Swingby Skybridge

资产跨链新方案——

基于权益证明的去中心化托管人

Yusaku Senga - yusaku@swingby.network

Swingby Labs

Malcolm Lerider - malcolm@lerider.com

2019年11月3日

目录

简介

自从2009年比特币诞生之时起，区块链生态系统始终保持着快速发展的劲头。然而，时至今日，区块链仍然面临着两大难题：可扩展性和跨链互操作性。在本文语境下，可扩展性指的是任何特定区块链网络在其性能降低前每秒可处理的交易数量；互操作性指的是资产从一条链到另一条链的安全转移。互操作性的重要性不言而喻，因为目的不同的区块链需要在不同的目的（如去中心化和性能）之间进行权衡，以满足各类应用场景的需求。本文重点讨论互操作性，同时本文中的解决方案对比特币的可扩展性也有积极意义。

区块链之间的资产转移主要依赖于两种技术，本文会简要解释。第一种是使用中继机制，如*原子交换*或*哈希时间锁定合约*；第二种是使用受信任的托管人。

中继机制的实现通常有赖于名为*预言机（oracles）*的外部观察系统。预言机会监视源区块链上的特定交易，然后将信息传达到另一条链上。

受信任的托管人是特定的受信任的业务中介，他们管控一条链上的币，然后在另一条链上为这些币出具“存托凭证”。托管人发挥着托管代理的功能，并扮演管理员的角色。

然而，这两种解决方案都存在固有的中心化和信任难题：我们需要信任中继机制中使用的预言机能够诚实地提供关键交易数据，也需要信任托管人能够保管好客户资产。因此，两种解决方案都需要人工管理员来运行受信任的中心化服务。一旦受信任的实体存在，它们就有可能受到内外部恶意参与者的攻击，致其无法正常运转。

本文阐述的Swingby Skybridge可以为技术托管人提供去中心化的管控方式。该技术托管人实际上是一个加密货币地址，该地址需要一个大型社区的子集来创建有效签名。和基于业务的中心化托管人相比，该技术托管人很难被攻击，而且可以被用于链间加密货币的转移，最大化地利用各项优势。

让每条链都用上比特币！

自从以太坊主网启动以来，使用公共区块链和智能合约平台的应用日益增多。这些区块链协议的特征各不相同，与比特币相比，某些应用场景的特征更具吸引力，如交易速度更快、交易吞吐量更大、匿名性更佳或交易费用更低。然而，很多此类的区块链都存在一个根本问题——没有足够的价值记录在这些区块链上。即便这些区块链有去中心化交易所（DEXes）和去中心化金融（DeFi）等用户无法抗拒的去中心化应用（Dapps），这个问题还是很突出。如果能有更多价值记录在这些区块链上并在其上进行交易，这些区块链将发挥更大作用，形成良性循环。

价值和流动性如今都在哪里？就在比特币区块链的比特币（BTC）上。比特币有大量的用户和资产总值，其代币BTC是流动的。如果我们能将BTC转移到其他区块链上，就有可能

增加其他链上的活动。如果我们能在无须信任某个特定中介的情况下完成比特币价值的跨链转移，可操作性将大大增加。

如果能在其它区块链上创造出“比特币稳定币”（即锚定比特币价值的稳定币），比特币持有者和其他区块链用户就能享受以下五点新优势：

- 比特币用户可以在其它区块链上使用Dapps、DEXes和DeFi服务，而无需先将BTC转换成其他链上的原生代币。
- 比特币用户可以充分享受其他链的创新特性，如更快的结算速度、更低的交易费用和更好的匿名性等，同时确保投资的始终是BTC。
- 如果一部分比特币交易被转移到其它链上，就可以减少比特币区块链的使用，从而缓解比特币吞吐量的压力。在实际操作中，其他链的第一层协议可以为比特币充当第二层协议。
- 其他链的用户可以从新一轮的流动性和比特币用户中获益。
- 在币安链[1]和以太坊[2]等区块链上运行的去中心化交易所可以交易比特币稳定币，从而增加这些代币的流动性和实用性。

在非比特币链上创建比特币稳定币且无需信任特定参与者的做法将是加密货币发展史上的里程碑，它有助于加快去中心化交易所和去中心化金融等Dapps的发展。

何为去中心化托管人？

如果一个企业代表其他参与者持有其资产，那么这个企业就是托管人。托管人把客户的资产存储在某些地址中，并且这些托管人知道和这些地址相关联的私钥，从而控制这些地址。

但是这些托管人要承担私钥丢失或被盗的风险，这两种情况都会导致托管人失去对客户资金的控制。所以，托管人现在通常是将客户的大多数资产都存储在多重签名的地址中，并且把决定性的私钥离线存储。这样做比把私钥存储在接入互联网的设备中更为安全，但仍有缺点——存储不便、托管人操作复杂。

