



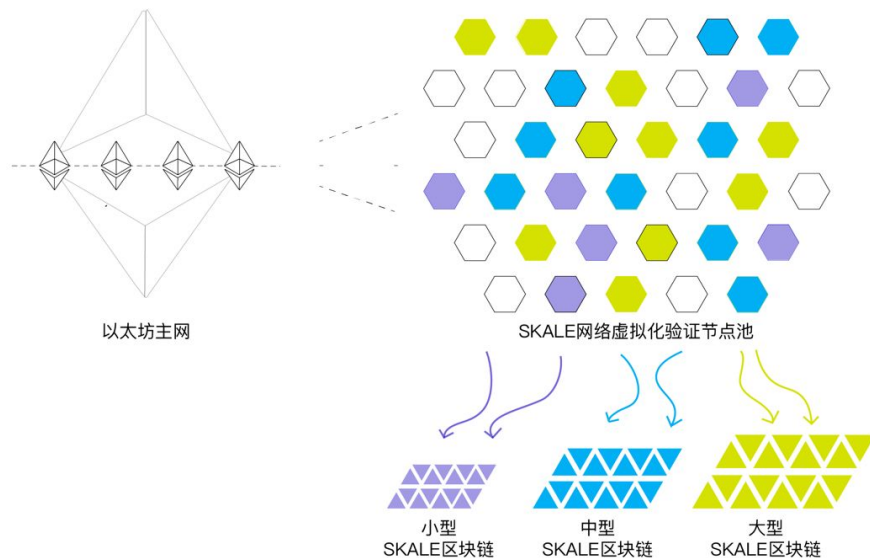
The SKALE Network

入门手册

关于SKALE网络

SKALE网络是一个连接以太坊主网的安全层和执行层，它为开发者提供更快的开发速度与更好的性能。SKALE是一个为支持成千上万个独立区块链、侧链、存储链和其他类型的子链而生的弹性去中心化网络——所有这些区块链都与以太坊主网相连，并且完全兼容整个以太坊生态。

SKALE网络最终将由上千个独立的验证节点组成，这些节点提供第一层区块链网络的安全保证，但使用资源的方式更加高效、性能更好和用途更广。例如，SKALE网络中的1,000个验证节点可以支持8,000个相互独立的区块链。这些区块链可以是最小的侧链，也可以是非常大型的公共和私有区块链——每个区块链运行的提交时间更快、交易费用更低和交易吞吐量更高。



SKALE是一个与以太坊主网紧密联系在一起弹性中心化区块链网络

SKALE所解决的问题

为了提升基于以太的应用程序（以及一般的去中心化解决方案）的采用率，加密行业需要解决的不仅仅包括扩展交易吞吐量，还有用户体验——扩展用户体验意味着解决每秒交易量（TPS）、延迟、基于API钱包的连接、成本效益、链间无缝通讯等问题。

SKALE网络是一个扩展区块链的完整解决方案，它解决了速度、安全性、生态系统互操作性以及TPS。它是一个可配置的弹性侧链网络，支持高吞吐量和低延迟的交易，而不像以太坊主网那样存在高昂的交易费用。该网络提供扩展的存储功能，以及与以太坊主网的嵌入式连接和链间通讯。以上特点是通过采用一个交易验证池和安全模型提供的，该模型高效、可扩展和抵抗节点间的相互勾结。

SKALE网络主要的优势是接近于零的gas费用、更快的提交时间和提升了的交易吞吐量。而更快的提交时间带来更低的延迟，从而提供更好的用户体验；降低gas成本对开发人员和用户大有裨益，能够消除大规模采用的障碍。

弹性侧链还可以为去中心化应用程序提供大量额外的链上存储空间。在公有链上存储数据价格昂贵并且容量有限，而在SKALE网络中存储数据的空间更大、更加经济，从而减少了应用程序开发人员在处理去中心化应用的存储需求时遇到的挑战。

对于开发和扩展基于以太的应用程序，使用像SKALE 网络这样的执行层解决方案是非常有效的，它为越来越多的使用场景打开了可能性——从游戏和去中心化金融，再到产品和媒体应用程序，以及其他应用。



去中心化金融

- 消费/储蓄
- 投资
- 交易
- 借贷
- 预测市场



游戏

- 对抗游戏
- 策略游戏
- 棋盘和卡牌游戏
- 集卡游戏



媒体/广告

- 去中心化流媒体
- 去中心化媒体中心
- 不受审查的社交网络
- 自主权的个性化
- 受审广告



去中心化商业

- DAO与LAO
- 企业注册
- 跟踪与追踪
- 交易与交换
- App批量化生产



物联网

- 供应链与物流
- 去中心化Mesh网络
- 设备注册
- 数据市场
- 环境监测



更多其他应用

- 医疗
- 房地产
- 数字身份
- 投票
- 募资
- 慈善

弹性侧链的使用场景

SKALE网络的独特之处

SKALE网络是一个去中心化云服务，用于提供和部署高吞吐量、低延迟的弹性侧链。这些侧链都兼容以太坊虚拟机（EVM），并且提供可配置的资源设置，包括网络大小、交易吞吐量、存储容量和增强的安全特性。

