孙宇晨入局WBTC惹争议 解析BTC锚定币及其安全性

作者：Hotcoin Research

### 引言

近期关于 WBTC 项目控制权转移的市场关注度十分火热，孙宇晨（Tron 创始人）宣布参与 WBTC 项目的消息迅速引发了加密社区的广泛争议，讨论焦点主要集中在 WBTC 的安全性、去中心化程度以及孙宇晨个人影响力对项目的潜在影响。



WBTC自2019年推出以来，已经成为比特币跨链应用的重要桥梁，通过将比特币锚定为ERC-20代币，WBTC为比特币带来了更广泛的DeFi应用。然而，WBTC的中心化托管模式也使其长期以来备受争议。孙宇晨的入局，再次激起了人们对这一问题的讨论，特别是在跨链资产安全性以及去中心化治理的重要性方面。

本文将通过对BTC锚定币的概述、机制原理以及代表性项目的深度解析，探讨孙宇晨入局WBTC所引发争议的根源，并展望BTC锚定币的未来发展方向。

## 一、BTC锚定币概述

### 1.1 定义和基本原理

BTC锚定币是一种通过特定的技术手段将比特币映射到其他区块链网络上的数字资产。这类代币通常通过1:1的方式与比特币挂钩，即每发行一枚BTC锚定币，背后都会有等量的比特币作为抵押。这一机制使得BTC锚定币在其他区块链上（如以太坊）能够具备比特币的价值属性，同时能够参与到这些区块链的去中心化应用DApps中。

BTC锚定币的产生主要是为了弥补比特币自身网络在智能合约功能上的不足，使得比特币可以在更复杂的金融生态中发挥作用。虽然比特币是最早且最具共识的加密货币，但其网络缺乏图灵完备性，无法直接支持智能合约和其他复杂的去中心化金融操作。例如，以太坊上的ERC-20标准代币可以轻松融入DeFi协议，而通过将比特币映射为ERC-20或其他标准的代币形式，可以使其在以太坊等智能合约平台上使用，参与到借贷、流动性挖矿、衍生品交易等多种DeFi场景中，从而极大地扩展了比特币的应用范围。

### 1.2 BTC锚定币的需求和意义

（1）跨链流动性的需求

比特币作为全球市值最高、流动性最强的加密货币，其用户数量和持有量远远超过其他加密资产。如果比特币能够无缝流动到其他区块链上，特别是那些具备智能合约功能的平台，将极大地提升其使用场景和价值创造能力。BTC锚定币正是为了满足这种跨链流动性的需求。通过BTC锚定币，比特币得以在其他区块链上发挥其资产优势，参与到更为多样化的去中心化应用中，例如借贷、流动性挖矿和衍生品交易等。

（2）去中心化金融（DeFi）发展的推动力

比特币作为“数字黄金”，在DeFi中具有极大的潜力。然而，由于比特币网络本身的技术局限性（如缺乏智能合约功能），直接在比特币网络上开发DeFi应用具有相当大的挑战性。因此，将比特币“搬迁”到具备智能合约功能的区块链上（如以太坊），成为了实现这一目标的关键路径。BTC锚定币通过将比特币映射到以太坊等区块链上，使其能够参与到DeFi生态中。这不仅提升了比特币的利用率，也为DeFi应用注入了更多的流动性和稳定性。

（3） 资产增值和风险管理工具

通过BTC锚定币，持有者可以在不放弃比特币长期持有的前提下，通过参与DeFi生态获取额外的收益。例如，持有WBTC的用户可以将其抵押在DeFi平台上，借出稳定币用于其他投资，或参与流动性挖矿赚取奖励。此外，一些去中心化交易所还提供了BTC锚定币与其他资产之间的交易对，为投资者提供了更多的套利机会。此外，BTC锚定币还可以作为一种风险管理工具，使用BTC锚定币作为抵押品，可以有效降低投资组合的风险，起到稳定器的作用。