一直以来，区块链业界始终渴望找到安全性和便利性之间的平衡之道。

2018年，Rosario Gennaro和Steven Goldfeder发表了题为*“基于快速和去信任设置的快速多方门限ECDSA签名算法”*[3]的文章，其中描述了史上首个ECDSA门限签名方案协议，该协议支持多重签名，密钥生成过程高效且无需经销商参与。

遵循本文中概述的设想，我们现在可以通过高效、无经销商参与的密钥生成过程和任意数量的参与者来创建ECDSA地址，预定*门限*数量的参与者拥有共同创建有效签名的权力。构建出的ECDSA地址可被用于比特币、以太坊、EOS、波场、币安链等区块链。

需要注意的是，此设想创建出来的不是*多重签名*地址，因为多重签名过程结束时，只有*一个*签名会被创建出来。此外，各参与者拥有的私钥份额是在不必依赖受信任经销商创建和分发密钥份额的情况下被创建出来的（经销商可能成为整个系统的单点故障）。

以上即为*去中心化托管人*的基础。

何为TSS？

门限签名方案（TSS）是一种可由多方共同创建私钥和加密货币地址的协议。全部参与者的门限数量部分（即所有参与者的一个子集）可以遵循此协议，协作产生有效签名，来签署加密货币交易，同时这些参与者彼此间无需分享任何秘密。该协议是完全去中心化的——无需任何受信任的经销商。

虽然TSS需要协调多方来创建用于加密货币交易的数字签名，但是TSS的优点之一在于其能创建一个伴随加密货币交易的*单一*有效签名。这和比特币中*多重签名*（以及类似的）脚本实现需要*多个*签名不同。TSS还意味着单一签名机制可以应用在*任何*ECDSA签名链上，该链本身是否有多重签名功能不影响该机制。

与多重签名交易相比，TSS交易的另一个优点是其只包含轻量级数据：TSS中包含的签名数据不会多于正常交易中的签名数据。因此，验证TSS交易的成本很低。因为伴随交易的只有一个签名，所以补偿给矿工的交易处理费（有时称为矿工费、交易费或燃料费）可以被控制在最低水平。

本文中使用的TSS方案的ECDSA变体形式可以和其他方案进行比较，如比特币使用的Schnorr签名方案MuSig[4]以及Dfinity[6]使用的BLS签名方案[5]。

