比特币权益质押：
释能 2100 万比特币，确保 PoS 经济安全

巴比伦团队[1]

第 1.0 版：2023 年 7 月 13 日

翻译：Ray Joe

摘要

权益证明（PoS，即 Proof-of-Stake）区块链的安全性来自于质押的资本，然而资本可能价格高昂。比特币是工作量证明（PoW）区块链，其市值达 6,000 亿美元，并且大部分比特币资本是闲置的。我们提出“比特币权益质押”概念，“比特币权益质押”让比特币持有者能够质押其闲置的比特币，从而增加 PoS 链的安全性，比特币持有者还能同时获取收益。我们提出了一套比特币权益质押协议，该协议让比特币持有者能够在无需信任任何第三方的情况下质押比特币；此质押“无需”将比特币跨链桥接到 PoS 链，就能为该 PoS 链提供“全面”可罚减（slashable）质押权益的安全保证。该协议支持质押权益的快速解绑（fast stake unbonding），从而帮助比特币所有者最大程度地释放流动性。不仅如此，该协议还以模块化插件的方式设计，以便其为各式各样的 PoS 共识算法所用，并为权益再质押类协议（restaking protocols）的构建提供关健要素（primitive）。我们还提出了一套系统架构—将被比特币质押所保护的巴比伦链作为控制平面（control plane），让比特币区块链与 PoS 链同步起来，使该协议具有极高的可扩展性（scalability），从而惠及千千万万权益质押者和 PoS 链。比特币权益质押孕育出新型的比特币应用案例，并在比特币网络与 PoS 经济融合的道路上，向前迈出了重大一步。

[1] 联系方式：contact@babylonchain.io。本精简版白皮书根据一篇即将发表的技术论文[9]撰写而成，该技术论文由巴比伦团队、Robin Linus（ZeroSync）和 Orfeas Stefanos Thyfronitis Litos（Common Prefix 与帝国理工学院）合作完成。

1 权益质押（PoS）的安全性依赖于资本

过去几年来，区块链行业的抗女巫攻击机制经历了由工作量证明（PoW）到权益证明（PoS）的转变。该趋势的一个决定性事件是 2022 年 9 月以太坊从 PoW 共识迁移到 PoS 共识的“合并（Merge）”。PoW 区块链由解决数学难题的矿工来保护，而 PoS 区块链的安全性则由持有权益的验证人来保障。验证人将质押权益作为“押金”，当验证人违反协议时，验证人的权益“押金”可被罚减（slash）。PoW 链不具备可罚减性（slashability），这是以太坊从 PoW 迁移至 PoS 的主要动机[18]。保障区块链安全的质押权益的总市值越大，攻击该链的成本越高，这条链的经济安全性就越强。因此，PoW 链的安全由工作量来保证，而 PoS 链的安全则通过“资本”来保障。

通常而言，吸引质押资本并非易事，特别是对于小型区块链或处于初创阶段的区块链，更是难上加难。为了吸引此类资本，区块链团队不得不采取高通胀来提供高质押收益。例如，在含有逾六十条特定应用链的 Cosmos 生态系统中，初始年化通胀率为 20% 至 100% 的情况比比皆是。此等高通货膨胀阻碍了区块链的长期发展。高成本也给链上的“效用（utility）”带来了安全压力：通货膨胀本可以用来激励链上的应用程序。

Akash[1]链便是一个很好的案例。Akash 是一条 Cosmos SDK 链（软件开发工具包区块链），运行着去中心化的人工智能（AI）计算平台。AKT 通证 100%的极高初始通胀率既用于支付安全性的保障费用，又激励了提供商出租高质量的计算硬件 [30]。久而久之，随着通胀率的下降，安全和效用之间的紧张关系变得愈加尖锐。

2 比特币：6000 亿美元的资产

尽管区块链行业经历了由 PoW 到 PoS 的转变，但比特币仍由 PoW 保护。截至本文执笔时，占加密资产总市值一半以上的比特币仍然是最大的加密货币资产。与 PoS 资产相比，比特币资产有如下显著差异：

（1）不受束缚。由于比特币的安全性由工作量保证，所以比特币资产本身并不用于保证比特币区块链的安全。相较之下，每种 PoS 资产都用于保障其自身区块链的安全。

（2）更闲置。大部分比特币资产是闲置的，且未被使用。由于大多数产生收益的活动（比如 DeFi 借贷—即去中心化金融借贷；以及安全性权益质押）都是在 PoS 链上进行的，所以想要参与这类活动并获取收益，比特币目前必须要“桥接”跨链到其他链，并/或将比特币发送到第三方中

心化机构托管。对于许多比特币持有者而言，这些桥与中心化托管机构风险太大。例如，最大的包装比特币（wrapped Bitcoin）资产之一 wBTC 的市值尚不足 50 亿 美元，仅占比特币总市值的百分之一。

（3）更去中心化。比特币，作为区块链的鼻祖，基本上可以说拥有着最去中心化的通证持有者群体：矿工、早期使用者和开发者、项目创始人、个人投资者、机构投资者、交易所等。相比之下，许多 PoS 链的资产（至少对项目早期而言），都集中在早期投资人、创始人和团队成员以及基金会手中。当资产被质押以验证区块链网络时，资产会集中起来，导致区块链网络面临中心化问题。

（4）更稳定。比特币作为最大的加密资产，其价格的波动性显著低于大多数 PoS 资产的波动性。对于 PoS 链的安全性而言，PoS 资产的波动性是一个重大问题，因为安全性是质押资产总市值的直接函数，一旦资产价值急剧下跌，攻击者将有机可乘。

3 比特币权益质押

既然比特币性质优越，何不将其质押、发挥其能，助力保证 PoS 链的安全?

