Bifrost Finance Whitepaper

Authors: Lurpis, Buffalo

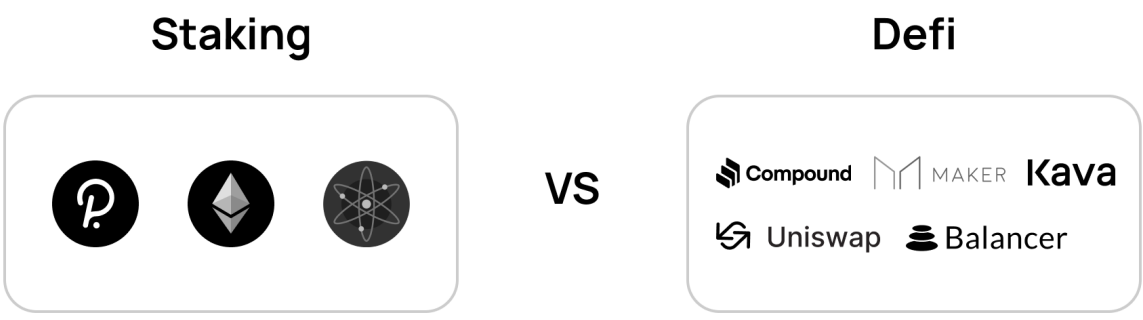
Update: 2021/03/23

Version 1.2.0

1. 项目背景

随着越来越多的公链采用 PoS 共识来提升项目可用性和去中心化，目前已有过百个总市值超过1,453亿美元的 PoS 公链诞生。通过PoS机制的质押（Staking）行为，每年将产生超过25亿美元的收益，对DeFi、Ethereum 2.0、Polkadot、异构跨链DEX（去中心化交易所）等生态发展的期待，充斥着当前的加密市场。DeFi 与 Staking 两种机制越来越多地在区块链版图中交互叠加，产生了无穷尽的可组合性，但新问题也接踵而至。做为示例，以下给出三个典型的问题描述。

1.1 Staking 与 DeFi 收益竞争

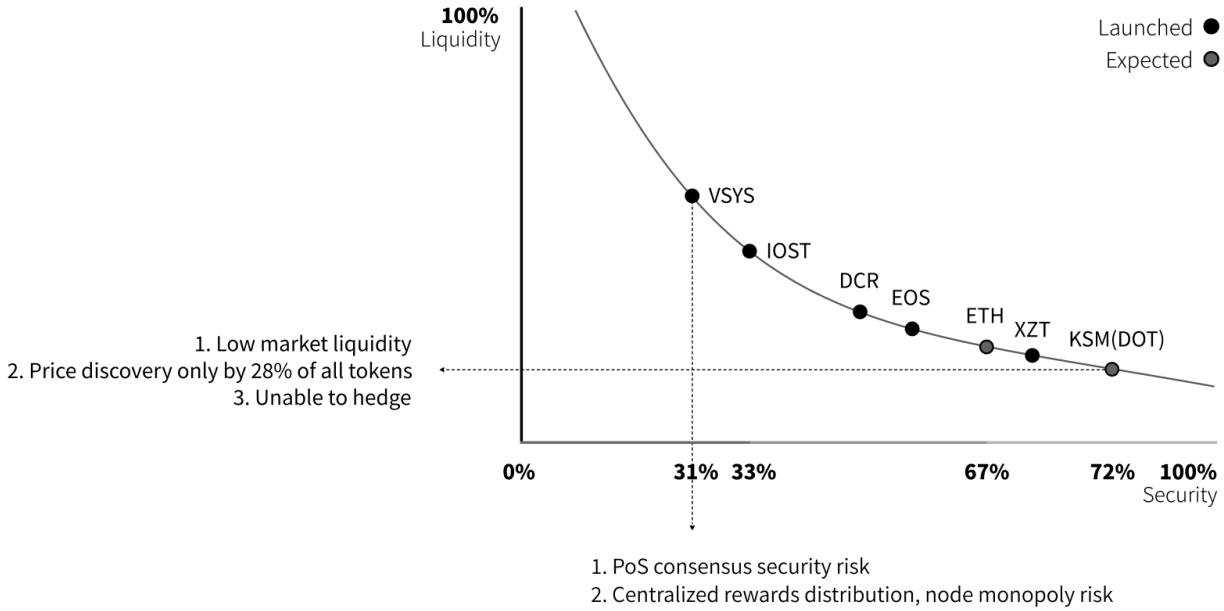


Staking 与 DeFi 收益竞争

流动性挖矿（Yield-Farming）等新兴DeFi项目持续不断地涌现，DeFi 产品或给投资者带来很高的年化收益率。由于PoS的Staking机制要求参与者锁定代币资产，因此投资者必须在Staking 与 DeFi 之间进行权衡与选择。Staking 收益与DeFi收益必然产生激烈竞争，若DeFi收益率无法超过Staking的

锁仓成本，持币者会选择参与Staking，反之，持币者必然会将资产投入DeFi活动。投资者面临艰难选择，亟需某种两全其美的解决方案。

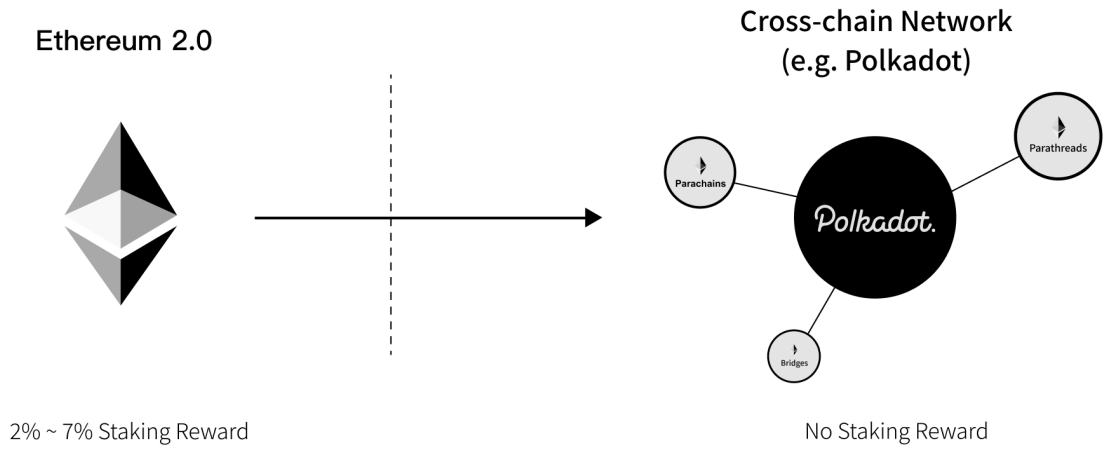
1.2 代币流动性与系统安全性互斥



PoS 共识网络安全性和流动性权衡

在PoS共识中，系统安全可持续运行，是由 Staking 机制维护的，这就意味着代币资产流动性和系统安全性处于此消彼长的互斥状态。增加 Staking 的流动性需要权衡网络安全性，若质押率过低则会产生 PoS 共识安全隐患，反之则会导致资产流动性不足，市场价格仅能通过少部分比例的资产表现出来，由此存在大量泡沫，并导致价格波动剧烈。对于正在进行 Staking 的用户来说，因为锁仓而丧失流动性，无法对冲价格剧烈波动的风险，造成 Staking 机会成本不断被放大。这就需要某种解决方案，即可降低用户参与 Staking 的机会成本，又能提高 PoS 公链的整体质押率。

1.3 参与跨链活动丧失Staking收益



PoS 网络跨链状态下 Staking 收益成本

随着Cosmos、Polkadot、Etherem2.0等明星项目的上线，用户会参与到很多跨链场景中，而参与跨链活动的代币资产锁定行为，会导致用户失去原有代币的 Staking 收益。比如用户将ETH通过去中心化桥，跨链发送到Polkadot平行链上参与DeFi活动，典型的桥解决方案是将ETH锁定到去中心化桥所对应的智能合约中，然后在Polkadot平行链上释放出等量的vETH。由于ETH锁定在合约中，不产生Staking收益，若存在某种解决方案，能够让用户在持有vETH的同时，又能获取到原链上的Staking收益，则可大幅降低跨链活动的成本。

