

Bifrost Finance Whitepaper

Author: Lurpis, Buffalo

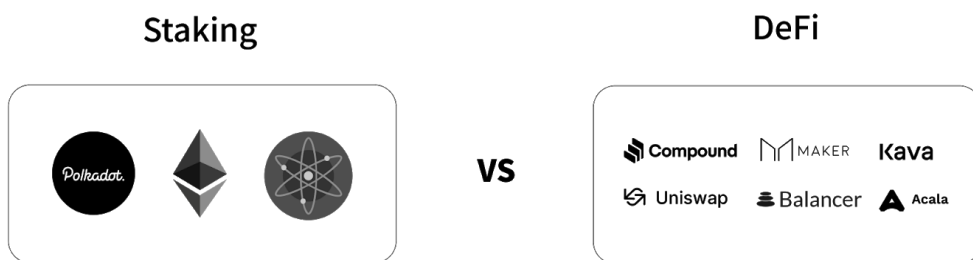
Update: 2020/10/28

Version 1.1.1

1. 市场概述

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 80+ 条总市值超过 1,453 亿美元的 PoS 公链诞生，仅通过质押（Staking）每年将产生超过 25 亿美元的收益，同时 DeFi 市场的火热以及对以太坊 2.0 Staking 机制推出的期待充斥着 2020 年的加密市场。而去中心化金融（DeFi）以及 Staking 市场的高速发展正在推动 DeFi 及 Staking 两种机制越来越多地在区块链版图中交互，并叠加产生了越来越多可组合性，不过问题也接踵而至。

1.1 Staking 和 DeFi 收益竞争问题

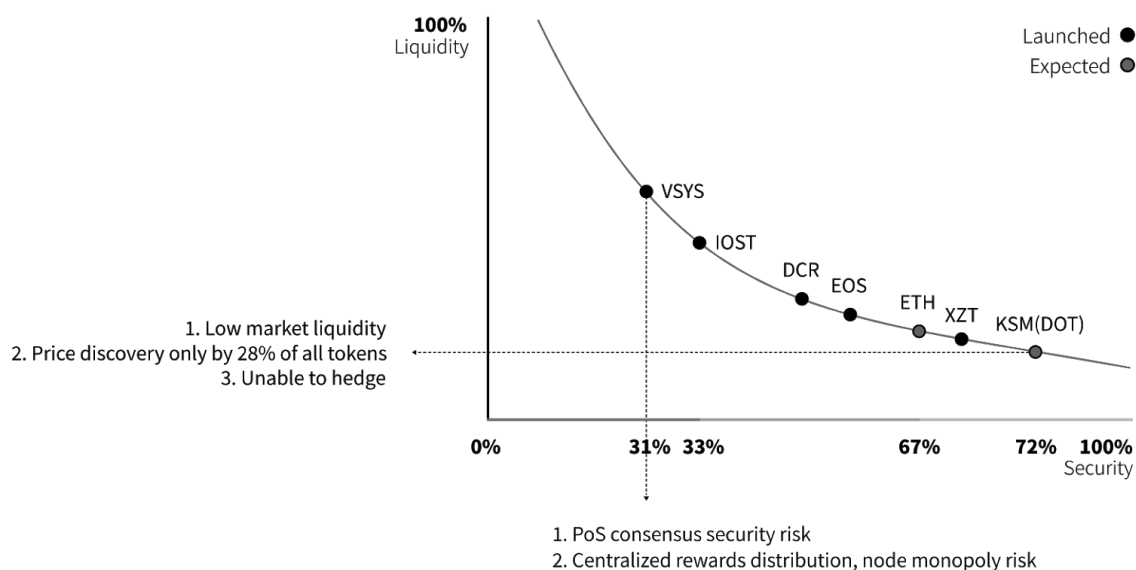


Staking 与 DeFi 收益竞争

由于目前包括流动性挖矿等新兴 DeFi 产品的涌现，DeFi 产品或给用户带来拥有超高的年化收益率，但这构建在 ETH PoW 共识上的繁荣是否能够在 ETH 2.0 或 Polkadot PoS 共识下延续是一个问题，对于用户来说在 Staking 和 DeFi 之间只能二选一，DeFi 会天然因为 Staking 收益问题而产生用户竞争，如果 DeFi 产生收益率无法覆盖 Staking 锁仓成本，那么用户将从 DeFi 将资产转移进入 Staking 锁仓，选择产生收益更高的方式，若反之用户将资产放入收益更高的 DeFi 产品，网络 Staking 率不足则会造成 PoS 网络共识安全出现问题，两种情况无论如何选择都将会面临双输局面。

同时 Staking 仍然存在如参与门槛高、无流动性、治理与利益冲突等诸多问题，PoS 与 PoW 同样存在拜占庭容错问题，需要更多的用户参与到 Staking，才能让整个网络更加去中心化、更加安全地运行，而部分项目为了解决 Staking 以上问题采用中心化托管的方案，我们认为这种本末倒置的做法在短期可能提升用户 Staking 的参与度，但从长期来说，它将逐渐侵蚀 PoS 生态的去中心化体系，让系统变得不再安全。

