

什么是波卡

通俗的讲，波卡是一个满足不同区块链之间的跨链协议。波卡的创始人Gavin Wood层级是以太坊的核心开发者，他发明了Solidity，并撰写了以太坊虚拟机的黄皮书。波卡是在2016年由Web3基金会创建，目的是为了通过一个区块链网络链接不同的区块链，实现跨链互通，成为下一代区块链网络基础设施。

为什么需要波卡

由于众多的区块链数据无法兼容，彼此孤立，例如比特币不能直接参与以太坊的庞大的生态，这就导致了一个个区块链是割裂的生态。而通过波卡，不同的区块链可以相互链接，实现跨链交互。

波卡网络的基础设施包括：

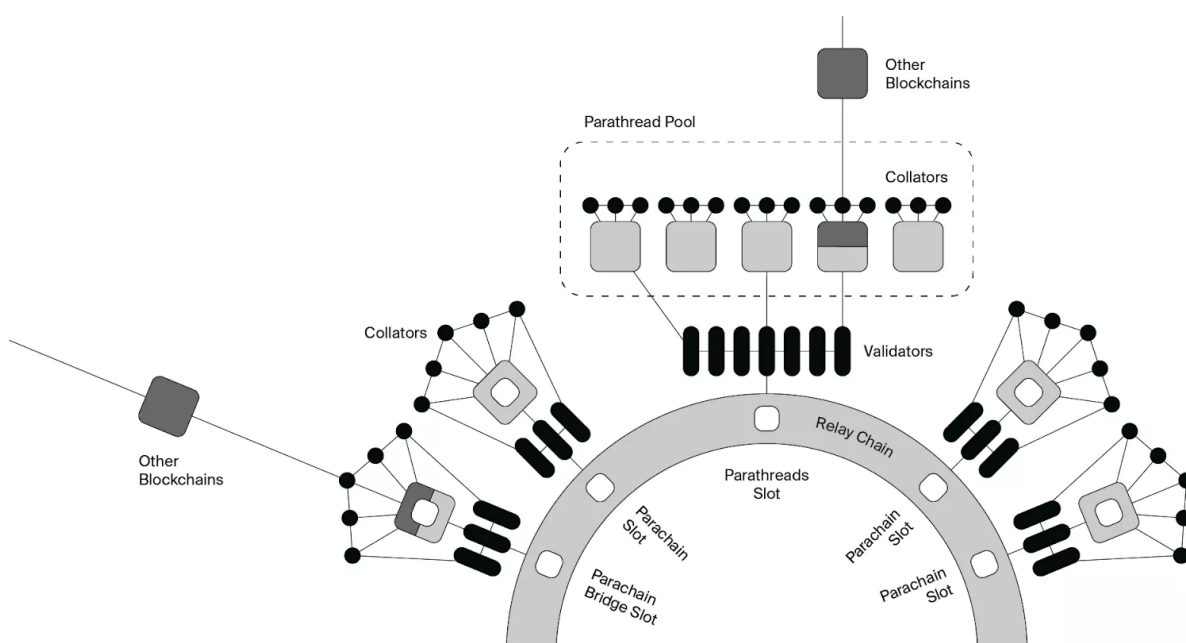
中继链（Relay Chain）：平行链和波卡“骨干”之间的主要通信枢纽中继链，确保平行链的安全并且实现平行链之间的通信，通信的内容可以是交易或者任意形式的数据。

平行链（Parachains）：平行链是平行于波卡网络的区块链，每个平行链都可以根据不同的业务需求独立设计自己的架构。平行链也会用来并发交易提高扩展性，其通过连接中继链保证其安全。

转接桥（Bridges）：转接桥是一种特殊的平行链，它允许波卡网络和独立的区块链网络通信。这些独立的区块链网络不通过波卡中继链进行安全验证，而是使用自己的安全机制，例如比特币和以太坊网络。