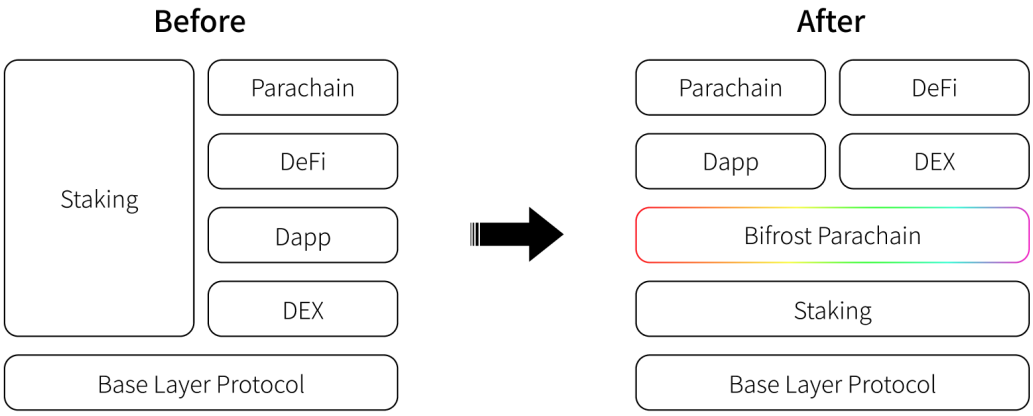
1.4 Bifrost项目的使命与愿景

Bifrost 项目就是为了解决以上所述的Staking问题而创立的，其使命和愿景是为尽可能多的链上质押资产（Staking、Collateral、PLO、跨链锁定...）提供流动性，并成为多链之间的连接器。项目首先以Staking场景为切入点，通过发行资产衍生品的形式提供流动性，经过持续迭代研发，未来将适配所有涉及链上质押资产的场景。Bifrost 项目已获得 Web3 Foundation Grant，是Substrate Builders Program 的一员，Web3 Bootcamp 孵化器的 15 个核心成员之一，获得了 Web3 基金会和万向区块链实验室在技术、产品、资本、法务、生态合作等领域全方位的支持。

2. 系统架构

Bifrost 在 Staking 与应用层之间提供了一个中间抽象层，让原本构建在公链底层架构上的Staking行为与应用层行为由并列互斥关系，变为上下兼容关系，由此解决 Staking与DeFi、跨链活动互相排斥

的问题。通过Bifrost 平行链，用户随时可将用于Staking的Token存入兑换成vToken，然后由Bifrost的跨链交互模块利用收集到的Token去原链上执行Staking操作。每一种 PoS Token将对应不同的 vToken，比如桥接 Polkadot 代币DOT，对应 vDOT、Ethereum代币ETH对应vETH。简单来说，通过提供 vToken 的流动性，能够兼顾原链资产流动性与原链系统安全性。用户持有 vToken即可持续获得Staking 收益，使用vToken参与DeFi、跨链活动，不再与Staking 收益发生冲突。



A Layer Between Staking and Applications

Bifrost提供中间层服务

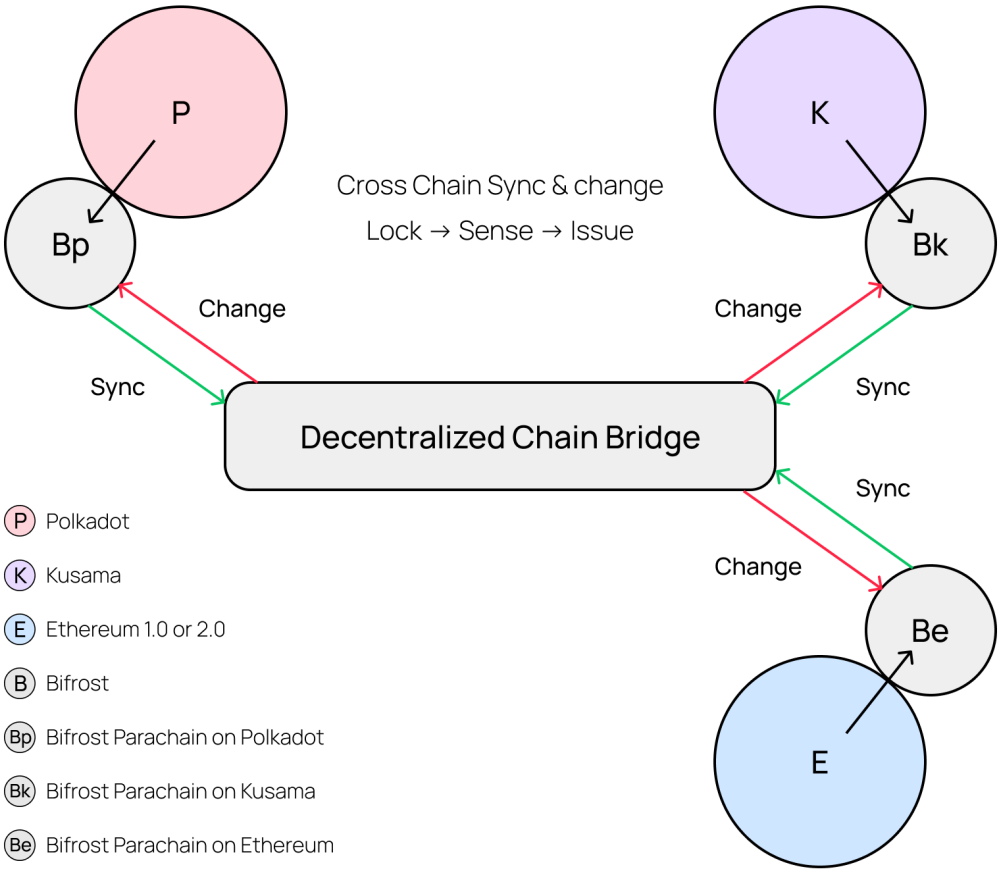
2.1 落地实施方案

从系统实现与落地运行的角度看，Bifrost是一个为多个PoS公链的质押资产提供流动性的去中心化异构跨链系统与多链连接器。Bifrost基于Substrate框架开发，属于Polkadot生态项目，以 Polkadot 和 Kusama 平行链的形式完成业务落地与持续安全运行，共享Polkadot和Kusama所提供的共识安全性以及社群用户。当Bifrost为多个PoS公链提供质押物流动性时，这些公链的共识安全风险也部分地转移到了Bifrost。

若 Bifrost 共识安全攻击成本低于原 PoS 共识安全成本，将导致黑客有意通过攻击 Bifrost 网络来完成原 PoS 网络的攻击。只有在 Bifrost 共识安全不低于原PoS 网络时，Bifrost 协议在客观条件下才能为其他PoS 网络提供Staking流动性。而维护一个足够安全的独立PoS共识系统，代价昂贵且沉淀与演化周期漫长，以 Cosmos 为例，根据当前 72% 的质押率和 8.09% 的收益率来计算，每年通胀率约为 5.8%，每年需要大约 15,344,540 ATOM（约为 $83,474,302）的网络安全维护成本。若系统生态不够繁荣，网络使用率较低、价值捕获能力不足，高额通胀很可能会将整个系统推向死亡螺旋的窘境。

独立运行PoS公链时，该网络能够安全承载的资产上限必然要低于其代币市值。若该网络中锁定的资产总量超过其代币市值时，黑客就有足够的动力发起攻击，导致资产流失。这不仅会让项目直接面临死亡，且会导致其所支持的其他共识系统遭受连锁打击。所以当前阶段的Bifrost系统没有运行独立的PoS共识网络，准备以平行链的方式运行，以共享Polkadot或Kusama提供的共识安全性。Bifrost 将以竞拍波卡平行链卡槽的方式支付合理范围内的共识安全费用，避免独立运行PoS网络的高额成本，同时确保Bifrost网络中锁定的资产更加安全，让Bifrost生态可持续健康发展。

若从顶层架构的角度观察Bifrost系统，可将Bifrost分解为部署在各个PoS公链上的代理模块集合，这些模块通过平行链、平行线程、智能合约的方式实现，通过去中心化的桥系统互联起来协同工作。在Ethereum和Polkadot生态中，有大量的项目正在研发去中心化的链桥系统，Bifrost会选择最优的链桥对接起来，Bifrost也在同步研发自己的链桥系统作为备选方案。由于采取了Substarte框架进行开发，Bifrost和Polkadot一样，可以进行有效的链上治理和无分叉升级，这非常有利于Bifrost项目快速迭代推进。



Bifrost系统架构与核心组件的顶层视图

若采取Bifrost的链桥解决方案，以上图为例，具体实现时，用户可以将Polkadot平台（P）的资金转入到Bifrost平行链（Bp），在Bp平台上执行锁定（Lock）操作，去中心化的桥系统感知（Sense）到之后，会在Bifrost平行链（Bk）释放（Issue）等量资金，通过这种方式，完成跨链资金流转，并实现BNC代币的统一记账。而链桥自身的去中心化与共识是通过Bp、Bk、Be上的用户进行多资产的Staking决定的。

