

节点引擎服务（NES）

质押指南

文档版本 01
发布日期 2024-11-25



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 概述	1
2 使用原理	3
3 以太坊质押操作	5
3.1 通过 Staking Launchpad 获取密钥.....	5
3.2 创建质押节点.....	12
3.3 创建并获取认证凭据.....	13
3.4 启动质押节点.....	14
3.5 监控质押节点状态.....	15
4 质押节点对接 VPC 终端节点	17

1 概述

以太坊质押是以太坊2.0版本的核心机制之一，旨在实现网络的共识算法从工作量证明 (PoW) 向权益证明 (PoS) 的过渡。质押是指存入32个以太币以激活验证者软件的行为。作为验证者，您将负责存储数据、处理交易以及向区块链添加新区块。这将确保以太坊的安全，并在此过程中为您赚取新的以太币。

质押作用

- **赚取奖励：**在以太坊中，有助于网络达成共识的行为都将被给予一定的奖励。作为质押者，只要正确运行将交易打包成区块并检查其他验证者工作的软件（验证者客户端），就可以获得一定的奖励，因为这样的行为保证了以太坊网络的安全运行。
- **提高网络安全性：**质押机制提高了网络的安全性和抗攻击能力。随着越来越多的以太币被质押，想要控制以太坊的网络就需要更多的以太币，这将使得以太坊的网络越来越强大。而作为质押者，也有经济利益去维护和保护网络。如果质押节点违反了规则或者攻击网络，它们质押的以太币将会被削减。
- **网络更快更持续：**相对于传统的工作量证明 (PoW) 机制，质押机制不需要大量的能源消耗，因为它基于验证者抵押的以太币，而不是计算能力。通过质押机制，以太坊网络能够更快更高效地验证和处理交易，从而提高整体的交易速度和吞吐量。

质押方案

以太坊质押提供多种质押方案，对于方案的选取主要取决于质押者想质押多少以太币。质押者一般需要32个以太币才能激活自己的验证者客户端，但是也可以选择更少的以太币进行质押。