SKALE网络中的每个弹性侧链都是由一组从更大节点池中挑选出来的虚拟化子节点所维护。弹性侧链使用节点的计算和存储资源——根据用户选择的侧链规格，使用一部分资源或者全部节点资源。每个侧链都使用异步二进制拜占庭协议作为共识机制，并且可以通过一个安全的链间通讯协议与其他区块链通讯。

本质上，SKALE网络可以看作是一个结合了支付系统的复杂容器调配机制——所有这些都服务于弹性区块链网络的运行。SKALE协议和相应的SKALE通证实现了这种处理潜力和激励执行的强大组合。

传统侧链通过使用数量更少的验证节点来提升性能与降低延迟，但该做法也面临着交易完整性的风险（理论依据为较小节点集更容易受到共谋和贿赂的影响）。SKALE网络通过使用一个验证者节点池模型来克服这种安全风险。该模型通过验证集之间的频繁节点轮换、随机分配节点，从而利用大量验证节点所提供的安全性优势。因此每个独立的侧链都受整个网络的资源所保护。

为了进一步保护网络，每个验证节点必须通过SKALE通证的方式向网络中注入大量的价值。用户还通过使用SKALE通证的订阅（subscription）模型为侧链提供资源。这些通证被质押到以太坊的主网，并由智能合约所控制（详细信息请参阅[SKALE 网络白皮书](#)中的“SKALE 管理员”章节）。主网上的智能合约还管理通证的通货膨胀率和每个月分发给验证节点的奖励（包括通货膨胀的收益）。这些智能合约还负责监视节点的性能，以及在节点出现任何渎职行为时进行惩罚。

SKALE网络是一个托管执行层（第二层）。在非托管方案使用一个欺诈证明允许资金在区块链间转移的情况，SKALE则使用BLS签名、以太坊主网的存款箱和其他的机制来保证托管所有权和内部网络的使用（也就是在获得主网安全性保证的同时，又继承了二层网络的性能）。尽管其他二层模型尝试使用主网交互来进行验证和/或欺诈证明，SKALE则使用以太坊主网进行质押和其他关键操作，这种方式更适合创建一个健壮且完全去中心化的安全层和执行层。SKALE网络还可以通过BLS Rollups支持非托管二层网络，并最终支持其他经过验证的L2解决方案，因为它们从研究阶段进入生产准备阶段。

弹性侧链的创建和使用

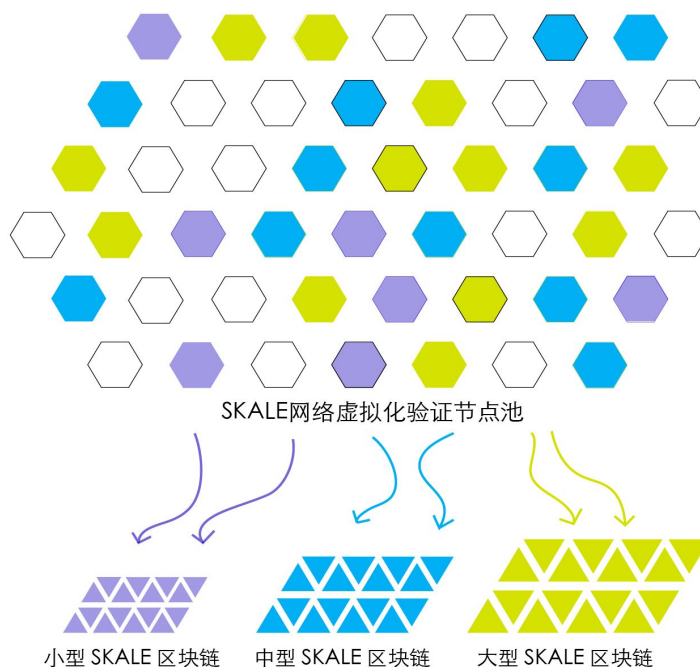
SKALE网络中的弹性侧链是高度可配置的，开发者可自由选择侧链规格、共识协议、虚拟机、母链以及额外的安全措施。

创建一个弹性侧链时，开发者首先通过一个去中心化界面配置该区块链，然后通过SKALE通证的形式向网络提交费用。所需要的通证数量由网络的规格以及他们期望利用网络资源的时间长短所决定。侧链有多种规格（小型、中型和大型）以及时长选项（3、6和12个月）。网络中的存储容量同样是可配置的。

