Core 链: 解锁比特币 DeFi

Core 链是第一个与比特币高度对齐的EVM区块链，旨在互補比特币的同时作为其具备高扩展性的智能合约平台。Core 链的主网推出了 Satoshi Plus 共识，通过结合委托工作证明（DPoW）和委托权益证明（DPoS），将比特币的矿工和矿池纳入了安全、可扩展的智能合约平台中。在未来几个月内，Satoshi Plus 共识将迎来第三个要素，即“非托管比特币质押”，任何比特币持有者均可以在不放弃自托管的情况下，通过质押其持有的比特币来获得收益。[1]

此外，Core 链正在实现与比特币网络、 EVM 链之间的无信任原子交换。整体还有 Core 原生的打包比特币（coreBTC）和其他比特币相关的基础设施改进。这将促进比特币 DeFi（BTCFi）生态系统的发展，而比特币网络将会是主要的受益者。目前有约**1**万亿美元的比特币等待通过**BTCFi**解锁。[2]

从本质上讲，区块链可以被描述为一种网络，该网络通过调整激励来管理系统或系统的安全性。各种区块链都是为不同的目的而设计的；一些专注于处理每秒数千次的交易，一些用于保护广泛的数据库，许多还用于促进智能合约，这些都为区块链网络的运营添加了复杂的层次。

比特币区块链是由利益一致的相关方所组成的网络，他们负责保护比特币资产的安全。通过其日常维护活动，比特币矿工、节点、用户等组成了使比特币具备类似于数字黄金的基本特性——硬度（有限供应）、去中心化、永恒性、透明性、抗审查性和无需许可性。

基于比特币作为完美类黄金价值储存的重要性，该网络在协议层面有着故意的限制以最大化实现其可保存性和永久性，而不是追求可扩展性。这些内在限制影响了比特币的速度、复杂性、可组合性、互操作性和灵活性。举个例子，比特币并不原生支持图灵完备的智能合约，而这些智能合约构成了 EVM 兼容区块链上的 DeFi 生态系统。尽管有时候比特币的简单性被认为是一种弱点，实际上它是协议的核心优势。

在已经提出的比特币协议演进中，其中一个有价值的研究案例是扩大比特币区块大小的争论，被称为“区块大小战争”。尽管其旨在将比特币扩展为一个可行的支付网络，扩大比特币的区块大小可能导致中心化，因为能负担全节点所需的存储、带宽和处理能力的参与者会更少。因此，比特币现有的区块大小其实是引导去中心化的利益相关方保护比特币资产的激励措施之一。

---

[1] 按照标准用法，大写“B”的“比特币”一词指的是整个网络，小写“b”的“比特币”指的是数字资产。
[2]这些数字于 2024 年 2 月 13 日从 https://bitcoinlayersreport.com/ 中提取（报告必须下载）。

尽管点对点的交易能力至关重要，但比特币的角色并不是为了满足全球所有的支付需求，而是为了保护比特币作为去中心化的价值储存[3]。其他非核心功能的建设都是次要的。任何无法帮助比特币网络参与者保持利益一致（以保留比特币基本特征）的扩展解决方案，最多只能算是中性的。

尽管比特币的区块大小最终保持不变，但支持更大区块大小的人仍然将协议分叉成了比特币现金(Bitcoin Cash)。尽管比特币现金在速度和成本方面取得了成功，但在去中心化共识、激励对齐和可持续性方面却失败了。最终，通过竞争安全预算资源，比特币现金成为了一种寄生虫威胁，尽管无能为力，但却可能稀释其自身和比特币的价值。为了实现比特币网络从未想要优化的一个功能，抛弃了构成比特币价值的基石，比特币现金是在试图把一个方形的木楔塞进一个圆孔。

从中可以反思什么？提升比特币的效用和性能需要有不改变基础层的解决方案。比特币第二层解决方案，如侧链、通道和状态链，是通过直接构建在比特币之上来实现可扩展性的。例如，闪电网络的设计是用来支持更快和更经济的交易的第二层解决方案。尽管它成功地提供了更快和更便宜的交易，但操作上的复杂性、资本效率、流动性问题和其他技术障碍阻碍了它被大规模采用的突破口，这样的情况也这正如许多人所设想的那样。

正如这个例子所说明的，直接在比特币之上构建意味着继承了它的许多局限性。其结果通常是在应用场景方面缺乏复杂性，而在用户和开发者体验方面过于复杂。

鉴于闪电在构建全球支付平台上的困难，比特币成为可扩展的基础层以用于虚拟机、智能合约等复杂功能的前景变得更加艰巨。但是，像 Stacks 和 Rootstock 等项目已经在比特币之上引入了智能合约。这些方法确实打开了提高效用的大门，但最终面临着类似的继承限制。

在设计一个通过比特币来保障安全的最佳智能合约平台时，关键的继承不是比特币基础层的刚性技术基础设施，而应当是激励对齐且利益一致的相关方组成的网络。总结来说，这些事实都表明，解锁比特币 DeFi 的关键在于将比特币的激励对齐从比特币资产拓展到智能合约平台。

Core链就是这样一个智能合约平台。通过平行且共生的共识模型 Satoshi Plus，它将两个链的权益持有者的利益保持了一致。中本聪共识和 Satoshi Plus 共识共同加强彼此，同时分别捍卫比特币资产和基于比特币的智能合约。

[3] 在情况中，即使增加块大小一百倍，也不足以使其成为大规模支付网络。

Core 链如何运作？

Core 链的设计旨在实现多个目标，其中包括：

- 利用比特币来保护一个去中心化、无需许可、无信任、抗审查、自主运转、图灵完备且多用途的区块链。
- 将比特币的治理、激励对齐和保护扩展到以太坊虚拟机兼容的智能合约。
- 通过让比特币利益相关者轻松接入由比特币保障安全、与比特币对齐且高度可扩展的智能合约平台的，解锁比特币 DeFi。
- 通过委托工作证明技术，让矿工的哈希算力实现再利用，为他们提供日益需要的额外奖励。
- 利用非托管质押等机制，将比特币从被动资产转化为生产性资产（而不占用新的区块空间），从而使比特币能够支持更多的应用场景的同时强化其核心功能。