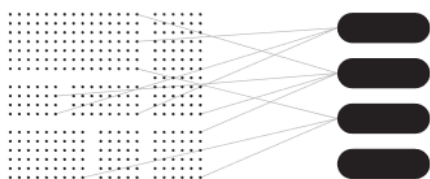
平行线程（Parathreads）：相比于平行链，平行线程是“轻量级”接入波卡，即插即用，用完就走。

波卡是如何运行的



如果把波卡的中继链看做成一个排插，那么不同排插上面的电器就是平行链，波卡的中继链是基于Substrate创建的中继链，平行链通过“插槽”的方式与波卡中继链连接，这样每条的平行链和中继链便组成了一个跨链系统，通过中继链就可以实现任意两条链之间的跨链了。因此波卡可以实现互操作性、可拓展性、共享安全的异构跨链系统。

在Polkadot上，不同区块链之间可以以去中心化的方式互相通信，允许开发人员开发跨链应用程序，允许一条平行链向另一条平行链发送消息，你完全可以放开想象，这里的消息可以是金融资产、聊天信息、大气监测数据等等，当然也可以是投资者从Bitcoin向Ethereum发送的10个比特币。



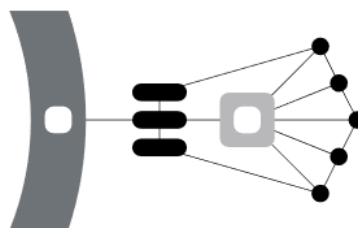
Validators

Secure the Relay Chain by staking DOTs, validating proofs from collators and participating in consensus with other validators.



Nominators

Secure the Relay Chain by selecting trustworthy validators and staking DOTs.



Collators

Maintain shards by collecting shard transactions from users and producing proofs for validators.

Fishermen

Monitor the network and report bad behavior to validators. Collators and any parachain full node can perform the fisherman role.

中继链本质上就是一条区块链，验证人（Validators）为这条区块链的安全性保驾护航，验证人会运行Polkadot的节点，验证人偶尔会被赋予生成新区块的权力，如果尽职尽责工作出色，他们就会得到奖励。

任何人都可以成为验证人，只要他们背后筹码够多，这里所谓的筹码就是波卡中继链的“本国货币”DOT，按照DOT质押数量，前几百名验证人将会被依次选举成为活跃验证人（active validators）。

被选举出来的活跃验证人会被随机分配给各个平行链，并且每隔几个小时，这样的分配就会再次以随机的、不可预测的方式进行一次轮转。

每隔6秒，平行链就会向中继链发送一个候选区块。这个候选区块将由中继链上这些时刻处于在线状态的验证人负责核验。如果核验通过，候选区块将会被纳入到中继链的区块中，然后平行链接着产生下一个候选区块。提交完成之后，这些区块就获得了不可改变性，平行链就是这样在中继链的保护下无忧无虑地生长。

所有平行链最终都需要以来中继链上的验证人获得最终授权，平行链越多，需要的验证人也越多，整个网络的安全性也就越高。重点提示，如果你想成为验证人，就必须质押DOT代币，当你执行验证人角色时，你的DOT都会被质押在Polkadot网络中。

就是用这种方式，中继链与平行链共享安全性，每一条链都成为整个网络抗攻击性的一部分。

一般来说，区块链在升级的时候分叉总是不可避免：有些节点升级了，有些节点没有升级，没有升级的节点就始终停留在分叉链上，直到这些没有升级的链更新之后，网络才算升级完成。更为痛苦的是，这些节点是分布在全球的，而且你没法与这些匿名节点实时通信。

而Polkadot通过“链上runtime与链上治理（on-chain governance）”的方式解决了这个难题。链上runtime是指包含生成新块的规则的代码存储在链上。因此，运行区块链的节点、程序只需读取这些信息，它们就可以更新了。那么我们如何更新这个代码呢？