2.2 Staking业务

Bifrost 通过安全的、去中心化的资产跨链技术，确保质押资产的安全，并通过vToken衍生品释放流动性。通过对质押资产生息、结算、权益保留进行标准化，可为各类质押资产提供流动性，但由于去中心化特性，质押物需要具备三个基本特点：

- 资产链上发行
- 收益链上结算
- 权益链上证明

目前的PoS 公链代币天然具备上述特点，是Bifrost提供质押物流动性的典型标的资产。以Staking 质押物提供流动性作为市场切入点，为多个PoS公链提供 Staking 标准流程与更灵活的金融工具，释放资产流动性，给用户带来额外收益和更多选择，是Bifrost项目的核心设计目标之一。直接进行 Staking与通过Bifrost 进行 Staking的区别与对比如下：

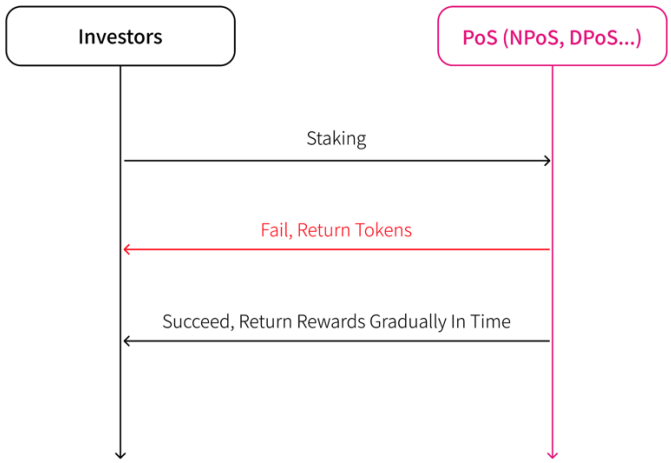


图 1 原生 Staking 交互流程图

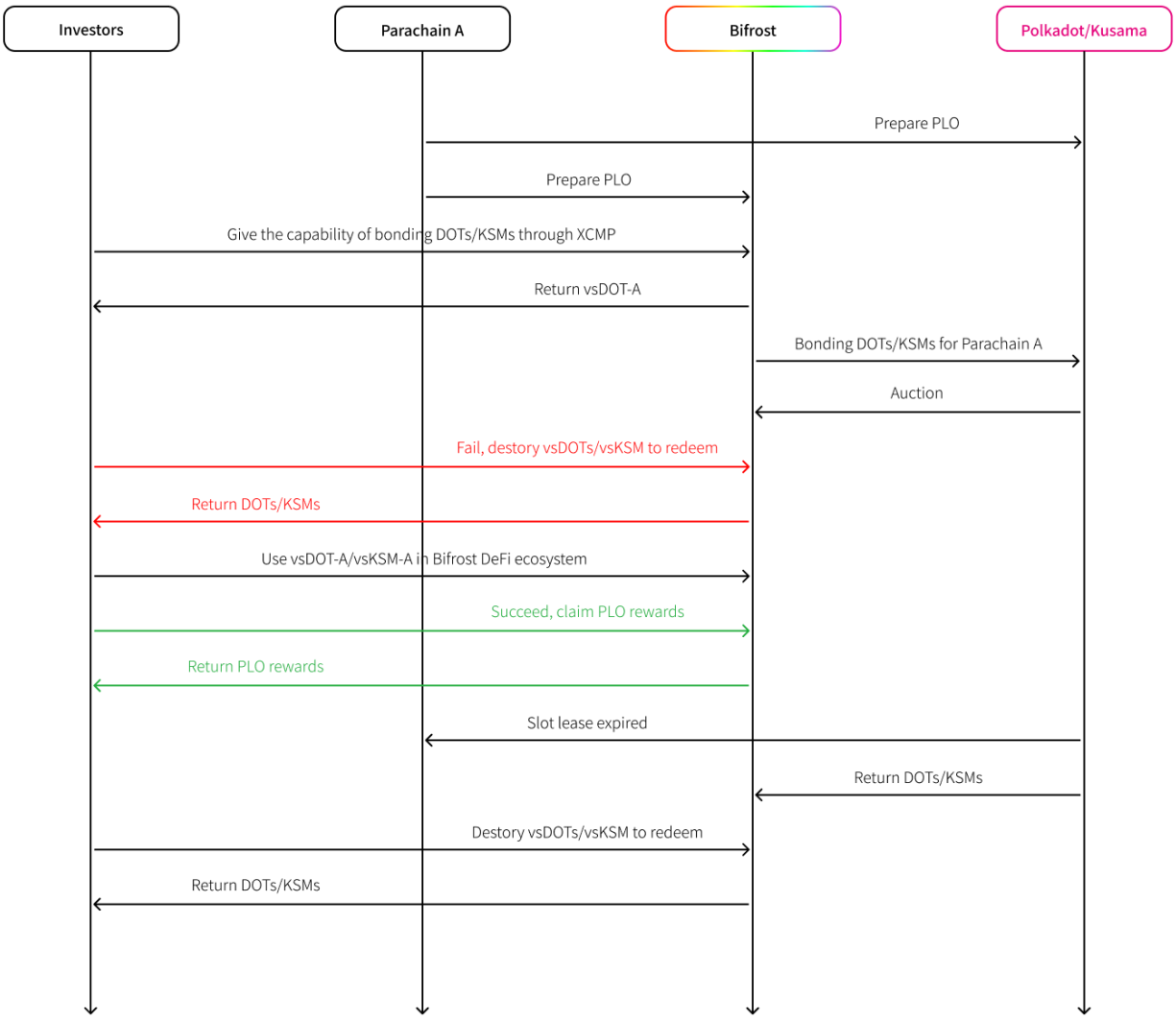


图 2 通过 Bifrost Staking 交互流程图

从Staking发出者角度看，PoS公链可分为两类，一类是必须通过外部账户发起Staking操作，另一类是可以通过可定制的代码模块（智能合约、平行链）发起Staking操作。对于第一类PoS公链，可采取门限签名技术去模拟出一个外部账户，然后由多个操作者进行门限操控，其能够承载的资金规模很有限，为了确保多个操作者不做恶，要求操作者抵押一定额度的资产，去中心化程度不够高。对于第二类公链，采取代码自动化地控制，可以做到完全去中心化，Bifrost优先考虑支持第二类公链。

2.3 PLO业务

在做好Staking 业务的同时，Bifrost也为那些与 Staking 资产质押机制具备较高相似度的经济模型提供基础支撑工具，为更多的生态应用场景贡献力量。PLO（Parachain Lease Offering）是 Polkadot 生态的关键经济模型之一，与 PoS 的 Staking 有很大的可比性与相似度，是 Bifrost 优先考虑实现的工具之一。直接进行 PLO 与通过 Bifrost 进行 PLO 的去呗与对比如下：