这些愿景的核心在于 Core 链独特的 Satoshi Plus 共识机制，其两个基本组成部分分别是利用了比特币矿工哈希算力的开创性委托工作证明技术，以及区块链领域广为人知的委托权益证明。在接下来的几个部分，将更详细地介绍这些主题。

委托工作证明（DPoW）

比特币网络是世界上最为去中心化和安全的网络，这在很大程度上要归功于比特币矿工的工作以及引导他们将物理能量转化为数字黄金的激励机制。有了 Core 链，这些激励得以扩展并支持一个多用途的智能合约平台。这不需要矿工在保护比特币资产而进行的最重要的工作之外增加任何额外的成本或复杂性。相反，矿工可以获得额外的补充奖励，从而进一步激励比特币挖矿。

要参与保护 Core 链，矿工只需在生成新的比特币区块时在 `op_return`字段中写入两个额外的信息：
1. 矿工委托哈希算力的 Core 验证节点的地址。
2. 矿工希望 CORE 代币奖励发送到的地址。

矿工通过委托他们的哈希算力为 Core 验证节点投票，以此参与共识。矿工除了获得既得的比特币奖励外，还会获得额外的 CORE 代币奖励。因此，Core 链与比特币是完全共生的。Satoshi Plus 获得了比特币矿工的参与，而比特币则获得了报酬更高（即更有动力）的矿工。

委托权益证明（DPoS）

Satoshi Plus 在一定程度上基于这样一个认知：Core 链的用户必须与比特币利益相关者一起参与共识过程。委托股权证明是实现这种平衡的方法。为了参与共识，任何 CORE 代币持有者都可以将他们的 CORE 代币质押给 Core 验证节点，从而为这些验证节点投票，就像矿工可以委托其哈希算力为验证节点投票一样。

同样，就像矿工会获得奖励，CORE代币的质押者也会因为对 Satoshi Plus 共识的贡献而获得 CORE 代币奖励。委托权益证明与标准的权益证明模型相比，前者的优势是允许所有代币持有者平等参与，而后者有时只允许大额持有者质押。

是什么让 Core 链与众不同？

在介绍了 Core 链的基本操作以及它在构建基于比特币的 DeFi 生态系统方面的独特优势的情况下，下一个主题是讨论 Core 链与具有类似愿景的其他协议有何不同。

Stacks

Stacks 是一个比特币第二层协议，旨在将来自于DeFi 生态系统的一些更广泛的想法引入比特币。尽管这个目标值得赞扬，但 Stacks 缺乏EVM兼容性是一个关键的缺陷。想要在 Stacks 上构建的以太坊开发者必须学习一种全新的语言，而这种语言既不是图灵完备的，也不可移植到其他生态系统。而在构建 Core 链时，这些开发者不会面临这样的障碍。

此外，Stacks 的区块时间目前较长且难以预测；Stacks 链上的每秒交易量并不令人满意，这进一步阻碍了其使用。尽管通过 Nakamoto 升级将在区块生产和吞吐量方面进行改进，但即使如此，Core 链在这两个领域仍具有竞争优势。

Rootstock

Rootstock 是一个 EVM 等效链，旨在通过创建去中心化应用程序等用例来作为一个支持比特币 DeFi的智能合约平台，这些用例在比特币第一层都不太适用。到目前为止，Rootstock 相对无法吸引到有意义的开发群体和用户基础。此外，由于 Rootstock 是 EVM 等效而不是EVM兼容，开发者在其上构建时面临更多挑战。

有关 Stacks 的一些评论也适用于 Rootstock，因为 Core 链的区块时间是其十倍快，每秒交易量是 Rootstock 理论数量的数倍。

Botanix

通过其 Spiderchain 原语，Botanix 希望将以太坊虚拟机的优势带到比特币。但与 Rootstock 一样，Botanix 是 EVM 等效而不是 EVM 兼容，这意味着开发者在使用它进行构建时会面临额外的挑战。

更广泛地说，Botanix 是高度实验性和未经验证的。它依赖于多重签名（multisig）结构，这是一种新的信任假设。正如 Liquid 项目所展示的，这是广泛采用的一个挑战。

最后，由于缺乏实际测试，很难确定这些假设是否能经受住真实挑战的考验。Botanix 的理论区块时间和每秒交易量是否能够与 Core 链设定的标准相匹配，还有待观察。

Sovereign Rollups

由 Chainway 和 Rollkit 等提供者开创的 Sovereign Rollups（SRs）通过使用独立的共识机制在链下处理交易，并通过利用比特币的数据可用性将这些交易的摘要或证明锚定到比特币区块链上，从而提高了交易吞吐量和智能合约功能。

在当前状态下，这些链下执行没有欺诈证明，支持 SRs 的单一顺序模型所依赖的假设可能破坏加密爱好者所珍视的去中心化。目前尚不清楚这些 “MEV” 机会在上线后是否会被利用。

最后，它们依赖于在比特币协议中引入新的操作码(op_codes)，而不能确保这样的代码会出现。从历史上看，对比特币进行任何改动都被证明非常困难，这对于这些新的提议可能也是如此。

Babylon

Babylon 是一个比特币再质押协议，允许用户在不使用桥接或依赖受信任的中介的情况下对闲置的比特币进行质押，并以此交换替代币的收益。Babylon 将实现 Core 链旨在实现的部分目标（即通过非托管比特币质押实现），然而，其目标并非创建由比特币支持的 DeFi 生态系统。

