WBTC FUD背后 1.2万亿比特币流动性如何安全解锁

你听说过 WBTC 么？

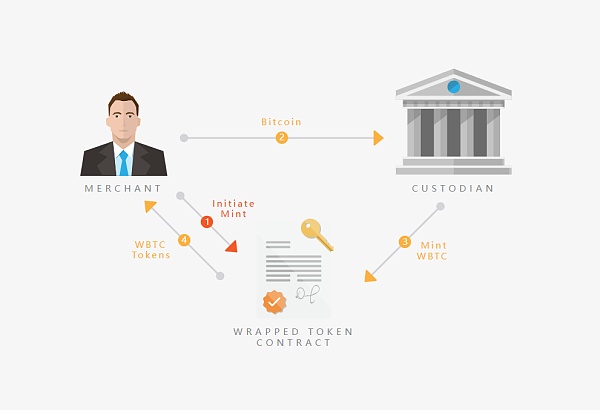
经历过 DeFi Summer 的老炮们一定对它耳熟能详，作为 2018 年诞生的最早一批稳定币，2022 年 WBTC 扮演了将比特币流动性带入 DeFi 和以太坊生态的旗手角色。

只是 WBTC 在近期却遭遇一场信任危机风波——8 月 9 日，BitGo 官宣与香港企业 BiT Global 的合资企业，并计划将 WBTC 的 BTC 管理地址迁移至这个合资企业的多签，而这个香港企业 BiT Global 的背后正是孙宇晨。这也由此引发市场对后续 WBTC 实控权安全性的纷纷讨论，同时孙宇晨回应称 WBTC 与之前相比没有任何变化，审计是实时进行的，完全由托管方 Bit Global 和 BitGo 按照与之前相同的程序进行管理。不过就在这一消息曝光后的过去 6 天内，仅 Crypto.com 和 Galaxy 就赎回了超 2700 万美元的比特币，也说明市场仍疑虑未消，本文就将探究 WBTC 运行机制，并一窥去中心化比特币稳定币的发展现状。

## 1.WBTC 风波背后的稳定机制缘由

我们可以首先简单温习一下 WBTC 的稳定机制，就能明白此次信任危机的核心争议点。作为基于以太坊的 1:1 完全抵押比特币的 ERC20 Token，WBTC 的运行依赖于一个联合体模型，有点像现有的银行二层运营体系，在托管商（此前仅 BitGo 一家）和普通用户之间还存在“承兑商”（需要资格认证，多家）的角色。

而承兑商则扮演了零售的角色，它们直接面向普通用户，执行必须的 KYC/AML 过程，验证用户的身份，最终为用户提供获取和兑换 WBTC 的服务，因此在这个过程中起到了桥梁的作用，可以大大促进 WBTC 在市场中的流通和交易；



来源：WBTC 官网

这就意味着，本质上托管商直接决定了 WBTC 处的铸造、燃烧和托管的可信度，是绝对中心化的存在——用户需要完全信任托管商不会有任何弄虚作假的行为，会严格按照规定进行 WBTC 的铸造和燃烧。譬如，如果托管商收到了 100 枚 BTC，但实际上却滥发了 120 枚 WBTC，抑或是将托管的 100 枚 BTC 进行再抵押等形式的挪用，那都是在破坏整个系统的平衡和信任基础。尤其是潜在的超发行为，会导致 WBTC 的价值与实际抵押的比特币价值脱钩，引发市场的混乱和投资者的恐慌，随时可能导致整个稳定币运行机制的崩塌。此前，WBTC 一直都只有 BitGo 作为唯一的托管商，而作为老牌的加密托管服务方，BitGo 从某种程度上来说也经受住了市场和时间的考验，为 WBTC 的发展提供了相对稳定的保障——从数据维度看，目前全网共发行了超 15.42 万枚 WBTC，总价值逾 90 亿美元，也说明了市场对 BitGo 的信赖。



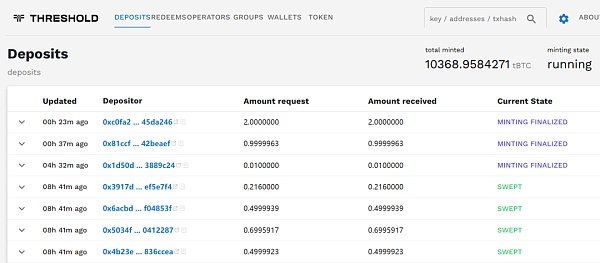
来源：WBTC 官网

所以归根结底，还是因为 WBTC 的储备资产多签权限要从 BitGo 转移到由孙宇晨控制的合资企业。这其实也折射出了对 WBTC 自身运行机制的中心化隐忧，市场因此也在呼吁探索去中心化的解决方案，以降低对中心化托管商的过度依赖，尤其是通过区块链技术减少单点故障和人为操纵的风险，提高 BTC 稳定币运行机制的安全性和可靠性。