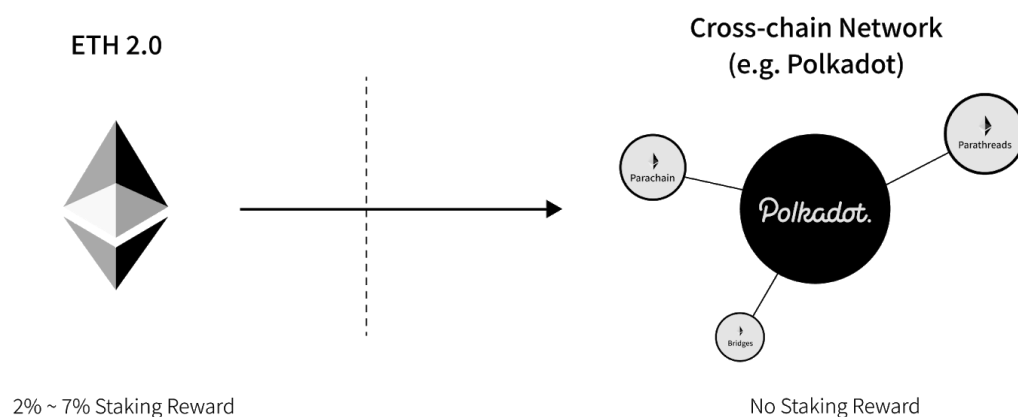
1.2 PoS 网络流动性和安全性互斥问题



PoS 共识网络安全性和流动性权衡

PoS 权益证明机制决定网络的安全性是由 Staking 机制维护的，这也意味着 PoS 网络流动性和安全性是处于此消彼长的互斥状态。通常情况下，增加 Staking 的流动性需要权衡网络安全性，而 PoS 抵押代币流动性解决方案则寻求打破这个掣肘，降低用户参与 Staking 的机会成本，同时提高 PoS 公链的整体质押率，若质押率过低（如 VSYS）则会产生 PoS 共识安全隐患，节点中心化风险更高，引起用户和开发者对安全引发担忧从而流失，反之质押率过高（如 KSM）则会导致市场流动性不足，价格发现仅能通过少部分的 Token 来完成，无疑存在很多泡沫，导致价格波动率较高，同时对于正在进行 Staking 的用户来说，因为锁仓没有流动性而无法对冲这部分波动风险，造成 Staking 的机会成本不断被放大。

1.3 跨链场景下 Staking 收益问题

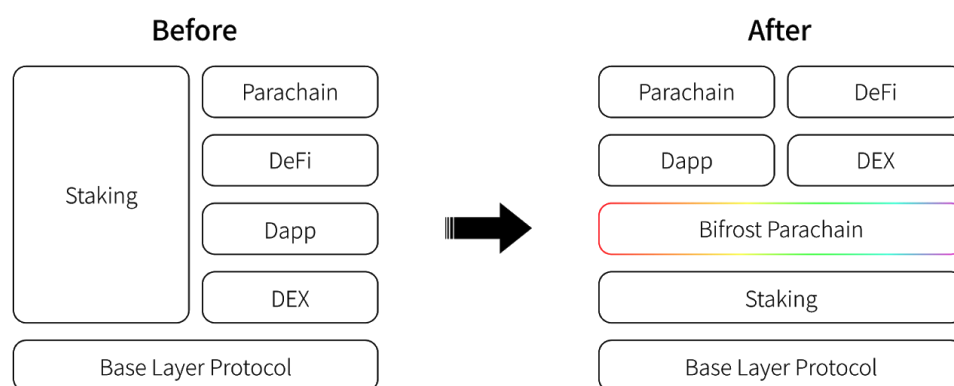


PoS 网络跨链状态下 Staking 收益成本

随着波卡及 Cosmos 等跨链项目上线，用户会参与越来越多的跨链场景，而目前跨链进行兑换的代币有可能会使用户失去原有代币的 Staking 收益，让需要将 Token 用于跨链场景的用户除了需要承担手续费等费用外，还需额外承担 Staking 收益随时成本，而随着区块链逐步打破壁垒，链上资产或数据可以自由流通，能够在跨链场景中获得 Staking 收益，可以大幅降低用户参与跨链的进入成本。

2. 项目简介

Bifrost 是一个为质押资产（Staking、Collateral、IPO...）提供流动性的跨链网络，当前从 Staking 切入，以 Staking 衍生品的形式为 Staking 提供流动性，基于 Substrate 开发，底层基于 WebAssembly，LIBP2P 和 GRANDPA 共识，构建在 Polkadot 网络之上，作为波卡生态中的 DeFi 项目，推出 Staking 衍生品 vToken（Staking Derivatives Voucher Token），通过 Bifrost 用户可以随时将 PoS 币种通过 Bifrost 协议兑换成 vToken 获得 Staking 收益和流动性。已经获得了 Web3 Foundation Grant，也是 Parity 下属的 Substrate Builders Program 的一员，同时位列 Web3 基金会与万向区块链实验室联合组建的 Web3 Bootcamp 孵化器的 15 个核心成员之一，获得由 Web3 基金会和万向区块链实验室从技术、产品、资本、法务、生态合作等全方位的支持。



A Layer Between Staking and Applications

Bifrost 提供了一个在 Staking 与应用层之间的中间抽象层，让本来构建在底层协议上 Staking 与应用层由互相并列的关系变成上下兼容关系，由此解决 Staking 和 DeFi 收益竞争问题。用户通过 Bifrost 平行链随时将 PoS 币种通过 Bifrost 协议兑换成 vToken 的机制，而每一种 PoS 代币将对应不同的 vToken，比如桥接 Polkadot 代币的 vDOT、桥接以太坊的 vETH 等。简单来说，用户只需持有 vToken 即可获得 Staking 收益，通过提供 vToken 的流动性，让 PoS 网络的流动性和安全性能兼得，从而解决 PoS 网络流动性和安全性互斥问题，再通过 vToken 构建在平行链中的跨链特性，使得跨链场景中也能获得 Staking 收益，从而解决跨链场景中 Staking 收益获取问题。