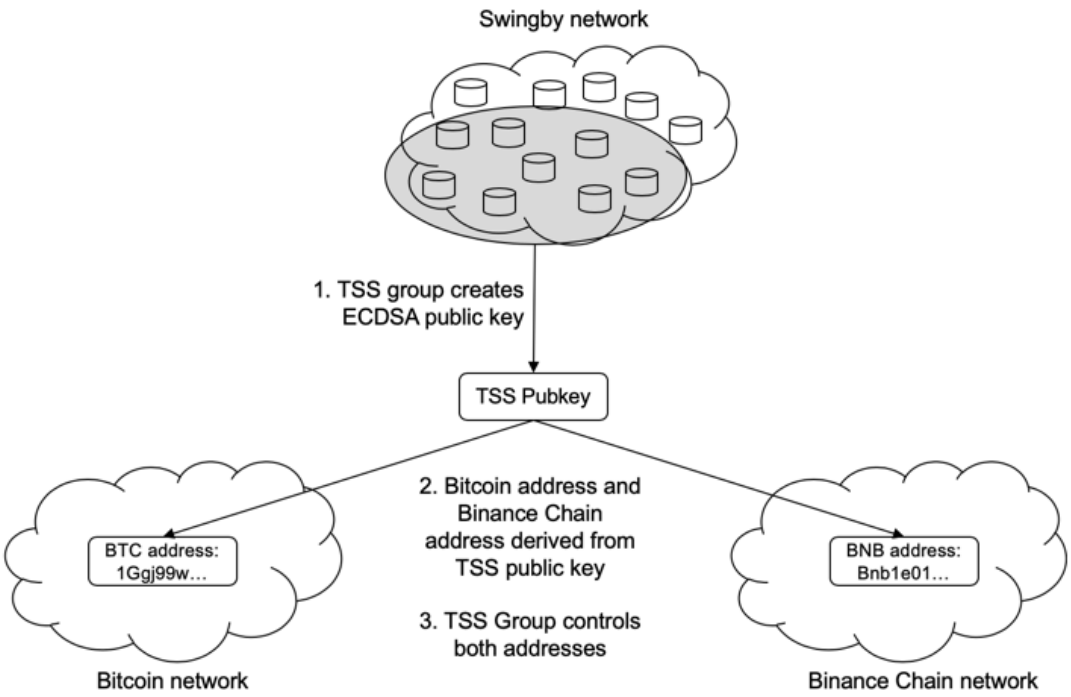
Swingby Skybridge

Swingby Skybridge的首次实现将创建出能够记录在币安链上的BTC稳定币，BTC稳定币可被视为真实比特币的*存托凭证*。随着未来不断迭代，BTC代币将能记录在其他链上，其它加密货币也将能记录在其它链上。最终，Swingby Skybridge将可被用来在任何链上创建存托凭证，而无需信任任何中心化的托管人。

系统参与者

参与者	**描述**	**首次实现**
资产	这是移动到另一条链上的加密货币。	BTC
源链	这是资产的原生区块链。	比特币主网
目标链	这是创建资产存托凭证的区块链。	币安链
存托凭证	这是目标链上资产的代表。	BTC成为币安链上的BEP-2代币。
Swingby Network	用于运行那些遵循TSS协议的Swingby Skybridge软件的P2P网络。	启动时确定：任何人均可参与。
TSS组	这是一组在Swingby Network上运行节点的参与者，他们有资格通过合作创建去中心化的托管人。	启动时确定：任何人均可参与。
TSS公钥	这是由一个TSS组协作生成的公钥。	由TSS组在密钥生成阶段使用TSS协议创建。
源链地址	这是源链上资产托管的地址。它源于TSS私钥，并由TSS组控制。	源自TSS公钥的比特币地址。
目标链地址	这是目标链上保管存托凭证的地址。它源于TSS私钥，并由TSS组控制。	源自TSS公钥的币安链地址。
Swingby质押代币（SBY）	用作质押代币的代币，它的存在是为了在无需协调者的情况下创建TSS组。	SBY成为币安链上的BEP-2代币。
代币桥（桥）	能够签署交易的源链地址、目标链地址和Swingby Skybridge节点完整结构的名称。	币安链上BTC存托凭证的代币桥。
BTC	比特币区块链上的比特币。	
BTC.S（币安链）	经过Swingby过程所创建的BTC存托凭证，以BEP-2类代币的形式记录在币安链上。	

参与者示意图



1. TSS组创建ECDSA公钥
2. 从TSS公钥衍生出的比特币地址和币安链地址
3. TSS组管控上述两个地址

Swingby network - Swingby network

TSS Pubkey - TSS公钥

BTC address: 1Ggj99w… - BTC地址：1Ggj99w…

Bitcoin network - 比特币网络

BNB address: Bnb1e01… - BNB地址：Bnb1e01…

Binance Chain network - 币安链网络

Swingby网络

Swingby网络是无需参与许可的P2P节点网络。这意味着，任何人都可以通过下载和运行Swingby节点软件加入网络，所有节点地位平等且不存在领导者。这些节点通过运行Swingby节点软件来互相交流。

该网络存在的目的是为了创建和运营去中心化的托管人。TSS*组*在该网络上生成，该网络主要运行两个过程——首先是*密钥生成（keygen）*过程：参与者共同创建公钥，衍生出源区块链和目标区块链上的托管加密货币地址。这是一个初始设置阶段，在两个区块链之间的桥（bridge）搭建完毕时结束。第二个是*交易签名（transaction signing）*过程：节点协作签名加密货币交易，让托管地址完成支付。这两个过程都遵循TSS协议。随着节点离开或加入网络，TSS组将进行重组，该过程称为*动态重组（dynamic re-grouping）*。

网络设置

质押资格

每个Swingby节点运营商都需要持有并质押SBY代币（也称“Swingby质押代币”，简称“SBY”）才能行使以下权利：

1) 参与托管地址的创建
2) 为交易签名

SBY是在币安链上发行的代币，SBY代币的质押也是在币安链上完成的。Swingby网络上的详细质押方式如下：

每个节点的参与资格将通过Swingby网络广播一则签名消息进行通知，签名消息包括来自币安链的交易哈希，通常被称为“Ping”消息。交易哈希是指在币安链上进行的交易，该交易需要在最小时间长度内（第一次实现为72小时）质押达到最低数额要求的SBY。广播的消息应包括币安链上质押地址的签名，以证明Swingby节点运营商对币安链上的质押地址有控制权。