“ 比特币权益质押（Bitcoin staking）“的概念便是本文工作的重点。

比特币权益质押是一个双边市场（图 1）。一方是有安全需求并愿意为此付费的 PoS 链，另一方是拥有资本并希望从中赚取收益的比特币持有者。“比特币权益质押协议 “即实现该双边市场的 ” 安全共享协议（security-sharing protocol）“。优质比特币权益质押协议应当为这两方均提供强有力的安全保证，既保证消费者 PoS 链（consumer PoS chain）的安全（以使他们愿意付费），又保证供给者比特币持有者的安全（以便他们愿意质押比特币）。

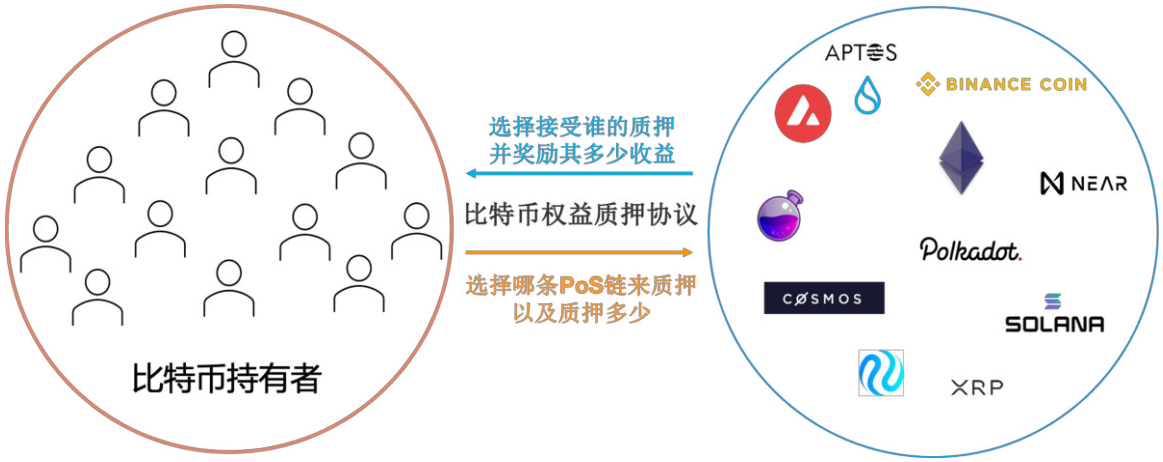

图 1. 比特币权益质押是双边市场

4 巴比伦比特币权益质押协议：安全性质

我们在此介绍一种比特币权益质押协议，该协议与现成的消费者 PoS 链结合使用，则具有三个重要的安全性质：

（1）全面可罚减的 PoS 安全性。 一旦区块链完好性遭破坏（safety violation）（如链分叉—译者注），则所质押比特币的三分之一必定会被罚减。 只要所质押比特币的三分之二诚实地遵守 PoS 协议，PoS 链就能保持良好的活性。

（2）质押者的安全性。只要诚实地遵守 PoS 协议，每一位比特币质押者都可以到期提取或提前解绑其质押的比特币。

（3）质押者的流动性。所质押比特币的解绑保证安全，并且无需社区共识、快速解除绑定。

性质 1 意味着，违反协议就会被罚减；性质 2 意味着，只有被罚减者才违反了协议。性质 1 与性质 2 结合起来，反映了 PoS 安全性的金科玉臬：全面可罚减性，这正是 Buterin 和 Griffith[18]所提倡的观点。实际上，全面可罚减性正是 PoS 以太坊的核心设计目标[19]，同时，也是 Tendermint 的核心设计目标[13,15]。Tendermint 是构建 PoS 区块链（Cosmos SDK 链、Polygon、BNB 链等）所最广为采纳的共识引擎之一。事实上，性质 2 甚至比独立的 PoS 协议更为强大：即使 PoS 链上的“所有”其他质押者都不诚实，诚实的比特币质押者仍然可以解绑其所质押的通证。提款审查制度不适用于我们的比特币权益质押协议。因此，我们的协议提供了“无需信任任何第三方的权益质押”。

像 PoS 以太坊或 Cosmos SDK 链这样的独立 PoS 链，天生自带安全性缺陷。它们受制于一种叫做”长距离攻击”的“零质押—无作恶成本（nothing-at-stake）“攻击。为抵御这种攻击，这类 PoS 链须要使用社区共识，这导致这类 PoS 链不得不将质押通证的解绑时间设置得很长（大约要几个星期） [16,21,12,22]。相比之下，我们的比特币权益质押协议是在比特币区块链上进行比特币质押分配的，因此不受此类远程攻击的影响。通过恰当地设计权益质押协议，我们证明了性质 3 是可以实现的。

5 挑战

我们考虑两种基本的比特币权益质押方法，这两种方法各自有其挑战：

（1）桥接到 PoS 链。比特币权益质押的一种方法是首先将比特币从比特币链连接到消费者 PoS 链，并在那里执行罚减规则。虽然这种方法能够为 PoS 链提供可罚减的安全性（性质 1），但从根本上却受限于桥接方案本身的安全性。现有的主流比特币桥的安全性建立在对中心化托管人（如 wBTC 之于 Bitgo）或多签桥委员会的信任之上（更多讨论请参见第 9.8 节）。即便是最完美的比特币桥也依赖于对目标链质押者的信任。因此，通过桥接解决方案，不可能实现性质 2，即无需信任任何第三方的权益质押。

（2）从比特币链进行远程权益质押。为了避免桥接比特币，另一种方法是“远程权益质押（remote staking)”：将质押的比特币锁在比特币链上的合约中，然后当质押者违反 PoS 链协议时，在比特币链上将该违反协议者所质押的比特币进行罚减。安全共享方案使用的就是这种方法，例如特征层（Eigenlayer）的以太坊权益再质押协议（Ethereum restaking protocol）[36]和 Cosmos 生态系统的网状安全（mesh security）[11,4]。在这两种场景中，供给者链（即安全源）均具有图灵完备的智能合约层。如此一来，在供给者链上实施罚减并没什么技术难度，因为违反协议规定的证据可以从消费者链发送回供给者链，并由供给者链上的智能合约完成罚减。然而，在我们的场景中，供给链是比特币链，它不支持智能合约，其脚本语言的表达能力也有限。因此，虽然我们凭借将比特币保持在比特币链上的手段实现了无需信任任何第三方的权益质押（性质 2），但现在关键的挑战是如何执行罚减，从而实现性质 1，即全面可罚减的 PoS 安全性。

我们的比特币权益质押协议遵循远程权益质押方法，但我们通过结合先进的加密技术、共识协议创新和比特币脚本语言的最优化使用，克服了比特币链缺少智能合约的挑战。在详细介绍这些技术之前，让我们首先透过质押者的视角，来对比特币权益质押协议的主要功能进行综述。