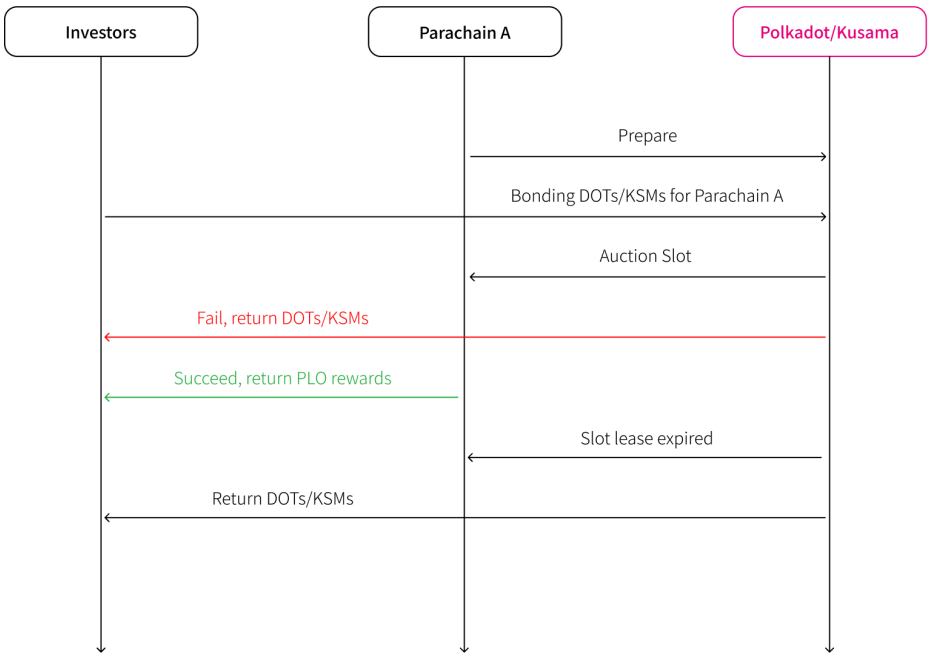


图 1 原生 PLO 交互流程图

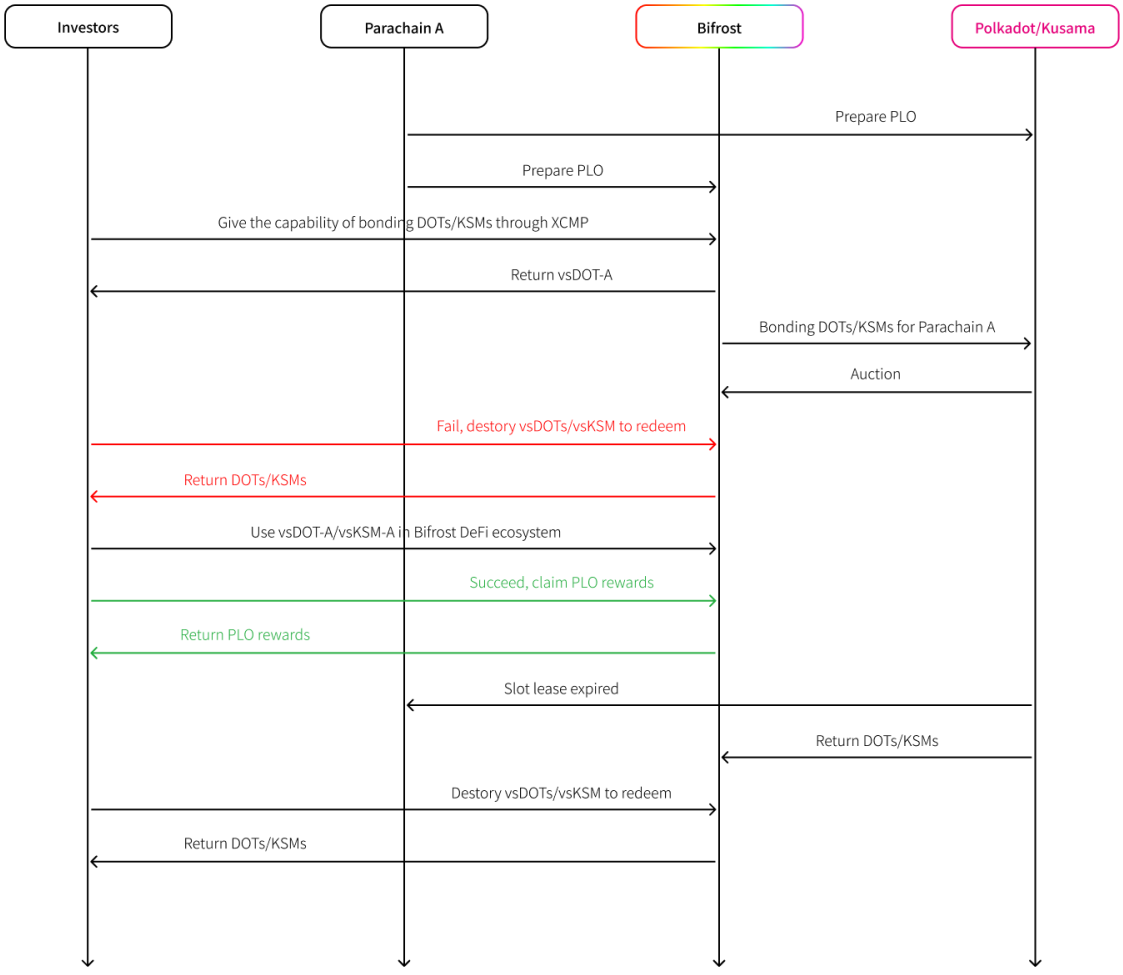


图 2 通过 Bifrost PLO 交互流程图

投资者用户通过Bifrost参与平行链项目的PLO活动，Bounding行为会分离解耦出两类Token：vsToken与vsBound-PLO-ID。vsBound-PLO-ID可通过XCMP转移到对应的平行链上，然后由该平行链按照自己设计的方式发放奖励给持有者，所以可将vsBound-PLO-ID看成是蕴含了投资奖励的特殊商品。系统设计两个池子：1:1承兑池、1:x（x <= 1）Bancor池。用户同时持有vsBound-PLO-ID和vsToken，且vsBound-PLO-ID所代表的Slot租约已到期，则可参与承兑池以1:1的价格兑换出Token，若用户只有vsToken，则可参与Bancor池，以1:x（x <= 1）的价格兑换出Token。只有当池子中存放有Token时，用户才可正常执行兑换功能。当Slot租约到期时，Relaychain将返还Token到Bifrost，系统会将所有的Token放入承兑池，然后每天从承兑池的余额中抽取5%放入Bancor池。若系统丢失vsBound-PLO-ID或者某些攻击者故意囤聚vsBound-PLO-ID而不愿意卖出，vsToken持有者仍然可以从Bancor池中兑换出Token，而不用担心vsToken不能兑付的风险。系统注入到Bancor池的资金，会以线性平滑的机制逐渐释放,而不是一次性全部释放，这样设计可以防止vsToken与Token兑换价格不合理地大幅度波动。这其实就相当于系统在用一部分Token持续购买用户持有的vsToken。只要在Bancor池中发生1:x（x <= 1）的兑换行为，Bifrost系统必然会盈利，这部分利润将进入国库,用于社区发展或回购BNC。vsBound-PLO-ID作为权益凭证，不需要高流动性交易，通过一口价形式挂单出售即可，因此Bifrost系统设计有挂单售卖vsBound-PLO-ID的机制，类似于电商平台中的C2C商品买卖市场，无需通过Uniswap/Balancer这类AMM/DEX提供交易流动性。

2.4 资产交易与DeFi业务

Bifrost为众多PoS公链提供Staking流动性，并以Polkadot与Kusama的平行链方式运行，是多链连接器，通过 PoS 将其他公链与DeFi项目跨入波卡生态。这种战略定位，决定了Bifrost平台必然承载则丰富多样的资产类别。大致可分为以下几个类别：

1、多种Staking 衍生品vToken；
2、多种PLO衍生品vsToken；
3、Bifrost平行链上的原生代币BNC（Bifrost Native Coin）；
4、Polkadot/Kusama原生代币DOT/KSM；
5、Polkadot/Kusama平台上的众多平行链转移过来的Token资产；
6、其他公链或桥转移过来的Token资产；
7、用户在Bifrost平台上部署智能合约发行的Token资产。

这些Token资产必然会参与到各种DeFi应用中。AMM/DEX是最典型的DeFi应用。目前比较流行的的AMM算法实现，有Uniswap、Bancor、Balancer等。Bifrost平台在Runtime中内嵌了Balancer、B

ancor等子模块，方便用户创建和配置多资产交易池，用户可方便地在多种交易池中进行各类资产的兑换交易，或提供交易流动性赚取交易费用。Bifrost还集成了Polkadot生态中的AMM创新项目Zenlink的交易模块，以增强交易深度，并可自动寻找最优兑换价格与路径。Bifrost内嵌EVM与WASM子模块，现有的DeFi智能合约代码，也可轻松地移植到Bifrost平台上运行。

3. 经济模型

Bifrost经济模型在设计时，以实现如下几个目标为基本原则：

1、尽最大努力做到完全去中心化；
2、降低用户的使用成本；
3、尽量降低区块生产者（矿工，Collactor）的准入门槛与节点运行费用；
4、避免高额共识安全维护成本；
5、有效抵抗Staking机制中可能发生的高额Slash风险；
6、实现vToken类资产以及vsToken类资产的可交易同质化。

以这6大基本原则为出发点，Bifrost经济模型对BNC、vToken、vsToken进行了精心设计：

1、Bifrost公链和其他公链的区别，主要体现为Bifrost系统本身是可以盈利的。Bifrost支持的PoS公链与质押资产越多，盈利能力就越强。部分盈利会用于回购BNC，所以BNC的价值支撑不仅仅来源于公链必须具备的基础能力，比如价值存储与转账能力、部署智能合约应用的能力。

2、Bifrost 将预留一定比例的BNC 作为支付平行链卡槽竞拍或以平行线程方式运行的成本，随着卡槽数量的逐步增多，该成本相较于独立运行主网将会大幅下降，网络产生的价值更容易被其用户所捕获和分享。