链上治理可以让任何DOT持有人发起全民公投，或对公投投票。公投是对区块链逻辑或数据的更改建议。通过治理，社区可以对链上逻辑的变更提出建议并对其进行投票，一旦该逻辑变更投票通过，就会自动更新，无需更新软件，也无需人工干预。

波卡代币的经济模型

波卡的代币是DOT，最初发行量为1000万枚，在2017年的众筹了约1.4亿美元，在2019年和2020年波卡进行了两次私募，共计募集约1亿美元。2020年8月，波卡对DOT代币进行了100倍拆分，将发行总量提升至10亿枚，价格变为原来的1/100。这有点像股市的增发，发行总量变大，但权益并没有变化，100倍拆分后，波卡开启了一波上涨。

DOT在波卡生态主要用于治理、质押、投票、运行节点等。与以太坊中的ETH类似，**DOT代币总量没有上限**，每年通过NPOS机制进行通胀增发。

NPOS即Nominated Proof of Stake，又称**提名权益证明**，是波卡团队提出的一种新的**POS共识机制**。在NPOS中，有两个重要的角色：验证人和提名人。二者均会获得DOT通货膨胀的收益，也就是Staking收益。

验证人数量有限，且数量由治理决定。是否可以成为验证人节点由自抵押数量和提名人的质押数量决定。

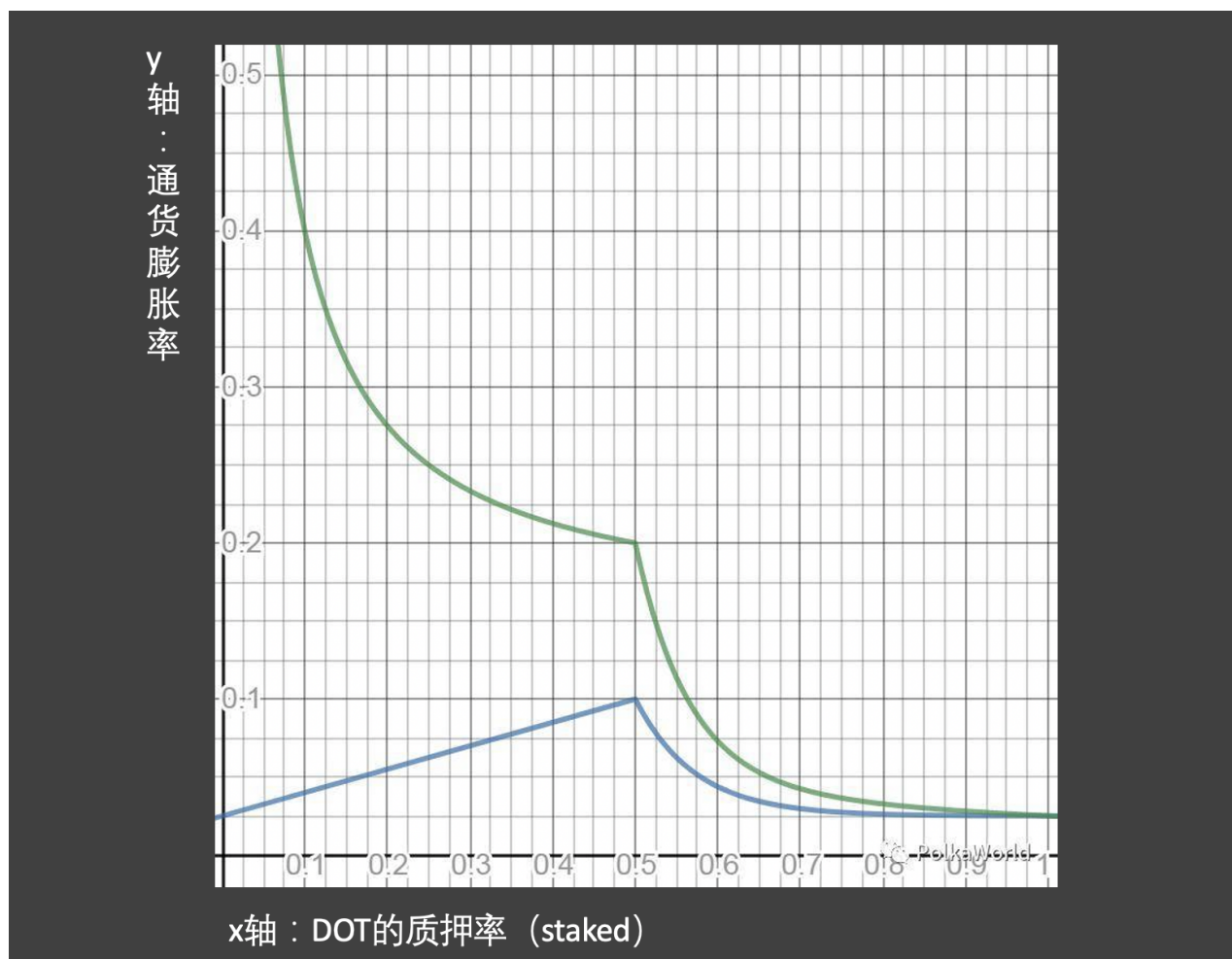
通俗的理解，验证人就是节点，需要运行和维护节点。提名人则是投票节点的人，不需要运行节点，但是提名人所获得的Staking奖励会有一部分给到所投票的验证人，以“补偿”运行验证人节点的费用。