此外，Core链的 Satoshi Plus 共识机制可以实现再质押。在未来的更新中，Core 链可能会支持比特币质押者和比特币矿工在其治理中发挥作用，这又将进一步区分这两种协议。

Core 链如何实现比特币去中心化金融（DeFi）？

尽管比特币在金融领域具有显著地位，但迄今为止，它一直是一种未开发的、被动的资产。扩展其效用和互操作性一直是一项艰巨的任务，但近期在质押、封装和交换方面的进展终于打开了这些领域的大门。

接下来的几个部分将讨论这些技术在 Core 链上的实施，它们的工作原理以及它们的重要性。

非托管比特币质押

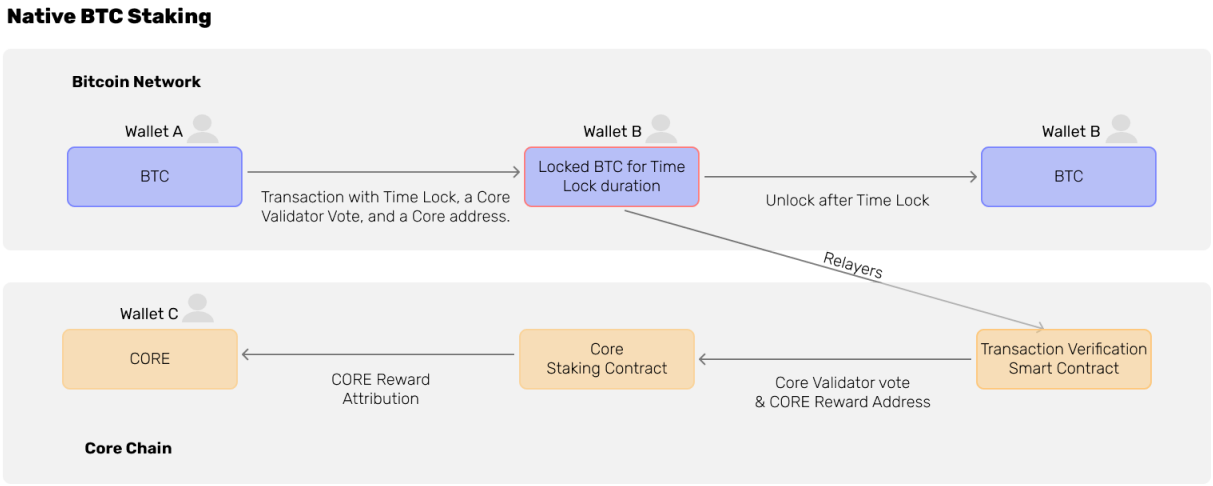
随着非托管比特币质押的引入，Core 链最近的协议更新会将比特币持有者纳入 Satoshi Plus 共识作为第三个元素。

Core 链实现比特币质押的方法集中体现在绝对时间锁上，这是比特币原生的密码学特性，它根据预定义的时间锁定交易的输出，期间这些输出无法被花费。与持有者将比特币委托给外部质押不同，Core 链上的质押者只需要在交易中将他们的比特币放入绝对时间锁中，交易可以被设计为在时间段过去后返回输出。在该交易中，质押者必须在区块中包含一个脚本[4]，这个脚本中包含的的信息与矿工质押的区块中包含的信息一样：

1. 质押者希望质押比特币的 Core 验证节点的地址。
2. 质押者希望将他们的 CORE 代币奖励发送到的地址。

在设定的时间锁长度内（即只要在质押比特币并投票给Core链的验证节点），比特币质押者可以获取 CORE 代币作为比特币被动收益。最终结果是，数十亿美元未被充分利用的比特币价值将变得富有成效，既奖励了质押者，也扩大了比特币的效用范围。

[4] 请参阅上面关于工作证明的部份。



Core 链的原生比特币质押提供了许多优势。

1. 它是专门为倾向于将资产保留在比特币区块链上的长期持有者和机构设计的。鉴于这些实体习惯于长期持有比特币而不频繁进行交易，原生比特币质押为它们提供了在一定期间内获得收益的机会。
2. 没有添加新的信任假设。用户可以在不将其比特币转移到比特币区块链以外的情况下进行质押，从而保持比特币强大基础设施所带来的高安全性和信任。
3. 它为比特币持有者提供了为 Core 链的共识做出贡献而获得被动 CORE 代币奖励的机会。

此外，Core 链实施的质押有一些独特之处。

1. 无需转移您的资产。与其他DeFi协议不同，其他协议要求将比特币转移到不同的区块链或进行封装，Core 链的质押允许用户直接在比特币生态系统内进行质押。
2. Core 链的比特币质押允许比特币持有者为扩大 Core 链整体安全预算做出贡献，保持了基本的区块链精神。
3. Core链有通过命令行或网页界面进行质押的选项，并且有一个简化的奖励领取流程。该产品设计简便易用，旨在同时迎合技术熟练的用户以及那些喜欢更简单直接方式的用户。
4. Core链的奖励系统有助于维护跨链激励。奖励池来自一个共享的共识奖励系统，整合了比特币矿工和 CORE 代币质押者的贡献，从而优化了所有参与者的奖励分配。此外，奖励也是可持续的，并将在81年的时间内进行分发。

Core链上原生的包装比特币[5]（coreBTC）

将资产从源链桥接到目标链的最常见方法是通过资产包装，这将在源链上锁定它们并在目标链上铸造它们的合成代表。当比特币是源链时，合成资产是包装比特币。将包装比特币（Wrapped Bitcoin）兑换成比特币涉及持有者燃烧包装资产以触发其原始比特币的解锁。只要包装比特币与比特币保持1:1的备份，并且用户有赎回的能力，包装比特币将保持与比特币相等的价值。

包装比特币在各种DeFi环境中得到了广泛接受，特别是在与EVM兼容的区块链中。然而，以前的包装比特币实现遇到了显著的集中化问题，因为包装比特币代币的铸造和赎回过程主要由一个单一的中心化实体控制。这种结构从根本上破坏了无需信任的性质，导致其安全性配置明显劣于比特币。

