【火线视点】六个月从 3000 枚到 15 万：解码以太坊链上 BTC 的驱动因素与技术手段

摘 要：

在过去的 6 个月，以太坊上的 BTC 锚定币数量快速增长了近 50 倍，从 3000 枚增长到如今的 15 万枚。截至 11 月 24 日，BTC 锁仓价值达 27 亿美元，几乎占到 DeFi 整体锁仓量的五分之一。这种增长幅度是前所未有的，也是区块链有史以来体量最大的一次大规模跨链。

那么究竟是什么原因，驱使着这些 BTC 进入以太坊网络呢？通过对主要锚定币链上数据的分析，我们可以发现大约 40%的锚定 BTC 流入到了头部 DEX 当中，而 30%的锚定币 BTC 流入到了头部借贷 DeFi 中，其余主要分布在一些 CEX、二线 DeFi 应用和一些个人、机构地址中。

换言之，驱动的主因是获取 DEX 提供的流动性“挖矿”奖励，其次是进行链上借贷。不过贷出资金仍有大量会继续投入流动性挖矿当中。当然，客观上，这样的迁移也带来了 BTC 的性能提升，并且提高了 DeFi 行业资产规模天花板。

目前主要的 BTC 锚定币按总量依次包括 WBTC、renBTC、HBTC、sBTC、tBTC、oBTC 、imBTC 以及 pBTC 等等。其中，除少量 sBTC 外，其余 98%的锚定币均采用了“托管+映射”的方式完成跨链，sBTC 则是通过资产超额抵押产生的。几种托管机制各有千秋，主要是对中心化机构的依赖程度不同。其主要通过 1）信用背书和 2）技术手段两大类方式来保证底层资产安全。

目前这些锚定 BTC 未出现过安全事故，总数量突破十万级，因此有效增加了铸币者对于此类技术的信心。不过这不代表说这些锚定币绝对安全的，例如黑客盗取、内部盗取、私钥损毁等“黑天鹅”风险是始终存在的。如何更好地应对这些潜在风险，每一个托管方都需要未雨绸缪。

综合来看，虽然流动性“挖矿”奖励幅度在持续下降，但是这些锚定 BTC 仍然没有离开的趋势，只是增速放缓。从长远来看，这些托管机制在安全和分布式程度上，仍然有继续提升空间。只要它们是安全的，随着技术成熟和应用落地，相信我们能够看到更高数量级的 BTC 进入以太坊网络。

作 者

【火币研究院】马天元，赵文琦，袁煜明

作者联系方式

火币研究院：huobiresearch@huobi.com

目 录

一、 为什么需要 BTC 跨链到以太坊

2020 年，以太坊链上的 BTC 实现了大幅增长。尤其是在过去的 6 个月，在以太坊上的 BTC 锚定币数量从 3000 枚增长如今 15 万枚，快速增长了近 50 倍。截至 11 月 24 日，BTC 锁仓价值达 27 亿美元，几乎占到 DeFi 整体 TVL 的五分之一。今年的这种增长幅度是前所未有的。

从发展轨迹来看，最早的 WBTC 诞生于 2018 年年末，但是直到 2019 年 12 月底，全行业的锚定 BTC 数量仅为 1000 枚左右。但是，自 2020 年开年以来，网络中锚定 BTC 快速从 1000 枚，增长到 6 月底的 1.1 万枚；随后，又从 1.1 万枚快速增长到如今的 15 万枚。从这些数据中，我们足以窥到 BTC 进入以太坊链上的强烈需求。

那么，BTC 为什么要跨链到以太坊上呢？BTC 跨链以太坊的现状如何？以“八仙过海”手段完成跨链的 BTC 背后的技术原理和机制又是什么呢？本篇报告将会阐述这些问题。

1.1 为什么这些 BTC 被称为 BTC 锚定币

ERC-20 标准，大家都很熟悉，是通过以太坊创建 Token 的一种规范。它是目前最为通用的区块链 Token 创建标准。构建于以太坊上的 BTC，如 WBTC，HBTC 等，大都是基于 ERC-20 标准的 Token（也有少量是基于 ERC-777 标准）。它们通过不同的算法技术对 BTC 进行 1：1 的映射，从而获取 ERC-20 Token 才能获得的特性，例如在 DeFi 中使用。本质上来说，这是一种真币换“映射 Token”的过程。因为赎兑通道非常通畅，它们的价格能够和 BTC 实现大致 1：1 锚定。因此，这些 Token 通常被称作“BTC 锚定币”。

1.2 为什么 BTC 需要跨链到以太坊上

半年以来，BTC 锚定币的总量快速增长近 50 倍，引起了业界的高度关注。那么为何会产生如此大量的映射 Token 需求呢？**答案并不复杂：BTC 持有者希**

望提升资产的利用效率，例如（1）参与挖矿获取收益；（2）作为抵押借出资金。当然，客观上这些锚定 BTC 也改善了 BTC 转账性能和可编程性，并且提升了整个 DeFi 板块的资产天花板，也有少量需求是来自这两方面。

（1）提高 BTC 持有者资产利用效率

从用户的角度来讲，不同的加密货币参与者有不同的持有偏好，在当前市场环境下，BTC 有着不容忽视的行业地位。但以太坊网络的生态则更加丰富，尤其是在 DeFi 领域，形成了更多创新应用。

和 PoS 区块链不同，BTC 自身并没有原生的“生息”方式。随着流动性挖矿的兴起，许多 DeFi 项目对 ERC-20 资金本身的注入进行激励，例如：DEX 会给流动性提供者奖励，借贷 DeFi 会给借贷双方 Token 奖励等。

一个想要生息收益，一个想要更多资产，两者“一拍即合”，大量 BTC 由此以锚定 BTC 方式，进入了以太坊的 DeFi 生态。通过 11 月初链上数据来看，超过 40%的锚定 BTC 被放到的借贷应用中，释放出了大量资金（稳定币和其他 Token）；另外有超过 30%的锚定 BTC 被直接投入到了 DEX 的流动性挖矿（yield-farming）当中，而这些 yield-farming 则为 BTC 提供了 10~30%的可观年化收益（APY）。

（2）BTC 可以因此获得更好的性能以及可编程的特性

从使用者角度来说，BTC 锚定币具备性能和费率优势。相对于 BTC 网络，以太坊网络在性能和费率方面略有优势，而 ERC-20 版 BTC 本质上是基于以太坊网络的 Token。目前 BTC 系统的 TPS 仅 7 笔，而以太坊系统的 TPS 则提升到约 15 笔，**同时以太坊出块速度更快，到账时间的确定性更高。因此，迁移到以太坊上的 BTC 一方面转账更便宜，确认更快，另一方面也为 BTC 主链疏通了拥堵。**

另外，ERC-20 版的 BTC 本质上来说是一种以太坊链上的 Token，这使得它

们具备了可编程特性。它将允许开发者基于 BTC 资产编写智能合约。这种可编程性也使得 ERC-20 版的 BTC 可以自由地与 DeFi 的各种创新应用结合。

（3）提升 DeFi 资产天花板

除了用户需要锚定 BTC 之外，DeFi 应用也同样需要。DeFi 应用大多数聚集于以太坊网络，但是以太坊存在资产天花板。DeFi 的资产天花板指的是，以 ETH 为代表的基于以太坊上资产的总体市值规模是有限的，逐渐会形成针对 DeFi 发展的制约。