## 2.几经沉浮的去中心化 BTC 赛道

其实早从上上一轮牛市周期开始，各式去中心化的 BTC 稳定币方案就是一个重要的创新赛道，诸如 renBTC、sBTC 等相继爆发，成为比特币进入 DeFi 生态的重要管道，并把 BTC 大体量的资金引到以太坊，也盘活了不少 BTC Holder 的多元化收益渠道。只是一轮轮牛熊过去，大部分昔日的明星项目相继折戟沉沙。首先是此前声量最大的 renBTC，当时几乎和 WBTC 各自代表了去中心化与中心化的 BTC 稳定币解决方案——它的整个发行过程较为去中心化，即用户将原生 BTC 存入指定的 RenBridge 网关作为抵押，RenVM 通过智能合约在以太坊网络中发行对应的 renBTC。且项目方与 Alameda Research 关系相当密切（没错，Alameda 其实收购了 Ren 团队），这也一度成为它的最大亮眼标签，但福祸相依，在 FTX 危机后 Ren 毫不意外地受到波及，不仅运营资金断裂，而且资金大规模外逃。虽然后续也尝试了自救，但截至发文时，最新的对外披露进展还停留 2023 年 9 月的 Ren 基金会公告，现下来看，几乎相当于脑死亡。

其次，Synthetix 推出的 sBTC 则是通过 SNX 质押生成的比特币合成资产，也曾是主要的去中心化比特币锚定币之一，只不过今年上半年 Synthetix 完全废除以太坊上的非 USD 现货合成资产，其中就包括 sETH 和 sBTC，始终未能大幅在 DeFi 生态中推广开来。目前最有意思的还在运行的项目实践，应该就是 Threshold Network 的 tBTC 产品。没错，它和此前 Keep Network 知名的 tBTC 其实是一脉相承的——Threshold Network 就是 Keep Network 后来与 NuCypher 合并而来的新项目。其中 tBTC 用在网络上运行节点的随机选择的一组运营商取代了中心化中介机构，这些运营商共同使用 Threshold 加密技术来保护用户存入的比特币，简言之就是用户资金由运营商的多数共识控制。截至发文时 tBTC 的总供应量超 1 万枚，总价值近 6 亿美元，而半年前则只有不到 1500 枚，增长还是相当迅速。



来源：Threshold Network

总而言之，各家方案的竞争，本质上还是围绕资产安全这个核心，而伴随着此次风波 WBTC 揭开了去中心化稳定币市场需求的盖子，未来无论是 tBTC 还是其他类似的项目，都需要在保障资产安全的基础上，不断完善自己的去中心化设计，以满足市场和用户的需求。

## 3.比特币 L2 的新解？

其实，无论如今的 WBTC、tBTC，还是曾经的 renBTC、sBTC，原因也很简单也很无奈，只有桥接到以太坊生态，借助其丰富的 DeFi 场景，才能有效释放比特币资产的流动性——某种角度上说，1.16 万亿美元体量的比特币（2024 年 8 月 15 日最新 CoinGecko 数据），正是加密世界最大的“沉睡资金池”。因此 2020 年 DeFi Summer 开始后，WBTC、renBTC 等就成了最主要的一种释放比特币资产流动性的尝试：用户可以质押 BTC，获得对应的封装Token，从而作为流动性桥接至以太坊生态，通过与以太坊生态耦合来参与 DeFi 等链上场景。这种依赖以太坊的困局，直到 2023 年由 Ordinals 热潮带起的比特币生态大爆发才终于迎来了新解——比特币 L2 为用户提供了新的可能，使大家能够直接在基于比特币的 L2 参与各种智能合约应用，如质押、DeFi、社交，甚至更复杂的金融衍生品市场，大大扩展了比特币资产的范围和价值。以 Stacks 推出的 sBTC（与上文 Synthetix 的 sBTC 同名）为例，作为一种去中心化的 1:1 比特币支持资产，sBTC 可以在比特币和 Stacks L2 之间部署和移动 BTC，并在交易中用作 Gas，而不需要额外的其他加密货币。，将智能合约引入比特币生态系统，再以去中心化的方式将比特币带入 DeFi 世界。未来随着比特币 L2 的持续演进和技术创新，类似于 sBTC 这样的新方案有可能会侵蚀 WBTC 等封装Token的市场，进一步提升比特币资产的流动性和应用场景。

## 4.小结

回过头看，其实 2020 年以来封装Token+以太坊的形式并未做大，总体吸引的 BTC 资金流入有限，只能算是比特币释放流动性的 1.0 模式。

不过坦诚地说，如果我们只是把比特币作为一个万亿美元级别的优质资产池，那没必要重复造轮子再搞一个比特币 L2，「封装Token+以太坊」的链上生态和 DeFi 用例就很够了——其实如今绝大部分的比特币 L2 的逻辑，也和当年把 BTC 用 tBTC、renBTC 这些 ERC20 封装Token引入 EVM 生态没有本质区别。只是从原生安全性和盘活比特币生态价值的角度，比特币 L2 的出现就具有了重要意义，即更好地保障比特币资产的安全，并遏制其跌落到以太坊生态，让肉烂在自己锅里。

此次 WBTC 的危机引起不小波动，对于比特币稳定币的未来发展你怎么看？欢迎评论交流。