参数共识

节点在创建地址时需要就TSS参数达成一致。TSS协议的关键参数包括：

- n - 组内能够作为一分子参与协作签名的参与者总数
- t - 组内需要协作签名交易的最少参与者数量（最低门限）

节点会在带外确认t和n的值，然后广播这些值的使用意图。节点只会尝试与使用相同参数的其他节点形成*组*。

在首次实现时，我们将使用n=100和t=60的参数。也就是说，新创建的这个组将需要100位参与者来创建TSS公钥，并且在这100位参与者中需要至少60位出席才能进行签名交易。

密钥生成阶段

TSS协议用于有效地创建任何一方或多方都不知道的单个私钥。*所有*参与者都知晓与该私钥关联的*公钥*。该公钥用于在源链和目标链上创建地址，形成*桥*。在首次实现时，比特币和币安链上都会衍生出托管地址。

在密钥生成阶段，我们会从Swingby Skybridge网络上运行的所有节点中*筛选*，形成子集，该子集称为TSS组。该组的筛选是基于：

1. 关于TSS参数n和t的共识（n=组内的节点总数、t=需要协作生成有效签名的门限节点数）、其他设置（例如费率）；
2. 节点同意在哪些链上运行以及它们是否使用测试网；
3. 节点在币安链上质押最低数额SBY的时间长度。

举个例子，在某个时间点，Swingby网络可能包含150个节点，其中140个节点想要创建一个参数为（n=100，t=60）的代币桥（可能其他10个节点想要建立一个参数为（n=8，t=5）的代币桥）。假设这140个具备参与资格的节点都质押了最低数额的SBY，那么系统将根据这140个节点在币安链上质押SBY的时间长短排序。该排序列表中前100个节点将组成TSS组来生成密钥，这就是筛选出TSS组节点的方式。

交易签名

什么时候需要交易签名呢？请参考以下两个场景：

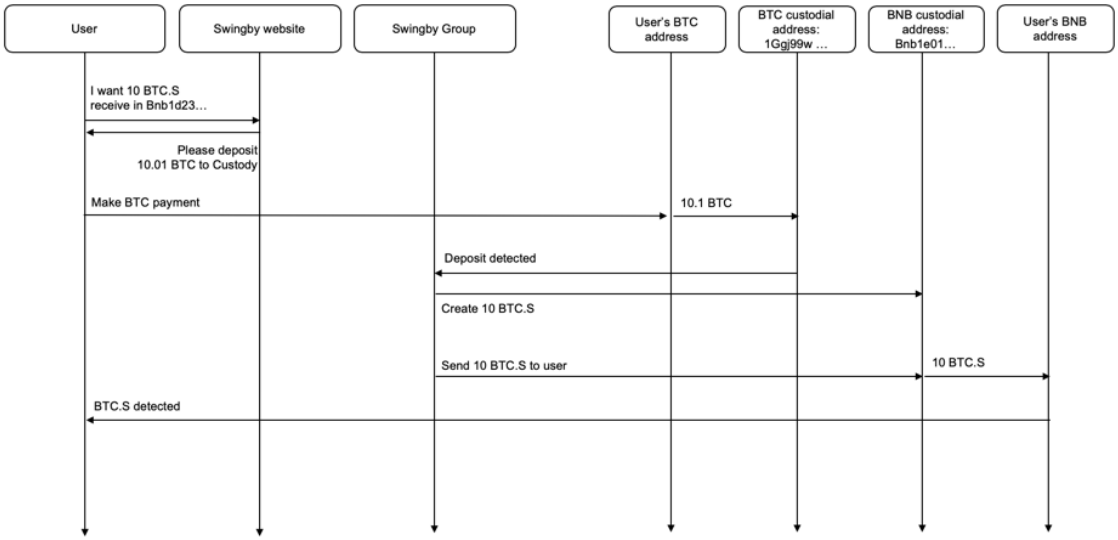
- 某第三方需要BTC.S（币安链上的BTC）。该用户可使用Swingby网站并输入需要的BTC.S数额和币安链上的接收地址。网站会询问用户需要从比特币地址向TSS组托管的BTC地址发送多少BTC。这要求TSS组在其托管的币安链地址中创建BTC.S，并将其发送到第三方的币安链地址。
- 某第三方希望将其币安链上的BTC.S交换为比特币上的真实BTC。他将BTC.S发送到TSS组托管的币安链地址。TSS组必须将BTC从其托管的比特币地址发送到第三方的比特币地址。