6 比特币质押者的行程

爱丽丝（Alice）有一枚比特币，她想将它质押在 PoS 链上。首先，她通过发送权益质押交易到比特币链来进入一个权益质押合约。该交易是一笔将她的比特币锁定到自我托管的金库的比特币交易。被锁定的比特币只能用爱丽丝的私钥通过下述两种途径之一解锁：

（1）爱丽丝发起“解绑交易（unbonding transaction）”，则比特币将在三日内解锁并返还给爱丽丝。
（2）爱丽丝发起“罚减交易（slashing transaction）“，将比特币发送至销毁地址。

一旦该权益质押交易进入比特币链，爱丽丝就可以开始用她的密钥签署区块以验证 PoS 链。在她的验证职责期间，有两种可能的路径。

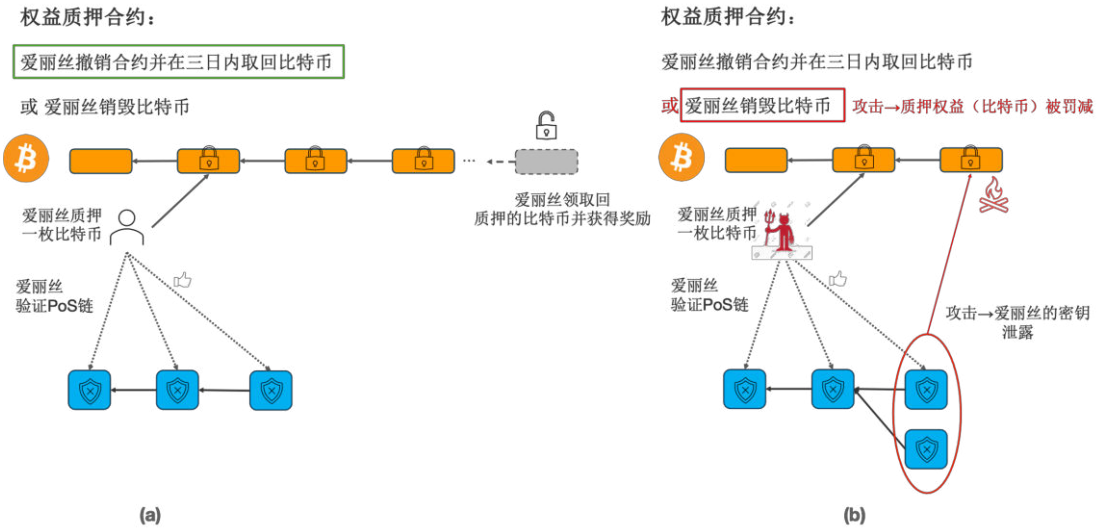

图 2：比特币质押者的行程：（a）快乐路径：爱丽丝质押比特币，验证 PoS 链，发起解绑请求，并在 3 日内解除质押；（b）不幸路径：爱丽丝质押比特币，攻击 PoS 链，然后，其比特币被销毁。

一是“快乐路径（happy path）（图 2（a））”，即爱丽丝诚实地遵循协议，而当她想要解除比特币质押时，她通过向比特币链发送解绑交易来发起解绑请求（图 2(b)）。一旦解绑交易进入比特币链，爱丽丝在 PoS 链上的验证义务就结束了，三天后，爱丽丝就可以提款并取回这枚比特币。该 PoS 链还将向爱丽丝授予奖励。

二是“不幸路径（unhappy path）（图 2（b））”，即爱丽丝变坏并参与 PoS 链上的双花攻击（完好性攻击）（图 2（c））。在这种情况下，权益质押协议确保爱丽丝的私钥将泄露于众。于是，任何人均可以爱丽丝的身份将罚减交易发送到比特币链并销毁爱丽丝那枚比特币。这条不幸路径的存在保证了攻击者必被罚减，这种震慑确保所有人都走“快乐路径“—所有人都正常运作。

7 技术要素

我们之所以能实现第 6 节所述之协议功能并攻克第 5 节所述之挑战，主要得益于以下关键要素。关于详细信息，请留意我们即将发表的完整论文[9]。

7.1 权益质押合约：通过比特币盟约模拟（Bitcoin covenant emulation）来实现

由于比特币区块链没有智能合约层，因此必须根据比特币脚本语言（Bitcoin Script）[10]里的UTXO（未花费的交易输出）交易来表达权益质押合约。每个 UTXO 交易花费的款项均来自 UTXO 集合，比特币脚本语言提供了少量操作码（opcode），以详细规定款项的使用条件。一份权益质押合约有四种交易：

- 权益质押交易，其中，质押者输入的是其比特币地址，输出（output）的花费可使用下述二种方式之一：
  - 解绑交易。该交易允许质押者在对应锁定时间（测量解绑时间）结束后再花费该输出（对应锁定时间可由操作码 OP_CHECKSEQUENCEVERIFY[10]执行）。

AN INDIVIDUAL VALIDATOR ν MUST NOT PUBLISH TWO DISTINCT VOTES,

$$\langle \nu, s_1, t_1, \mathrm{h}(s_1), \mathrm{h}(t_1) \rangle \quad \text{AND} \quad \langle \nu, s_2, t_2, \mathrm{h}(s_2), \mathrm{h}(t_2) \rangle \ ,$$

SUCH THAT EITHER:

I. $\mathrm{h}(t_1) = \mathrm{h}(t_2)$.
Equivalently, a validator must not publish two distinct votes for the same target height.

OR

II. $\mathrm{h}(s_1) < \mathrm{h}(s_2) < \mathrm{h}(t_2) < \mathrm{h}(t_1)$.
Equivalently, a validator must not vote within the span of its other votes.

Figure 2: The two Casper Commandments. Any validator who violates either of these commandments gets its deposit slashed.

