发布的技术规范中发布。

[1] https://github.com/keep-network/tbtc-v2/blob/main/solidity/contracts/relay/LightRelay.sol
[2] https://github.com/ethereum/annotated-spec/blob/master/altair/sync-protocol.md
[3] https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

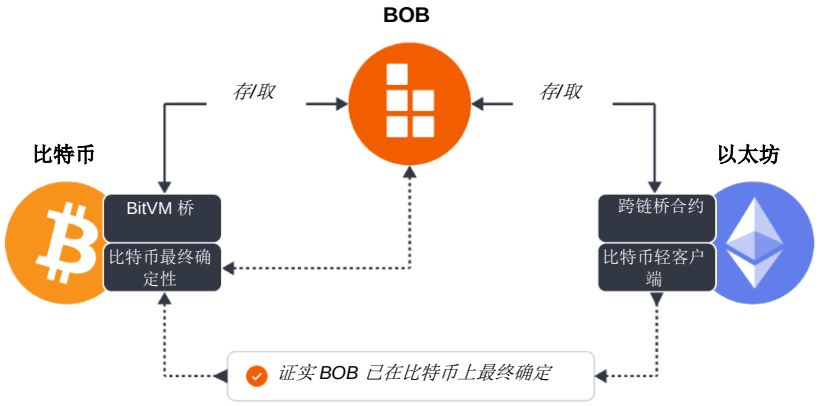

图 1：BOB 混合 L2 将采用信任最小化跨链桥连接比特币（通过 BitVM）和以太坊中。以太坊跨链桥智能合约使用内置的比特币轻客户端验证 BOB 已在比特币中最终确定。

4.2 信任最小化的比特币跨链桥

通过 BitVM2 错误证明进行的乐观验证也支持 BOB 创建信任最小化的比特币跨链桥。具体来说，这是一种轻客户端跨链桥，比特币可在 BitVM2 中为 BOB 运行一个轻客户端，使我们可以执行正确的跨链桥支取。任何将比特币存入 BOB 的用户都确信，只要比特币安全，且网络中有一个在线节点触发错误证明，他们就可以将资金撤回到比特币系统。

跨链桥的安全模型被称为*存在性诚实*，即它的正确操作只需要 n 分之一的诚实假设。相较而言：当前绝大多数的比特币跨链桥都依赖于多重签名方案，并采用*诚实多数*假设，即需要 n 个签名者中的 t 个诚实，使 t>50%。如果大多数签名者不诚实，他们就可以盗用桥中的所有资金。相比之下，在我们的 BitVM2 跨链桥设计中，*即使所有的跨链桥操作者都不诚实，跨链桥设计资金也不会被盗*。只要有一个在线参与者（可以是桥用户本身），不诚实的操作者就可以受到质疑，并被逐一清除出操作流程。在最坏的情况下，所有操作者都将被清除，其资金也将被冻结。这个过程仍将构成操作失败，它与现有跨链桥模型有微妙但重要的区别：操作者实际上无法盗取比特币，因此，他们没有尝试攻击的经济动机。这构成了比特币历史上最安全的比特币跨链桥设计。

4.3 信任最小化的以太坊跨链桥

BOB 的混合设计支持以太币和 ERC20 的安全存取。它的工作方式类似于原生乐观桥：当用户想要将资产撤回以太坊时，以太坊主网上的跨链桥智能合约就会等待 L2 完成。对于 ETH L2，这意味着需要等待 7 天，确保以太坊主网上没有发布错误证明。在 BOB 的混合 L2 设计中，以太坊桥智能合约会等待 BOB *在比特币系统中完成*，即确保比特币上没有错误证明。该过程通过比特币轻客户端实现，该客户端是可以验证比特币区块链的跨链桥智能合约的一部分。因此，任何将以太币和 ERC20 存入 BOB 的用户都可以撤回到以太坊，只要比特币是安全的，并且网络中有一个在线节点可以触发*比特币系统中*的错误证明。