DeFi 板块和与整个加密货币市场对比而言规模很小。截至 11 月 23 日，数字货币的总市值近 6000 亿美金。其中，BTC 市值为 3400 亿美金，独占总市值的 2/3。一定程度上，ETH 上各类 DeFi 锁仓量占如果想要继续增长，必须要纳入 BTC，否则相对较少的 ETH 和 ERC-20 资产将成为 DeFi 发展的天花板。

通过 ERC-20 版 BTC，用户可以体验更好的流动性。这些 ERC-20 版 BTC 把更大的流动性带到了以太坊生态，大大提高了 DeFi 总资产的天花板。

那么，这些 BTC 进入以太坊网络的速度到底如何？去向又都是何处？赎回又是什么情况呢？我们会在第二章进行展开分析。

二、 BTC 跨链以太坊现状

2.1 各种类分布和整体增长

根据链上数据统计，如表 2-1 和图 2-1 所示，目前主流的 BTC 锚定币按总量排行依次包括：WBTC（约 21 亿美金），renBTC（约 3 亿美金），HBTC（约 1 亿美金），sBTC（约 3000 万美金），tBTC（约 2400 万美金），oBTC（约 1600 万美金），imBTC（约 1400 万美金）和 pBTC（约 250 万美金）等。其中 WBTC 占比超过 80%。

	类型	数量/枚
1	WBTC	**124,260**
2	renBTC	**18,261**
3	HBTC	**6,010**
4	sBTC	**1,775**
5	tBTC	**1,436**
6	oBTC	**964**
7	imBTC	**862**
8	pBTC	**213**

表 2-1 BTC 锚定币统计

数据来源：Etherscan 2020-11-17

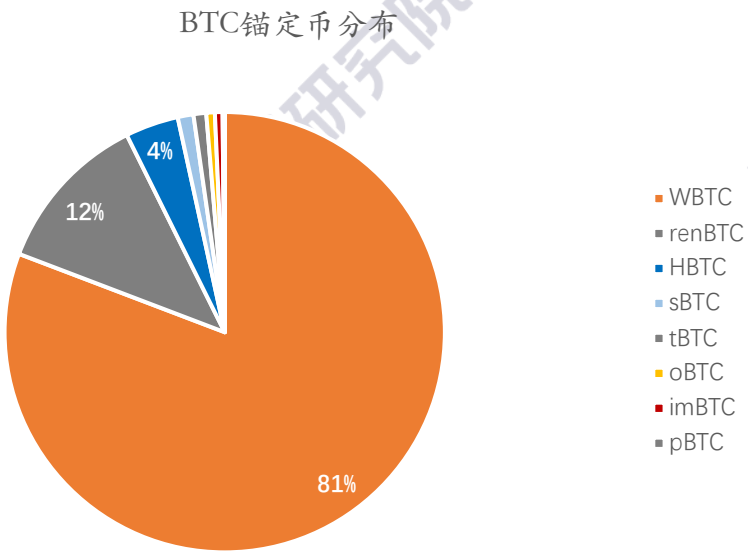

图 2-1 BTC 锚定币分布

数据来源：Etherscan 2020-11-17

由图 2-2 可见，以太坊上的 BTC 在近 6 个月开始飞速增长，曲线相对陡峭。由于 WBTC 占有绝对优势的份额，和总体曲线的走势一致性也较强。不过随着近个月流动性挖矿热度的下降，目前增长稍有放缓，但仍呈总体上升趋势。

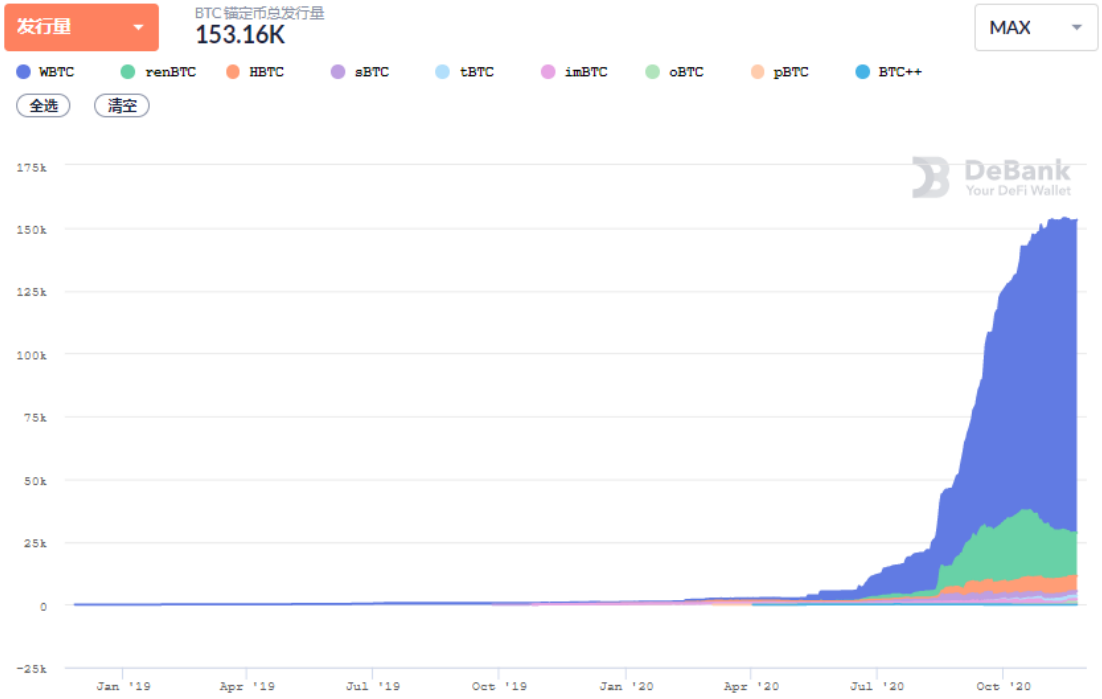

图 2-2 以太坊上的 BTC 整体增长情况

来源：DeBank 2020-11-23

2.1 主要锚定币去向

WBTC 和 renBTC 是目前总量最多的锚定币，占到整个板块的 90%以上。因此，这两种锚定币的去向可以代表整体锚定币去向。那么这些 BTC 锚定币到了以太坊网络之后，又都去做什么了呢？

我们选取了两个时间点对其分布进行统计，11 月 5 日和 11 月 24 日，分别是 Uniswap 停止流动性挖矿奖励的前后。

首先是 11 月 5 日，WBTC、renBTC 的主要去向如表 2-2、表 2-3 所示：

WBTC 的分布情况	数量（取整）	比例	价值（USD）
Uniswap V2:WBTC 2	27,841	22.80%	4.0 亿
Compound Wrapped BTC	23,774	19.40%	3.4 亿
Maker:WBTC	15,322	12.50%	2.2 亿
Aave:Lending Pool Core	11.656	9.50%	1.7 亿
Curve.fi:REN Swap	8,327	6.80%	1.2 亿
Nexo:Wallet	2,850	2.30%	4000 万
Balancer:ETH/WBTC	1747	1.40%	2498 万
Curve.fi:sBTC Swap	1565	1.30%	2248 万

表 2-2 WBTC 主要分布情况

数据来源：Etherscan，2020-11-5

renBTC 的分布情况	数量（取整）	比例	价值（USD）
Curve.fi:REN Swap	13000	63.60%	1.9 亿
Curve.fi:sBTC Swap	1977	9.70%	2819 万
Cream.Finance	165	0.80%	236 万
Uniswap V2:renBTC 2	164	0.80%	234 万
未注明地址若干			