（4）提升比特币网络的实际效用

比特币网络是最早出现的区块链，具有高度的安全性和共识强度。然而，其自身的技术限制使得比特币的应用场景相对有限，主要集中在价值存储和简单的支付转账上。随着时间的推移，市场对比特币的需求已经不再局限于这些基础功能，而是希望能够在更广泛的金融服务中使用比特币。BTC锚定币的出现，为比特币提供了更广阔的应用舞台。通过在其他区块链上发行锚定币，比特币得以在这些链上参与到更复杂的金融操作中，不仅提高了比特币的实际效用，也巩固了其作为全球首选数字资产的地位。

## 二、BTC锚定币的机制原理

### 2.1 中心化锚定与去中心化锚定

BTC锚定币的核心在于如何将比特币锁定在其原生链上，并通过跨链技术生成与其等值的代币。根据这一核心机制的不同，BTC锚定币的工作机制可以分为中心化和去中心化两大类。

中心化锚定机制依赖于可信的第三方托管机构，这些机构负责保管用户锁定的比特币，并根据锁定的比特币数量铸造相应的锚定代币。例如，WBTC就是一种典型的中心化锚定币。用户将比特币发送至托管机构（如BitGo），由托管机构负责管理这些比特币，同时在以太坊网络上铸造等量的WBTC代币。当用户希望赎回比特币时，托管机构则销毁相应数量的WBTC，并将比特币返还给用户。这种模式的优点在于操作简便且交易速度较快，但由于依赖中心化机构，存在信任风险和集中化管理的潜在安全隐患。

去中心化锚定机制则通过分布式网络和加密技术来实现比特币的跨链转移和代币化。以renBTC为例，其工作机制不依赖单一机构，而是通过Ren Protocol的分布式节点网络来管理和验证比特币的锁定和代币铸造。Ren Protocol使用安全多方计算（MPC）技术，将比特币的托管过程分布在多个独立的节点上，确保没有单个节点可以控制比特币的私钥。这种机制大幅减少了中心化风险，增强了系统的安全性和透明性。然而，由于技术复杂度较高，去中心化锚定币的铸造和赎回过程通常较为复杂且时间较长。

### 2.2 铸造与销毁过程

BTC锚定币的铸造和销毁过程是其工作机制的核心环节，这两个过程分别代表着比特币与锚定币之间的转换。

铸造过程：铸造BTC锚定币的过程通常涉及将原生比特币锁定在一个多签名地址或智能合约中，并在目标区块链（如以太坊）上生成等量的锚定代币。以WBTC为例，当用户希望获得WBTC时，他们需要将等量的比特币发送至BitGo管理的托管地址。一旦比特币的交易得到网络确认，BitGo会在以太坊上通过智能合约铸造等量的WBTC，并将其发送到用户的以太坊地址，用户可以通过区块浏览器验证每一步操作。

销毁过程：当用户希望将BTC锚定币兑换回比特币时，需要触发销毁过程。用户首先将锚定币（如WBTC）发送至相应的智能合约进行销毁，同时向托管机构发出赎回比特币的请求。一旦销毁交易得到确认，托管机构将原本锁定的比特币释放，并发送到用户指定的比特币地址。

在去中心化模式下，如renBTC的铸造和销毁过程更加复杂，涉及分布式网络节点的共识与协作。用户发送比特币至Ren Protocol的托管地址后，多个独立的节点会进行验证，并通过安全多方计算技术共同生成renBTC。销毁过程则是通过逆向操作，将renBTC销毁后，由多个节点共同决定释放相应的比特币。

### 2.3 去中心化托管与信任模型

与中心化托管不同，去中心化托管通过分布式网络和加密技术来确保比特币的安全管理，避免了对单一机构的过度依赖。

多方签名机制：以tBTC为例，其使用了多方签名（threshold signature）机制，随机选择多个签名者来共同管理比特币的私钥。这些签名者通过提供抵押物（如ETH）来确保其行为的正当性，如果签名者试图进行恶意操作，他们将面临经济损失。这种机制在理论上可以实现更高的安全性和去中心化。