而解决之类问题的关键在于如果给 Staking Derivatives 提供一个交易场景，满足其流动性需求，通过 Bifrost 内建 vTokenSwap（AMM 交易池）可以完成单池 8 币种 64 个交易对之间的交易需求，后续还将开放 vTokenSwap 交易池之间的最优路径兑换，vTokenSwap 的流动性提供者将获得交易手续费分成和流动性激励。vTokenSwap 为 vToken 提供初始流动性场景，同时 vToken 无需结算的设计方式使得其可以中心化和去中心化的场景，对于进行 Listing

vToken 的第三方中心化交易或存储场景中，合作方无需额外开发即可将 Staking 收益派发至用户手中，使得 vToken 的流动性跟容易得到扩展。

2.1 实施方案

Bifrost 将以 Polkadot 和 Kusama 平行链的形式完成业务落地，同时共享 Polkadot 和 Kusama 共识安全性，从而避免高额的共识安全维护成本，想要维护一条独立的 PoS 共识网络花费成本是巨大的，以 Cosmos 为例，根据当前 72% 质押率和 8.09% 收益率来计算每年通胀率约为 5.8%，则每年需要大约 15,344,540 ATOM（约为 \$83,474,302）的网络安全维护成本，若网络用量较低、价值捕获能力不足，高额的通胀甚至会将网络推向死亡螺旋的窘境。

另一方面，Bifrost 当前从 Staking 衍生品切入为多数 PoS 网络提供流动性，势必导致多数 PoS 网络中原生资产及其对应票权在 Bifrost 协议中进行映射，而此类原生资产所对应的共识安全也相应被转移到了 Bifrost 网络中，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，这将使 Bifrost 网络不再被信任，甚至遭到其他 PoS 网络的技术反制，所以只有在 Bifrost 共识安全高于或等于原 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。

所以 Bifrost 将竞拍波卡平行链卡槽，通过成为平行链共享波卡共识安全，一方面给予 Bifrost 所支持的其他 PoS 网络及平行链更多共识安全保障，另一方面，降低 Bifrost 为维护独立 PoS 网络共识安全所支出的高额成本。

2.2 交易工具

在众多的区块链DeFi应用中，目前比较流行的交易工具的算法实现，有Uniswap、Bancor、Balancer等自动化做市商（AMM）程序。Bifrost平台在Runtime中内嵌了Balancer子模块，方便用户创建和配置多资产交易池。在Bifrost平台生成的多种vToken，以及从Polkadot/Kusama流转至Bifrost平台的各类Token与资产，都可以很方便地在多个Balancer交易池中进行兑换交易。Bifrost自带有EVM子模块，Uniswap、Bancor以及其他流行的DeFi智能合约代码，也可很轻松地移植到Bifrost平台上运行。

2.3 典型业务 - Staking Liquidity

为基于 PoS 的公链或其他系统提供 Staking 标准流程与更灵活的金融工具，给 Bifrost 社区用户带来额外收益，是 Bifrost 项目的核心设计目标之一。Bifrost 通过安全的、去中心化的资产跨链技术，确保 Staking 资产的安全。通过 Bifrost 进行 Staking 活动，和直接进行 Staking 活动的区别，可以参考以下流程：