鉴于比特币作为最安全自主的独特存储价值，要作为与比特币挂钩的资产的标准极高。任何旨在完全解锁比特币供应的封装资产必须且必然继承某些基本原则，包括安全性、分散性、无需信任、无许可和抗审查性。这些是 Core 链的本地包装比特币资产 coreBTC 的最高优先事项。

负责在比特币区块链上安全持有用户比特币的节点称为 “**Lockers**”（保管者）。任何人都可以通过锁定抵押品注册为 Core 链上的保管者，并且 Core DAO 本身将运行许多保管者中其中一个。

保管者抵押的特定资产和所需的抵押比率是由 Core DAO 确定的网络参数，保管者需抵押资产意味着锁定的比特币会始终由价值更高的资产支持。如果比特币的价格相对于抵押品价值发生变化，保管者必须调整其抵押品，否则可能面临潜在的清算。

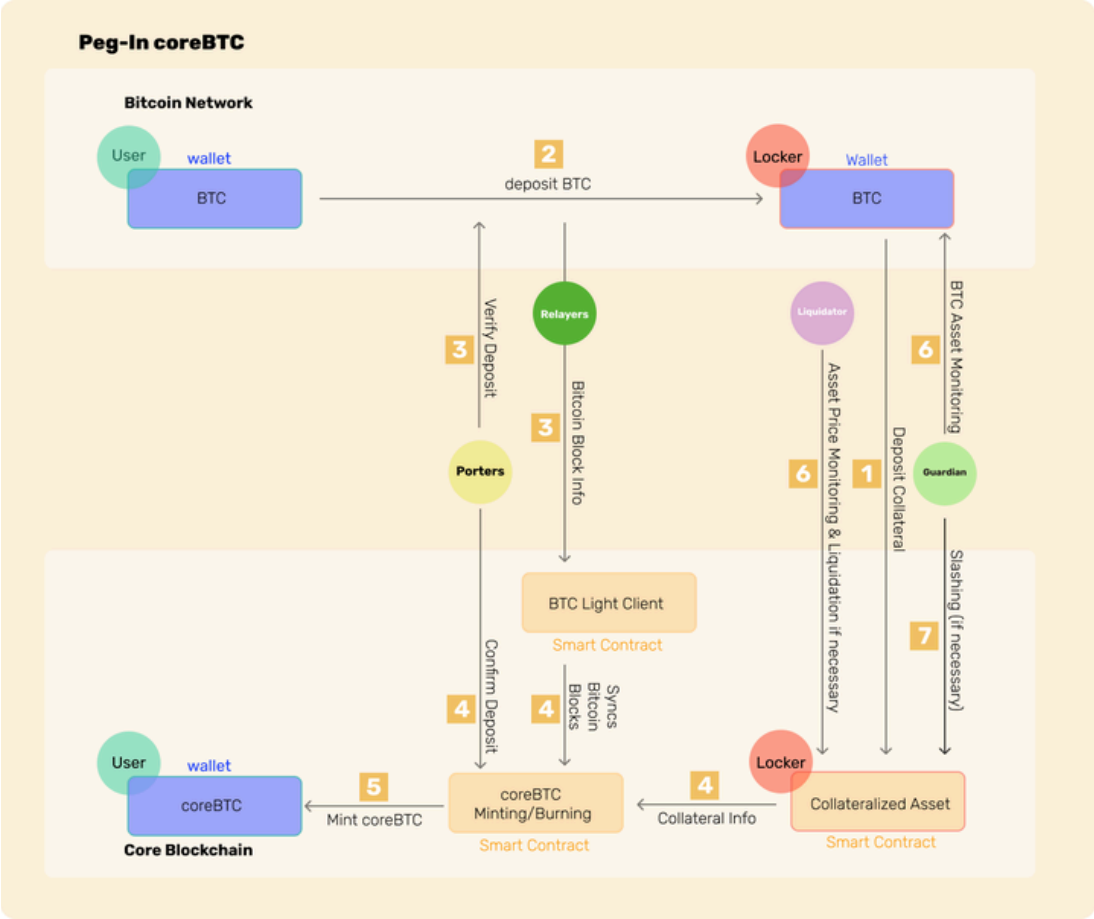
此外，抵押品将作为对恶意行为的威慑手段，如果保管者未经授权转移比特币或在包装比特币被燃烧时未能及时归还比特币，则可能会受到削减处罚。保管者可以随时注销并索回其抵押品，只要它们没有尚未解锁的比特币和没有未履行的解锁请求。作为提供服务的回报，保管者将可以获得小额费用。

要铸造 coreBTC，用户需识别合法的保管者并将比特币发送到保管者的比特币地址。此操作旨在将其比特币锁定为获取等值 coreBTC 的请求和前提。搬运工（Porter）监视比特币区块链以检测

[5]包装代币是与另一种加密货币价值相锚定的加密货币代币。之所以称其为“包装代币”，是因为原始资产被置于“包装”之内。这是一种数字保险库，支持在另一条区块链中创建资产的包装版本。