安全多方计算（MPC）：Ren Protocol采用了MPC技术，允许多个节点在不泄露私钥的情况下共同参与比特币的管理。这种技术确保了即使个别节点遭受攻击，整个网络的安全性也不会受到影响。通过这种方式，Ren Protocol实现了BTC锚定币的去中心化管理。

### 2.4 跨链通信与智能合约执行

BTC锚定币的跨链操作离不开跨链通信协议和智能合约的执行。跨链通信协议负责在比特币网络和目标区块链（如以太坊）之间传递信息，而智能合约则用于自动化管理铸造、销毁等操作。

跨链通信：跨链通信通常依赖于中继器或观察者，这些组件监控比特币网络的交易情况，并将相关信息传递至目标区块链。以Ren Protocol为例，Ren的Darknodes节点负责监听比特币网络中的交易，并将其信息广播至以太坊网络，触发相应的智能合约操作。

智能合约执行：智能合约是BTC锚定币工作的自动化核心。无论是WBTC的中心化铸造过程，还是renBTC的去中心化铸造过程，都离不开智能合约的执行。这些合约确保每一笔代币的铸造和销毁操作都是透明且不可篡改的，同时自动处理用户请求、验证交易和更新链上数据。

## 三、BTC锚定币代表项目与现状分析

最早期的BTC锚定尝试主要集中在跨链技术的探索上。早期的尝试包括比特币的侧链概念，如Rootstock（RSK），试图通过侧链的方式实现比特币与其他区块链的互操作性。然而，这些早期的项目由于技术复杂性和实施难度较大，并未在市场上取得广泛应用。

### 3.1 WBTC的诞生与市场化应用

2018年，WBTC（Wrapped Bitcoin）项目正式推出，成为BTC锚定币发展的重要里程碑。WBTC由BitGo、Kyber Network和Ren Protocol等多家机构联合发起，是第一个在以太坊上实现1:1比特币锚定的ERC-20代币。WBTC通过中心化托管的方式，将比特币锁定在BitGo的托管账户中，并在以太坊上铸造等量的WBTC代币。WBTC的出现为比特币在以太坊生态中的应用打开了大门，使得比特币可以参与到DeFi应用中，由于其透明性和较高的市场接受度，WBTC迅速成为市场上最受欢迎的BTC锚定币之一。

根据WBTC官网数据，目前WBT的发行量达到15万个，价值约90亿美元。其中40.6%用于借贷，32.6%为买入和持有、11.3%用于跨链互操作性。





### 3.2 去中心化锚定币的崛起

随着DeFi市场的快速发展，用户对去中心化和安全性的需求日益增加。一些去中心化的BTC锚定币项目应运而生，旨在避免中心化托管带来的信任风险。

renBTC： renBTC由Ren Protocol推出，是一种去中心化的BTC锚定币。Ren Protocol通过使用安全多方计算（MPC）技术，实现了比特币的跨链转移和托管。Ren的网络由一系列分散的节点（称为Darknodes）组成，这些节点共同负责比特币的托管和renBTC的铸造。renBTC的主要优势在于去中心化程度高，降低了对单一机构的信任依赖，但其技术复杂度也相对较高。

tBTC： tBTC是由Keep Network推出的另一种去中心化BTC锚定币。tBTC采用了一种独特的多方签名（threshold signature）方案，随机选择多个签名者来共同管理比特币的跨链转移。tBTC的设计目标是最大限度地减少对中心化机构的依赖，确保用户对其比特币的完全控制权。然而，tBTC也因为其复杂的机制和较高的技术门槛，在推广上面临一定挑战。