图 3：Casper 的罚减条件（本图摘自[18]）

  - 罚减交易。该交易可将质押者的输出直接花费到销毁地址里（该地址的 UTXO 无法被花费）
- 解除权益质押交易。该交易可以在对应时间锁（timelock）到期后，才花费解绑交易的输出。

权益质押合约是“比特币盟约（Bitcoin Covenant） [25,26]”的一个例子，比特币盟约对如何花费交易的输出（the output of a transaction）有约束。该等盟约可通过OP_CHECKTEMPLATEWERIFY[8]执行，这是一组比特币脚本语言操作码，已有提案将其加入比特币脚本语言的下次升级中。在该升级之前，加密从业者提议了多种模拟比特币盟约的方式。我们工作的创新之一是比特币盟约模拟的新型方式，它几乎无需信任任何第三方。 有关更多详细信息，请参见[9]。

7.2 自动罚减质押的比特币—通过可问责断定（accountable assertions）与终局性小工具（finality gadget）

由于比特币没有智能合约，因此无法简单地将破坏区块链完好性的犯罪证据，发给比特币网络以期其处理该证据。我们的协议发送的证据则更加直接—直接到可以直接实现罚减：这个证据就是质押者的私钥。为了确保质押者的私钥在攻击后一定会泄露，我们结合了两种思路：（a）来自于加密学的可问责断定（accountable assertions）[32]；（b）来自于区块链共识的终局性小工具（finality gadget）[18,27,28]。

第一条思路是可提取的一次性签名（extractable one-time signature）。该签名保证了：如果签名者用同一组私钥签署两条消息，则其私钥可以通过这两个签名提取出来并导致该私钥泄露。EOTS 已被一些论文（如[32]）提议作为惩罚双关攻击（equivocation）（比如同一比特币双花）的通用方法。然而，对共识协议的罚减场景远比对双签的罚减场景复杂。例如，在 PoS 以太坊协议的可罚减性模组（the slashability module）— Casper[18]中，有两组罚减条件（图 3）。第一组罚减条件是双关攻击，即在相同高度上签名两个区块；第二组罚减条件没那么简单，无法表述为双关攻击。类似地，在 Tendermint 中，也有两组罚减条件。一组罚减条件是在同一高度、同一轮次中，签署两个区块；另一组罚减条件则来自于所谓的健忘症攻击（amnesia attacks）[14]，健忘症攻击也不能直接表述为双关攻击。

我们另辟蹊径，不改变基本共识协议本身的签名方案，而是在基础共识协议用可提取的一次性签名确定一个区块后，加入一轮新的由 EOTS 签名的投票。如果一个区块不仅由基础共识协议进行了最终确认，“还获得”超过三分之二质押权益的 EOTS 签名，则该区块被视为已真正最终确定。这轮额外签名可称为“终局性小工具[27]”—一种 EOTS 终局性小工具。我们的工作结果表明，在此修改后的协议下，如果还发生破坏区块链完好性的事件，那就说明超过三分之一的质押权益在同一高度用 EOTS 签署了两个区块[9]。这会导致这些权益质押者的私钥被提取。此外，这些 EOTS 签名方案能用施诺尔（Schnorr）签名（比特币链所使用的签名）来执行。因此，就可以用这些提取的私钥来完成削减交易。

该基于终局性小工具的解决方案，具有一个非常重要的优势，即“模块化特性（modular nature）”：它可以在所有拜占庭容错（BFT）共识协议上使用，且无需更改基础共识协议本身。这使得该项技术的应用不局限于特定的 PoS 链。

7.3 快速解绑质押的比特币—通过基于比特币的时间戳（Bitcoin timestamping）

在有着原生权益质押（native staking）的 PoS 链中，因为区块链需要社区共识来抵御远程攻击，所以质押权益的解绑耗时很长（比如，在 Cosmos 中心（Cosmos Hub）解除质押权益的绑

定需要三周）。在远程攻击中，攻击者在解绑套现后构建一条（译者注：从解除质押前的区块开始的）分叉链来代替原链，因此该攻击毫无成本。相反，对像比特币区块链这样的 PoW 链发起远程攻击，要耗费巨额成本，因为这需要花费大量的资源来构建一条更长的分叉链来代替现有的最长链。在我们的比特币权益质押协议中，由于解绑请求是提交到比特币链上的，因此，从比特币链中删除该交易将需要相当高昂的成本。这表明，我们的比特币权益质押协议可以无需社区共识，快速解绑质押的比特币。不过，问题在于，虽然质押的权益分配在比特币链上完成，但对区块的投票却是在 PoS 链上进行的。攻击者可以减缓 PoS 链的出块速度，造成由已解除了质押的那部分过期（out-of-date）质押者集合（staker set）来校验 PoS 区块。这意味着攻击者可以在比特币链上取消质押，却仍然拥有分叉 PoS 链的投票权。即使质押者的私钥被泄露，但想要罚减其质押资产也为时已晚，因为质押者已经在比特币链上解除了质押。

为了避免这种攻击并实现质押通证的快速解绑，PoS 链应当与比特币链紧密同步。这可以通过一种称为“基于比特币的时间戳（Bitcoin timestamping）”的技术来实现，将 PoS 区块的哈希值和参与其投票的质押者集合的信息记录在比特币上。有意思的是，这种基于比特币的时间戳的技术，也能非常有效地对有着原生权益质押的 PoS 链实施完好、快速的质押权益解绑[35]。我们正在重新定位这项技术，以实现在比特币权益质押协议下，能快速解除绑定。

8 系统架构

基于上述关键要素，比特币权益质押协议的核心基础设施是比特币链与 PoS 链之间的控制平面（图 4）。该控制平面负责多种关键功能，包括：

- 为 PoS 链提供基于比特币的时间戳服务，使 PoS 链与比特币链同步；
- 运行市场，匹配比特币质押权益和 PoS 链，并追踪权益质押和验证信息（例如，EOTS 密钥注册与刷新）；
- 记录 PoS 链的终局性签名。