每个TSS节点都需要监管桥接的两条区块链上的托管地址。首次实现时，连接的两条链是比特币和币安链。

当TSS组需要创建新交易并签名时，过程如下：

1. 每个Swingby节点独立发掘Swingby网络的节点伙伴并搭建列表。
2. 每个Swingby节点独立通告该列表上的其他节点，表示希望TSS组签名。该回合称为“签名列表搭建”。
3. 每个Swingby节点独立且筛选创建一组符合条件的（t）名签名者。该回合称为“签名列表投票”。

4. 每个Swingby节点会同时独立运行多个TSS回合，从其他节点伙伴收集“签名份额”。这个阶段存在大量沟通和交叉检查工作。
5. 通过使用签名份额，每个Swingby节点可以独立地为消息创建完整的ECDSA签名。
6. 任何一个Swingby节点都可以向关联的区块链（此处指比特币或币安链）广播已签名交易。这意味着区块链将收到多个类似的交易，这些交易都是相同的，并且只有其中一个能够被记录。



User - 用户

Swingby website - Swingby网站

Swingby group - Swingby组

User’s BTC address - 用户的BTC地址

BTC custodial address: 1Ggj99w... - BTC托管地址：1Ggj99w...

BNB custodial address: Bnb1e01... - BNB托管地址：Bnb1e01...

User’s BNB address - 用户的BNB地址

I want 10 BTC.S received in Bnb1d23... - 我希望在Bnb1d23...收到10个BTC.S

Please deposit 10.01 BTC to custody - 请在托管地址存储10.01个BTC

Make BTC payment - 发起BTC交易

10.1 BTC - 10.1个BTC

Deposit detected - 发现存款

Create 10 BTC.S - 生成10个BTC.S

Send 10 BTC.S to user - 发送10个BTC.S给用户

BTC.S detected - 发现BTC.S

10 BTC.S - 10个BTC.S

动态重组

根据我们的预想，Swingby网络中会有一定程度的节点流动。如果大量节点伙伴离开，导致能够签名交易的节点数量少于t，那么TSS组实际上已经失去了对托管钱包的控制。这是我们要避免的情况。

动态重组这一机制允许节点加入和离开TSS组，但该组为交易签名的能力不会受到影响。

举个例子，在一个节点总数为100、门限为60的组中（n=100，t=60），最多40个节点可以离开该组。首先，如果节点离开、脱机或发送恶意数据，他们将被候补节点取代，节点总数保持n=100。剩下的节点（只要总数超过门限t）可以重新创建组。如果候补节点不足并且在较长的时间内候补节点总数接近t，有可能影响节点可用性，在这种情况下，上述做法可能是必需的。

假设当前密钥x由门限为t_1的一组节点（P_1，…，P_n）共享，该组可以将所有权转移到新门限为t_2的另一个组（P_1，…，P_n）。

这意味着即使网络存在节点流动，新节点也会接管对托管钱包的控制权。然而，旧节点仍然拥有秘密份额。如果网络节点波动很大，那么秘密份额有可能被利用。节点波动需要通过经常性地运行密钥生成来缓解。

铸币和存款

当发起交换时，Swingby在目标区块链上主要有三种特定的代币释放方法，具体方法取决于区块链平台的费用结构。

第一种方法是当源区块链发起代币交换时，在目标区块链上铸造新代币。当交换回源链代币时，目标区块链代币会被销毁。这是真正意义上的锚定，因为在目标区块链上发行的代币是由源区块链上锁定的相同数量代币支撑的。从用户的角度来看，这种方法意味着Swingby Skybridge充当着网关的角色，以使具有确定价值的数字代币（例如BTC）映射到其他区块链上，发挥额外效用。然而在一些场景中，这可能是一种相对昂贵的方法，因为交换过程需要支付交易费和铸币费，而且铸币通常比交易费更贵。

第二种方法是在两条区块链上都使用存款（使用现有代币或新铸造的锚定代币）来撮合区块链之间的交换。这种方法的优点是计算简单，并且可以最大程度地减少用户的交换费用。不过，这样的操作为平衡两条链上的存款增加了难度。这个方法需要确保每条区块链上始终有足够的代币支持用户进行任意数额的交换。针对存款方面增加的复杂性，有几种解决方案：质押存款人可以获取交易费用作为奖励；如有需要，收到的锚定代币

