SKALE

The SKALE Network
技术亮点

SKALE网络的技术亮点

SKALE网络是一个可配置的弹性侧链网络，它支持高吞吐量和低延迟的交易，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信。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。
以下为SKALE网络的一些技术亮点。更详细的介绍请参阅SKALE网络白皮书。

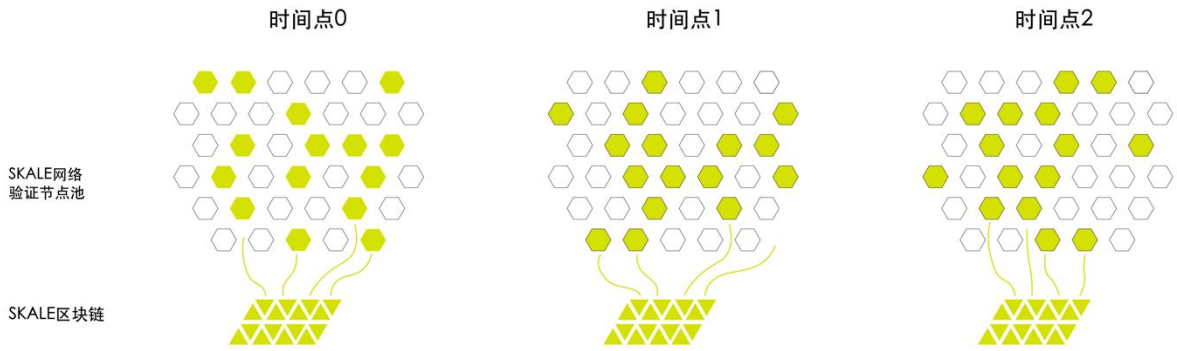
- 费用接近于零甚至为零
- 随机节点挑选/频繁节点轮换
- 虚拟化子节点
- 容器化的验证节点
- 异步二进制拜占庭协议（ABBA）共识
- BLS Rollups
- 节点监控服务
- 与以太坊的互操作性

Gas费用接近于零甚至为零

无论某个SKALE链的规格多大，只要它低于某个特定的资源阈值，那么SKALE网络中的gas费用就为零。在开发和运行去中心化应用方面，gas费用接近于零甚至为零的架构是一个显著的优势。当前，在获取用户和拓展可盈利的使用场景时，一个很大的限制因素是区块链gas费用所带来的摩擦。从范式中除掉这些成本能够带来更容易市场进入机会、更高的采用率和更成功的去中心化解决方案。
SKALE链的容器按照CPU、内存和磁盘大小，按照一定比例对操作划分零gas费用或某个特定的收费标准。只有达到某个标准以后，才需要收取gas费用。这种资源切换模式有以下两点好处：其一是防止拒绝服务（DOS）攻击，其二它提醒用户可能需要扩展到一个更大规格的SKALE链。（后者的提醒指标类似于升级一项云服务，例如从亚马逊的t2.micro迁移到m3.large。）

随机节点挑选/频繁节点轮换

验证节点通过一个主网合约仲裁的随机程序分配到弹性侧链。区块链共识的安全性进一步由频繁的节点轮换保障。根据一个非确定性的计划，原有节点会从一个或多个侧链中移除，然后加入新的节点。这种轮换的实现过程如下：通过节点核心不断地检查主网，根据主网合约及其随机分配算法退出当前链，同时连接和服务新的侧链。