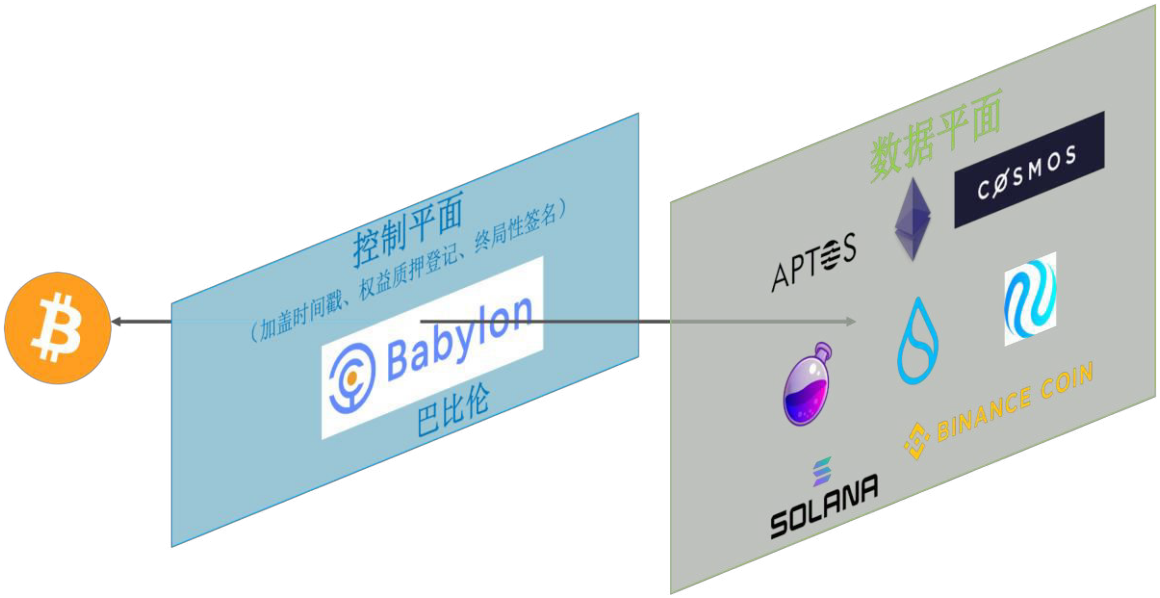

图 4：由控制平面与数据平面组成的系统架构

另一方面，除了生成区块和验证区块这些基础的共识协议的工作之外，每条 PoS 链的验证人还在终局性小工具上签署终局性签名。这些校验者共同运行该架构的数据平面。

控制平面以链的形式实现，以确保其去中心化、安全、抗审查和可扩展。例如，比特币链网络的区块空间有限且价格昂贵，这使得每个 PoS 链无法可持续、可扩展地直接在比特币链上加盖时间戳，这给比特币权益质押的采用造成了困难。为了解决这一问题，巴比伦团队设计了一套安全的基于比特币的时间戳协议，并通过基于 Cosmos SDK 的巴比伦链来实现。通过标准的 IBC（区块链间通信）协议，巴比伦链能够高效地聚合任意数量 Cosmos SDK 链的时间戳。巴比伦链的测试网于 2023 年 2 月首次推出，至今已集成了不同垂直领域的逾 30 个 Cosmos SDK 链（图 5）。

于是，这就形成了一个三层架构，其中，巴比伦链充当控制平面，实现比特币链与数据平面（即 PoS 链）之间的交互。这种架构还可以带来网络效应并发挥互操作性的潜能。例如，可以根据巴比伦链上两条 PoS 链的终局状态（finality status），来结算巴比伦链上的跨 PoS 链交易。

9 相关工作成果

9.1 跨链权益质押、权益再质押与网状安全

图 5：基于比特币的时间戳测试网与 31 条基于 IBC 的区块链

现有的每条 PoS 链均由该链账本里的原生资产保障链的安全。例如，PoS 以太坊由以太币（ETH）保障安全、Cosmos 中心由阿童木（ATOM）保障安全，BNB 链由币安币（BNB）保障安全。然而，仅依靠原生通证来保障 PoS 链的经济安全，则其安全程度无法突破原生通证总市值的上限。用“远程“加密资产的权益质押，来“替代”或助力 PoS 链的原生资产，可以通过增加质押资产的总市值来增强该链的安全。最近涌现了一种方法，称为“跨链权益质押（cross-chain staking）”：被质押的外来资产还是存储在其原本自己的链上，但它们是锁定在权益质押合约中的，并将权益委托给目标链的特定验证者。当且仅当该校验者犯下可罚减质押资产的过错时，该质押资产即被罚减。这是 Cosmos 生态系统的“网状安全”概念提案背后的思想[11,4]。一条 Cosmos

应用链（供给者链）的资产可以“跨链质押”，从而帮助另一条 Cosmos 应用链（消费者链）增强安全。该跨链权益质押协议则是受到了特征层（Eigenlayer）的以太坊权益再质押概念的启发而创作的[36]。该权益再质押的思想，是将质押在 PoS 以太坊链上的以太币再质押，从而利用特征层（Eigenlayer）网络来保障中间件（所谓的 AVS，即积极验证系统，比如数据可用性层、桥、预言机服务等）的安全。这些项目促进了 PoS 广义形式的诞生，于是，加密资产可用于保护各种区块链及服务，而不仅仅是保护其原生链。

我们的比特币权益质押协议可视为跨链权益质押协议的一个用例，但与 Cosmos 的网状安全和以太坊的权益再质押有两个重要区别。首先，在以太坊的权益再质押和 Cosmos 的网状安全中，资产已经被质押以保证供给者链的安全。相较之下，在我们的比特币权益质押协议中，比特币的安全不是由比特币资产本身，而是由 PoW 机制来保证的，因此，比特币资产不受束缚。这减少了权益再质押有可能导致的过度杠杆风险[17,36]。其次，比特币区块链没有智能合约来执行质押权益的罚减。取而代之的是，我们将比特币脚本语言使用到了极致，并使用先进的加密机制来实现相同的目标。

9.2 可问责性与可罚减性

许多 PoS 链都有一重要性质，即它们都可以将违反协议者以可证明的方式绳之以“码”[18,20,33]。由于 PoW 链的矿工没有链上身份，因此 PoW 链不具备该性质。实际上，“可问责的完好性（accountable safety）”这一性质（即当区块链完好性遭破坏时，有能力对三分之一的校验者实施问责并惩罚）是 PoS 以太坊链的设计核心[18,20]。然而，在可问责性与链上罚减之间还存在一道鸿沟—即依据破坏者对区块链协议的违规证据，在链上对破坏者的质押权益实施实质性的罚减。尤其是当链的完好性被侵犯时，说明该链已经有超过 1/3 的恶意校验者了。因此，这些恶意校验者拥有足以阻止证据上链的投票权，并可以藉此阻止罚减。在这种情况下，必须在区块链之外执行复杂的社区共识流程，以便能够罚减违规者的质押权益，并将其踢出校验者集合，其余这些诚实的验证人随即重启区块链[35]。相比之下，我们的比特币权益质押协议不会为此问题所困，因为质押的比特币是在比特币链上，而不是在 PoS 链上的，所以，一旦 PoS 链的完好性遭破坏，比特币质押权益当即被自动罚减。