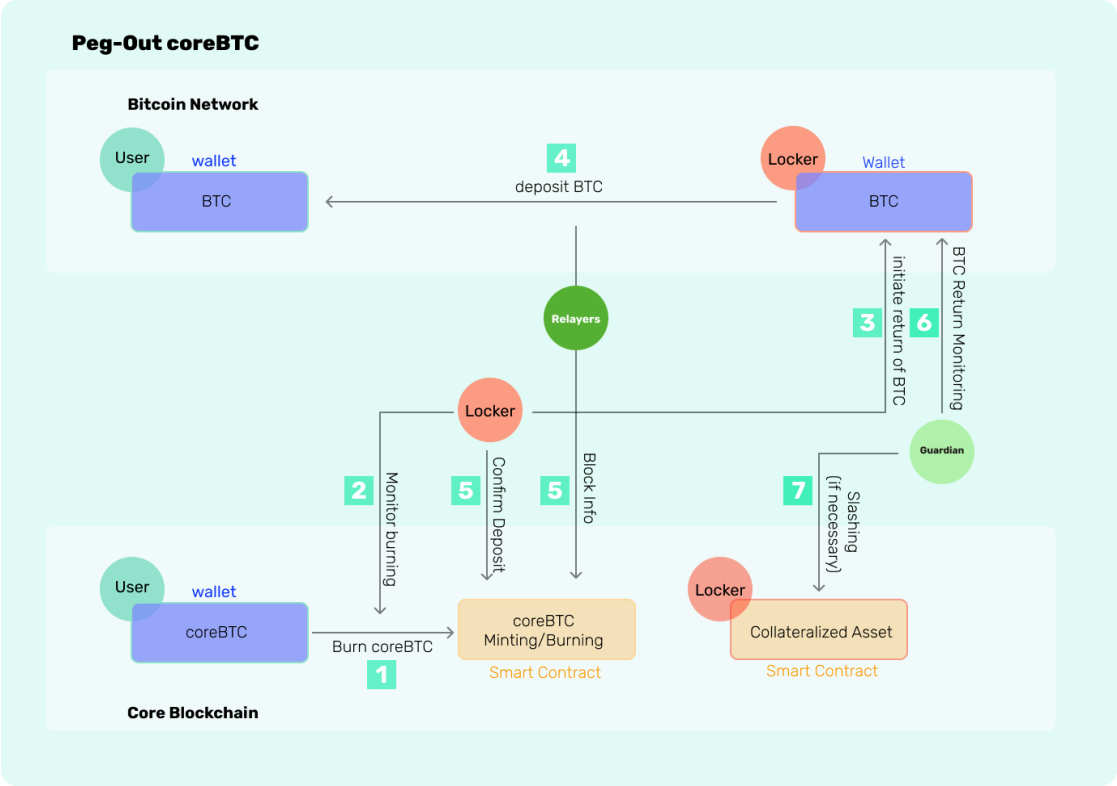
到保管者地址的传入交易，并检测用户对 coreBTC 的请求;在比特币网络上经过足够数量的确认后，搬运工将其提交给Core链上的智能合约，附带比特币交易的证明。搬运工消除了用户需要分别与比特币和Core链交互的需求，这是一个耗时的过程，需要在每个链上支付交易费用。

收到请求后，coreBTC智能合约调用比特币轻客户端验证相关比特币交易的真实性和最终性，然后铸造相应数量的coreBTC。

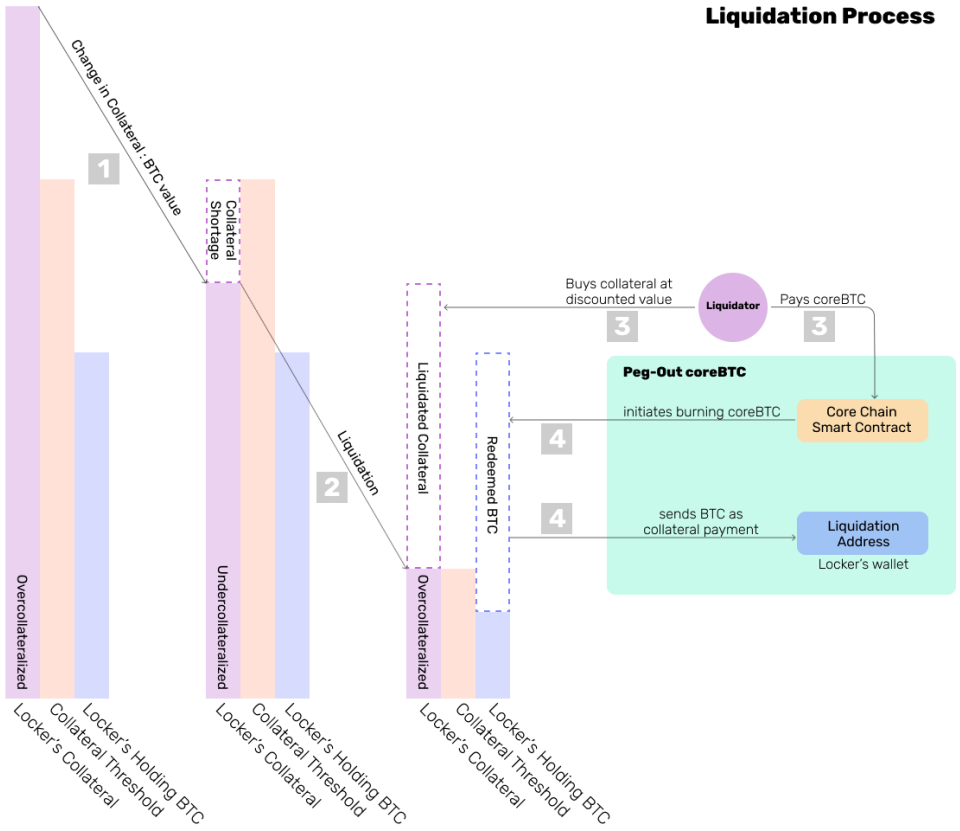


要将 coreBTC 兑换成比特币，用户向 Core 链智能合约发送请求，以燃烧指定数量的 coreBTC，并包含用户希望接收比特币的比特币地址。

然后，智能合约燃烧指定数量的 coreBTC，将其从 Core 链上的流通中移除。然后，智能合约通知保管者释放相应数量的比特币到用户的地址。在收到提醒后，保管者解锁比特币并将其发送到正确的地址。一旦比特币交易得到确认，保管者将其传输到 Core 链，最终由比特币轻客户端验证。