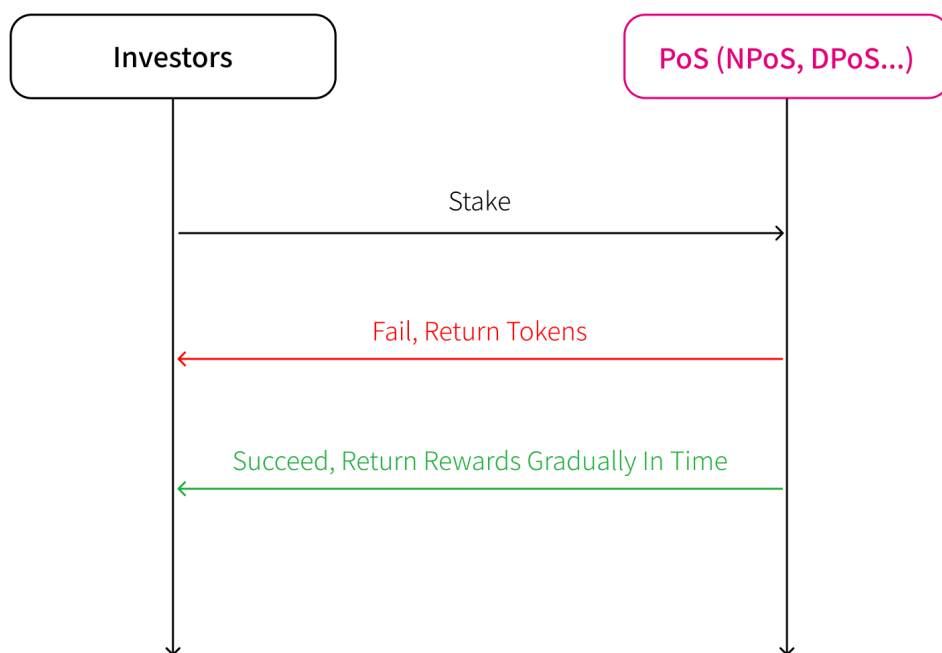


图 1 原生 Staking 交互流程图

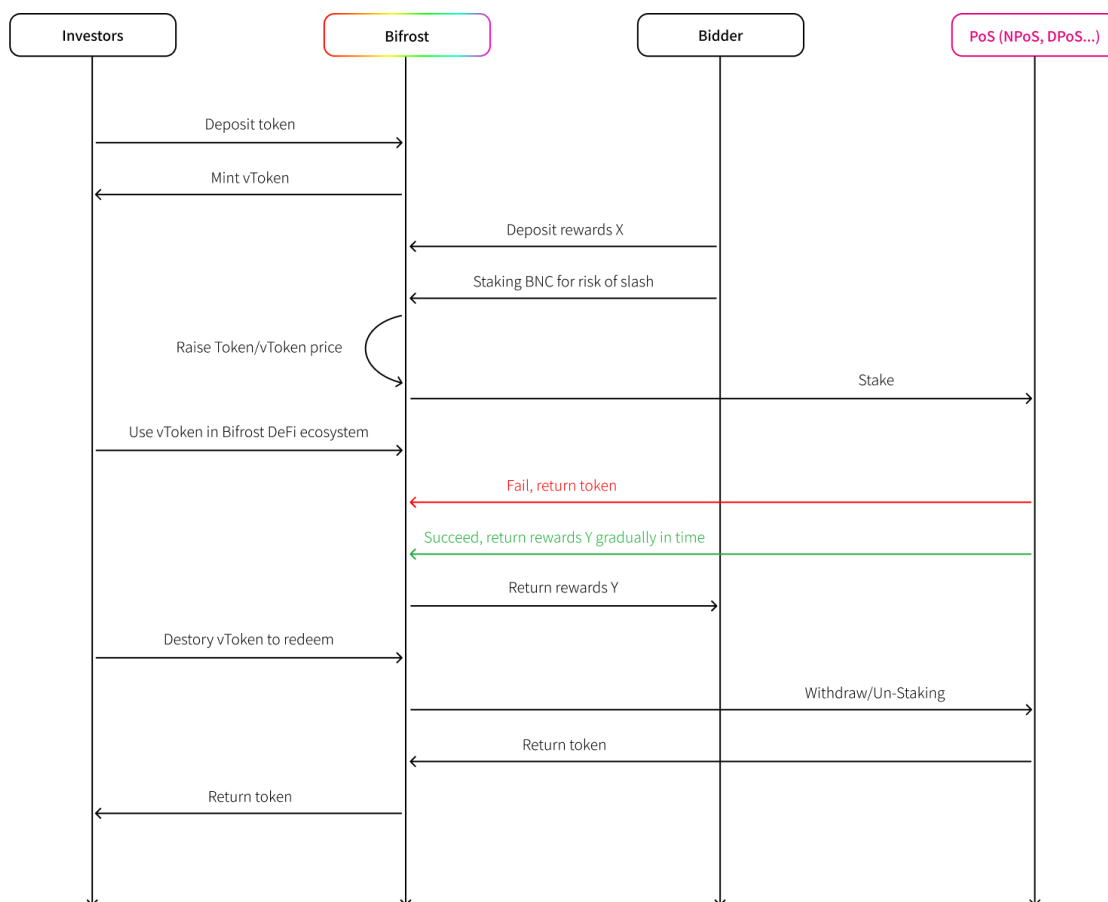


图 2 通过 Bifrost Staking 交互流程图

2.4 典型业务 - IPO Liquidity

Bifrost 作为 Polkadot 生态的一条预备平行链，在整个生态中做好 Staking 业务的同时，也为那些与 Staking 具备较高相似度的 DeFi 经济模型提供基础支撑工具，为整个生态的健康发展贡献力量。IPO（Initial Parachain Offerings）是 Bifrost 优先考虑实现的工具之一。IPO 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，直接进行 IPO 与通过 Bifrost 进行 IPO 的交互流程对比如下：