9.3 可问责断定与 Stakechain

用可提取的一次性签名来惩罚双关攻击—这一总体概念起源于[32]。该工作中，分布式协议中的一方当事人如果想要做出“可问责断定”，需满足一先决条件，即比特币链上必须有一笔被“时间锁（time-lock）”锁住的该当事人的存款。每当该方当事人对同一环境做出了两个不同的断定，则其私钥就被泄露，任何人均可用其私钥来提款。[24]在此概念的基础之上，创建了一条由比特币

支持的 PoS 侧链。然而，该文作者提出的 PoS 协议在每一个区块高度，仅涉及一个投票阶段。虽然这样可以将破坏区块链完好性的行为，直接设计为相互矛盾的两个可问责断定（将区块高度作为一个环境，并将破坏区块链完好性视为一同一高度的两个区块上的双关攻击），但即便攻击者只质押了很少权益，该协议也毫无活性。相反，已知的拜占庭容错协议的设计均以“多个”投票阶段来确保协议的活性。相比之下，我们并不试图从头开始设计一套 PoS 协议，而是将比特币权益质押协议与任意 PoS 共识协议“结合起来”，作为附加的终局性小工具来使用。这就保证了，只要底层共识协议是有活性的，那么整个协议就有活性；同时，可罚减性也得以实现，因为所有对完好性的攻击都是用 EOTS 在终局性小工具上对同一区块高度签名二次的双关攻击。此外，我们的协议中的存款合约允许质押者（在一定的延迟后）随时按需提取资金，而[32]中的合约规定存款必须是定期存款。

9.4 终局性小工具

从广义上讲，可以将终局性小工具视为覆盖协议（overlay protocol），它在已有的共识协议之上使用，从而提供额外的安全保证。首个终局性小工具是 Casper FFG[18]，用于最长链协议以保证网络分区下的区块链完好（这是最长链协议自身所不具备的安全特性）。另一个终局性小工具是波卡（Polkadot）的“祖父（GRANDPA）”[34]。PoS 以太坊的信标链共识协议 Gasper[19]使用 Casper FFG 作为 LMD（最新消息驱动）幽灵协议（GHOST protocol）的终局性小工具。然而，[27]表明，Gasper 的活性容易遭到攻击。首个被正式证明可以确保安全的终局性小工具结构是快照协议（the snap-and-chat protocol）[27]。[28]提出的可问责性小工具（accountability gadget）让最长的区块链协议具有额外的可问责性质。我们的比特币权益质押协议的 EOTS 终局性小工具结构遵循类似的理念。它将比特币质押的可罚减性质添加到现有的拜占庭共识协议中。

9.5 比特币合并挖矿（merge mining）

合并挖矿是第一个共享比特币安全的技术，由中本聪（Satoshi Nakamoto）发明于 2010 年。它用以保证比特币链的首个侧链—域名币链（Namecoin）的安全。目前，由合并挖矿支持的最大的比特币侧链是根砧木链（Rootstock）[5]。使用合并挖矿技术，比特币矿工可无需耗费额外资源，即可在比特币链和另一条 PoW 链上同时挖矿。然而，作为安全共享协议，合并挖矿受到“零质押—无作恶成本”问题的威胁：基本上，矿工可以一边诚实地在比特币链上挖矿，一边攻击其侧链。由于比特币是矿工的主要收入来源，因此在侧链上，对作恶行为可能缺乏足够的威慑力。相比之下，有了比特币权益质押，则币网恢恢疏而不漏：PoS 链上的作恶者将自取其咎，其质押权益被罚减。因此，比特币权益质押是一种比合并挖矿强大得多的安全共享技术。

9.6 基于比特币的时间戳

另一项共享比特币安全的技术是加盖时间戳[35]：将 PoS 区块的哈希值与签名作为交易提交并记录到比特币链上。这给 PoS 区块提供了一层额外的排序层，可在 PoS 链出现分叉时用以打破僵局。该技术是巴比伦基于比特币的时间戳测试网的基础。因为比特币需要很长时间来确认交易，因此在比特币链上安全记录这些时间戳是一个缓慢的过程。因此，基于比特币的时间戳可以有效提供远程安全性—比如抵御远程攻击。相比之下，比特币权益质押增强了 PoS 链的经济安全，从而保护其免受短程攻击。此外，如前所述，基于比特币的时间戳也是比特币权益质押协议不可或缺的一部分，起到同步 PoS 链与比特币链的作用。

9.7 转账证明（Proof-of-transfer）与堆栈区块链（Stacks）

堆栈区块链团队[7]开发了一套转账证明（PoX）共识机制，在该机制下，矿工们通过将比特币发送到比特币链上的特定地址，来相互竞争成为下一个区块的提议者，发送的比特币数量越多，机会就越大。该机制与 PoS 协议有着根本上的不同，所以可罚减性与质押者的安全性质并不适用于堆栈区块链的 PoX 机制。

尽管如此，为了将比特币与堆栈区块链桥接起来，以便堆栈区块链的智能合约能够访问比特币资产，堆栈区块链团队提出了一种铸造并销毁 sBTC（一种合成比特币通证）的方法，该通证的安全由 STX 通证质押者（称为“堆栈者（Stackers)”）保障[6]。堆栈者作为 70%阈值签名组，承担两项职责：（1）sBTC 的铸造与赎回；（2）批准已经最终确定的堆栈账本的分叉。因此，倘若超过 30%的堆栈者是诚实的，那么 sBTC 桥的安全性就是完好的；如果不少于 70%的堆栈者诚实地签署交易，则 sBTC 桥就是具有活性的。与堆栈区块链（Stacks）相比，我们的一大关键优势是：我们做到了无需跨链桥接的比特币原链质押，而比特币桥的安全程度通常受限于该桥项目所发行的通证的整体锁定资产价值。

与堆栈区块链相比，我们的比特币权益质押协议不需要花费比特币，而是将比特币质押保存起来，只要不发生破坏区块链协议安全的事件，就不会罚减这些比特币。这让安全应用程序能够更高效、更有扩展性地利用资产。