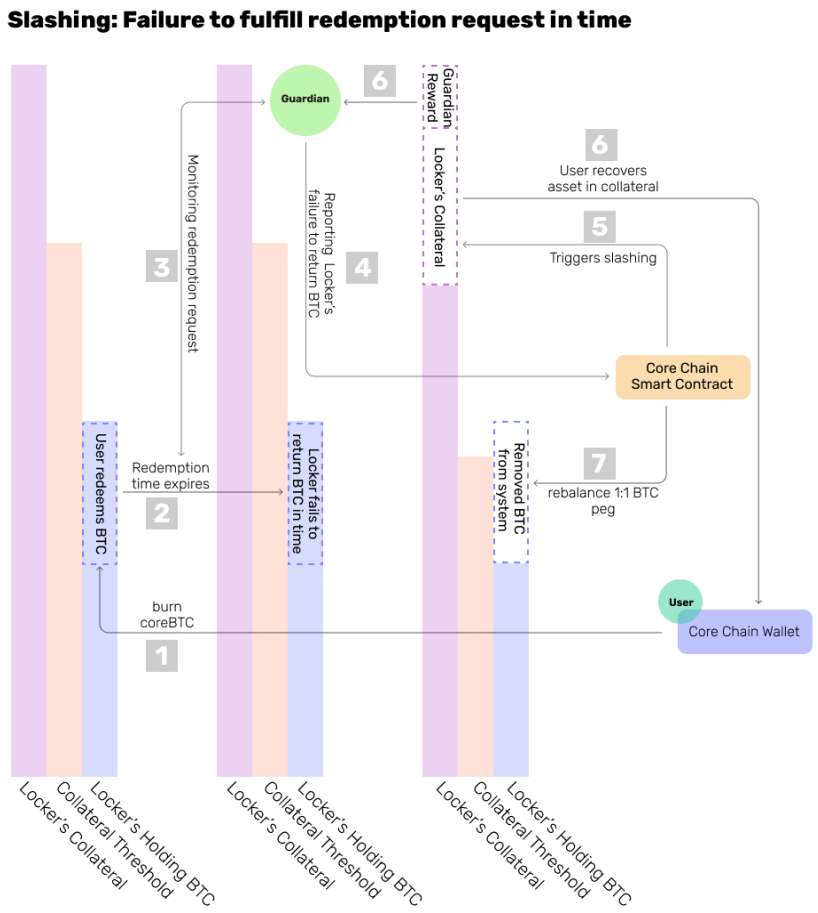
在整个铸币、赎回和中间期的过程中，被称为清算者（Liquidators）的实体监视着所有保管者的健康状况（即抵押比率）。随着抵押品价值相对于锁定的比特币价值的下降，清算者会开始强制清算抵押品。在此过程中，清算者使用 coreBTC 以折扣价购买抵押的 CORE 代币，并燃烧coreBTC。这将推动抵押比率上升，并将保管者恢复到健康状态。



当 coreBTC 被燃烧时，其供应减少，变得更为稀缺，从而使保管者能够拥有相当于被消除的 coreBTC 价值的底层比特币。然后，保管者根据抵押要求重新平衡;如果向该保管者地址发送比特币的原始用户希望收回他们的比特币，他们可以选择任何保管者来获取。兑换 coreBTC 和比特币发生在系统层面，不是一个用户和一个保管者之间的关系。

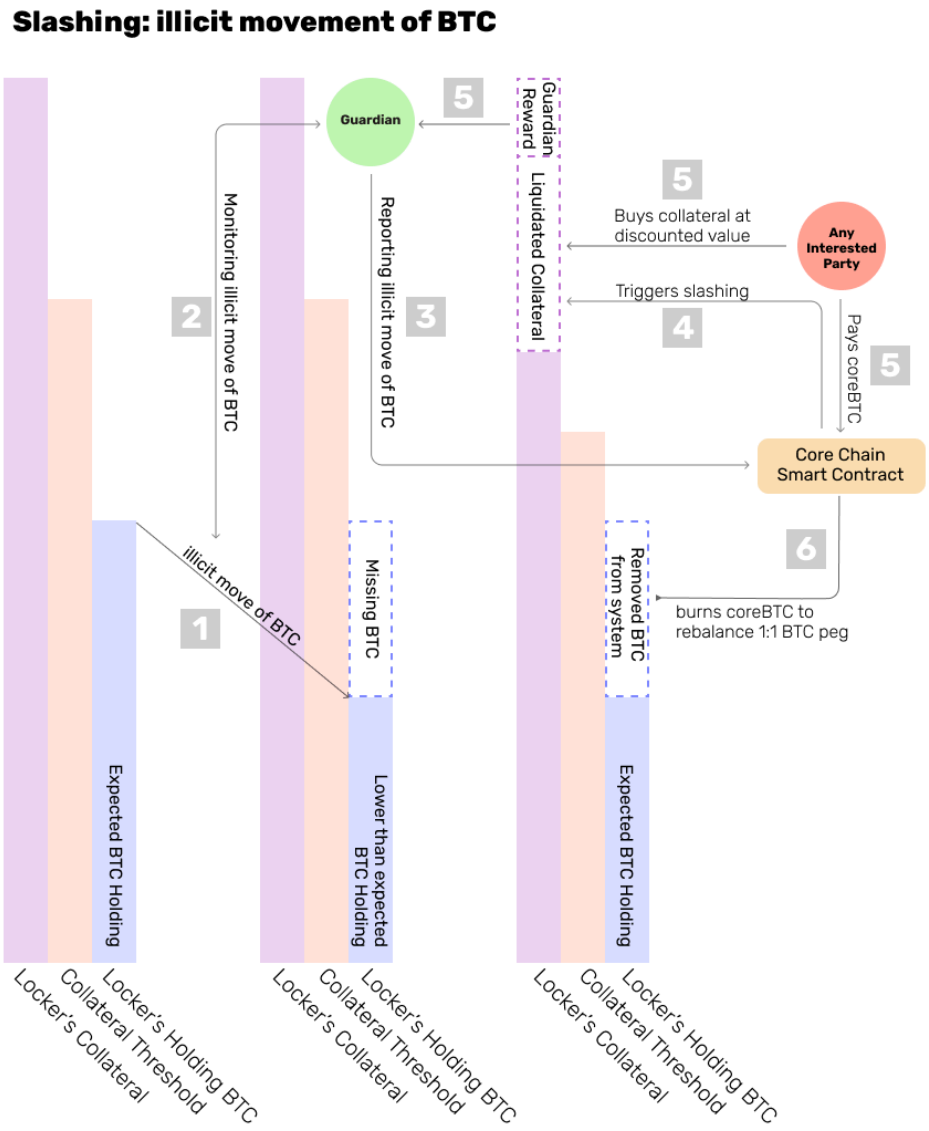
除了清算外，消减惩罚是维持 coreBTC 价值的另一个关键组成部分。由于每个 coreBTC 都锚定了等值的锁定比特币，因此保管者必须(1)在没有燃烧请求的提示下永远不移动锁定的比特币，以及(2)必须始终及时将锁定的比特币兑换给提交燃烧请求的用户。未能执行这两个功能之一将导致保管者存放的抵押品受到消减惩罚。守护者（Guardians）监视保管者的活动，检查任何不当行为并适用适当的削减。用户可以充当削减者，但 Core 链已经实施了守护者制度来永久监视保管者的不当行为。用户也可以无需许可地成为守护者。