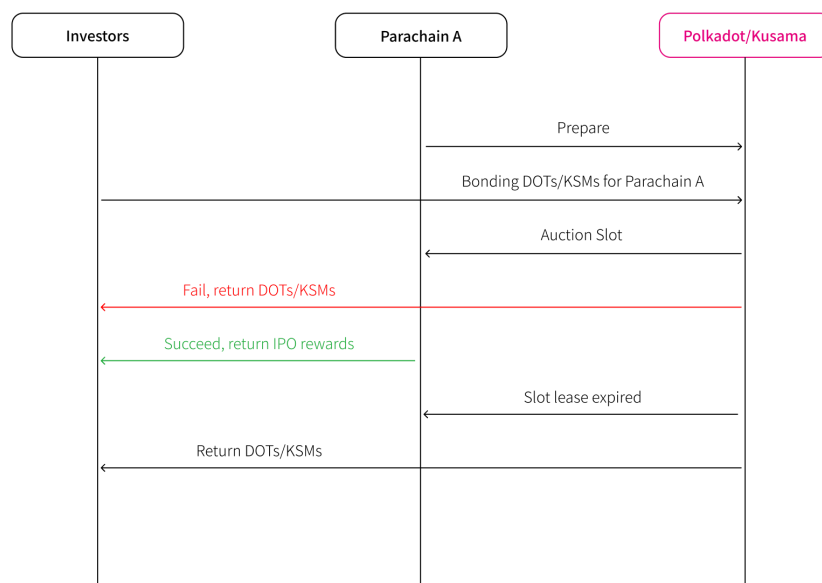


图 1 原生 IPO 交互流程图

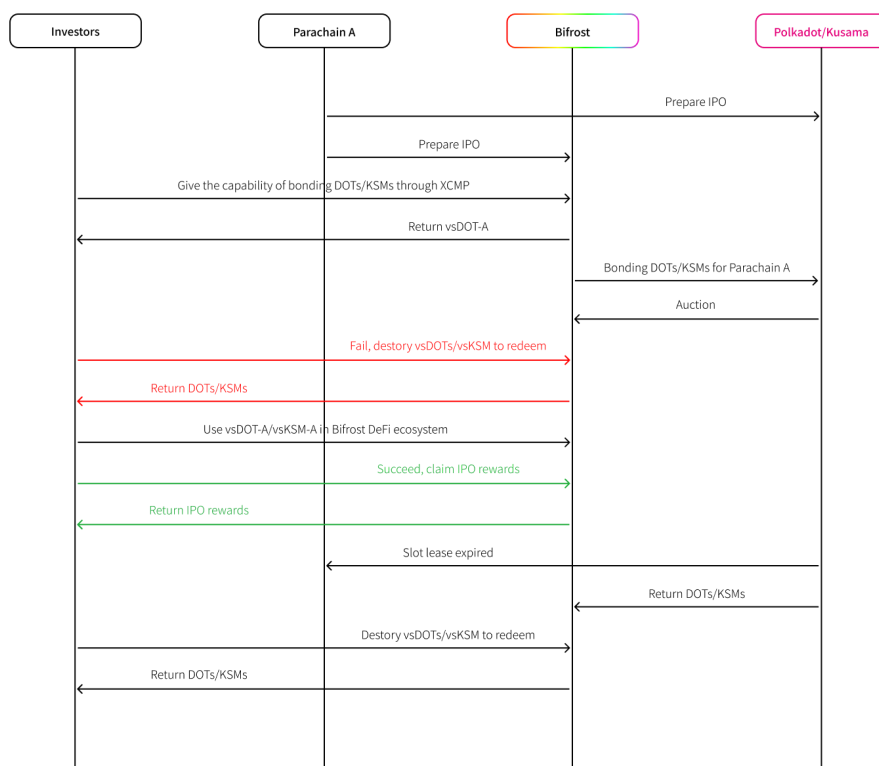


图 2 通过 Bifrost IPO 交互流程图

3. 经济模型

3.1 经济模型设计目标

为 80% 质押资产提供流动性作为 Bifrost 的使命和愿景，我们认为实现愿景的道路首先是规则的设计，Bifrost 将以共享 Polkadot 安全性的形式为用户提供服务，我们认为当为其他 PoS 公链提供质押物流动性的同时，其他公链也间接的将相对应其共识安全转移到了 Bifrost，而与此同时，维护一个足够安全的独立 PoS 共识是十分昂贵且漫长的，当独立主网运行时，若该网络中锁定资产总量超过其市值时，黑客就有足够的动力攻击该独立主网并转移资产，这不但会让项目直接面临死亡的同时还会导致支持的其他网络安全遭受打击等连锁反应，所以当运行独立主网时，该网络能够锁定资产的上限就是该独立主网的市值，所以 Bifrost 将会共享 Polkadot 或 Kusama 的共识安全性，而不维护一套独立的 PoS 网络，让 Bifrost 网络中锁定的资产更加安全。

综上所述 Bifrost 将预留一定比例的 BNC 作为支付平行链卡槽或线程的成本，随着卡槽数量的逐步增多，该成本相较于独立主网将会大幅下降，Bifrost 则更容易将网络产生的价值为其用户捕获，同时 vToken 兑换和持有激励、Collator 激励、Slash 保险基金等经济模型均为 Bifrost 网络的可持续发展带来保障。

3.2 Voucher Token (vToken)

Voucher Token 凭证代币简称 vToken，是由用户使用可质押类资产通过 Bifrost 网络而铸造成的一种 Polkadot 或 Substrate Based 通用资产，vToken 代表原质押物所有权和收益权，持有 vToken 即可获得原始质押物所产生的质押收益，是一个具备交易流动性的可替代同质化资产，可以解锁原质押物的流动性，甚至成为新的质押物帮助用户完成杠杆交易，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。



Transparent

All behaviors operate transparently on the parachain



Governance

Business parameters can be adjusted through the democratic governance



Cross-chain

Support to cross into other chains through polkadot relay



Fully Backed

100% backed for staking, no risk of principal loss



Fungible

No matter which validator you staking with, you will receive the vToken and rewards



Unlimited

compatible with centralized & decentralized settlement scenarios

vToken 的六个特性

3.2.1 Staking 衍生品

Bifrost 是一个完全去中心化的网络，将质押资产产生息、结算、权益保留标准化，可以为各类质押资产提供流动性，但由于去中心化特性，所支持的质押物同样需要具备：

- 资产链上发行
- 收益链上结算
- 权益链上证明

这三个基本特点，而目前 PoS 共识资产天然具备上述特点，是 Bifrost 提供质押物流动性非常好的资产标的，Bifrost 将为 Staking 质押物提供流动性作为市场切入点，为各类 PoS 网络提供 Staking 衍生品 vToken 的流动性。