9.8 比特币桥接

从广义上讲，当今的比特币桥分为三类：中心化的、基于抵押品的和基于侧链的，还有硬件解决方案所提供的潜在安全强化（potential security hardening）。我们撇开了原子性互换（atomic swap）不谈，因为它们尚未被主流的比特币桥采用，这可能是由于其在可用性、延迟和流动性获取（liquidity sourcing）这几个方面的挑战。

中心化桥由其用户信任的中心化机构运行，一个典型的例子便是中心化交易所，中心化交易所允许用户从其他链存入比特币及其包装通证（wrapped tokens），并提取到任何这类受支持的链上。例如，币安的用户可以将其原生比特币存入其币安账户，然后提取 BNB 链上的包装比特币通证。另一个例子是 wBTC，其中 Bitgo 担任原生比特币的托管人[37]。这些解决方案必须满足非常强的前提假设，即其中心化机构要么不故意制造伤害，要么在他们遭受攻击时，充分补偿用户的损失。

Interlay 是一种通过超额抵押金库将比特币引入波卡生态系统的解决方案，该金库提供比特币锚定（在收到原生比特币时，创建包装比特币）和脱锚（在销毁包装比特币后，赎回原生比特币）的功能[23]。此处有一个关键点，就是要在安全（即提高抵押率，以防金库作恶并窃取比特币）与容量（桥接的比特币的数量受到抵押币数量及抵押率的限制）之间求得平衡。同样，堆栈区块链团队在其中本升级”Nakamoto upgrade”[7]中提出的 sBTC[6]要求“堆栈”STX 通证持有者在堆栈区块链上，集体执行比特币与 sBTC 通证之间的锚定与脱锚操作。

还有一种桥是 Nomic，Nomic 是基于 Tendermint 的区块链，它提供了一种将比特币桥接到 nBTC 的方法，nBTC 进而可以通过 IBC（区块链间通信协议）[3]用于 Osmosis 及其他 Cosmos 区域（Cosmos Zones）[29]。这种桥接解决方案的局限性在于，桥接通证的整体安全取决于 Nomic 链的安全性，并且大体上也受到 Nomic 链的总质押价值的限制。类似地，根砧木链在其矿机上运行比特币轻客户端，并依赖后者，在其链上将原生比特币与合成比特币通证锚定与脱锚[5,31]。如果不考虑由硬件提供的额外安全性（如下文所述），其包装比特币通证的安全性与根砧木链的 PoW 链的安全性相当。

此外，名为 PowerPeg[31]的根砧木链的比特币锚定机制，利用安全硬件来加强比特币锚定的安全性。Avalanche 的比特币桥通过运用英特尔 SGX（Intel SGX），也采用了类似的基于硬件的安全增强解决方案[2]。原则上，使用硬件信任根（root of trust）可以减少此类桥的受攻击面，尤其是代码正确性可被实时验证的情况下。然而，在实践中，我们也需要考虑软件安全因素：（a）假如安全硬件内部运行的桥接逻辑依赖于从外部源所获取的关键信息，则会降低该桥的安全性，以致于其安全性与该外部组件的安全性相同；（b）假如安全硬件内部运行的代码存在安全漏洞，则该硬件提供的安全性增加方案可能会失效。

正如我们之前所言，比特币桥普遍都存在一个关键的风险：包装比特币通证的可赎回性风险。这是由于该可赎回性由一条远不如比特币链安全的区块链保证。幸运的是，我们不要求锁定的比特币具备完全的可转账性，比特币权益质押就足以保证外部链和系统的安全。我们提出的比特币权益质押方案，限定了对锁定的比特币的花费操作，使之仅用于对破坏区块链完好性的违规者进行质押

权益罚减，从而规避了主流比特币桥面临的安全及容量挑战。因此，我们的方案提供了第 4 节中所述之强有力的完好性保证。

10 结论

比特币是第一条区块链，且就总市值而言仍是顶级区块链。然而，除了价值存储之外，其效用却受到了比特币区块空间小、延迟高和可编程性不强所限制。特别是，区块链从业者也曾努力通过构建侧链及其他第二层项目来扩展比特币链、拓宽其使用范围，却因无法将大量的比特币桥接到这些链上，而步履维艰。这些桥要么受到安全性的限制，要么受到容量的限制，要么兼而有之。

我们的工作为比特币资产带来了史无前例的重要用例：通过质押比特币，为 PoS 世界提供安全。我们证明了，至少在此用例中，无需将比特币资产桥接至其他区块链，仍可为 PoS 链提供全面的经济安全。要实现这一突破，最大的挑战是能够在没有智能合约的比特币链上，对一切破坏区块链完好性的违规者的质押权益实施远程罚减。我们将四个概念融合到单个协议中，从而实现了这一目标：

（1）“可问责断定”，让实施双关攻击者的私钥泄露；

（2）“终局性小工具”，将所有破坏区块链完好性的行为转化为可问责断定的双关攻击；

（3）“比特币盟约模拟”，确保私钥一旦泄露，资金强制销毁；

（4）“基于比特币的时间戳”，在质押者解除质押之前确保完成罚减交易。

我们的结构是模块化的，可以适用于所有的 PoS 共识协议。实施我们的比特币权益质押协议，不需要对比特币链实施软分叉或硬分叉。

近来，比特币生态诞生了诸如 Ordinals 此类新用例，比特币实现了某种意义上的复兴。我们相信，比特币权益质押的用例将为此次复兴增砖添瓦，助其大放光明，并激励 Web3 从业者在巨大的比特币资产中，努力找到更多无需信任任何第三方的用例。

生于比特币，用于比特币，留于比特币。

11 致谢

本精简版白皮书由巴比伦团队、Robin Linus（ZeroSync）和 Orfeas Stefanos Thyfronitis Litos（Common Prefix 与帝国理工学院）共同合作完成。我们在 2023 年迈阿密比特币大会上会见了 Robin Linus，他向我们介绍了他的项目 Stakechain。当时，我们已经在紧锣密鼓地在进行着比特币权益质押的工作了，于是，我们决定一起合作完成这项工作。

参考文献

[1] Akash 网络. https://akash.network/. 访问: 2023-07-10.