表 1-1 质押方案

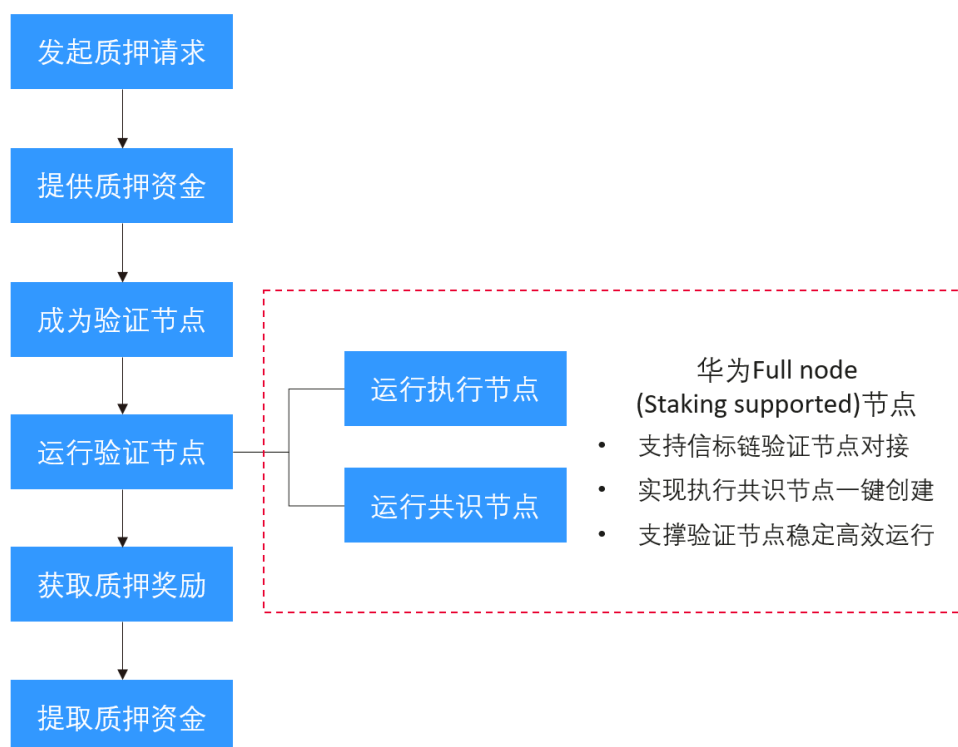
质押方式	单独质押	质押即服务	联合质押
描述	<p>在以太坊上单独质押是质押的黄金标准。它提供全部参与奖励，提升了网络的去中心化，而且资金的使用不再需要信任任何人。</p> <p>考虑单独质押的用户，应该至少有 32 个以太币和一台全年无休连接到互联网的专用计算机。</p>	<p>如果你不想或者不熟悉和硬件打交道，但是仍然想质押你的 32 个以太币，质押即服务方案将允许你委托在赚取原生区块奖励时所使用的硬件。这些选项通常会带你创建一套验证者证书，给他们上传你签名的密钥，同时质押你的 32 个以太币。这将允许服务代表你进行验证。</p> <p>这种质押方法需要对提供商有一定程度的信任。为了限制对方风险，提取你的以太币的密钥通常保存在你手中。</p>	<p>现在有几个资金池提供解决办法来帮助没有或不愿意质押 32 个以太币的用户。其中许多选择包括所谓的“流动性质押”，即用一种 ERC-20 流动性代币代表你质押的以太币。</p> <p>在流动性质押期间，你可以随时退出，质押就像代币兑换一样简单。此方案还允许用户将资产保管在自己的以太坊钱包中。但是，联合质押并非以太坊网络原生。</p>
奖励	<p>可以获取最多的奖励方案。验证者客户端通过打包新区块和检查其他验证者的工作，都可以获取相应的奖励。</p>	<p>通常为获取的全部奖励减去交给运营商的费用，通过运营商提供的监控服务可以更轻松的监控跟踪自己的验证者客户端。</p>	<p>联合质押者将获得不同的奖励，具体取决于所选择的联合质押方法。许多联合质押服务提供一种或多种流动性代币，代表你质押的以太币，以及你的验证者奖励份额。流动性代币可以保存在你自己的钱包中，在去中心化金融中使用，如果你决定退出，则可以出售。</p>
风险	<p>以太币处于质押状态，不可进行交易。并且对于验证者客户端的离线或者恶意行为，会导致以太币被削减甚至强制驱逐出以太坊网络。</p>	<p>单独质押的风险再加上运营商服务可能带来的风险。</p>	<p>风险因所用方法而不同。一般来说，风险包括交易对手、智能合约和执行风险的组合。</p>
要求	<ul style="list-style-type: none"> • 必须存入32个以太币。 • 维护运行以太坊验证者客户端以及执行客户端和共识客户端。 	<ul style="list-style-type: none"> • 存入 32 个以太币并在帮助下生成你的密钥。 • 安全地保存你的密钥。 • 根据不同运营商来完成相应的操作。 	<ul style="list-style-type: none"> • 需要很少的以太币要求，有些项目仅需 0.01 以太币。 • 直接从你的钱包存入不同的联合质押平台，或简单地交易其中一种质押流动性代币。

2 使用原理

华为云节点质押当前支持单独质押。在这个过程中，您只需购买一个华为云 Full node (Staking supported) 节点，激活一个验证者并对接华为云 Full node (Staking supported) 节点即可完成质押操作。华为云仅负责以太坊节点（执行层 (EL) 客户端和共识层 (CL) 客户端）的稳定运行，不会保存您的私钥。