数额可以与存款数额钩挂；或者如果两条区块链上操作都很活跃，则可以直接接受零散存款。

第三种根据需求进行调整的方法更加动态，能汇率，预先铸造代币按比例交换而非一对一锚定。举个例子，在源区块链智能合约（以太坊）中用5000 ETH创建一个ETH Skybridge，同时在币安DEX上创建相应数量的ETH-B。随后，汇率根据“锚定”双方的存款数额成比例变化。在双方都有5000 ETH作为保证金的情况下，交换汇率是1比1。如果从ETH交换到ETH-B的参与者多于从ETH-B交换到ETH的参与者，则汇率会变化，您每交换一个ETH都会得到更少的ETH-B。按照目前采纳的趋势看，第三种方法可能是最积极的。如果对币安DEX感兴趣的人想要接近1比1的交换，那么他们需要在源链上重新存币，从而增加对源链和目标区块链的信任。

激励措施

Swingby Skybridge节点运营商要承担两个费用：

1) 运行节点的运营成本 - 服务器成本
2) 质押成本 - 他们必须先购买SBY才能质押

参与两种类型的质押可以抵消这些费用：

1) SBY质押 - 节点质押SBY参与交换可以获得交换费/n。
2) 浮动质押 - 存入桥代币的节点将获得与其代币存入数量成比例的交换费。

浮动质押是Swingby Skybridges独有的质押类型，是通过源区块链和目标区块链上的存款来进行简单的计算交换，尽量为用户降低交换费用。存款越多，交换的摩擦就越小，可能更重要的是让用户能够更放心地使用桥代币，因为在存款足够的情况下，用户就可以随时交换回源区块链。从本质上讲，这些存款是“借给”桥的，所以需要考虑存放代币的机会成本。因此，在Skybridge上存款会提供丰厚的代币利息回报，吸引代币持有者。在这些情况下，需要向存款人支付额外的交换费。

未来的激励措施还可能在每次交换费中抽取一部分从去中心化交易所自动回购SBY进行立即销毁。这样做可以提高关联DEX上的流动性并自然地调节代币的供应/需求，以适应所有Swingby Skybridge今后的质押要求，防止代币供过于求。

SBY代币

在Swingby Skybridge上使用的代币称为“Swingby代币”（简称为“SBY”）。SBY将被部署在币安链上，发挥BEP-2代币的功能。

SBY是用于衡量节点是否满足加入TSS组的条件，我们也会分配SBY来支持Swingby网络生态系统的发展。

除了币安链以外，SBY也可在其他与Swingby Skybridge相连的区块链上发行。

质押功能

Swingby Skybridge是一个无需许可的网络，没有中心机构决定谁能进组。Swingby Skybridge的节点运营商如果要进组，必须证明自己在币安链上持有SBY代币，且在预计参与的时长范围内始终锁定（或质押）其持有的SBY代币。

要加入TSS组，申请人必须获得SBY并且已持有一段时间，这样他们就能在TSS回合（如创建公钥、签名事件）发生的时候证明自己持有SBY。

风险

本节将介绍基于权益证明的TSS组可能会遇到的攻击。因为任何人都能加入TSS组，所以我们有必要考虑恶意参与的情况——恶意参与者可能会组织女巫攻击。我们需要重视这种隐患，因为获得TSS组的控制权意味着控制了托管钱包，牵扯金额可能极大。

女巫攻击

对Swingby Skybridge发起女巫攻击需要考虑两个重要门限：当攻击者控制*（n-t+1）*个节点以及当攻击者控制*t*个节点的时候。

当恶意参与者控制*（n-t+1）*节点的时候，他们可停止所有交换，因为正常参与者无法达到控制t个节点签名。这种攻击不会给恶意参与者带来任何经济收益，而且尝试的成本非常高。更何况现在已经有通过重组和按照节点年龄分配任务的机制，要发起此类攻击非常困难。

若想通过女巫攻击获得经济收益，攻击者需要控制*t*个节点，这样才能成功组织新的群组以及新的*n*和*t*值，从而获得所有节点的控制权并把所有费用收入囊中。正如前一段所解释的，控制t个节点也同样成本高、难度大，在这点上和控制*（n-t+1）*个节点并无二致。

若要成功发起其中一种女巫攻击，攻击者几乎需要在交换发起后马上分别建立*（n-t+1）*个或*t*个节点。否则，攻击者需要尝试在暗处发起攻击，成本高且无法保证能成功。在实际操作中，链上可能已经存在比攻击者的所有节点存在时间更长的*t*节点，导致根本无法发起女巫攻击。攻击者也因此不愿尝试攻击。