5 展望：BOB 是比特币 DeFi 的中心

混合 L2 利用比特币和以太坊的网络效应，独特地将 BOB 定位为最大的 DeFi 生态系统，并有望在未来扩展到其他链。

通过以太坊进行引导：对于 BOB 上的 dApp 来说，这意味着它们可以通过以太坊的网络进行引导，并从一流的基础设施和工具中受益，同时引导 DeFi 超级用户并利用与所有交易所和机构参与者的连接。值得注意的是，几乎所有以太坊用户都有比特币，大多数比特币超级用户也使用以太坊 DeFi。

运用比特币推动增长。随着时间的推移，比特币安全性和通过信任最小化 (BitVM2) 跨链桥获得的可及性的提高，将释放越来越多迄今尚未开发的比特币流动性，让 BOB 上的 dApp 不仅赶上其以太坊竞争对手，而且超越它们。比特币在全球的广泛采用和多样化的社区进一步增强了这种效果：当以太坊 L2 继续争夺相同的用户群时，BOB dApp 可以挖掘比特币的 3 亿全球用户和数千家现实世界的企业。

比特币是多链 DeFi 枢纽：比特币、以太币和稳定币占据了 90% 的市场份额。然而，就像存在数百家银行一样，也可能存在数百个专注于不同使用案例和地理位置的链。它们的用户需要安全地存取比特币，并能进行资产交易。

目前，这一角色由集中交易所担当：交易所与所有链互联互通，允许用户存入、交易，然后将资产撤回到各自的 L1。然而，集中交易存在截止日期。它们在过去造成了重大问题，并将持续存在，直到我们完全过渡到 DeFi 为止。

相反，BOB 的使命是让比特币成为安全透明的 DeFi 生态系统的支柱。

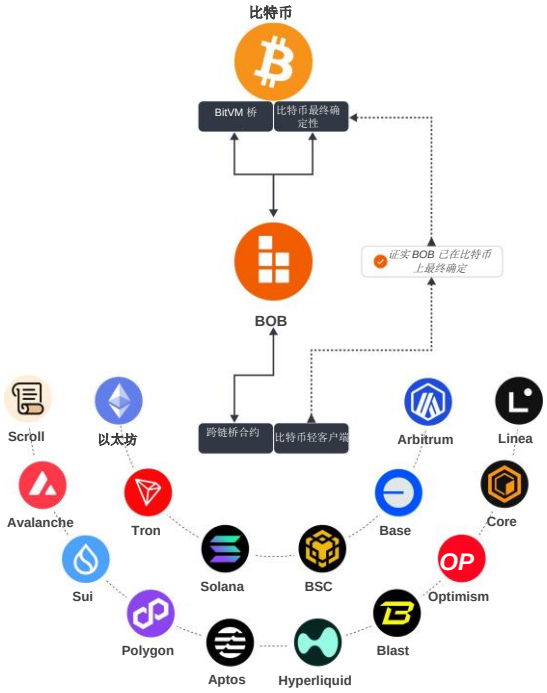

图 2：任何可以通过智能合约等方式操作比特币轻客户端的 L1 链都可以创建连接 BOB 的信任最小化跨链桥。

作为一种混合 L2，BOB 将操作由比特币担保的信任最小化跨链桥，这些跨链桥可连接任何可以验证比特币区块链的智能合约链。这意味着 90% 的现代 L1 和 L2，包括 Solana、Tron、Sui、Aptos、Monad、Avalanche、Cosmos、Polkadot，……这样的例子不胜枚举。只要比特币安全，这些链的用户将把以太币、SOL、TRX、DOT 等原生资产存入 BOB，与比特币或其他数字资产进行交易，并撤回到各自的 L1 链。用户不再需要信赖币安或 Coinbase，只需信任比特币即可。用户不再依赖第三方桥梁，而是依靠比特币来保护多链存取。