表 2-3 renBTC 主要分布情况

数据来源：Etherscan，2020-11-5

从表中不难看出，不管是 WBTC 还是 renBTC，其主要去向多为头部的 DeFi 应用。也许这些应用 APY 并不是最高的。但由于品牌可信度等综合因素，头部 DeFi 应用吸纳了最多的流动性资金。

在分类上，锚定币主要去向分别是如 Uniswap，Curve 等主流支持流动性挖矿的 **DEX，大约占到 40%左右；**以及 Compound、MakerDAO 等**主流借贷平台，大约占到 30%左右。**当然，目前还有一些未注明合约地址，可能是个人账户或待添补信息的某些新的 DeFi 地址。

在本报告的撰写过程中，正好在 11 月 18 日，Uniswap 的流动性挖矿奖励停止。Uniswap LP Pool 作为曾经 WBTC 的第一大去向，停矿之后，整体 BTC 分布发生了什么变化呢？让我们看一看 11 月 24 日的数据，如表 2-4 和表 2-5 所

示。

WBTC 的分布情况	数量（取整）	比例	价值（USD）
Compound Wrapped BTC	25108.87	20.17%	4.6 亿
Aave: Lending Pool Core	15522.81	12.47%	2.8 亿
Maker: WBTC	15370.36	12.35%	2.8 亿
Curve.fi: REN Swap	8222.49	6.60%	1.5 亿
疑似个人地址	6681.47	5.37%	1.2 亿
SushiSwap	5503.55	4.42%	1.0 亿
Uniswap V2: WBTC 2	4912.19	3.95%	9000 万
Nexo	2850.01	2.29%	5200 万
Curve.fi: sBTC Swap	2784.04	2.24%	5100 万
Balancer: ETH/WBTC	2769.81	2.22%	5000 万

表 2-4 WBTC 主要分布情况（UNI 停矿后）

数据来源：Etherscan，2020-11-24

renBTC 的分布情况	数量（取整）	比例	价值（USD）
Curve.fi: REN Swap	8537	0.508359	1.5 亿
Curve.fi: sBTC Swap	2711	0.161448	5000 万
KeeperDAO	1511	0.089964	2800 万
UMA	946	0.056308	1750 万

表 2-5 renBTC 主要分布情况（UNI 停矿后）

数据来源：Etherscan，2020-11-24

整体来看，WBTC 和 renBTC 在主流 DEX 板块的占比下降到 25%，而在主流借贷应用中的占比则上升到 40%。其主要原因是，UNI 停矿后，大量 WBTC 从 Uniswap 撤出，仍然在 Uniswap 提供流动性的 WBTC 骤降 80%。表 2-4 中，疑似个人地址的 6681 枚 WBTC 从链上看就是从 Uniswap 撤出的，另外 AAVE、Sushiswap 也是此次停矿的 WBTC 主要流入对象。

由此我们可知，锚定币的两大最主要去向中，DEX 提供的流动性挖矿激励一度是锚定币的最主要目标。**不过，随着 DEX 纷纷减产或者停止流动性激励，DEX 中锚定币占比下降。不过，大量锚定 BTC 并未因此而大批赎回比特币网**

络，反而是进入到了其他以太坊借贷应用当中，用户通过抵押锚定币借出了大量其他 Token，例如稳定币。

2.3 主要 BTC 锚定币的铸造和销毁情况

截至 2020 年 11 月初，WBTC 和 renBTC 的铸造销毁情况如表 2-6 所示。

	铸造	铸造次数	销毁	销毁次数
WBTC	120714.6	313	2431.83	23
renBTC	60925.82776	24345	39348.37	3977

表 2-6 WBTC 和 renBTC 的铸造销毁情况

其中，WBTC 销毁很少，而 renBTC 销毁非常频繁。如表 2-7 和图 2-3 所示，renBTC 销毁最高的一笔金额相当于 BTC 1003.3 个，其次为 601.97 个，两笔均发生在 2020 年 9 月 18 日。数量区间上来看，笔数最多的在 0.1 到 1 之间，为 1733 笔，其次是 1 到 10 个，为 930 笔。相比之下，WBTC 的销毁次数总共仅 23 次，而且集中在其中的 4 次销毁，这 4 次销毁量占总销毁量的 98.47%。

销毁数量/枚	笔数
<0.01	156
0.01~0.1	402
0.1~1	1733
1~10	930
10~100	670
100~200	56
>200	30

表 2-7 renBTC 的销毁数量与笔数

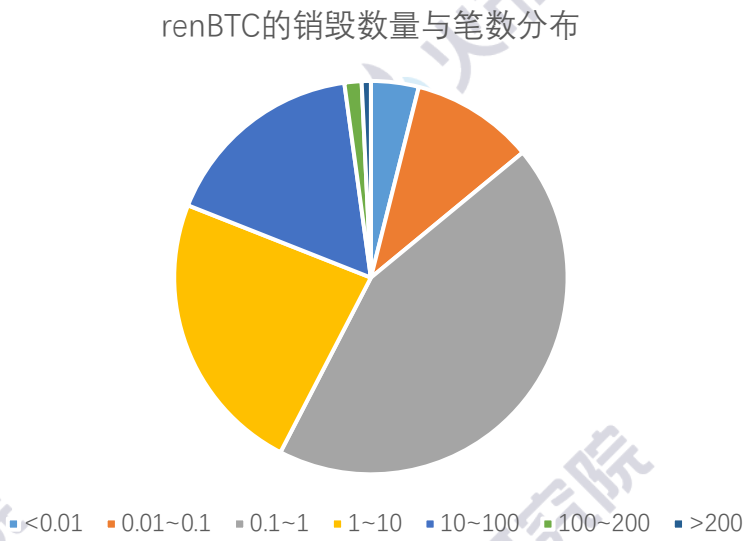

图 2-3 renBTC 的销毁数量与笔数分布

为什么 renBTC 会比 WBTC 销毁数量更多呢？原因其实是两者的运行机制不同。WBTC 采用商户模式，用户每次赎回实际上是向负责承兑的商户兑换，换走承兑商手上的头寸，而不需要真正的销毁。但是，renBTC 没有承兑商设计，因此每一次赎回都需要链上销毁，这带来了两者销毁笔数的不同。

关于各类 BTC 锚定币运行机制，我们将会在下面一章进行详细分析。

三、锚定 BTC 模式详解

之所以会有锚定 BTC，是为了让因技术体系不兼容不能直接出现在各类非 BTC 区块链的 BTC，以“替身”形式出现。目前所有生成锚定 BTC 的方案都由**等值或超额抵押**资产背书。这其中，总量 98%的锚定币是以“托管+映射”方式完成。

根据抵押物的不同主要有两类思路：**抵押 BTC** 生成锚定 BTC，和**抵押其他区块链资产**生成锚定 BTC。

前一种方式不会扩张流通中的 BTC 及锚定 BTC 的总数，并且由于是真实 BTC 抵押不会出现因“资不抵债”而发生频繁清结算流程。

但是，正因为是真实 BTC 抵押，再到另一条链上释放锚定 BTC，所以必然会涉及到跨链模式的设计，跨链机制设计的不同是各个锚定 BTC 模式差异的核心点之一，如 WBTC 通过托管方和商户之间的交互实现人工跨链，而 renBTC 通过 RenVM 实现跨链。但本质上，这些机制都会将 BTC 托管给某个或某些特定群体完成的。