3、Bifrost设计了简单有效的铸币公式，可让vToken、vsToken自动蕴含资产质押所产生的收益，无需额外进行结算。这种设计方式有利于交易平台上架这些资产，包括中心化交易所、去中心化DEX。交易平台方无需额外考虑如何派发收益给持币者，需额外开发对应的收益派发功能，即可支持 vToken、vsToken的交易兑换和使用，使vToken 、vsToken的流动性很容易得到扩展和加强。

4、Bifrost用BNC对铸造和持有vToken、vsToken、提供交易流动性、执行交易打包（Collactor节点）等行为进行激励，并预留一部分BNC作为Slash 保险基金，这些设计可有效保障Bifrost生态可持续健康发展。

3.1 Bifrost Native Token（BNC）

Bifrost Native Token（BNC）是 Bifrost 网络中的主网代币，初始总供应量为 80,000,000，目前在 Bifrost 测试网中已经可以收到可在主网进行 1:1 兑换的 BNC 凭证用于前期社区分发，目前 BNC 不具备转账功能，开放转账功能将在Bifrost网络启动过程中的第三阶段进行。分为：启动PoA网络、主网上线、开启转账提案、删除Sudo账户，通过这四个步骤进行。

3.1.1 价值捕获

- **衍生品流动性手续费**：Bifrost 网络中转账、交易、抵押等行为均需要支付一定的手续费来维持网络的问题，Bifrost 较提供 Flexable Fee 模块来支持各类资产支付手续费用，如 BNC、DOT、vDOT、KSM、vKSM 等资产均可以作为手续费使用，用于支付手续费的资产将被统一兑换为 BNC 后进入国库（Treasury）等待下一步治理分发。
- **竞价 Slash 抵押物**：参与票权竞价的节点需要抵押部分 BNC 用于获得 Bifrost 锁仓池中资产的投票，同时提高节点的 Slash 成本，该抵押物将根据节点的评分表现进行增加或减少。
- **治理凭证**：BNC 可以作为链上议会、技术委员会、国库拨款、公投治理、节点选举等所有链上治理功能，持有 BNC 即可获得 Bifrost 网络治理中的一份权利。
- **Staking 收益捕获**：通过 Bifrost 产生的 Staking 收益的 10% 将会用于 BNC 回购进入国库治理发放或销毁。

3.1.2 激励模型

预留和基金会部分根据 Bifrost 发展可能会推出更多激励方式，但是 Bifrost 不会进行零成本空投，任何激励方式都将满足基本价值捕获的原则。

- **vToken 铸币激励**：vToken 流动性是 Bifrost 所能带来的最大价值，也是其经过长时间积累的壁垒所在，总量 20.25% 的 BNC 将于用来奖励铸造 vToken 的用户。
- **PLO（Parachain Lease Offering）**：平行链首次竞拍成功对于 Bifrost 网络将会带来巨大价值，Bifrost 将会拿出总量约 15.75% 的 BNC 用于奖励帮助 Bifrost 参拍 Kusama 和 Polkadot 平行链的团体。

3.1.3 参与角色

- **Validator**：通过平行线程或平行链卡槽随机分配的 Validator，该角色为 Polkadot 或 Kusama 网络中的 Validator，将执行 Bifrost 业务代码并进行区块最终态验证。
- **Collator**：负责收集用户调用数据及传递查询信息，Collator 将产生区块并交由 Validator 做最终验证。
- **Bidder**：票权竞价人，通过提案公投选举，选举通过的账号成为Bidder可以将需要被投票的节点地址进行绑定，具备竞价获得Bifrost投票池中投票的权利，如该角色发生Slash级别或次数触发上限，将被取消Bidder权限。
- **Asker**：vToken 兑换或持有人，为协议委托票权拍卖方。
- **Council**：理事会主要被要求执行三项治理任务：提出全民公决，取消毫无争议的危险或恶意的全民公决以及选举技术委员会。
- **Technical Committee**：当系统处于危急状态，面临严重风险时，技术委员会可与 Bifrost Council 一起制定紧急公投，以快速进行投票和实施系统急救方案。
- **Sudo**：超级管理员，在系统上线最初期阶段，有权设置调整大部分系统参数以维护系统发展，但在 Bifrost 主网稳定运行之后，将通过社区提案公投移除Sudo权限。

3.2 BNC分配结构与解锁期

BNC的分发目标，是让Bifrost网络更加去中心化、构建Staking衍生品vToken的市场规模，激励 Staking 衍生品 vToken 的流动性市场。BNC 分配的每个环节都对 Bifrost 协议及其生态的健康发展至关重要。

为保障 Bifrost 功能开发、上线及生态系统的发展，不同部分的 BNC 分配将有着不同比例的锁仓时间，团队部分的 BNC 也将在 Day0 （流通日）之后180天（半年）开始线性解锁，持续两年时间解锁完毕。

Token Allocation							
Distribution of Tokens			Share	Price	Tokens	Funds	Lockup
Ecosystem	Kusama PLO (tentative)	2.25%	45%	-	36,000,000	-	Locked for governance
	Polkadot PLO (tentative)	13.50%					
	vToken Mint Incentive	20.25%					
	Collator Incentive	4.50%					
	Slash Insurance Fund	4.50%					
Founders and Team			20%	-	16,000,000	-	TGE 0% unlocked, unlock starting 6 months after TGE, unlocked every month, divided into 24 months to unlock
Seed Round I			6%	$0.06250	4,800,000	$300,000	TGE 25% unlocked, the remaining 75% unlocked every day 0.25%, 300 days unlocked
Seed Round II			4%	$0.09375	3,200,000	$300,000	
Strategic Round			2%	$0.31250	1,600,000	$500,000	TGE 30% unlocked, the remaining 70% unlocked every day 0.23333%, 300 days unlocked
Private Round			3%	$0.43750	2,400,000	$1,050,000	
Treasury (Foundation)			10%	-	8,000,000	-	Locked for governance
Reserved			10%	-	8,000,000	-	Burn/Incentive/PLO/Mint Drop/Community Build etc.
Total Supply 80,000,000 BNC							

BNC分配比例

3.2 生态系统

BNC 将预留 45% 的代币作为整个生态系统的激励，是为了保障Bifrost平台可以落地，并能够持续健康运行。包含 vToken 铸币挖矿（激励）、PLO卡槽租赁、Collator 节点激励，Slash风险保证金，Oracle 使用及跨链成本等。

3.2.1 vToken 激励

vToken激励分为三个部分，分别为铸币激励、流动性激励、Staking激励。

铸币激励：vToken 铸币数量对其流动性影响至关重要，所以 vToken 铸币挖矿将作为 BNC 重点分发环节，具体分发规则及公式请参考 3.2.6 章节。

流动性激励：持有vToken的用户若在系统自带的交易池中提供流动性，除了获取交易手续费的提成之外，还可获得BNC奖励，即为**流动性挖矿**。系统中也保留了一部分代币，用以奖励开发者研发、部署、运营其他各类交易工具（比如Uniswap），具体的奖励规则、奖励数量、奖励时长，由社区投票治理完成。系统池、第三方交易池的BNC份额占比，等同于各自的社区投票评分与总评分之和的占比。

Staking激励：持有vToken的用户可通过Staking，以实施某些行为，比如调整币种的评分；Bidder提供Slash保证金，若没有发生Slash行为，则被当作Staking进行处理，由此获得Staking激励；Collator需进行Staking，然后才能打包交易生成有效区块。

3.2.2 首次平行链发行（PLO）

获得平行链卡槽的项目才能够成为 Polkadot 和 Kusama 平行链，实现共享安全、中继跨链等特性，根据 Parity 策略，Kusama 网络将优先于 Polkadot 开启平行链卡槽拍卖功能，同时平行链卡槽将分阶段开放，以 DOT 锁仓数量拍卖进行，平行链卡槽具备 6 个月至 24 个月的租赁时间，Bifrost 计划竞拍至少 4 年的平行链卡槽，Bifrost 将预留总量 13.5% (45% * 30%) 的 BNC 用于 Polkadot 平行链卡槽的拍卖，2.25% (45% * 5%) 的 BNC 用于 Kusama 平行链卡槽拍卖，进行 Bifrost 平行链卡槽锁仓的 DOT 和 KSM 将拥有 BNC 的收益权，同时 Bifrost 也将发挥自身业务特性，为用户提供平行链锁仓 DOT/KSM 的流动性 vsDOT 和 vsKSM (Voucher Slot DOT/KSM)，目前波卡平行链具体竞拍规则尚存在不确定性，具体 PLO 参与相关细则将在波卡平行链竞拍规则推出后公布。