使用比特币作为信任锚来创建可互操作的 DeFi 生态系统是混合 L2 设计的强大能力。BOB 不会将比特币的流动性分散到几十个链上，而是将比特币的流动性集中，作为集中式交易所的信任最小化替代方案，将比特币置于 DeFi 的中心。

6 路线图

第一阶段：作为一种以太坊 L2 的引导：BOB 首先推出了以太坊 L2，采用 OP 堆栈[4]构建，运行原生以太坊跨链桥，并支持多个第三方比特币桥。

第二阶段：比特币“软”最终确定性：在第二阶段，BOB 将把比特币最终确定性添加到以太坊 L2 设置中。每个纪元（一个或多个 BOB 块），定序器都会请求比特币最终确定性协议[5]的参与者签署一次，这些参与者可完全验证 BOB 链的状态。使用 BitVM，我们可以构建一个受该比特币“软”最终确定性协议保护的信任最小化的比特币跨链桥，即，要攻击比特币跨链桥，就需要操控大多数比特币最终确定性协议参与者（哈希率或 BTC 质押）。以太坊跨链桥将继续由以太坊保护。因此，比特币“软”最终确定性可用于加速以太坊桥的提款，将延迟从 7 天减少到数分钟/小时。

第三阶段：完整的比特币安全性 最后一步是继承比特币的安全性，详见 4.1 节。在缺少支持链上 zk 验证器的比特币分叉的情况下，BOB 就需要通过 BitVM 利用乐观验证。在没有其他信任假设的情况下实现比特币的乐观卷叠，需要使用比特币主链作为数据可用性层。这需要十分巨大的相关成本，对经济方面构成挑战。因此，为完成向第三阶段的过渡，BOB 必须在活跃用户方面达到足够的规模，使得额外产生的数据可用性费用不会增加超过竞争对手以太坊 L2 的交易费用。替代数据可用性层引入了比特币之外的额外信任假设，因此可以被视为成本和安全性之间的权衡。

7 结论

BOB 混合 L2 是一种解决比特币表达能力限制以及由此导致的 DeFi 能力缺乏的新方法。它继承了比特币的安全性，并利用该安全性打造通往以太坊和其他 L1 智能合约链的信任最小化跨链桥，改变了比特币在 DeFi 中的使用方式。用户无需通过中心化跨链桥将比特币封装至其他网络。而是将比特币和其他资产存入一个比特币安全的 DeFi 环境中。

8 免责声明

本文仅供参考。文中内容不构成投资建议或买卖任何投资的建议或邀约，也不应用于任何投资决策的评估。不得将本文用作会计、法律或税务建议或投资建议的依据。本文仅反映作者的当前观点，并不代表 BOB 基金会或其附属机构的观点。其中的内容可能会发生变化，但不会在此更新。

参考文献

[1] Jens Groth.2016.On the size of pairing-based non-interactive arguments.In *Advances in Cryptology – EUROCRYPT*.Springer, 305 – 326.
[2] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S Matthew Weinberg, and Edward W Felten.2018.Arbitrum: Scalable, private smart contracts.In *27th USENIX Security Symposium (USENIX Security 18)*.1353 – 1370.
[3] Robin Linus.2023.BitVM: Compute Anything on Bitcoin.*URL: https:// bitvm.org/ bitvm.pdf* (2023).
[4] Robin Linus, Lukas Aumayr, Alexei Zamyatin, Andrea Pelosi, Zeta Avarikioti, and Matteo Maffei.2024.BitVM2: Bridging Bitcoin to Second Layers.*URL: https:// bitvm.org/ bitvm_bridge.pdf* (2024).
[5] Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios KokorisKogias, Pedro Moreno-Sanchez, Aggelos Kiayias, and William J Knottenbelt.2021.Sok: Communication across distributed ledgers.In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1 – 5, 2021, Revised Selected Papers, Part II 25*.Springer, 3 – 36.

[4] https://docs.optimism.io/
[5] 目前正在测试的两项比特币最终确定性协议是合并挖矿和比特币权益质押。做出这一决定的一个关键因素是 BitVM 中验证的简便性。