### 3.3 BTC锚定币的多样化与生态扩展

随着更多区块链平台的出现和市场需求的多样化，BTC锚定币开始向多样化和多链化方向发展。不仅在以太坊上，其他区块链平台如Binance Smart Chain、Tron和Polygon等也开始支持BTC锚定币的发行和应用。

sBTC（Synthetix BTC）：由Synthetix平台发行，作为一种合成资产，通过超额抵押的方式模拟比特币的价格变化。sBTC为用户提供了更多的灵活性，尤其是在合成资产交易和DeFi应用中。

BBTC（Binance Wrapped BTC）：由Binance推出，严格遵循1:1的资产担保原则，实现了BTC在以太坊和Binance Smart Chain上的无缝流动。

### 3.4 BTC锚定币现状分析

WBTC的主导地位：截至2024年8月，WBTC仍然是市场上占主导地位的BTC锚定币，占比高达94.7%。这一数据表明，尽管市场上存在多种BTC锚定币，WBTC凭借其较早的市场进入时间、广泛的DeFi支持以及较高的信任度，仍然是用户的首选。

其他BTC锚定币的表现：tBTC、BBTC和HBTC在市场上也有一定的占有率，但总量相对较少。其中，tBTC占比为1.9%，BBTC为1.8%。这些BTC锚定币主要用于特定应用场景或由特定社区支持。





## 四、BTC LSD代币的兴起

质押和再质押概念的兴起，为BTC锚定币带来了新的发展方向。Babylon推出非托管的比特币质押方案，通过密码学方式实现比特币质押，并生成流动性质押代币。这一项目通过提高质押资产的资本效率，开辟了BTC staking的新赛道。

### 4.1 stBTC

stBTC是BTC LSD代币中的一个重要代表，由Lorenzo Protocol推出。stBTC的铸造过程涉及将原生比特币质押在Lorenzo Protocol的托管合约中，然后根据质押的比特币数量生成相应的stBTC代币。用户可以将stBTC用于其他金融活动，并在需要时通过销毁stBTC代币来赎回原生比特币。stBTC不仅提高了比特币的资本利用率，还允许持有者在DeFi生态中自由流动和增值。

### 4.2 LBTC

LBTC是由Lombard推出的一种BTC LSD代币，旨在通过去中心化的质押管理，为比特币持有者提供更加安全和透明的质押收益。与stBTC类似，用户能够通过铸造LBTC参与DeFi生态系统，利用LBTC在去中心化交易所、借贷协议和收益策略平台中获取收益。用户还可以将LBTC委托给Babylon，获取权益证明（PoS）安全性收益。除此之外，Babylon还为存入的BTC提供额外的奖励激励，包括可能的收益和其他激励措施。

### 4.3 SolvBTC

SolvBTC是由Solv推出的一种BTC LSD代币，旨在通过整合比特币和以太坊等多个链上的质押收益，提供一种高效的流动性质押解决方案。SolvBTC通过创新的去中心化资产管理架构，为用户提供更灵活的质押和流动性管理服务。由于其集成了多链质押收益，SolvBTC为用户提供了更广泛的投资和套利机会。用户可以将SolvBTC用于多种DeFi协议，如去中心化交易所、借贷协议和收益农场，并在需要时通过销毁SolvBTC赎回相应的资产。

## 五、BTC锚定币的风险与机遇分析

BTC锚定币作为一种将比特币引入其他区块链生态的创新工具，在提升比特币流动性、扩大其应用范围方面展示了巨大的潜力。然而，正如其他金融创新一样，BTC锚定币在发展过程中也伴随着一系列的风险和挑战。

### 5.1 BTC锚定币的风险分析

（1）中心化风险：托管机构的安全性至关重要。一旦托管机构遭到黑客攻击或内部管理不善，可能导致比特币的丢失或盗窃，从而严重影响锚定币的价值和市场信心。中心化托管也意味着如果托管机构出现运营问题，如破产、监管干预或其他形式的失败，用户可能无法赎回他们的比特币，面临资金损失的风险。