[2] Avalanche 桥如何工作？. https://support.avax.network/en/articles/6349640how-does-the-avalanche-bridge-work.

[3] 区块链间通信协议. https://ibcprotocol.org/.

[4] 网状安全. https://github.com/osmosis-labs/mesh-security.

[5] Rsk. https://www.rsk.co/. 访问: 2021-11-3.

[6] SBTC：一种无需信任任何第三方的比特币双向锚定机制的设计. https://stx.is/sbtc-pdf.

[7] 堆栈：使能智能合约的比特币层. https://stx.is/nakamoto.

[8] Bip 119: OP_CHECKTEMPLATEVERIFY, 2023. https://github.com/bitcoin/bips/blob/master/bip0119.mediawiki.

[9] 比特币权益质押. 正在撰写中, 2023.

[10] 脚本语言, 2023.

[11] Sunny Aggarwal. 在“Cosmoverse 2022 大会“关于网状安全的讲话. https://youtu.be/Z2ZBKo9-iRs?t= 4937.

[12] Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. 咬尾蛇创始记（Ouroboros Genesis）：具有动态可用性的可组合 PoS 区块链. 计算机与通信安全大会, CCS '18, 第 913–930 页. 计算机协会（ACM）, 2018.

[13] Ethan Buchman. Tendermint：区块链时代的拜占庭容错. 博士论文, 圭尔夫大学, 2016.

[14] Ethan Buchman, Rachid Guerraoui, Jovan Komatovic, Zarko Milosevic, Dragos-Adrian Seredinschi, and Josef Widder. 重温 Tendermint：设计的权衡、可问责性与实践中的使用. 可信系统与网络（DSN）（增刊), 第 11–14 页. 国际电气电子工程师协会（IEEE）, 2022.

[15] Ethan Buchman, Jae Kwon, and Zarko Milosevic. 拜占庭容错共识的最新闲言碎语. *arXiv* 预印本 *arXiv:1807.04938*, 2018.

[16] Vitalik Buterin.权益质押证明：我如何学会爱上弱主观性, 2014.

[17] Vitalik Buterin. 不要让以太坊共识超载. 可在此阅览: https://vitalik.ca/general/2023/05/21/dont_overload.html, 2023 年 5 月.

[18] Vitalik Buterin and Virgil Griffith. Casper – 友好的终局性小工具. *arXiv:1710.09437*, 2019.

[19] Vitalik Buterin, Diego Hernandez, Thor Kamphefner, Khiem Pham, Zhi Qiao, Danny Ryan, Juhyeok Sin, Ying Wang, and Yan X Zhang. 将“幽灵”与 Casper 结合起来. *arXiv:2003.03052*, 2020.

[20] Vitalik Buterin, Diego Hernandez, Thor Kamphefner, Khiem Pham, Zhi Qiao, Danny Ryan, Juhyeok Sin, Ying Wang, and Yan X Zhang. 将“幽灵”与 Casper 结合起来. *arXiv preprint arXiv:2003.03052*, 2020.

[21] Phil Daian, Rafael Pass, and Elaine Shi. 白雪公主：坚决可重构的共识和应用程序—可证实地保证 PoS 安全. 金融加密学与数据安全. FC '19, 第 23–41 页. 施普林格（Springer）, 2019.

[22] Evangelos Deirmentzoglou, Georgios Papakyriakopoulos, and Constantinos Patsakis. 关于 PoS 协议远程攻击的调研. *IEEE Access*, 7:28712–28725, 2019.

[23] Interlay 实验室. Interlay 第二版：比特币金融，无银行账户. 2023 年 2 月. https://gateway.pinata.cloud/ipfs/QmWp62gdLssFpAoG2JqK8sy3m3rTRUa8LyzoSY8ZFisYNB.

[24] Robin Linus. Stakechain：基于比特币的 PoS, 2021 年 12 月. https://coins.github.io/stakechains.pdf.

[25] Gregory Maxwell. 使用 SCIP 签名的币盟约, 一种可笑的坏主意, 2013. https://bitcointalk.org/index.php?topic=278122.0.

[26] Malte Moser, Ittay Eyal, and Emin Gun Sirer. 比特币盟约. 金融加密学, 2015.

[27] Joachim Neu, Ertem Nusret Tas, and David Tse. 潮起潮落（ebb-and-flow）协议：可用性-终局性两难困境的解决方案. 安全与隐私研讨会, S&P '21. IEEE, 2021.

[28] Joachim Neu, Ertem Nusret Tas, and David Tse. 可用性-可问责性两难困境及其（利用可问责性小工具的）解决方案. 金融加密学, 2022.

[29] Nomic. Nomic 比特币桥. https://www.nomic.io/.

[30] Greg Osouri and dam Bozanich. Akt: Akash 网络通证的挖矿经济学, 2020 年 1 月. https://ipfs.io/ipfs/QmdV52bF7j4utynJ6L11RgG93FuJiUmBH1i7pRD6NjUt6B.

[31] 根砧木链. Powpeg: 创建最安全、无需许可且不可审查的比特币锚定. https://dev.rootstock.io/rsk/architecture/powpeg/.

[32] Tim Ruffing, Aniket Kate, and Dominique Schröder. 骗子、骗子、币失火啦！通过扣除比特币来惩罚双关攻击. 第二十二届 ACM SIGSAC 计算机与通信安全会议记录, CCS '15, 第 219–230 页, 美国，纽约，2015. 计算机协会.

[33] Peiyao Sheng, Gerui Wang, Kartik Nayak, Sreeram Kannan, and Pramod Viswanath. 拜占庭协议取证技术. 计算机与通信安全会议（CCS）, 第 1722–1743 页. 计算机协会, 2021.

[34] Alistair Stewart and Eleftherios Kokoris-Kogia. 祖父：一种拜占庭终局性小工具. *arXiv:2007.01560*, 2020.

[35] Ertem Nusret Tas, David Tse, Fisher Yu, Sreeram Kannan, and Mohammad Ali Maddah-Ali. 由比特币增强的 PoS 安全：可能与不可能. IEEE 安全与隐私研讨会. IEEE, IEEE, 2023.

[36] 特征层项目团队. 特征层：再质押的联合组织. https://docs.eigenlayer.xyz/overview/ whitepaper.

[37] WBTC. 包装比特币（wbtc）. https://wbtc.network/.