后一种方式的清结算机制会更复杂，但由于抵押物可以是同一条链上的资产所以通常可以避免跨链，如 sBTC 的生成流程都发生在以太坊上。这类机制以智能合约作为工具，因此不需要任何托管，但是坏处是资产利用效率低且存在无法清算的风险。

但无论前者还是后者，由于都是基于抵押，所以围绕抵押机制会有所不同，如图 3-1 和表 3-1 所示，比如 WBTC 由中心化托管机构托管抵押的 BTC，renBTC 由去信任化网络托管抵押的 BTC(但目前尚未完全实现)，而 sBTC 是由合约控制抵押的 SNX。

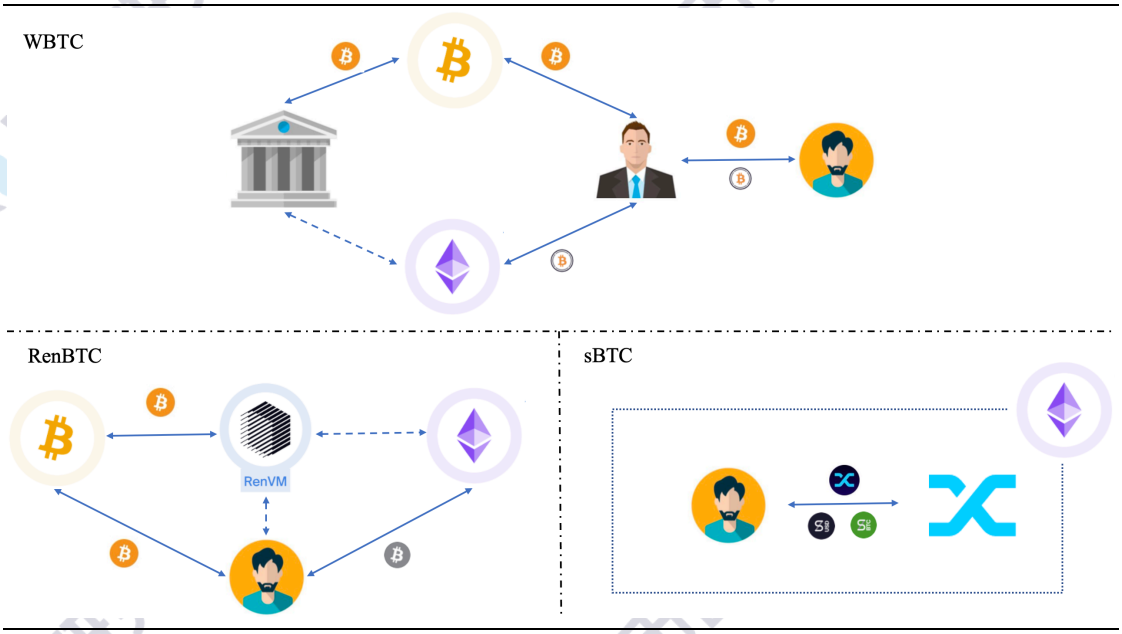

图 3-1 WBTC、renBTC、sBTC 模式简要对比

进一步来说，理解各锚定 BTC 解决方案的运行逻辑，最主要的是理解两个问题。

1.锚定 BTC 如何铸造和销毁？

该问题向下细拆又会变成 3 个小问题：

1)谁来负责铸造和销毁？

2)谁来负责抵押的托管？

3)跨链信息如何进行交换？

2.如何解决锚定 BTC 铸造、流转、销毁等生命周期中的资金安全问题？

下表对本章将要介绍的几类锚定 BTC 做了简要对比。在后文我们还会对每一种锚定 BTC 进行详细分析并讨论前述问题。

名称	发行方	发行标准	发行量	托管方式	上线时间	抵押方式	铸造特点
WBTC	Kyber RenProtocol BitGo	ERC-20	12.4 万枚	中心化	2019.01	等额 BTC 抵押	双层分发
renBTC	Ren Protocol	ERC-20	1.76 万枚	非中心化*	2020.05	等额 BTC 抵押	RenVM
HBTC	Huobi	ERC-20	6010 枚	中心化	2020.02	等额 BTC 抵押	多签名机制
sBTC	Synthetix	ERC-20	1778 枚	非中心化	2019.07	750% SNX 超额抵押	合成资产
tBTC	Keep Network Cross-Chain Group Summa	ERC-20	1352 枚	非中心化	2020.05	等额 BTC 抵押	t-ECDSA 椭圆曲线签名算法
imBTC	Tokenlon	ERC-777	958 枚	中心化	2019.10	等额 BTC 抵押	锁仓兑换
oBTC	BoringDAO	ERC-20	862 枚	非中心化	2020.10	等额 BTC 抵押	双层抵押机制
pBTC	Provable Things	ERC-777	211 枚	非中心化	2020.3	等额 BTC 抵押	可信执行环境（TEE）

*renBTC 的整体设计方案是非中心化托管，但当前开发阶段还在中心化阶段

表 3-1 几种锚定 BTC 对比

数字来源：链上数据，2020-11-18，火币研究院整理

3.1 WBTC

WBTC（Wrapped Bitcoin），于 2019 年 1 月发行上线，托管方为知名数字资产托管机构 BitGo，是最早基于以太坊网络与 BTC1：1 挂钩的 ERC-20 代币，在各类锚定 BTC 中占比份额最大，发行量已超过 12 万，其发行规则也被诸多后来者加以参照。

WBTC 体系是基于信任的联盟治理模式，其核心为两层分发结构。如 0 所示为 WBTC 的两层分发结构，其中涉及三种角色，**托管方(Custodian)、商户(Merchant)以及用户(Customer)**。在该结构下，托管方与商户之间的交互负责铸造和销毁 WBTC；商户与用户之间的交互负责向二级市场投放和收回 WBTC；用户不会越级直接和托管方交互。