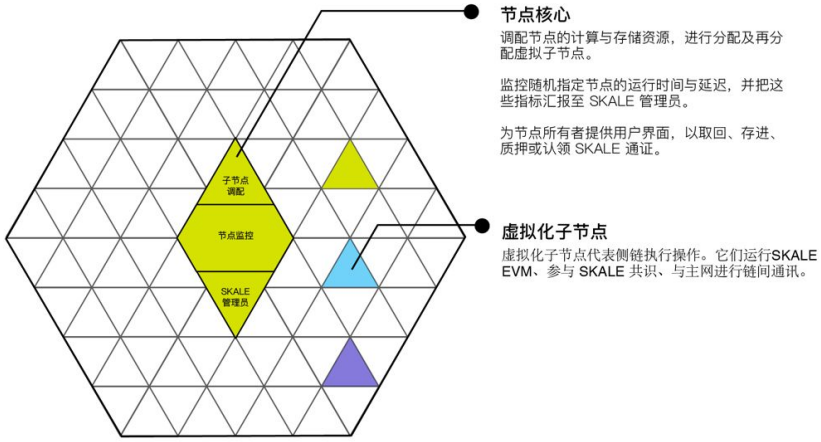


SKALE链中的节点会规律性和随机性地轮换，从而代表每个链利用整个网络的安全池

虚拟化子节点

、

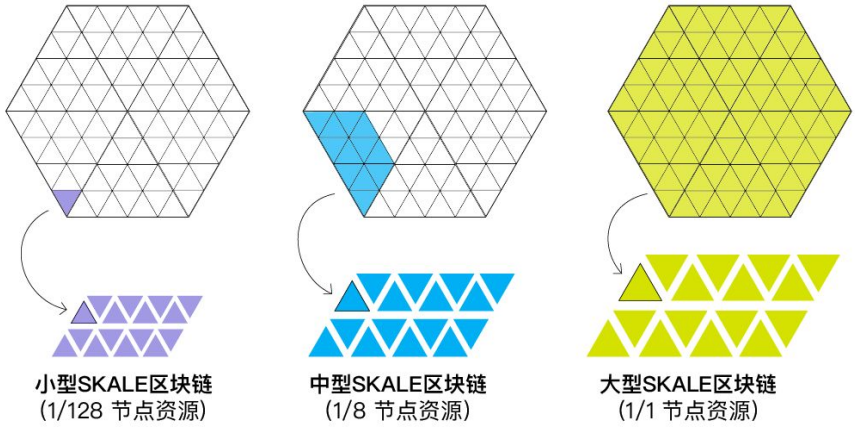
每个弹性侧链都由一组随机指定的虚拟子节点所组成，这些节点运行着SKALE守护进程和SKALE共识机制。通过利用虚拟化的子节点，SKALE网络中的节点不限定于某一个侧链，而能够同时服务多个侧链。这种多用功能通过对网络中每个节点部署容器化子节点架构而实现。每个节点都是虚拟化的，同时能够利用该子节点结构充当多个独立侧链的验证者。



验证节点包含虚拟化子节点和一个节点核心

容器化的验证节点

虚拟化子节点是通过一个创新性容器化架构实现的，该架构为去中心化应用开发者提供企业级的性能和可选项——与传统中心化云服务和微服务系统类似的性能与灵活性。容器被划分为几个主要组件，通过容器化的Linux操作系统封装——从而允许每个节点可以托管在任何操作系统上。



根据弹性侧链的规格，可以使用一部分资源或者全部节点资源

异步二进制拜占庭协议（ABBA）共识

每个弹性侧链用于出块和提交的共识模型为异步二进制拜占庭协议（ABBA）的一个变种（它由Mostefaou等人发明，虽然在满足特性属性的前提下，可以使用其他共识协议）。ABBA协议的优势在于，当由于潜在和/或宕机的子节点被认定为一个慢性链接时，它的健壮性就体现出来了。关于此协议的更多细节请参看这里。

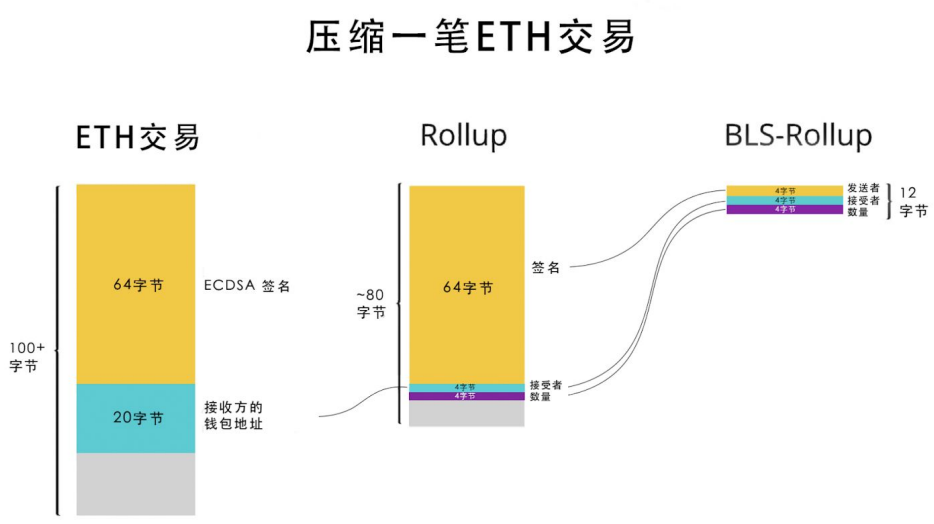
ABBA共识协议

BLS阈值签名链间通讯

每个弹性侧链都支持BLS（Boneh–Lynn–Shacham）阈值签名，这一点对于链间通讯非常重要。某个区块链通过群签名技术，它的虚拟化子节点都能够验证另一个区块链子节点所签名和提交的交易。通过发布到以太坊主网，其他所有侧链都可访问该签名。
这种通讯能力代表着一种微服务模型，在这个模型中，一个侧链能够执行一个或多个特定操作，然后将这些输出直接推送到另一个侧链或这一个消息队列（例如以太坊主网），接着这些输出能够作为其他侧链和它们处理需求的输入。SKALE网络的链间通讯支持所有的主流以太坊代币标准，包括ETH、ERC20、ERC721、ERC777和Dai。