抢先交易

恶意参与者可能会一直关注着源区块链上的内存池，并尝试识别那些输入有误或未完成同步的交换交易，利用网络空挡抢先将原来的目标地址改为恶意参与者的地址。因此需要针对抢先交易制定专门的区块链解决方案。

由于BTC不支持交易备忘录，我们可以通过以下编码公式把目标地址加密到数额里，这样可以消除BTC交换中的抢先交易隐患：

$$floor(x) - rs(sha512\_256(nonce + dest\_addr + floor(amt\_coin) + nxt\_round\_no)\ \%0x400)$$

其中x代表交换数额，$dest_addr$代表目标区块链地址，amt_coin代表<数额,代币>的字符串对。$floor()$函数会把数额改为以“000 satoshis”结尾，比如：0.12341234会被改成0.12341000。因为这些哈希无法被提前计算，所以能预防抢先交易。选用SHA512/256算法是因为运行这种长度为64位的加密算法效率更高，而且能更好地抵御长度扩展攻击。

存款

在Skybridge的其中一种存储方法是预先铸币或连接已铸造的代币。此方法的优点之前也提到过，它的计算复杂性较低，交换计算简单而且产生的费用应该比其他方法低。然而，为了确保能即时交换，此方法要求两个区块链上都有存款。如前文提到的，这点可通过存款激励措施（如利息）来确保。无论出于何种原因，如果用户放弃了通过Skybridge桥接的区块链，那么桥两头的区块链都有可能因为来不及补充而耗尽存款。用户需要了解自己选择的交换方法及相关风险，这点很重要，因为此存款方法存在耗尽各端存款的可能性，而且网络阻塞还可能带来额外风险。

通过给Skybridge提供代币换取浮动质押奖励的参与者也需要考虑存款被耗尽的风险。浮动质押的用户需要充足的激励措施来弥补机会成本和“大规模逃离”产生的损失。“大规模逃离”指从Skybridge桥接的区块链一端大规模转移到另一端，这会不断消耗存款，如果不能恢复平衡的话用户将失去大部分存款。这个风险可以通过动态调整交换价值来降低，即被锚定的代币按照需求以它们在每个区块链上的存款比例来进行交换。这种方法需要根据具体情况做出选择。

技术背景和相关尝试

就实现比特币与其他链之间的双向锚定这一问题，已经有人提出了各种方法，以下会具体介绍。然而，这些方法都存在问题，且目前还没有找到任何去信任的解决方案。

接下来我们会简单介绍实现双向锚定的主要方法，包括锚定法、中继法和用抵押品担保稳定币的方法。

Kyber的WBTC

WBTC[7]是由Kyber Network牵头的项目，它采用了可信的多重签名钱包技术。Kyber通过受信任的托管人来发行ERC-20代币，以此作为BTC在以太坊区块链上的存托凭证。

然而，“受信任的托管人”要求终端用户信任，而托管人易受网络欺诈和服务器攻击，也会被托管组织内部的恶意参与者影响。

驱动链

Rootstock（RSK）[8]项目希望为比特币区块链添加*智能合约*功能，因此创建了能连接到比特币区块链的*侧链*，以实施他们自己的*智能合约*。为了能成功运作，他们需要双向锚定*侧链*与比特币区块链的方法，也就是他们提出的“驱动链”概念。

驱动链[9]是一种对比特币进行*合并挖矿（merge mining）*且依赖简单支付验证（SPV）的方法。这个方法有可能高效地证明两个区块链之间的代币流动。

然而：

- 为了实现合并挖矿，侧链的挖矿过程需要与主链具有同等的安全性；
- 需要信任侧链区块里的merkle root；
- 若两条链在同一侧，则很难维持两条链的一致性；
- 为了实现驱动链，以后会需要比特币软分叉（soft fork）。

Cosmos和Peg-zone

Cosmos[10]提出了创建多个区域（zone）并通过链间通信（IBC）协议实现这些zone之间的互操作性。然而，IBC协议连接区块链需要“快速终结性”，因此这些区块链需要能支持“快速终结性”的共识算法。

为了能连接到没有“快速终结”功能的区块链，Cosmos提出了Peg-zone的概念，它能够为底层区块链提供“虚拟终结性”。Peggy[11]是Cosmos团队的实践成果，它为以太坊虚拟机（EVM）提供可兼容的Peg-zone。