如图 3-2 所示，下面我们将通过介绍 WBTC 的铸币与销毁流程，及其中各种角色的权责来探讨该种模式的优缺点。

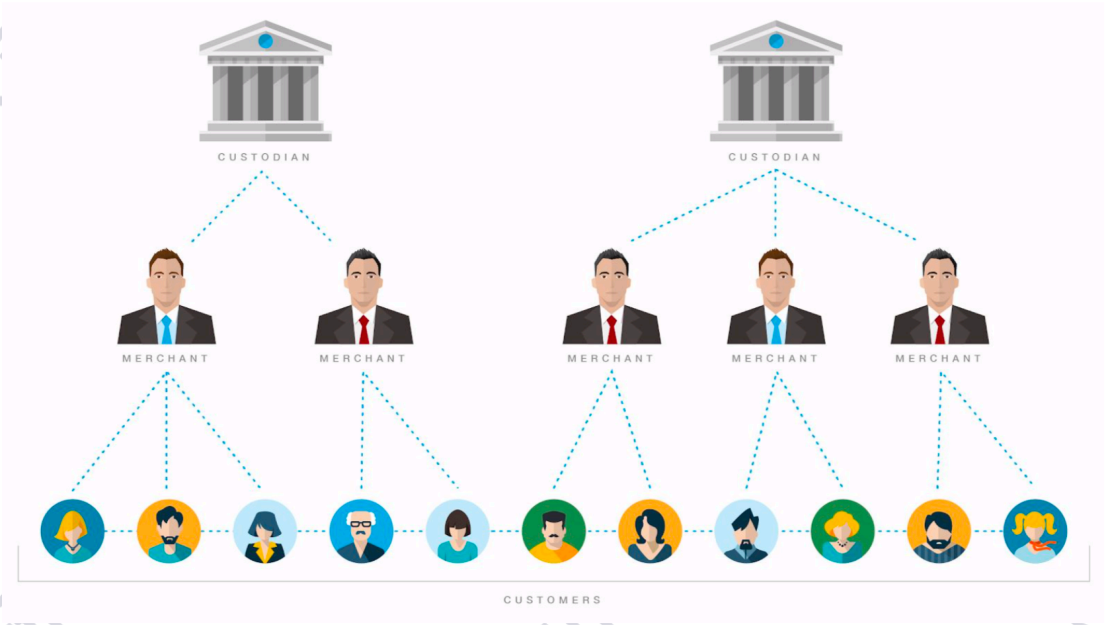

图 3-2 WBTC 两层分发结构

来源：Wrapped Tokens 白皮书

3.1.1 铸造、销毁、分发与回收：两层分发

1) 铸造与销毁

WBTC 的铸造与销毁均发生在托管方与商户之间，并且会同时在 BTC 和以太坊上发生交易。铸造的核心点是在 BTC 链上锁定 BTC，并在以太坊链上释放

等值的 WBTC。WBTC 的铸造流程如下：

- **转账 BTC：**首先，在 BTC 链上，商户会向托管方发送一定数量的 BTC；
- **申请铸币：**而后，在以太坊链上，商户会向 WBTC 的智能合约发起申请铸币的请求，该请求的参数中会带上 BTC 链上转账的交易 id；
- **铸币：**托管方看到申请铸币请求，并根据其中的 BTC 转账的交易 id，确认交易已经完成后，会向合约发送确认铸币请求。确认铸币请求会触发合约中的铸币操作，合约会自动铸币并放入商户的以太坊地址中。

销毁是与铸币相反的流程，但不同的是，铸币过程中最终确认发起铸币动作的是托管方，但销毁过程中，确认发起销毁操作的是商户。具体流程如下：

- **创建销毁交易：**商户在以太坊链上通过合约创建销毁 WBTC 的请求，销毁指定数量的 WBTC；
- **转账 BTC：**待销毁操作完成后，托管方会在 BTC 链上向商户转移对等数量的 BTC；
- **交易确认：**完成转账后，托管方会在以太坊链上发起交易，确认销毁操作已经完成。

值得注意的是，铸币和销毁的过程由于并不是全自动化完成，通常需要耗费数小时到几十小时(一般在 48 小时以内)。

2) 分发与回收

WBTC 的分发与回收发生在商户与用户之间。商户完成铸造过程后，其就持有了 WBTC 代币。WBTC 模式中没有对商户与用户之间的 BTC-WBTC 的兑换形式进行约束，理论上，商户可以通过再次实现跨链通信来完成每笔和用户之间的交易，但更通常的是，商户作为中心化机构，会在其体系内的交易所或者钱包应用中完成不上链的兑换交易。

3.1.2 角色权责：基于信任的联盟治理

在 WBTC 的模式中，主要存在着 4 大类角色，托管方、商户、用户以及 DAO 成员。在前文中已经涉及到了其中 3 类角色，下面我们来逐一讲述。

1) 托管方

托管方的名字已经显而易见地揭示了其在 WBTC 模式中最核心的作用——负责托管用于生成锚定 BTC 的质押资产。

此外，托管方也是铸币行为的实际执行方(mint 函数由托管方的合约调用触发)。但在 WBTC 模式中，也通过 3 个层次限制托管方的权力，避免其滥用铸币权或擅自转移托管资产：1.托管方不能自行铸币，必须由商户首先发起铸币请求，托管方基于此请求进行铸币；2.托管方托管地址中的 BTC 只能转给在白名单中的商户链上地址，无法随意转走；3.商户的增删由 DAO 决定，不受托管方直接控制。

当前，在 WBTC 体系中，BitGo 是唯一托管方。

2) 商户

商户在 WBTC 模式中是一个中转的角色。成功铸造的和待销毁的通证都会在商户的地址上存储，面向用户的分发与回收也由商户来执行。实际销毁的操作也由商户来执行。

此外，由于商户可以以中心化的方式运作，其可以避免在每次用户请求铸币或者归还的时候都发生跨链交易，而是可以在链下完成该过程，大幅提升效率。用户将 BTC 托管给这些机构换取 WBTC，将 WBTC 归还再换回 BTC。这也是我们在第二章发现链上数据 WBTC 销毁次数极少的原因。

商户实际上是动用了自己的头寸，在与用户进行赎回和兑换，理论上用户不需要相信任何商户，只需要相信最终的托管方 BitGo 即可。

3) 用户和 DAO

用户是 WBTC 的最终需求方，但他们不直接参与铸币和销毁的过程。但 WBTC 在其规则中，明确要求了参与(间接)铸造和销毁的用户必须通过 KYC 和 AML。

WBTC 通过 DAO 的形式管理托管方和商户的进出及角色权限。托管方和商户可以作为 DAO 成员。当前根据 WBTC 官网公布的信息，DAO 成员共有 17 家，包括唯一托管方 BitGo，部分商户如 Ren、Loopring、Maker 等，以及一些纯 DAO 成员如 Compound、Blockfolio 等，相对比较分散。

3.1.3 模式优缺点

在 WBTC 模式下，最大的优点在于其两层分发的结构。这种设计结构能带来两个主要的好处：一是把相对耗时和复杂的操作在第一层上解决，如批量的铸币、销毁以及信任治理的问题，因此在第二层上就能实现面向用户的快速分发和回收，极大提升用户体验；第二个主要好处是，在机制上由于商户是使用自身头寸帮助用户兑换，使其无法作恶，因此实际面向用户分发和回收的商户的性质就不再重要，因此使得生态中本来就拥有大量用户基础的服务商可以成为 WBTC 体系中的商户，加快 WBTC 的扩张。当前 WBTC 成为锚定 BTC 中铸币量最高的产品与其设计模式关系重大。

但该模式也有其潜在的安全问题。虽然机制设计上对商户作恶有了非常好的约束。但是整体信任，仍然是建立在对少数机构的信任上的，例如唯一的托管方 BitGo。

3.2 renBTC

renBTC 是基于 Ren Protocol 发行的 ERC-20 锚定 BTC，发行量约 2 万枚，与 WBTC 共同占据了锚定 BTC 95%以上的市场。

相比于 WBTC，renBTC 的模式更为扁平，铸币和销毁机制也更去信任化。其核心思想是依赖于一个 BFT 类的网络 RenVM 实现铸币、托管与销毁，利用了

分布式签名的公证人机制来实现跨链。用户或者 DAPP 可以直接与 RenVM 中的 Darknode(即网络中的节点)交互 1:1 抵押生成 renBTC 释放到目标网络中。

3.2.1 铸币与销毁

1) 铸币

RenVM 模式下的铸币是全自动化的，因此该过程不仅可以由用户手动发起，也可以被内化到 DApp 的逻辑中，主要有如下过程：

- **转账 BTC：**用户或者 DApp 将 BTC 转移到 RenVM 的托管地址，并告知 RenVM(0 中的步骤 1、2)。值得注意的是，在未来，RenVM 的托管地址的私钥将由网络中的 Darknode 基于多方安全计算生成的，除非网络中超过 1/3 的节点联合作恶，这个私钥不会被任何一个节点掌控；但是，目前因为技术进展有限，根据其官方披露，其托管工作仍然是由“Greycore”而非 Darknode 完成的。Greycore 即 Ren 团队。
- **生成铸币签名：**RenVM 确认转账完成后，会基于前一步骤中提到的私钥生成一个铸币签名给用户或 DApp(0 中的步骤 3、4)；
- **铸币：**用户或 DApp 获取到签名后可以利用该签名完成铸币(0 中的步骤 5)。这个过程也可以在 DApp 中被触发，省去用户自行操作的成本。