每个弹性侧链都随机分配一部分的验证节点。默认节点数量为16个，但该数量可配置成 $3n+1$ 个（其中 $n \geq 1$ ）。侧链的规格决定了它所能利用的虚拟子节点的数量。其中，侧链可使用每个节点资源的1/128（小型）、1/16（中型）或1/1（大型）。随着SKALE网络的持续发展，用户最终能够指定虚拟子节点数量、签名者数量、虚拟子节点规格以及其他增强功能。

SKALE网络兼容EVM，因此开发者同样可以使用他们在以太坊主网开发时所使用的工具。这些工具包括通过web3.js和web3.py连接网络，以及Truffle和Remix。

SKALE网络同样将链间通讯作为一个原生功能。链间通讯通过虚拟子节点实现，通过BLS（Boneh-Lynn-Shacham）阈值签名，这些虚拟化子节点能够验证另一个区块链子节点所签名和提交的交易。这种独特而去中心化形式的通讯带来了一种新模式，而不像传统Web2开发那样使用推送通知或远程进程调用。



可配置选项包括网络规格、交易吞吐量、存储容量和增强的安全特性

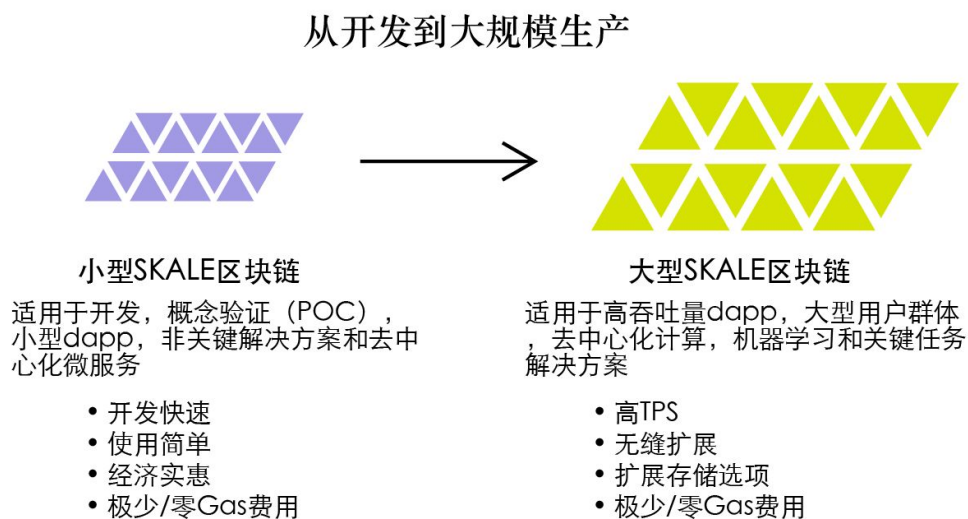
从开发到大规模生产

SKALE网络在开发中易于使用，在生产中则可扩展且性能优越。开发者设定区块链特性、质押通证，便可立即创建一个或多个弹性侧链。这些侧链配置的资源也可以无缝地修改，从而适应随着业务发展而增加的交易负载、存储需求、安全考虑和其他项目需求。该网络不仅是快速开发的最佳解决方案，而且能配合最大的生产解决方案一起使用。

SKALE网络中弹性侧链的规格调整非常简单，因此它能让一个小型侧链和受限的交易吞吐量切换到每秒处理2,000笔交易和高度扩展存储容量的大型侧链。并且该资源切换是实时发生的，不需要用户进行任何额外的操作或节点管理。

最终带来的结果是，SKALE网络为即使是最苛刻的defi、游戏、媒体和创新应用程序都提供了使用简便和准备就绪的资源。独立开发人员、供应商网络、联盟和任何其他组织类型都可以利用SKALE网络的一个或多个侧链，为去中心化解决方案提供随时可用、安全可靠的交易。

SKALE网络的设计和结构也使得从Web2迁移到Web3相对容易。SKALE的开发环境与在以太坊主网的开发完全相同，而以太坊有着全球最大的区块链开发者社区（数以万计的开发人员、一套现成的工具以及其他开发人员资源）。通过链间通讯和侧链存储，现有的云开发者能够按照他们开发云程序那样相同的模式来开发。此外，除了配置侧链选项和为侧链资源进行质押以外，运行侧链不需要任何操作。



SKALE网络在开发中易于使用，在生产中则可扩展且性能优越

关于SKALE网络

SKALE网络是一个开源的弹性区块链网络协议。它的愿景是让创建运行全状态智能合约的低成本、高性能侧链更简单快捷。SKALE网络旨在不牺牲安全性或去中心化的前提下，为开发者提供快速与功能的高效体验。

您可以通过以下渠道关注SKALE网络：[电报群](#) (@SkaleOfficial)，[推特](#) (@SkaleNetwork)和[Discord](#) (www.skale.chat)，浏览[SKALE官网](#) (www.skale.network)，在[SKALE 开发者门户](#) (skale.network/docs) 阅读开发者文档，在[Github代码库](#) (github.com/skalenetwork)查看代码。