波卡和平行链

波卡[12]提出了“平行链（parachain）”的概念，意指任何与它们的中继链相连的区块链。他们的平行链通过绑定验证者来支持互操作性，这些验证者可以将交易从一条*平行链*转移到另一条链上，且他们持有的保证金可被罚没。

然而，他们在白皮书里也写到，对于比特币这样的区块链来说，这个概念更加难以实现，因为它的脚本功能有限。在以太坊，实现安全的验证者轮换机制是比较简单的，但是对于比特币来说，要实现完全安全的交易转移是个更大的挑战。截至目前，暂时还没有用波卡实现比特币桥接的具体计划。

比特币中继、中继网络以及Dogethereum

比特币中继（BTC Relay）[13]模型使用SPV证明直接在EVM验证来自比特币网络的交易。

中继网络（Relay Network）是比特币中继的实践，目的是通过在比特币网络外处理尽可能多的交易从而将处理成本降到最低。然而，要想做到这一点，*中继器*需要信任别的节点提供的merkle root，这意味着节点之间必须要维持好共识。

Dogethereum[14]实现的双向锚定会为Dogecoin在以太坊网络上生成ERC-20代币。Dogethereum的双向锚定是为了给Dogecoin找到去中心化的储存解决方案。然而，目前Dogecoin储存在多重签名钱包中。

抵押品担保稳定币（DAI）

“DAI”[15]采用的方法是以一种代币作为抵押债券来担保货币（如美元）的价值。当担保货币的代币价值下降或上升时，需要通过结算抵押债券来防止担保不足。这种稳定币值的动态结构也被称为软锚定（非完美锚定）。

DAI是通过对抵押物进行去中心化托管而获得独立性的，这种方法很有意思。根据DAI在主网的历史，DAI已被证实是稳定锚定代币价值的有效手段。

然而，这种安全模型在提交预言机价格的过程中依赖的是抵押物的评估价值，因此即使有智能合约也很难一直保证抵押品的安全。

TEE和Intel SGX飞地（enclave）

可信执行环境（简称“TEE”）主要是一种安全层技术，代表产品包括Intel SGX和ARM-TrustZone。

TEE可向其他节点远程验证计算过程，也可以远距离验证不同芯片的处理状态。然而，目前的Intel芯片将使用由Intel管理的认证服务，而且这种芯片易受侧通道攻击。尽管复

制安全的执行环境比较容易，但是就目前市场上的选择来说，它不能作为去中心化工具来使用。

参考文献

[1] Binance, Binance Chain (DEX) https://docs.binance.org, 2019

[2] Vitalik Buterin. Ethereum - A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] Rosario Gennaro, Steven Goldfeder. Fast Multiparty Threshold ECDSA with Fast Trustless Setup (GG18) https://eprint.iacr.org/2019/114.pdf

[4] Gregory Maxwell and Andrew Poelstra and Yannick Seurin and Pieter Wuille, Simple Schnorr Multi-Signatures with Applications to Bitcoin https://eprint.iacr.org/2018/068, Jan 2018

[5] S. Mitsunari. Barreto-Naehrig curve implementation and BLS. https://github.com/dfinity/bn, 2017.

[6] Timo Hanke, Mahnush Movahedi and Dominic Williams. DFINITY Technology Overview Series Consensus System https://dfinity.org/static/dfinity-consensus-0325c35128c72b42df7dd30c22c41208.pdf

[7] Kyber Network, BitGo Inc, Republic Protocol. Wrapped Tokens - A multi-institutional framework for tokenizing any asset. https://www.wbtc.network/assets/wrapped-tokens-whitepaper.pdf, Oct 2018

[8] Sergio Demian Lerner. RSK White paper Overview. https://docs.rsk.co/RSK_White_Paper-Overview.pdf, Nov 2015

[9] Drivechain - The Simple Two Way Peg http://www.truthcoin.info/blog/drivechain, Nov 2015

[10] Jae Kwon, Ethan Buchman. Cosmos - A Network of Distributed Ledgers https://cosmos.network/cosmos-whitepaper.pdf

[11] Cosmos. Peggy https://github.com/cosmos/peggy

[12] Gavin Wood. Polkadot: Vision for a Heterogeneous Multi-Chain Framework https://polkadot.network/PolkaDotPaper.pdf

[13] BTC Relay https://github.com/ethereum/btcrelay

[14] Dogethereum Contracts https://github.com/dogethereum/dogethereum-contracts

[15] Maker Team. The Dai Stablecoin System. https://makerdao.com/whitepaper/DaiDec17WP.pdf, Dec 2017