（2）技术风险：去中心化协议通常涉及多方签名、MPC（安全多方计算）等复杂技术。这些技术的实现需要高度精确的代码和精细的管理，一旦出现漏洞或设计缺陷，可能导致系统崩溃或安全事故。去中心化锚定币依赖于多个节点之间的共识。如果这些节点遭到攻击、出现故障或发生恶意行为，可能会影响锚定币的稳定性和安全性。

（3）智能合约漏洞：BTC锚定币通常通过智能合约管理铸造和销毁过程。智能合约代码一旦部署就难以更改，任何未发现的漏洞可能会被恶意利用，导致资金损失。历史上曾发生过多次由于智能合约漏洞而引发的大规模攻击事件，BTC锚定币项目也不例外。BTC锚定币往往与其他DeFi协议进行互操作，这种依赖关系可能会带来额外的风险。如果与之交互的协议发生故障或被攻击，可能会影响锚定币的正常运行。

（4）监管不确定性：随着加密货币市场的发展，各国监管机构对加密资产的监管力度逐步加大。BTC锚定币可能面临合规压力，特别是在KYC和AML法规方面。严格的监管可能限制锚定币的流动性或增加运营成本。

### 5.2 BTC锚定币的机遇分析

（1）跨链流动性与DeFi应用的扩展：BTC锚定币的最大机遇在于其能够为比特币带来跨链流动性，使其能够参与到以太坊等智能合约平台的DeFi生态中。这一能力使得比特币从仅限于储值和简单支付，转变为可以参与借贷、流动性提供、衍生品交易等复杂金融活动的动态资产。

（2）多链生态的兴起：随着跨链技术的发展，BTC锚定币的应用不再局限于以太坊，而是逐步扩展到多个区块链平台，如BSC、Solana等。这种多链生态的兴起为BTC锚定币开辟了新的应用场景和市场空间，从DeFi到NFT市场，再到去中心化治理，BTC锚定币的潜在应用范围正在不断扩大。

（3）BTC LSD的发展：BTC LSD代币使得比特币持有者在质押的同时，依然可以保持资产的流动性，从而在DeFi生态中实现更高的资本效率。LSD代币的出现使得比特币质押变得更加灵活和高效，吸引了更多比特币持有者参与质押和DeFi活动，进一步推动了BTC锚定币的市场发展。

（4）机构投资者的参与：随着加密货币市场的成熟和基础设施的完善，越来越多的机构投资者开始参与BTC锚定币的市场。机构投资者的进入不仅带来了大量资金，还提升了市场的信任度和稳定性。机构投资者的需求推动了项目方在技术安全性和监管合规性方面的改进，提升了整个行业的标准和可信度。

## 总结

孙宇晨入局WBTC引发争议，主要是因为WBTC在BTC锚定币市场占据绝对主导地位，拥有近95%的市场份额，且广泛应用于DeFi生态。作为去中心化金融的核心资产，WBTC的安全性和托管透明度至关重要。孙宇晨的参与引发了社区对中心化控制增强和潜在利益冲突的担忧，尤其是在BitGo托管权转移背景下，增加了对WBTC管理和底层资产安全性的质疑，担心其可能影响DeFi市场的稳定性和信任度。

但是不可否认BTC锚定币为比特币开辟了新的应用场景和价值空间。如何在保障安全性的前提下，充分利用BTC锚定币的潜力，将是未来发展的关键。BTC LSD代币的兴起反映了比特币在DeFi领域应用的一个重要趋势：将静态资产转变为具有流动性和收益属性的动态资产。这一趋势不仅提高了比特币的资本效率，还为用户提供了更多元化的投资机会。BTC LSD代币的成功不仅取决于其技术实现和市场应用，还需要在安全性、去中心化程度和用户体验之间取得平衡。随着跨链技术、DeFi生态和流动性质押衍生品的进一步成熟，BTC锚定币有望在未来的加密货币市场中扮演更加重要的角色，为比特币持有者提供更加丰富和灵活的资产管理工具。