3.2.3 Collator

当 Bifrost 接入平行链，上线主网时，将支持 Collator 提供服务，为激励质量更高，服务范围更广的 Collator，协议将根据 Collator 提供服务的工作量进行激励 BNC，系统将预留生态系统中的 10% 的 BNC 作为 Collator 激励。

3.2.4 Slash Insurance Fund（SIF）

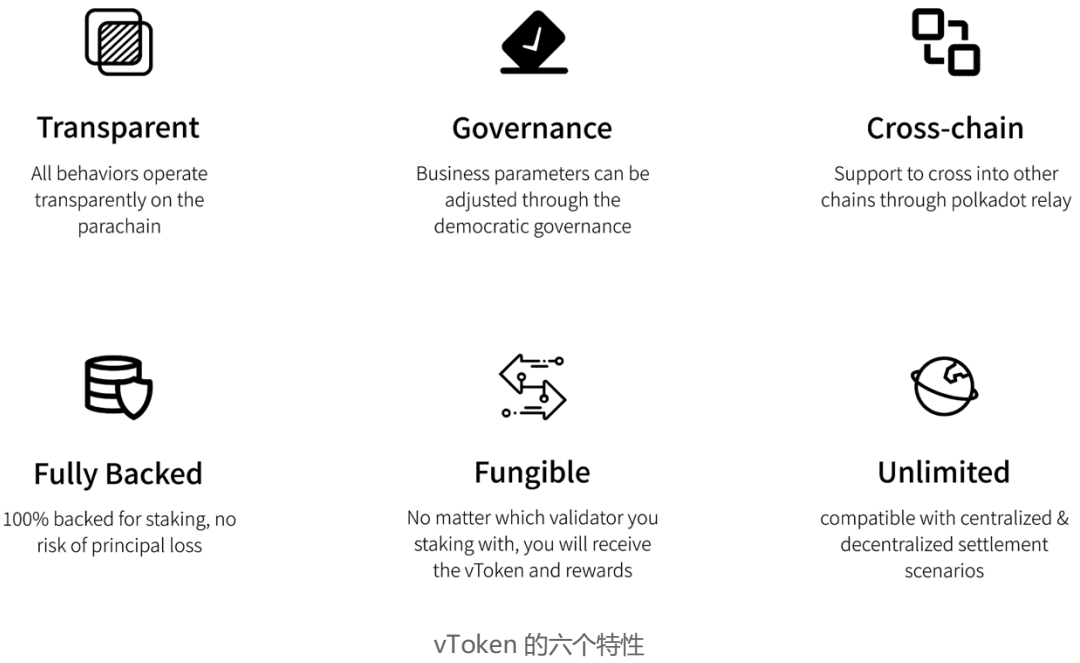
Bifrost 将预留 10% 的 BNC 作为 Slash 系统保险金，在 Vote Bidder 抵押、公共保险金等风控措施失效时，将由系统预留的 10% BNC 作为 Slash 保险资金进行赔付。Slash 通常设计为渐进式惩罚，一般在多次触发非法操作时（如漏块、丢块）才会进行部分金额的惩罚，所以 Bifrost 将穷举所支持 PoS 网络 Slash 规则，根据严重程度警告或惩罚竞价人，成为竞价人，将需要抵押一定数量的 BNC 作为 Slash 保险金，由于竞价人主动获得投票权，所以应当承担其 Slash 带来的资金损失风险，所以当 Slash 发生时，将先从竞价人所抵押的 BNC 中扣除，若当 Slash 规模较大，竞价人所抵押金额不足以支付 Slash 罚金时，将从公共保险金中扣除，由全体 vToken 持有者承担 Slash 风险，当 Slash 保险金少于 0 时，将从锁定池中进行扣除，此时 vToken 的铸币价格表现为下跌，由所有 vToken 持有者共担 Slash 风险，整体 Slash 若达到 Token 总量的 10% 时，相关 Token 协议将进入紧急停止阶段，该阶段所有进行 Staking 的原 Token 将会被赎回，同时暂停票权竞价和 Staking 功能，vToken 铸币价格将不再变化，用户可以随时将 vToken 赎回成原 Token，系统将排查 Slash 原因并防止损失进一步扩大，问题排查完毕后，可通过公投再次将协议重新启动。对于存在一次性100%罚款额度的公链，Bifrost会对节点进行检查，要求其自身抵押金额不少于55%，才会跟投不多于45%的份额，以免节点故意引发大额Slash行为。

通过以下提高 Slash 抗风险能力：

- Fishman 方式开放式 Slash 信息提交与验证（带有奖励与惩罚机制）；
- 风控委员会；
- 逐级风险控制；
- Vote Bidder Slash 抵押金；
- Slash 公共保险基金；
- Slash 系统保险金。

3.4 Voucher Token（vToken）

Voucher Token（凭证代币）简称 vToken，是由用户使用其他公链上的可质押类资产，在Bifrost 平台铸造而成的可交易同质化资产。vToken 代表原质押物的赎回权和收益权，持有 vToken 可获得原Token资产质押时所产生的收益，同时兼具流动性。在某些应用场景下，vToken甚至可以再次成为新的质押物，具备一定的杠杆功能。同时 vToken 还具备可追溯、可治理、可跨链、全储备、可替代和全场景等六个特性。



vToken 的六个特性

3.4.1 收益结算方式

为了去中心化产生收益，同时有能简单高效地提供流动性，增加衍生品兼容场景，vToken 的收益结算方式被设计为可同时兼容中心化和去中心化场景。用户只要持有vToken，无论是自己保管私钥，还是充值到中心化交易所或托管机构，皆可持续获得vToken所产生的质押收益。这得益于vToken摒除了传统的链上交易结算方式，而采取铸币价格上调的方式让vToken自动蕴含资产收益功能。为了

避免后来用户瓜分先前用户的收益，任意时间的铸币行为必须遵循当时的Token与vToken比例价格，vToken价格表现相对于原 Token 持续上涨，用户收益直观。

参数说明

- 铸币价格 $vToken_{mint\ price}$
- 铸币数量 $vToken_{mint}$
- 原币 Staking 数量 $Token_{staking}$
- Staking 收益 $Token_{staking\ rewards}$
- 年化收益率 $vToken_{yield}$
- 赎回价格$vToken_{redeem\ price}$
- vToken 持有时间 $vToken_{holding\ days}$

计算公式

- 铸币价格$vToken_{mint\ price} = Token_{staking} \div vToken_{mint}$
- 铸币价格初始值$vToken_{mint\ price} = 0.01\,Token$
- vToken 铸造 $vToken_{mint} = Token_{staking} \div vToken_{mint\ price}$
- 铸币价格上调 $vToken_{mint\ price} = \left(Token_{staking} + Token_{staking\ rewards}\right) \div vToken_{mint}$
- 年化收益率 $vToken_{yield} = \left(vToken_{redeem\ price} - vToken_{mint\ price}\right) \div vToken_{holding\ days} \times 365$

案例 A：A 用户使用 10 DOT 通过 Bifrost 根据铸币价格（$0.01\,Token$）铸造 1000 vDOT，原 DOT 通过 Voucher Notary 和 Voucher Bidder 博弈完成 Staking 操作，一周后原 DOT 通过 Staking 产生 0.5 DOT 收益，而通过 Staking 产生的 DOT 收益不会对应铸造新的 vDOT，所以铸币价格由原先的 $0.01\,Token$ 上调至 $0.0105\,Token$ $(10.5 \div 1000)$，此刻 1000 vDOT 将可以赎回 10.5 DOT，多产生的 0.5 DOT 则为 A 用户持有一周 vDOT 的 Staking 收益。

案例 B：经过案例 A 后，铸币价格上调至了 $0.0105\,Token$，当前 B 用户使用 10 DOT 根据当前铸币价格可以铸造 952.380952381 vDOT（vToken 精度为 10^{12}），同样 B 用户持有 952.380952381 vDOT 一周后，产生 0.5 DOT Staking 收益，所以铸币价格由原先的 $0.0105\,Token$上调至 $0.011025\,Token$ $(10.5 \div 952.380952381)$，此刻 952.380952381 vDOT 将可以赎回 10.5 DOT，多产生的 0.5 DOT 则为 B 用户持有一周 vDOT 的 Staking 收益。

3.4.2 收益产生方式

当 Bifrost 协议锁仓池中的资产进入投票池中时，进入投票池方法将分为竞价投票（默认）和自行治理，竞价投票原 Token 所对应的票权将由竞价人（具备竞价票权权利的候选验证人）竞价获得，通过此方式，用户的投票权将通过 Bifrost 进行代理，指定投票给特定时间内出出价最高的竞价人。该方式本质上是将原先 Staking 收益由收益分账的模式改变为 “先付后租”，将不同 PoS 公链的 Staking 收益标准化，绕过不同收益规则带来的限制。