3.2.3 收益结算方式

如何保证衍生品对应收益的去中心化产生，同时又使其提供流动性更加简单，增加衍生品兼容场景是关键，所以 vToken 的收益结算方式被设计为可以同时兼容中心化和去中心化场景的，中心化场景中，第三方无需额外开发即可支持 vToken 的兑换和使用，同时将 vToken 托管在中心化热钱包或者冷钱包中的用户，依然可以无损获得 vToken 所产生的收益。这得益于 vToken 摒除了传统的链上交易结算的方式，而采用铸币价格上调的方式来完成 vToken 收益的结算，所以为避免后来用户瓜分先前用户的收益，不同时间段进入的用户都将遵循当前时刻的铸币价格。

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 $vToken_{mint\ price} = (Token_{staking} + Token_{staking\ rewards}) \div vToken_{mint}$
- 年化收益率 $vToken_{yield} = (vToken_{redeem\ price} - vToken_{mint\ price}) \div vToken_{holding\ days} \times 365$

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 ÷ 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。

通过铸币价格上调结算收益优点是显而易见的

优点：

- 兼容中心化场景，无需额外开发
- 用户收益直观
- 价格表现相对原 Token 持续上涨

缺点：

- 价格脱离锚定，用户会有价格波动担心

3.2.3 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价最高的竞价人。该方式本质上是原先 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

3.2.4 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。

3.2.5 衍生品不可能三角

原链票权

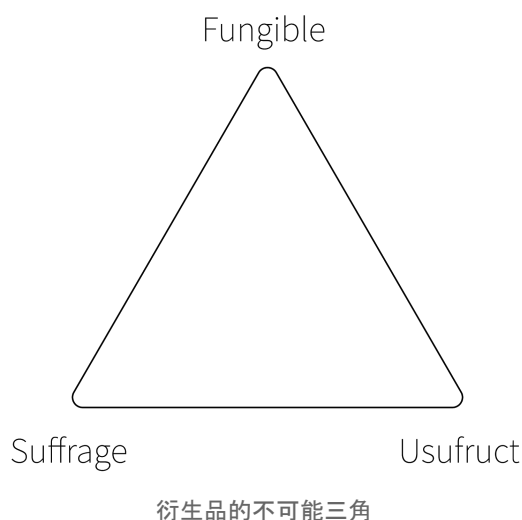
持币人选择验证者，就像是代议制民主当中的议员选举。每个 Token 都代表一个选票，投票权属于 Token 的持有人。Staking 衍生品协议作为一个中间层，不应该改变这个基础，应该让用户自己来选择验证者。但这样做将导致一个严重的问题，那就是衍生品不具备同质性（non-fungible），委托给不同的验证者，将产生不同的衍生品。

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，而用户在有特殊需求时，仍然可以选择指定的竞价人进行委托。

3.2.6 vToken 代币激励

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 代币激励，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，以激励用户更主动的兑换和持有具备权益、同质性和流动性的 vToken。

参数说明

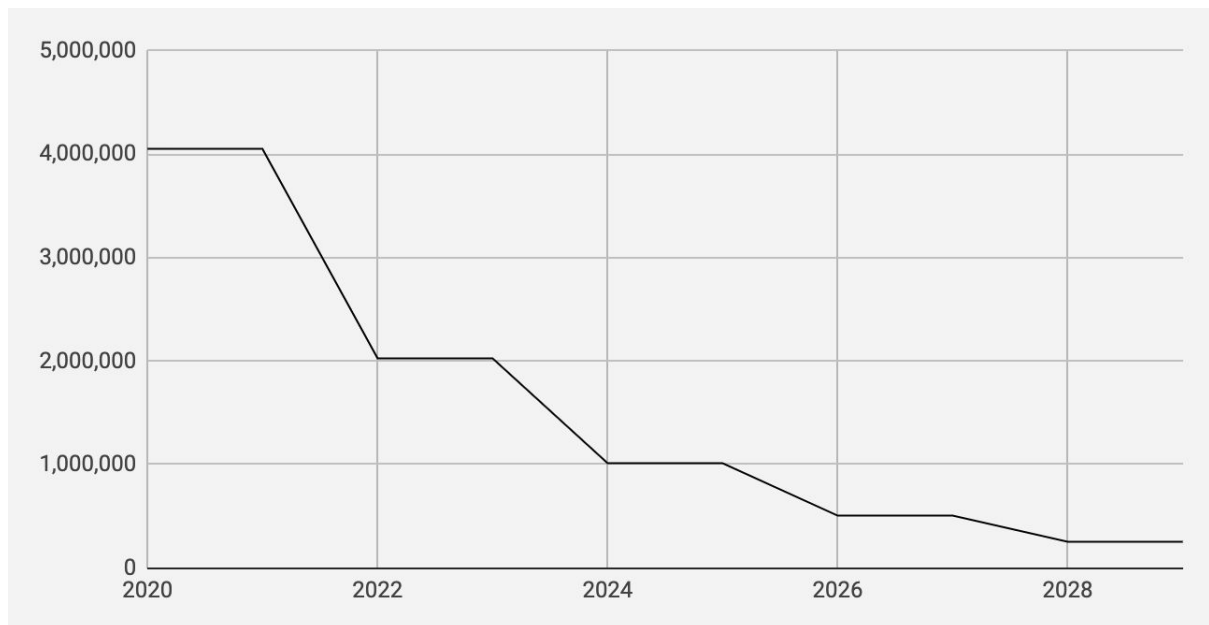
- $BNC^{total\ incentive} = 16200000$
- $Block^{time} = 6s$
- $Proportion^{initial} = 0.25$
- $Year^{launched} = 2020$