如果保管者未在指定的截止日期内履行兑换请求，守护者可以触发Core链智能合约削减保管者的一些抵押品。在此事件中，保管者的抵押品中等同于用户燃烧的 coreBTC 价值的部分，将转移给用户。此外，削减者将因其行动而获得此抵押品价值的一定比例的奖励。



如果保管者非法转移锁定的比特币，削减者可以通过提供未经授权的交易的详细信息来通知 Core 链智能合约有关违规行为。Core 链智能合约接着确认该交易与任何合法的燃烧请求不一致，一旦确定了被盗比特币的数量，就会以折扣价出售保管者的一部分抵押品以获取 coreBTC。出售削减的抵押品的过程旨在获取与被挪用比特币相等的 coreBTC 数量，并使保管者的价值损失超过其偷走的价值，从而使恶意行为失去动机。

收集到的 coreBTC 随后由 Core 链智能合约燃烧，确保每个 coreBTC 都以等值的比特币支持。此外，削减者将获得恶意保管者抵押品价值的一定比例作为奖励。



HTLC 原子比特币闪兑（Atomic Bitcoin Swap）

HTLC 原子交换（Atomic Swap）实现了在 Core 链和其他区块链之间（尤其是比特币）的无信任点对点代币交换。散列时间锁合同（Hashed TimeLock Contracts, HTLCs）将加密散列函数与时间锁机制结合起来，以确保以下结果择一：

1) 双方都能同时访问对方的资金，或是
2) 双方都不能同时访问对方的资金。

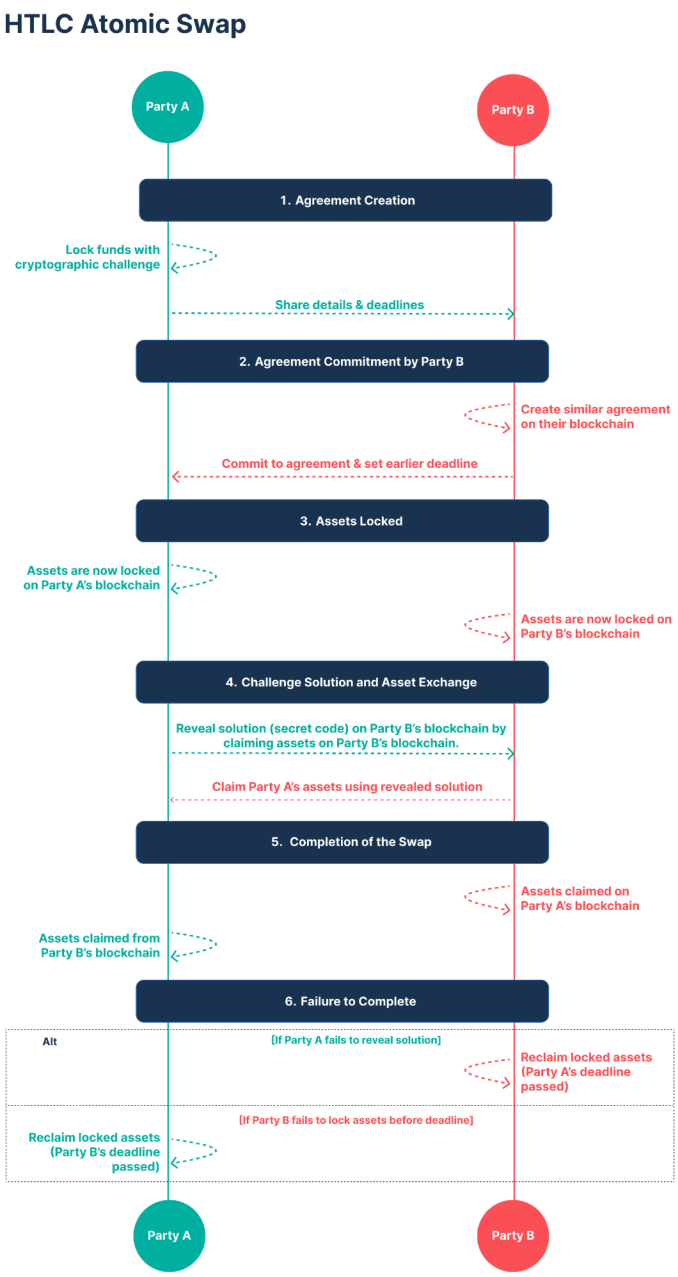
HTLC 是一种加密技术，赋予了锁定交易的能力，使用散列函数并在代币可以花费的时间上设置附加时间限制。