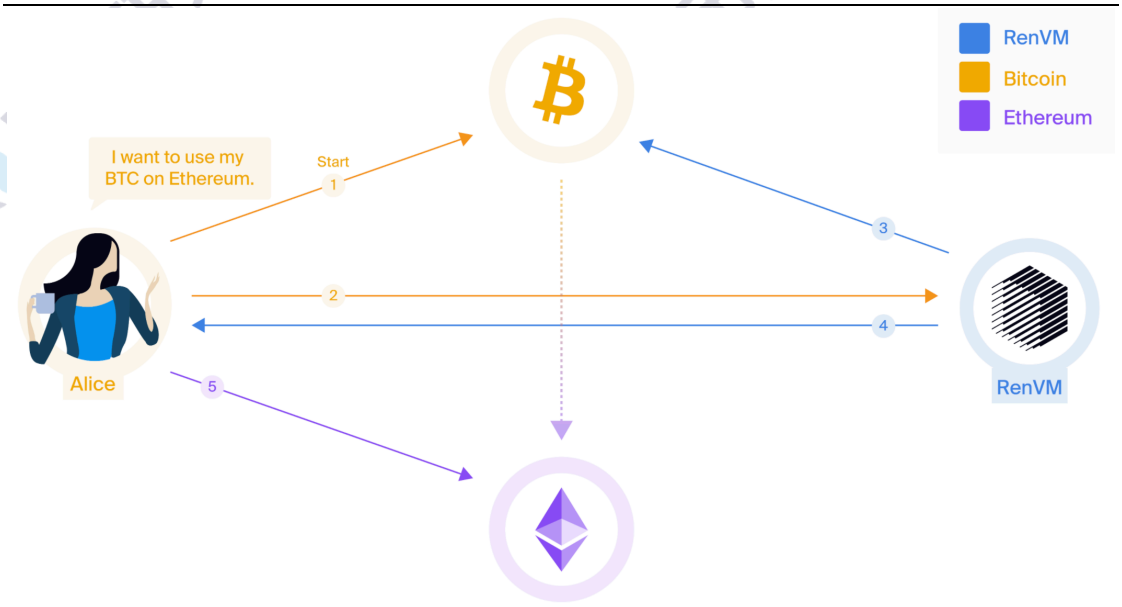

图 3-3 renBTC 的铸造过程

来源：RenVM 官方文档

2) 销毁

销毁过程相对简单，如图 3-4 所示。用户或 DApp 将 renBTC 销毁并提供其 BTC 地址，RenVM 会在交易确认后自动将 BTC 释放到该地址上。

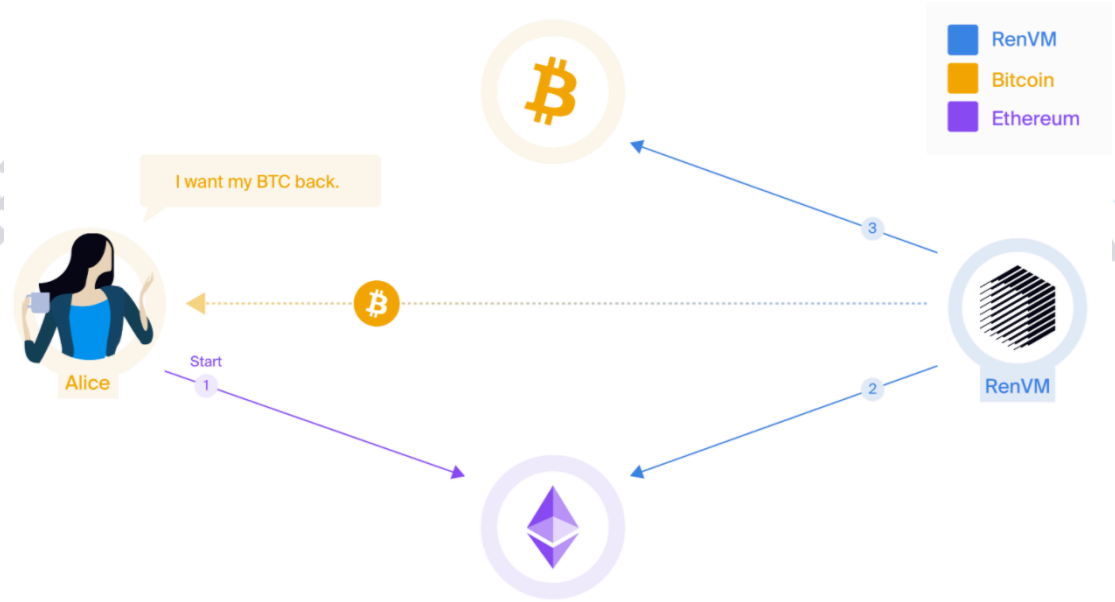

图 3-4 renBTC 的销毁过程

来源：RenVM 官方文档

除了上述经典的“销毁”过程外，RenVM 还支持销毁后在另一条链上(如波卡)再铸造 renBTC。其过程相当于是销毁和铸币过程的结合。用户或 DApp 在以太坊上销毁 BTC，并提供波卡网络上的地址，RenVM 在监测到交易后会生成一个铸币签名，用户或 DApp 使用该铸币签名可以在波卡网络上铸造出 renBTC。但目前该功能尚未得到实际应用。

3.2.2 Darknode 托管机制

RenVM 网络中的 Darknode 是整个体系的核心，铸币、销毁与托管都会经由 Darknode 处理。防止 Darknode 作恶主要通过三方面，**一方面是质押**，每个 Darknode 都需要质押 10 万枚 REN，节点作恶会被罚没一部分质押代币；**第二方面是隐私计算的技术**，多方安全计算的技术保证网络中的 Darknode 可以合作生成私钥，但每个节点都无法单独获取到整个私钥(除非超过 1/3 的节点作恶)；**第三方面是分片**，每个分片中的 Darknode 会利用 MPC 合作生成私钥，但每个分片中的 Darknode 每天会被重新随机分配的不同分片中，降低共谋的可能。

因此，在这种模式下，质押的 BTC 能实现去信任托管。但是，这是 RenVM 全部能力都实现之后的状态。当前 RenVM 按照官方的阶段还分还处于 Sub-Zero 阶段，在这个阶段下，网络由 RenVM 自己的开发团队（即 Greycore）维护，**所以在这个阶段下，RenVM 还是一个非常中心化的结构**。

3.2.3 模式优缺点

RenVM 的设计模式最大的特色之一就是其通过一个网络来桥接，实现跨链的资产传递，并且这个过程可以自动化完成，这使得其能力能被直接嵌入到智能合约中调用，能比较好地融合到 DeFi 生态中。这也是 renBTC 能成为第二大锚定 BTC 的重要原因之一。