计算公式

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

Bifrost vToken Incentive (16,200,000)				
Year	Rewards (BNC)	Proportion	Reward/Block (BNC)	Daily (BNC)
2020	4,050,000	25.00%	0.7705479452	11,096
2021	4,050,000	25.00%	0.7705479452	11,096
2022	2,025,000	12.50%	0.3852739726	5,548
2023	2,025,000	12.50%	0.3852739726	5,548
2024	1,012,500	6.25%	0.1926369863	2,774
2025	1,012,500	6.25%	0.1926369863	2,774
2026	506,250	3.13%	0.09631849315	1,387
2027	506,250	3.13%	0.09631849315	1,387
2028	254,340	1.57%	0.04839041096	697
2029	253,530	1.57%	0.04823630137	695
10 years total	15,695,370	96.89%		

代币激励十年产量预期



持币激励十年产量折线

持币激励产量折线

- X 轴：挖矿年份
- Y 轴：BNC 产量

3.2.7 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，该参数会根据铸币价值为对应渠道进行贡献记录，在上篇 Staking 收益结构中 3% 将作为渠道金由所有渠道根据自身贡献占比总贡献比例进行分配，当渠道贡献记录高时，将收到用户产生渠道金的更多分成，激励更多开发者将 Bifrost vToken 铸币协议集成在钱包、Dapp、交易所中，渠道贡献值将不断增加直至每六个月进行公投提案清零。

3.2.8 风险控制

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）才会进行金额惩罚，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。

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。

3.3 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，且开放转账将分为 Bifrost 完成 PoA 启动、主网上线、删除 Sudo、转账提案通过这四个步骤进行。

3.3.1 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 Flexible Fee 模块来支持各类资产支付手续费，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。

3.3.2 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 代币激励**：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 15.2% 的 BNC 将用于奖励兑换 vToken 的用户。
- **IPO (Initial Parachain Offer)**：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 12.8% 的 Token 用于奖励帮助 Bifrost 参拍平行链的团体。

3.3.3 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。
- **Vote Bidder**：票权竞价人，通过提案公投选举，选举通过的账号成为 Vote 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 的权限。
- **Vote 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**：技术委员会可以与 Bifrost Council 一起制定紧急公投，快速进行投票和实施。这些紧急公投仅在紧急情况下使用。

- **Sudo**：超级管理员，可有权限操作网络中任何参数，在网络测试阶段起到调整网络发展方向的功能，在 Bifrost 主网稳定运行之后将通过提案公投删除 Sudo 权限

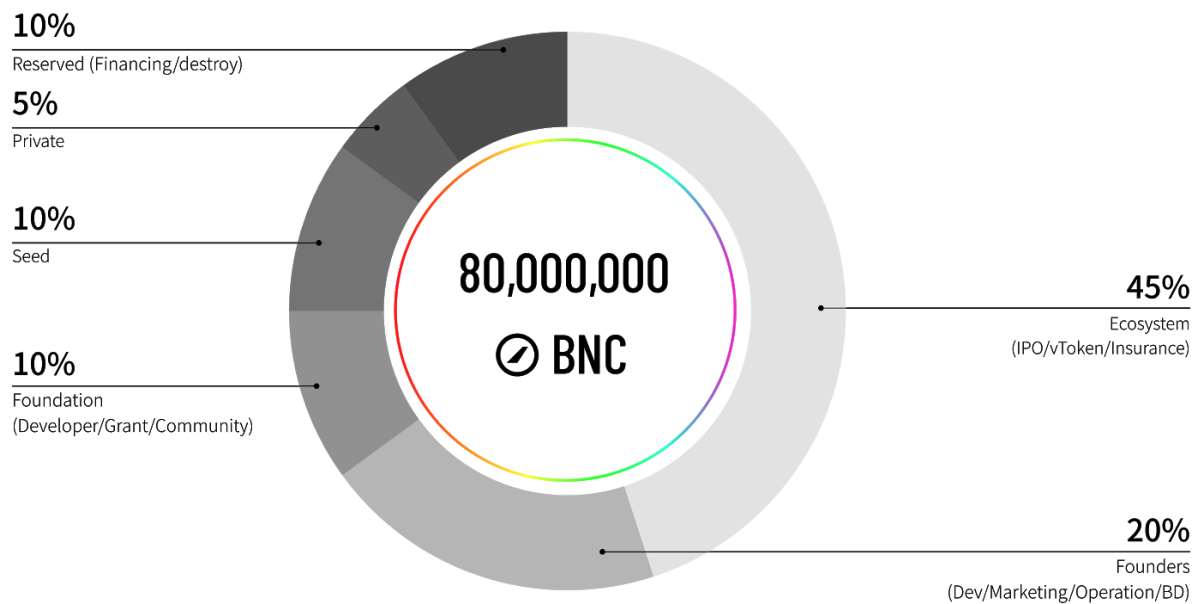
4. 代币分发

BNC 分发目标为让 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，所以 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，为达到目标，BNC 将预留 40% 的代币作为整个生态系统的激励，包含 vToken 铸币挖矿、IPO 卡槽拍卖、Collator 节点激励，Oracle 使用及跨链成本等。

4.1 BNC 代币结构

Usage	Proportion	BNC
Ecosystem	45.00%	36,000,000
Founder	20.00%	16,000,000
Private Sale	5.00%	4,000,000
Foundation	10.00%	8,000,000
Seed	10.00%	8,000,000
Reserved	10.00%	8,000,000