由于其简单性，HTLC 是实现跨链价值转移中最符合比特币友好且安全的方式。它们实现了在比特币、EVM 区块链和 Core 链之间进行原生资产完全无信任的交换，无需中央机构、预言机或中继。这些网络之间的原子交换（Atomic Swap）也可以涉及其他资产，如 ERC20、BRC20、NFTs、Ordinals 等。这引入了一种新的互操作性方法，并使比特币和 Core 链之间访问流动性变得更简单。

至于原子交换（Atomic Swap）的过程，它是由 A 方发起的，A 方通过在其区块链上使用 HTLC 将其资产锁定来创建约定。这个合同的无信任性是由密码学挑战支持的，其中包括一个唯一生成的密钥的散列，最初只有 A 方知道。合同进一步规定了交易完成的精确截止日期。A 方的承诺然后成为区块链的一部分，在 B 方可见，B 方通过在其各自的区块链上使用与 A 方相同的HTLC 机制锁定其资产来做出回应。B 方还为此交易设置了在 A 方截止日期之前到来的截止日期；出于本文讨论范围之外的密码学原因，这减轻了时间退款攻击的可能性。

此时，双方的资产都安全地锁定在各自的 HTLC 中，有效地将它们隔离，使它们对任何外部实体都无法访问。在 HTLC 中的资产保持锁定，直到相关的密码学密钥来解锁它们。当 A 方在 B 方的区块链上揭示密码学挑战的解决方案（密钥）时，A 方能够索取 B 方锁定的资产。由于此揭示使解决方案在区块链上公开可见，因此 B 方随后可以使用现在已知的密钥来解锁和检索 A 方锁定的资产，从而完成交换[6]。

[6] 这并不意味着任何拥有秘钥的人都能解锁HTLC，因为解锁地址的签署者必须是交易的另一方。HTLC脚本被设置为解锁的资金会自动发送到正确的钱包，因此即使其他人调用该交易，资金也会被发送到正确的地址。



原子交换（Atomic Swap）确保交易要么完全完成，要么完全未完成。在 Party A 未在 Party B 的截止日期前披露秘密的情况下，Party B 仍然保留撤回其资产的权利。相反，如果 Party B 在秘密被揭示之后且在 Party A 的截止日期之前未能领取 Party A 的资产，则 Party A 有权撤回其锁定的资产。

与比特币一样，HTLC原子交换（Atomic Swap）的基本优势在于其简单性和安全性，但这些属性也可以看作是约束。这些协议的刚性要求双方必须主动且同时参与交易的执行。尽管这种同时性

确保了安全性，但它也缺乏在订单簿上下订单或立即结算的灵活性（除非每个人都同时在线）。为了解决这些局限性，提出了一种新的原子交换（Atomic Swap）实现，其中包含一种新颖的做市协议。这将使市场制造商能够履行订单并实现即时交易结算。

此提出的系统将为希望执行基于HTLC的原子交换（Atomic Swap）的用户提供一个熟悉的订单簿用户体验。该系统的基本操作取决于其能够在不同的区块链网络之间持续提供撮合服务。一旦识别到一致的订单（即在两个链上以资产类型和数量相对应的订单），系统将自动在匹配的双方之间启动HTLC流程。此程序确保安全地在它们之间交换资产。

该系统的优雅之处在于任何参与者都可以以完全无需信任的方式调用它，从而使访问和参与变得更加民主化。用户无需主动寻找和与交易对手协商；相反，系统自动识别和匹配相应订单，从而显着简化了交易流程。这种方法不仅扩展了HTLC的实用性，还增强了其效率和用户体验，使用户体验更加接近传统金融市场机制，同时保持比特币区块链的去中心化和无信任性。做市商还有提供流动性的激励，因为做市商可以添加交易费用以换取结算互换。

未来方向

Core 链是一个不断发展的生态系统，着眼于未来，本节将介绍在这方面的一些重大项目。

首先，随着时间的推移，Core 链的治理可能会扩展，包括比特币持有者和比特币矿工。这很重要因为它可以增加比特币和 Core 链之间的一致性，并使比特币网络到 Core 链的资产桥接变得更容易。目前，有许多比特币持有者对此过程感到不安，这意味着他们不太可能积极参与BTCFi。Core 链将其治理结构扩展到包括矿工和比特币持有者可能有助于缓解这个问题。此外，尽管比特币持有者目前通过 CORE 代币获得奖励，但在将来的更新中，他们可能可以直接以比特币获得奖励。

其次，Core 链可能采用本地费用市场，使比特币交易更快且可预测地更便宜。回想一下，比特币最初的愿景是使其成为货币，这是不可能实现的，除非它支持快速、廉价、可预测和可扩展的交易。希望本地费用市场能首次将这些特性引入比特币。Solana 项目已经在部分程度上验证了这个想法。

第三，原子交换（Atomic Swap）的运作方式可能会有一些补充以使其更通用。流动性池可以添加以补充当前负责兑换过程的订单簿，这将使部分订单的成交变得可能，同时减少做市商的需求。

第四，通过将 Core 链的共识机制与多签钱包集成，可能会加强 coreBTC 的无信任性质。锁定者还可以获得更多的抵押选择，这可能会扩大在Core链上运作的潜在锁定者的范围。

第五，在将来的迭代中，可能会修改抵押机制，使持有者可以参与去中心化金融（DeFi）而无需进行封装。这将允许用户以其原生形式保留其资产。

最后，Core 链有能力支持比特币作为支付手段，并可能在以后得到更充分的扩展。这些变化上线后，每个人都可以在 Core 链上先将比特币交换为 coreBTC 以实现比特币的全周期使用。