BLS Rollups

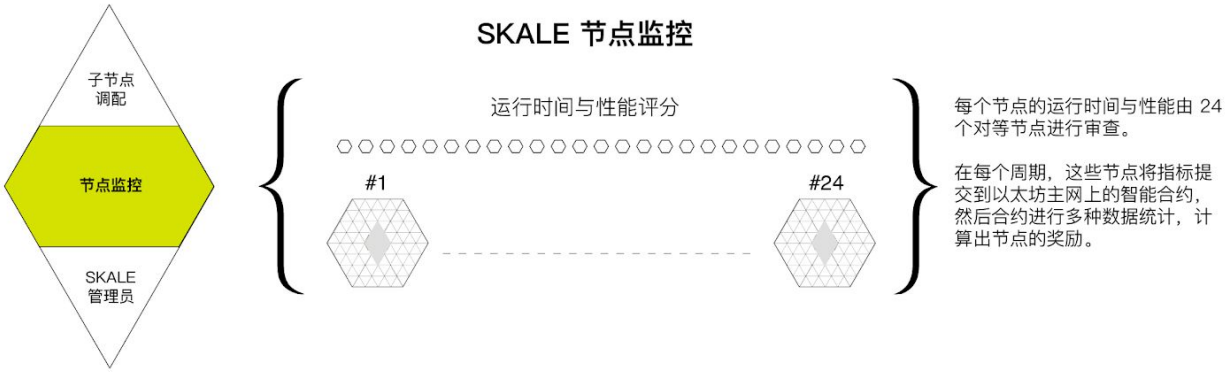
每个侧链还支持BLS　Rollups，这种方式的Rollups提供了一个更加高效和安全的方式去使用SKALE网络，以提高吞吐量和更低的以太坊主网gas费用。rollup通常被定义为一种解决方案，其中交易发布在链上，但运算和交易结果的存储则通过不同的方式，从而节省gas。BLS Rollups则是通过利用一种称为聚合BLS签名的加密算法来压缩ETH交易的大小。
将BLS　Rollups集成到SKALE的过程包括三个开发阶段，第一阶段让ERC-20通证转移速度最高达到每秒50笔交易。其他阶段将进一步改进交易性能指标。关于BLS Rollups工作原理和路线图的更详细概述可点击这里。
旁注：除了BLS　Rollups以外，还有其他的rollup方案例如Optimistic　Rollups和ZK　Rollups。Optimistic　Rollups的问题在于，它们可能允许将不正确的结果发送到链上（然后只能通过交易后的诉讼程序来解决）。在技术上ZK　Rollups比Optimistic　Rollups更好，因为它们在链上保持了状态的正确性。然而，由于ZK-S*ark操作是计算密集型的，这会导致有时交易可能需要几个小时才能确认。BLS　Rollups则是一个更现实的解决方案，因为它使用了能提供闪电般速度的BLS密码算法。



与其他形式的Rollups技术相比，BLS Rollups具有显著的优势

节点监控服务

每个 SKALE 节点都会运行一项节点监控服务（NMS），优化网络中其他特定数量节点的追踪性能。性能追踪通过一个常规程序，同时衡量运行时间与延迟，该程序连接每个对等节点并把测试结果记录在本地数据库。在每个周期的结束阶段，这些指标会算出平均值并提交至主网的智能合约，合约使用这些指标确定分配给节点的奖励，同时标记可疑节点随后进行审查和潜在的惩罚。



每个节点的核心节点会对网络中其他节点的性能进行评估和打分

与以太坊的互操作性

SKALE网络被设计成一个安全层和执行层，它与以太坊网络紧密联系在一起，为其安全性与操作模型服务。维护节点操作的智能合约全部都在以太坊主网执行。此外，验证节点质押和用户订阅（更不用说通证通胀），也都是由运行在以太坊主网的智能合约所维护或控制。

支持Solidity语言

SKALE网络使用Solidity作为智能合约的编程语言，让开发者免去学习一门新语言的时间。Solidity是一门用于实现智能合约的面向对象、高层次的语言。它受到了C++、Python和JavaScript的影响，专为以太坊虚拟机（EVM）而设计。

以太坊EVM兼容性

SKALE的执行模型完全兼容以太坊虚拟机（EVM），因此原本在以太坊主网运行的智能合约也能够在SKALE网络运行。无需要重写或移植智能合约，为EVM所编写的任何代码都能在SKALE执行。因此开发者

能以分阶段的方式迁移到SKALE弹性侧链——根据实际和利益诉求，将个别智能合约转移到SKALE。

开发者工具支持

对Solidity和以太坊虚拟机的支持同样扩展到通用的以太坊开发工具。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。

通证支持

SKALE网络支持所有的主流以太坊代币标准，包括ETH、ERC20、ERC721、ERC777和Dai。链间通讯，存款箱和通证克隆确保了SKALE网络通证操作的完整性与保真性。

常见支持钱包

SKALE网络支持支持许多主流加密钱包、浏览器插件以及网桥。包括Bitski、 Fortmatic、Metamask、Portis和Torus。这些接口组件在社区中很受重视，并被成千上万开发人员所使用。

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。