票权市场

竞选机制，放弃了收益分账的模式，验证人如果想要进入 Bifrost 的验证者集，必须首先进行收益率出价，即告诉协议，愿意给使用协议的 Staker 多少比例的收益。倘若出价为10%，并最终被协议所接受，无论该验证者的实际收益率是多少，都将按照 10% 向协议分享收益，《Share Holder Votes For Sale》为该功能提供了更多延展和论证说明。

- 竞价人出价 < Staking 收益，类比为竞价人配置佣金 > 0%
    - 存在利润，用户获得正常收益
- 竞价人出价 = Staking 收益，类比为竞价人配置佣金 = 0%
    - 不存在利润，用户获得原链最高收益
- 竞价人出价 > Staking 收益，类比为竞价人配置佣金 < 0%
    - 存在补贴，用户获得高于原链的溢价收益

根据市场对票权需求，投票竞价将产生不同的结果，通常情况下，用户提名产生的 Staking 收益将由验证人扣除佣金后进行发放，而通过投票竞价的方式，验证人将转变为竞价人角色，出价高低将根据市场需求进行波动，根据对市场的理性判断，竞价人将出价控制在低于 Staking 收益的范围，获得用户 Staking 收益的利润，当市场对票权需求旺盛时，竞价人将支付溢价才能获得投票，用户将获得竞价人支付的溢价作为 Staking 收益，该情况下用户获得的 Staking 收益将会高于原链的最高收益。

自行治理

用户将绕过竞价人出价过程，根据自身决策选择指定竞价人进行成交，但是所产生收益依然需要遵循 Bifrost 收益分发规则，进行回购金、保险金和渠道金的扣除。

收益结构：

- **10%** - 回购金，定期回购 BNC
- **1% ~ 5%** - 公共保险金，抵押资金被 Slash 时风险分摊，根据 Slash 历史情况进行浮动
- **3%** - 渠道金，根据渠道贡献进行分发
- **82% ~ 86%** - 用户发放，进入原 Token 铸币池，通过提升铸币价格将收益发放至用户

3.4.3 保留治理权

持币人发生 vToken 铸币行为时，可以选择指定的竞价人无条件获得对应票权，当持币人不进行指定竞价人时，默认进入竞价市场进行竞价。

3.4.4 衍生品不可能三角

原链票权

持币人选择验证者，就像是代议制民主当中的议员选举。每个 Token 都代表一个选票，投票权属于 Token 的持有人。Staking 衍生品协议作为一个中间层，不应该改变这个基础，应该让用户自己来选择验证者。但这样做将导致一个严重的问题，那就是衍生品不具备同质性（non-fungible），委托给不同的验证者，将产生不同的衍生品。

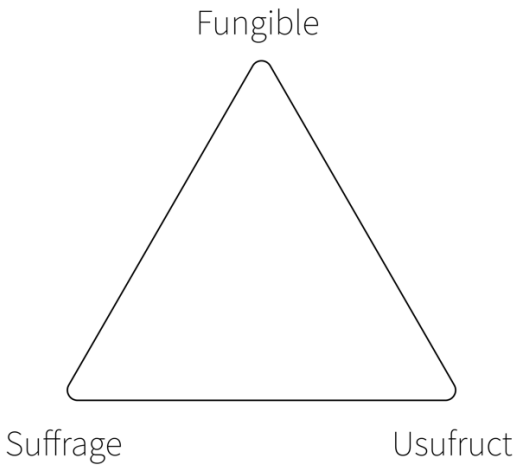
同质性

持币人选择任意验证者都将产生相同的收益，实现不同持币人铸造的 Staking 衍生品都对应相同的权益，具备同质性的 Staking 衍生品将获得更好的流动性，但对于持币人来说，此种方式免除了选择验证人带来的 Slash 风险，更容易导致公地悲剧发生，使整体 Staking 收益下降。

表达权益

Staking 衍生品在解放 Staking 流动性的同时，可以继承其 Staking 抵押物产生的收益，当 Staking 衍生品发生转移时，其收益和赎回权都将随之转移。

Bifrost 在 Staking 衍生品不可能三角中，为提供更好的 Staking 衍生品流动性，协议设计上更侧重于同质性和表达权益两个方面，默认将用户原链票权委托给协议通过票权竞价方式进行分配。



衍生品的不可能三角

3.4.5 vToken 铸币激励

Bifrost 经济模型中将预留 16,200,000 BNC（Bifrost Native Coin）占总量 20.25% 的 BNC 作为 vToken 铸币激励，激励期限被设置为线性释放十年，每两年产量减半，根据用户 vToken 铸币价值进行分配，以激励用户更主动铸造具备权益、同质性和流动性的 vToken。

参数说明

- $BNC^{total\ incentive} = 16200000$
- $Block^{time} = 6s$
- $Proportion^{inital} = 0.25$
- $Year^{launched} = 2020$

计算公式

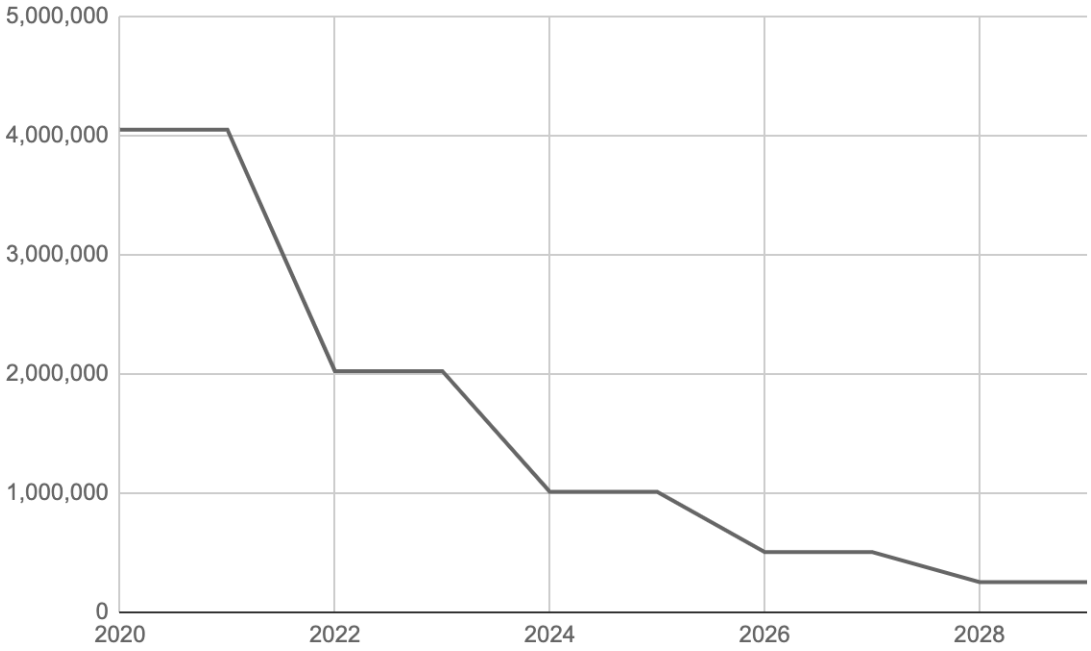
- $Block^{year\ number} = 365 \times 86400 \div Block^{time}$
- $Proportion^{year} = Proportion^{inital} \div 2^{INT((Year - Year^{launched} \div 2)}$
- $Reward^{per\ block} = BNC^{total\ incentive} \times Proportion^{year} \div Block^{year\ number}$

Bifrost vToken Incentive (16,200,000)				
Year	Rewards (BNC)	Proportion	Reward/Block (BNC)	Daily (BNC)
2020	4,050,000	25.0000%	1.5410958904	**11,096**
2021	4,050,000	25.0000%	1.5410958904	**11,096**
2022	2,025,000	12.5000%	0.7705479452	**5,548**
2023	2,025,000	12.5000%	0.7705479452	**5,548**
2024	1,012,500	6.2500%	0.3852739726	**2,774**
2025	1,012,500	6.2500%	0.3852739726	**2,774**
2026	506,250	3.1250%	0.1926369863	**1,387**
2027	506,250	3.1250%	0.1926369863	**1,387**
2028	253,125	1.5625%	0.0963184932	**693**
2029	253,125	1.5625%	0.0963184932	**693**
10 years total	**15,693,750**	**96.8750%**		