加入验证人节点池的最小质押数量每天都不同，这取决于想要加入验证人节点池的候选数量和每个验证人上的质押数量。在NPOS机制中，每一个被选举的验证人在共识上拥有同等的发言权。

在波卡上，运行验证人节点没有最小的自抵押数量。只要你100%被提名的DOT满足所需的最小stake数量，就可以加入节点池。目标是不需要太高于最小值的情况下进入节点池。因此，许多验证人保持一个较低的自我抵押，并从另外一个单独的账户将其大部分DOT质押给自己。这种设置允许他们保持灵活性，并当节点池发生变化时，可以以最低的stake数量加入验证人。

[波卡](#)（Polkadot）采用非线性模型来设置主网上线后的通货膨胀。那些在早期就开始进行staking的公司将看到通胀率稳步上升，直到50%的DOT被质押。这种模式对于代币持有者来说是一种重要的激励，促使他们在网络最早、最关键的时期参与进来。

蓝线是网络中的通货膨胀率，绿线是回报率（通货膨胀除以质押率）。



波卡通货膨胀模型由上图可知，波卡代币的最高通胀率为10%，最低为2.5%，根据质押率决定。由于可知，参与时间越早，通货膨胀率越低，收益也越高，因此，若参与波卡网络节点应提前准备。

波卡生态

一个项目能否成功，不仅取决于技术，而且取决于生态。在诸多公链当中，波卡生态的发展仅次于以太坊网络，今年诞生了Chainlink、Kusama的黑马项目，可见市场认可度较高。

Kusama

Kusama是波卡的测试网络，又叫金丝雀网络。

简单来说，任何部署在波卡上的新功能，都需要先在[Kusama](#)上部署，测试，成功之后，再迁移到波卡。

Kusama，不要把它看成单纯一个测试网，而是要把他看成一个存在于真实经济环境中的，早期的高度实验性版本的波卡——你可以理解为波卡Beta版，或者小波卡。

- 他有自己的代币系统，现在已经疯涨到了100美金一个；
- 有自己的社区，超过 400 个验证人（包括很多国内外知名的投资机构、staking 机构）；
- Dot的100倍拆分投票和提案，都是在Kusama上进行的；
- Kusama 并不会像其他测试网随着波卡的上线而消失，只要社区一直存在，Kusama 网络就会一直存在，也会作为第一批的平行链桥接到波卡网络中。