总量分配结构表格



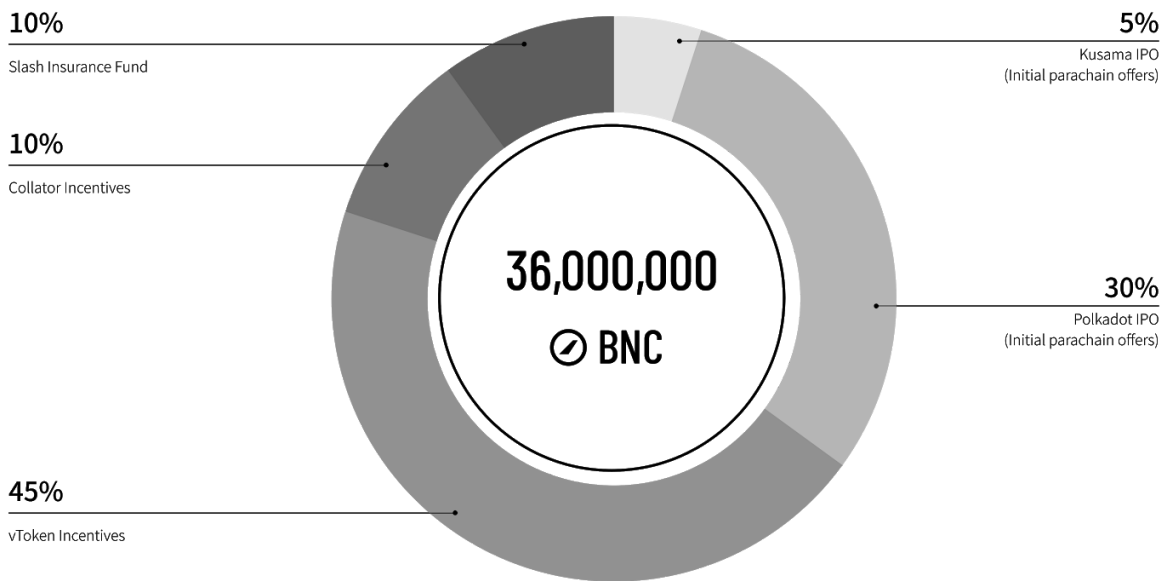
总量分配结构饼图

4.2 生态系统

Ecosystem	Proportion	BNC
Kusama IPO	5.00%	1,800,000
Polkadot IPO	30.00%	10,800,000

vToken Incentives	45.00%	16,200,000
Collator incentives	10.00%	3,600,000
Slash Insurance Fund	10.00%	3,600,000

生态系统分配表格



生态系统分配饼图

4.2.1 vToken 持币激励

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

4.2.2 首次平行链发行（IPO）

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 IPO 参与相关细则将在波卡平行链竞拍规则推出后公布。

4.2.3 Collator

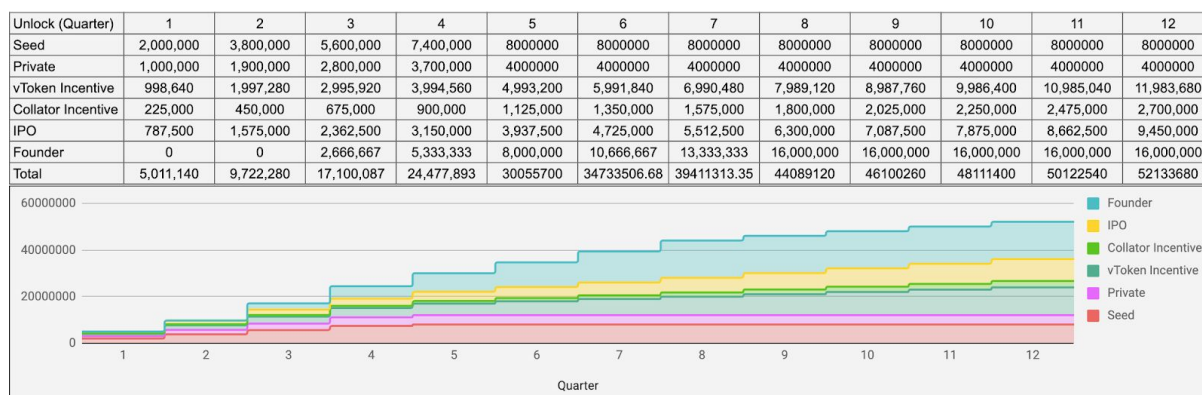
当 Bifrost 接入平行链，上线主网时，将支持 Collator 提供服务，为激励质量更高，服务范围更广的 Collator，协议将根据 Collator 提供服务的工作量进行激励 BNC，系统将预留生态系统中的 10% 的 BNC 作为 Collator 激励。

4.2.4 Slash Insurance Fund

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。

4.3 解锁期

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（流通当天）之后半年开始线性解锁，持续两年时间解锁完毕。



十二季度解锁释放预期

5. 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 IPO detail & Auction page
 - IPO & Auction Polkadot SLOT
 - Support sDOT (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)

6. 结论

Bifrost 的当前设计目标是在多个著名 PoS 公链、众多 Pokadolt 平行链、Polkadot 中继链之间，为投资者提供统一的业务与服务抽象层，并提供去中心化的、安全的、标准的、可配置的金融工具，形成丰富灵活的资产抵押收益票权市场。Bifrost的远景目标是强化整个区块链行业的 PoS 生态环境建设，并助力推动 DeFi 科技与应用的普及与深度演化。

7. 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, "Phragmen'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 Bourgoïn, 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>