其第二大特色是去信任化，不过在前文中也有提到，当前的 RenVM 还并没有实现这个能力，仍处于非常中心化的模式，是存在一定的资金安全风险的。

3.3 sBTC

sBTC 是通过去中心化合成资产发行协议 Synthetix 在以太坊上生成的加密货币合成资产（Synths）。其价值由网络通证 SNX 支撑，用户需首先通过一个与 Synthetix 协议交互的 dApp Mintr 超额抵押 SNX 铸造 sUSD 稳定币，然后在 Synthetix.Exchange 平台上交易新铸造的 sUSD 以换取 sBTC。整个过程不涉及跨链，也未委托第三方托管人。下面我们将依次介绍 sBTC 的发行、退出流程及该模式的优缺点。

3.3.1 发行和退出流程

1) 发行 sBTC

具体来说，sBTC 的发行流程有以下步骤：

- **发起抵押 SNX 的请求**：Mintr 中的智能合约检查用户是否可以进行抵押，其抵押率需遵照社区治理机制规定的超额抵押率，这么做的目的是为了降低 SNX 因共识度不足所导致的价值波动风险；
- **登记债务：**在经过抵押确认后，系统会在债务登记簿中添加用户所欠“债务”，并不断更新累计债务增量比率，跟踪每个抵押人的债务百分比；
- **铸币**：债务分配后，sUSD 的智能合约更新总供应量，并将新铸造的 sUSD 分配到用户的钱包中。

这样一来，用户就可以使用铸造出的 sUSD 来购买换取合成资产 sBTC。究其本质就是销毁原合成资产，生成新合成资产的过程：

- **销毁原 sUSD**：包括减少用户钱包地址中所需兑换的 sUSD 和在系统内更新 sUSD 总供应量；
- **兑换 sBTC：**按照预言机自动推送上链的汇率确定能兑换的 sBTC 数量，期间收取交易手续费；
- **交易完成：**由目标也就是 sBTC 的智能合约发行，并更新用户钱包中的 sBTC 余额和系统中 sBTC 的总供应量。

2) 退出流程

当抵押人想要退出系统解锁抵押的 SNX 时，必须首先偿还债务登记簿中所记录的剩余债务。具体流程如下：

- **确定债务：**通过 Synthetix 智能合约确定抵押人所欠债务余额；
- **销毁欠款：**销毁 sUSD，设置抵押人 SNX 余额为可转让状态，并将其从债务登记簿中删除。

sBTC 与其他锚定 BTC 最大的区别在于其不是通过抵押 BTC 生成锚定 BTC，而是通过抵押其平台代币来生成合成资产，因此不会有处理跨链交易的过程。另外，抵押品并不直接生成 sBTC，而是先生成 Synthetix 体系内的交易媒介 sUSD，再由 sUSD 去交换 sBTC。

3.3.2 模式优缺点

在该种模式下，sBTC 的交易主要是根据智能合约执行，不涉及交易簿和交易对手，通过预言机追踪资产实时价格信息来分配汇率，实现合成资产的自由转换，没有滑点问题。另外，Synthetix 协议对 SNX 质押人也提供了激励，包括交易奖励和代币增发奖励。前者通常按照 0.3%的比率对每笔在 Synthetix.Exchange 上完成的交易收取交易手续费，然后存入费用池中每周按比例分配给 SNX 抵押人；后者是利用 Synthetix 协议自身通胀政策产生新增 SNX，同样每周按比例分配给 SNX 抵押率不低于目标阈值的抵押人。

但 Synthetix 的债务计算会随着系统内汇率变动而波动。这意味着，即便用户在借出 sBTC 后没有做任何操作，只要 BTC 上涨，用户的债务就会增加，在归还时需要归还更多的 sUSD；不仅如此，即便用户只借出了 sUSD，但如果由于别的用户的资产价格上涨导致系统整体债务的增加(比如别的用户用借出的 sUSD 换取了 sBTC，结果 sBTC 价格上涨导致系统整体债务增加)，该用户也需要归还更多的 sUSD。

此外，作为抵押物的原生代币 SNX 价值波动也会对系统造成不良影响，当 SNX 的价格大幅下跌，用户可能会选择不补充抵押品偿还债务造成系统抵押不足，从而影响整个体系，这也是 Synthetix 设置了超高倍数(750%)的抵押资产规则的原因。同时，SNX 作为抵押资产，其市值上限也会约束合成资产的上限。此外，该模式还面临着预言机风险、不完善的清结算机制和繁琐的债务计算方法等问题，在后续发展中，还有待改进和完善。

3.4 其他锚定 BTC

HBTC

HBTC 是 Huobi 于 2020 年 2 月在以太坊上推出的 ERC-20 标准锚定币，该资产 1：1 锚定 BTC，由 Huobi 负责铸币、销毁以及托管，截至目前（2020 年 10 月）HBTC 合约地址内发行数量已超过 6000 枚，活跃在如 Uniswap、Curve、Balancer、Nest 等应用中。

用户可以通过 HuobiGlobal 或 HBTC 官网进行双向兑换业务。将 BTC 资产充入 Huobi Global，在提现时选择提出 HBTC 资产，或者在 HBTC 官网存入 BTC 就可以快速换取到 HBTC 资产。同理，兑换为 BTC 的过程就是将 HBTC 资产充入 Huobi Global，在提现时选择提出 BTC 资产或者在 HBTC 官网存入 HBTC 来换回 BTC 资产。

tBTC

tBTC 是由 Keep Network、Cross-Chain Group 和 Summa 联合在以太坊上发行的 ERC-20BTC 锚定币，发行时间为 2020 年 5 月，上线近半年发行量超过 900 枚。

tBTC 使用 t-ECDSA 椭圆曲线签名算法来签署交易，运行机制开源透明；另外，tBTC 最大的特点就是去信任化，它使用了“签名者团体”系统。当用户要铸造一个新的 tBTC 时，系统通过随机信标从“团体”中选择三个签名者，并在

BTC 网络上为用户创建一个地址，用于锁定参与兑换的 BTC。当三个签名者行动一致并且 BTC 成功锁定后，新的 tBTC 才会按照 1：1BTC 的比例铸造出来。而为了保证这个去中心化系统稳定运转，签名者必须超额抵押价值用户所存 BTC 1.5 倍的以太坊，一旦任何签名者出现作恶行为，这份抵押将被系统全部没收并归还给被盗用户，得不偿失。

但同时，为了最大程度地实现去信任化，tBTC 牺牲了其扩展性。例如，单次兑换只允许 1BTC，且兑换完成后有长达半年的锁定期，这对用户来说是非常不友好的；同时，签署者需要 150%的超额抵押也给签署者设置了很高的资金门槛，导致了该模式的隐形天花板；另外，技术上的瓶颈也是限制其发展的重要因素之一，tBTC 依托的 Keep 协议进展缓慢，且没有经过验证，主网上线仅两天时间就发生了重大安全漏洞事件，导致项目紧急暂停。如果后续能突破技术瓶颈，还是具备较大的发展潜力。

oBTC

oBTC 是一个较新的锚定 BTC 币种，是由 BoringDAO 基于 ERC-20 发行的 1：1 锚定 BTC 的代币，主网于 2020 年 11 月 12 日上线。目前铸币量达到 800 枚，其期望搭建一个衔接不同区块链的去中心化资产桥，并以 DAO 的形式扩展其兼容性。

oBTC 的铸币过程比较简单。用户将 BTC 发送到机构和社区控制的多签名托管地址，并通过 BTC 的 op_return 功能向对方提供自己的以太坊地址。当托管者收到资金并在网络达成共识后后，便在以太坊上铸造等值的 oBTC 并将这些锚定代币发送到用户的 ETH 地址上。期间会收取资产总价值的 0.2%作为铸币手续费，但是能够通过铸币挖矿获取 0.4% BOR 补贴。整个过程用户提供自己的 ETH 地址和需兑换的 BTC，进行一次转账操作即可。因为 op_return 是 BTC 原生功能，因此整个过程中不需要借助任何中心化服务器。