今年KSM代币最高涨幅超过50倍，受到市场的追捧，甚至超过波卡DOT的涨幅。

数据来自<https://www.bixiaobao.com/cn/coinlist/kusama>

Acala Network

被称为波卡上的DeFi之王，当之无愧的波卡生态一哥，目前代币暂未上市。Acala是波卡上最早做DeFi的团队，从2018年就开始做波卡上的DeFi，早期名字叫做PolkadotDeFi，后来在曹寅的建议下改名为Acala，2018年开始做稳定币的协议，2019年生态扩大之后，开始做抵押资产衍生品协议。

为什么Acala Network要做抵押资产衍生品？这是因为当你参加Polkadot的抵押生息之后，就无法再用你的DOT去参加DeFi了，那么Acala就做了一件事，就是让你抵押在波卡节点吃利息的资产，能够打包变成一种名为Ldot的资产，这里的Ldot其实就相当于一种票据，你有了这种票据，然后就能够换成Acala的稳定币AUSD，然后自由参与其它项目的DeFi，这个过程就像是在MakerDAO中质押ETH然后获得稳定币DAI一样。

通过Acala在波卡生态中可以质押DOT、KSM未来还可以质押比特币、ETH，然后获得AUSD，再去其它波卡生态中进行资产质押与置换。

波卡生态一位大牛说，Acala基本上做的是MakerDAO+Compound+Uniswap+SNX，一个系统里把稳定币铸造，借贷，DEX，衍生品做全乎了。

Stafi

Stafi是一个中间件协议，专门做PoS流动性释放。

简单说来，ETH2.0，XTZ，ADA，Cosmos，波卡等PoS公链，安全性需要由质押（Staking）来保证，不管是担心手里的币被增发所稀释掉，或者想要为网络的安全性做贡献，很多人都会去选择Stake，然而像是ATOM，赎回期需要21天，这段期间无论币价上涨还是下跌，你都只能干瞪眼，像是312那一波，许多质押的用户都损失惨重。

那么有没有一种办法，可以在选择Staking的同时，又能获得100%的流动性？

Stafi做的就是这个，用户在Staking币的时候，使用Stafi协议，这样就能得到一个1:1的对应所有权和Staking收益权的债券——Rtoken，Rtoken可以在二级市场自由流通，完全不受影响，而所对应的代币的Staking收益又完全不受影响，就这样，熊掌与鱼兼得了。

创始人卡咩，Wetex的创始人，圈内很多人都知道，可能是国内最懂PoS共识的团队，也是国内最知名的Staking委托代理服务商之一。

Zenlink

Zenlink由imtoken团队推出，我们知道，在波卡上都是一条条平行链，如果这些平行链都开发自己的DEX，大家流动性被分散成导致流动性很差，Zenlink的作用就是让每一条波卡的平行链都可以通过Zenlink共享DEX流动性。所以Zenlink既可以所有平行链拥有DEX，同时又能够把这些平行链流动性归到同一个地点，让使用者享受到最好的流动性。我们知道Zenlink是imToken的团队在做，这个钱包本身也是最懂DEX的团队来做的生态项目。

波卡就像一座城市，庞大而复杂，其提出了许多前沿的设计，例如NPOS共识、平行链等，可以预见的是，随着波卡平台链拍卖的推出，未来的波卡生态必将更上一层楼。

Polkadot 和其他链的比较

EOS

其实 EOS 白皮书也有类似「异步 BFT，准入制开启 Parachain」等构想，但遗憾的是波卡可能更早实现。而且波卡的 Relaychain 三权是分立，不像 EOS 21 区块验证人独大，被迫又引入一个更中心化的组织做仲裁，问题多多。

ETH2.0

ETH 2.0 的 Casper 共识和波卡的 Relaychain 有类似的 PoS 机制，波卡更像美国的政治制度——钓鱼人，验证人，提名人，收集者之间互相有制衡。而 ETH 2.0 更去中心化，追求过高的分散。