铸币激励十年产量预期

铸币激励产量折线

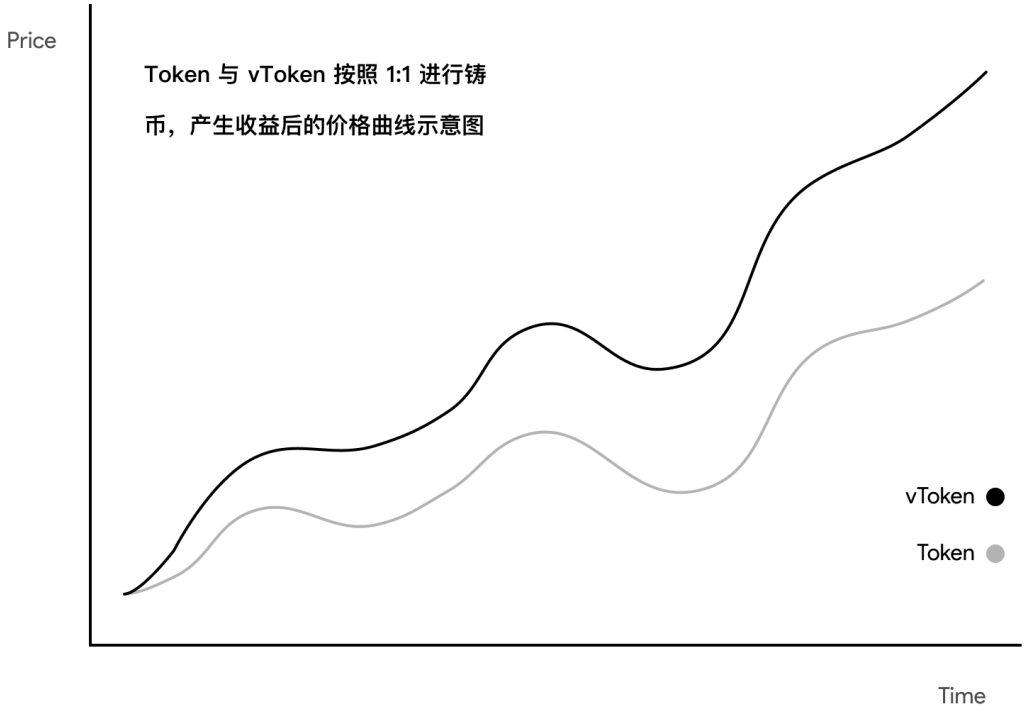
- X 轴：挖矿年份
- Y 轴：BNC 产量



铸币激励十年产量折线

vToken与Token价格曲线的相似度

- *X 轴：时间*
- *Y 轴：价格*



铸币激励分配算法

具体的激励算法采取瓜分模型，按照轮次进行，每一轮中的每一笔铸币交易，按照铸币量占本轮的总量比例分享本轮次释放的激励总量。大体流程：

1、设当前每个区块释放N个BNC用于铸币奖励，其中有D个BNC专用于vToken铸币行为；

2、记录本轮次中铸币交易的最大值，若在其之后的X个区块没有更大的铸币额，则进行本轮次的结算（X是一个常数，比如50，其具体值需在测试网上进行充分测试后再做确定）；

3、本轮次的区块数量Y是不确定的（Y >= X + 1），铸币者瓜分Y*D的BNC总奖励；

4、Bifrost平台支持多种Token对应的vToken，每个币种按照评分占比机制分割N个BNC；

5、不同币种按照可兑换的BNC数量对铸币量做比较大小的运算。

6、评分机制：社区投票形成vToken的基础分S，用户可通过抵押M个BNC调整权重，

抵押BNC是有收益的，可参考Staking激励部分的设计。评分公式为 S+F(M)，F为M的对数函数，F(M) = $log_2(M - 512)$。若SUM是所有币种的评分之和，则有D / N = (S+F(M)) / SUM。

3.4.6 vToken 铸币渠道金

通过 Bifrost 协议进行 vToken 铸币时，可选择传递铸币渠道参数，该参数会根据铸币量记录渠道提供方的贡献值， Staking 收益结构中的 3% 将作为渠道金由所有渠道提供方根据自身贡献占总贡献的比例进行分配，渠道贡献占比高时，可获得的渠道金分成则更多，以此激励 Bifrost vToken 铸币协议被集成到钱包、Dapp、交易所等入口渠道系统中。随着铸币交易的产生，渠道提供者的贡献值将持续增加，直至每六个月进行公投提案将其清零。每当有Bidder出价时，Bifrost会进行一次结算，将3%的渠道金分配给渠道值排名256位以内的渠道贡献者。256是系统设定的初始参数，可通过社区投票进行更改。

4. Roadmap & Milestone

- 2019 Q3
    - First Line Of Code
    - Launch Official Website
    - Smart Contract MVP

- 2019 Q4
    - Substrate Hackathon

    - Whitepaper
    - Apply Web3 Foundation Grant

- 2020 Q1
    - Launch Bifrost POC-2 Testnet
    - Delivery Web3 Grant
    - Dashboard online

- 2020 Q2
    - Support EOS Jungle Testnet
    - Parachain on Kusama
    - Launch Bifrost Asgard CC1

- 2020 Q3
    - Open Staking bidding beta
    - Support EOS Cross Chain
    - Launch Bifrost Asgard CC2
    - Release Bifrost Dapp Beta

- 2020 Q4
    - Staking drop
    - Security Audit begin
    - Internal AMM Swap pool
    - Launch Bifrost Asgard CC3
    - Launched Mainnet

- 2021 Q1
    - Announce PLO detail & Auction page
    - PLO & Auction Polkadot SLOT
    - Support vsDOT/vsKSM (Parachain slot auctions DOT)
    - Support vDOT/vKSM/vETH(2.0)/vEOS

- 2021 Q2
    - Derivatives Dapp Grant Program
    - vToken Listing on DEX/CEX/Parachain
    - Launch vToken statistics page
    - Support vATOM/vALGO/vONE

- 2021 Q3
    - Release vToken screening/support standards
    - Mortgage derivatives (More than Staking)

5. 总结

Bifrost 的近期目标是在多个著名PoS公链、以及Pokadolt生态中的多个平行链与中继链之间，为投资者提供统一的业务抽象层，并提供去中心化的、安全的、标准的、可配置的金融工具，构建丰富灵活的资产抵押收益票权市场。Bifrost的愿景目标是成为多链之间的联接器，强化整个区块链行业的生态环境建设，并助力推动 DeFi 科技的普及应用与深度演化。

6. 参考文献

[1] Gavin Wood, "Polkadot, Substrate and Ethereum", https://medium.com/polkadot-network/polkadot-substrate-and-ethereum-f0bf1ccbfd13

[2] Markus Brill, Rupert Freeman, Svante Janson, Martin Lackner, "Phragme´n' s Voting Methods and Justified Representation", https://pdfs.semanticscholar.org/1843/c728cb56caf908247f8473b17734299cd24a.pdf

[3] Jeff Burdges, Alfonso Cevallos, Peter Czaban, Rob Habermeier, Syed Hosseini, Fabio Lama, Handan Kilinc Alper, Ximin Luo, Fatemeh Shirazi, Alistair Stewart, Gavin Wood, "Overview of Polkadot and its Design Considerations", https://eprint.iacr.org/2020/641.pdf

[4] Web3 Foundation, "The Polkadot Host Protocol Specification", https://github.com/w3f/polkadot-spec/releases

[5] Vitalik Buterin, Virgil Griffith, "Casper the Friendly Finality Gadget", https://arxiv.org/pdf/1710.09437.pdf

[6] Colin Schwarz, "Ethereum 2.0: A Complete Guide. Casper and the Beacon Chain", https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-casper-and-the-beacon-chain-be95129fc6c1
[7] Dan Larimer, "DPOS BFT — Pipelined Byzantine Fault Tolerance", https://medium.com/eosio/dpos-bft-pipelined-byzantine-fault-tolerance-8a0634a270ba
[8] Jae Kwon, Ethan Buchman, "Cosmos: A Network of Distributed Ledgers", https://www.chainwhy.com/upload/default/20180628/d849f659762a2fbbd2685f9b37c5d24c.pdf
[10] Victor Allombert, Mathias Bourgoin, Julien Tesson, "Introduction to the Tezos Blockchain", https://arxiv.org/pdf/1909.08458.pdf
[11] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich, "Algorand: Scaling Byzantine Agreements for Cryptocurrencies", https://eprint.iacr.org/2017/454.pdf
[12] ConsenSys, "Ethereum 2.0 Staking Ecosystem Report", https://cdn2.hubspot.net/hubfs/4795067/Codefi/Ethereum%202.0%20Staking%20Ecosystem%20Report.pdf
[13] Loizos Leracleous, "Shareholder Votes for Sale", https://hbr.org/2005/06/shareholder-votes-for-sale