其运行模式基于“隧道”，即其为每种区块链资产都创建了一个以 DAO 形式

运营的、在区块链资产和 ERC-20 代币之间进行铸币和赎回的隧道。任何社区用户都可以通过质押来创建新的隧道，但每种加密货币只能有一个隧道，在本文中主要关注 BTC 的隧道。

资金安全方面，BoringDAO 采用了三层质押机制，换句话说，每一枚 oBTC 都有大约 200%的抵押物，其中 100%由原生区块链资产也就是 BTC 组成；第二层约 100%由隧道合约层抵押 BOR 等其它资产。第三层还有一些链上保险。这样一来，即便发生黑天鹅事件，社区也可以通过合约层清算和保险来补偿用户。

imBTC

imBTC 是 imToken 旗下 Tokenlon 负责发行、托管和承兑的以太坊 ERC-777 代币，上线时间为 2019 年 10 月，总发行量已超过 900 枚。其托管地址公开透明，用户可以通过链上信息跟踪所有 imBTC 的铸造和销毁，保障与 BTC1：1 锚定。

imBTC 发行的锚定币是通过“锁仓兑换”的方式产生的，用户每将一个 BTC 锁定在 Tokenlon 账户内，就能认购相同数量的 imBTC，也可以通过 DApp 调用智能合约将 imBTC 销毁。同时，为了补偿质押在 Tokenlon 安全冷钱包中 BTC 产生的流动性损失，用户可以获得交易手续费和赎回手续费的补贴。此外，与其他锚定 BTC 代币不同的是，imToken 基于的是 ERC-777 而不是 ERC-20 协议，ERC-777 是 ERC-20 协议的升级版，具有简化交易流程、避免误发导致的代币丢失等优点，可以看出 Tokenlon 是希望选用更好的协议带来更好的用户体验。

凭借 imToken 的用户基础，按理说 imBTC 有着与生俱来的优势。但上线时间已过一年，发展态势仍不温不火，其原因可能与 ERC-777 代币与 Uniswap/Lendf.me 合约组合存在重入攻击漏洞有关。攻击者曾通过多次迭代调用名为 tokensToSend 的方法函数来盗取平台上的 ETH/imBTC 交易对。

pBTC

pBTC 是 pTokens 公司于 2020 年 3 月基于 TEE 技术在以太坊上发行 BTC 锚定币，其同样与 BTC1：1。pBTC 中心化色彩较淡，未来计划向 DAO 模式转变，目前在以太坊上发行数量大约为 200 枚

使用 pTokens，用户可以通过可信计算来铸造 pBTC，用户只需在对应的 pToken 智能合约上存入一定数量的 BTC 并提供接收地址，交易就会在一组可信执行环境（TEE）中进行，在经过飞地（the enclave）程序验证后，相应金额的 pBTC 就会铸造并转移到用户提供的地址上，整个过程透明可见，并且不收取中间费用。

3.5 潜在风险

目前，这些锚定 BTC 在比特币层，从未出现过资产丢失、被盗的安全事故。不过在以太坊层曾经发生一次事故，imBTC 因为采用了 ERC-777，其中有一些因素导致其在 Lendf.me 和 Uniswap 上被黑客盗取了流动性池，不过其比特币层的 BTC 资产仍然是安全的。

因为比特币层的技术是相对稳健的，并没有复杂的合约逻辑，因此出现风险的概率相对较低。再加上，目前 BTC 锚定币总量已经突破十五枚，因此有效增加了铸币者对于此类技术的信心。

当然，没有出现过安全事故，不代表说这些锚定币绝对安全的，例如黑客盗取、内部盗取、私钥损毁等“黑天鹅”风险是始终存在的。如何更好地应对这些潜在风险，每一个托管方都需要未雨绸缪。

四、总结

短短半年，十五万枚 BTC 以“八仙过海”的方式完成了跨链。受制于 BTC 本身的技术特点，BTC 几乎不可能有非托管的方案。因此，目前 98%以上的 BTC 使用了“托管+映射”方案。考虑到目前这些方式运转都较为顺利，并未出现安全事故，而且 DeFi 仍然在持续提供 yield-farming 奖励，因此，铸币者

意愿较高，其整体发展势头仍是向上的。同时，客观上，这样的跨链既为 BTC 带来了智能合约功能和性能提升，也为以太坊区块链增加了资产总量。所以，我们认为未来还会有更多 BTC 进入以太坊网络中，也许还能再提高一个数量级。

参考文献和资料

[1] WBTC 官网：https://wbtc.network/

[2] renVM 官方文档：https://github.com/renproject/ren/wiki

[3] HBTC 官网：https://www.htokens.finance/zh-cn/

[4] Synthetix 官方文档：https://synthetix.community/docs/intro

[5] Keep Network 官方文档：https://github.com/keeperdao/docs/wiki

[6] BoringDAO Whitepaper: https://boringdao-prod.oss-accelerate.aliyuncs.com/BoringDAO_WhitepaperV2.52.pdf

[7] pBTC 官网 https://ptokens.io/how-it-works

关于火币研究院

火币区块链应用研究院（简称“火币研究院”）成立于 2016 年 4 月，于 2018 年 3 月起致力于全面拓展区块链各领域的研究与探索，以泛区块链领域为研究对象，以加速区块链技术研究开发、推动区块链行业应用落地、促进区块链行业生态优化为研究目标，主要研究内容包括区块链领域的行业趋势、技术路径、应用创新、模式探索等。本着公益、严谨、创新的原则，火币研究院将通过多种形式与政府、企业、高校等机构开展广泛而深入的合作，搭建涵盖区块链完整产业链的研究平台，为区块链产业人士提供坚实的理论基础与趋势判断，推动整个区块链行业的健康、可持续发展。

联系我们：

咨询邮箱： huobiresearch@huobi.com

官方网站： https://research.huobi.cn

微信公众号： HuobiCN

新浪微博： 火币区块链研究院
https://www.weibo.com/u/6690456123

Twitter： Huobi_Research
https://twitter.com/Huobi_Research

Medium： Huobi Research
https://medium.com/@huobiresearch

欢迎加入研究院学习交流小组

扫码添加学习小助手微信

免责声明

1. 火币区块链研究院与本报告中所涉及的项目或其他第三方不存在任何影响报告客观性、独立性、公正性的关联关系。
2. 本报告所引用的资料及数据均来自合规渠道，资料及数据的出处皆被火币区块链研究院认为可靠，且已对其真实性、准确性及完整性进行了必要的核查，但火币区块链研究院不对其真实性、准确性或完整性做出任何保证。
3. 报告的内容仅供参考，报告中的结论和观点不构成相关数字资产的任何投资建议。火币区块链研究院不对因使用本报告内容而导致的损失承担任何责任，除非法律法规有明确规定。读者不应仅依据本报告作出投资决策，也不应依据本报告丧失独立判断的能力。
4. 本报告所载资料、意见及推测仅反映研究人员于定稿本报告当日的判断，未来基于行业变化和数据信息的更新，存在观点与判断更新的可能性。
5. 本报告版权仅为火币区块链研究院所有，如需引用本报告内容，请注明出处。如需大幅引用请事先告知，并在允许的范围内使用。在任何情况下不得对本报告进行任何有悖原意的引用、删节和修改。