在跨链上，ETH 的 Plasma 更像功能机，只能简单的账本余额跨链，可编程数据完整性在跨链上都还不行，而 layer2 规范标准不一致，需要 layer2 自身去建立桥接。

Cosmos

Cosmos 也有类似的 Parachain，但是不同于波卡，Cosmos 的 Parachain 需要有自己的共识机制，需要自己维持网络安全性。

相似在于 Cosmos 有 Cosmos SDK，类似波卡里的 Substrate。这两者都可以被开发者用于快速搭建区块链的框架，网络结构也很相似。

最后说一下我为什么这么看好波卡，波卡是非常稳定的，这个稳定指的是技术开发团队和底层技术的稳定，稳定对区块链来说是非常重要的，一旦因为开发团队图一时的利益，发现新的区块链项目，就去寻找新的区块链项目，这会对原来项目在社区产生巨大负面的影响（如果连核心开发者都转去做其他事情了，项目自然就GG了），回过头来再看波卡创始人Gavin Wood，从2013年下半年开始帮助V神开发ETH1.0，到2015年设计ETH2.0架构，再到2015年下半年开始着手开发波卡，Gavin的工作是有连续性的，也是有目标支撑的，这个终极目标就是Web3.0。为此，Gavin与波卡开发者们在2018年创建了“区块链开发者工具箱Substrate”，让开发者能够在10分钟内构建一条全新的区块链，2017年创立了Web3基金会，全力支持波卡和 Web3.0生态的研究和开发。此外，Parity Technologies也为全球的波卡生态开发者提供很大的技术支持。以上这些，其实都是在说明一个问题，那就是Polkadot的创始人是一个稳定的，专一的，有格局的开发者，从“人”的角度保证了波卡项目的稳定性。

为什么要反复强调这个稳定性？因为底层公链的稳定性对项目长期发展来说太重要了。2019年之前，我们经常听到“某某公链是以太坊杀手”这样的口号，类似于某某公链又提出新的治理理念，性能远超ETH，正在成为以太坊杀手。然而，最终结果是，那些曾经喊过类似口号的区块链底层公链，很多已经销声匿迹了。根本原因就是，“无论你的公链性能有多么强劲，费用有多么低廉”，最终还是要落实到“应用”的层面，即到底有多少项目愿意在你的公链上开花结果。

目前，我们看到的已经在ETH上开花结果的DeFi项目，例如MakerDAO/Compound/Uniswap等，其实早在2018年就已经开始在以太坊上面开发，也就是说，这些团队绝对不是看重以太坊的性能，而是以太坊的稳定性。因为，区块链远不是Window与MAC，尚达不到一键迁移的性能，所有的区块链项目，都要面临一个问题：极为昂贵的迁移成本。

所以，众多区块链项目，宁愿花费高昂的费用在以太坊上堵着，也不愿意去EOS，因为以太坊足够稳定，虽然也足够拥堵。问题来了，波卡足够稳吗？是的，我认为从波卡创始人Gavin，到Parity CEO Jutta Steiner，再到Polkadot Co-Founder Robert Habermeier，他们都是稳定的，再到波卡愿景，更是稳固朝前的，所以波卡生态吸引了众多项目与开发者。截止12月15日，polkaproject.com已经收录了

312个波卡项目，超过除以太坊之外的所有公链。

开发者的选择，或许就是最好的答案。

参考文献

[Polkadot: Decentralized Web 3.0 Blockchain Interoperability Platform](#)

[Official Substrate Documentation for Blockchain Developers · Substrate Developer Hub](#)

[PolkaWorld](#)

[Gavin Wood - Wikipedia](#)

[想要搞懂波卡，先弄清楚这3个概念 - 知乎 \(zhihu.com\)](#)

[波卡为何是一条“新”的区块链？ 开发 \(sohu.com\)](#)