以太坊质押流程如下：

图 2-1 质押流程图



其中，红框标记部分由Web3节点引擎服务服务一键提供，其他部分操作需要您自行操作完成。

具体的操作流程介绍如下：

1. **发起质押请求**

参与者发起质押请求，了解并完成以太坊提供的质押检查咨询。

2. **提供质押资金**

参与者锁定一定数量的以太币作为质押资金，将其存入质押合约中。这些资金将用于支持验证节点的运行。

3. **成为验证节点**

参与者将质押资金用于成为验证节点，参与以太坊网络的共识过程中。成为验证节点需要满足一定的条件和要求，例如质押所需的最低金额（单独质押所需的32个以太币）和一定的技术要求（设置并启动一个验证者客户端）。

4. **运行验证节点**

作为验证节点，参与者需要执行验证任务，包括验证交易的有效性和打包区块。在这个过程中，一般参与者需要自己启动至少一个执行节点和共识节点并进行监控维护，以保证验证节点能够正常运行并执行任务。对于Web3节点引擎服务提供的质押服务中，您可以直接在华为云购买Full node (Staking supported)节点，开放gRPC服务，支持信标链Validator对接，实现EL/CL节点一键创建，免用户运维，默认提供高规格配置（8u32g），华为云自研算法优化引擎支撑验证节点的稳定高效运行。

5. **获取质押奖励**

作为验证节点，参与者有机会获得质押奖励，包括区块奖励和交易手续费。这些奖励将根据参与者的质押资金和贡献程度进行分配。

6. **提取质押资金**

在Shanghai/Capella升级启用后，参与者可以根据自己的需求来选择是否进行质押资金的提取。

3 以太坊质押操作

3.1 通过 Staking Launchpad 获取密钥

Staking Launchpad是一个开源应用程序，可帮助你成为质押人。它将指导你选择客户端、生成密钥并将你的以太币存入质押存款合约。会提供一份清单，确保已经涵盖安全设置验证者需要的所有内容。

Staking Launchpad支持以太坊主网和Holesky测试网，建议现在Holesky测试网上进行设置和操作。

步骤1 了解质押。

Staking Launchpad提供了一个质押清单，供用户了解和学习质押。

图 3-1 质押清单



步骤2 选择执行层和共识层客户端。

如果您想运行自己的节点，可以查看各种 Eth1和Eth2提供商的选项并设置您的节点。**如果你选择使用购买华为云Full node (Staking supported)节点，Web3节点引擎服务将作为您的执行节点和共识节点提供商，完成执行节点和共识节点的创建工作，支持您快速高效地完成质押流程。**

说明

目前Web3节点引擎服务支持的共识层客户端有Prism和Lighthouse；支持的执行层客户端有Geth。

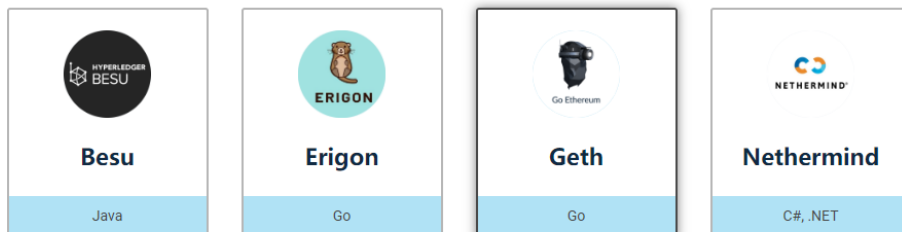
图 3-2 执行客户端选择

选择 执行 客户端

选择您的 执行 客户端并设置节点

若要处理来自执行层（原为“以太坊 1”链）的传入验证者存款，您需要运行执行客户端及您的共识客户端（原为“以太坊 2”）。您可以使用 Infura 等第三方服务，但我们建议您运行自己的客户端使网络尽可能去中心化。

[阅读此文档，学习如何在 Goerli 上运行节点](#)



[查看广泛的客户端比较](#)

目前有 66% 以上的网络使用 Geth。

客户端多样性对以太坊的网络健康至关重要：客户端内的错误占比超过 33% 会导致以太坊离线。如果这个比例占绝大多数（超过 66%），错误会导致链错误拆分，并可能造成罚没。

如果可能，此时考虑运行另一个客户端，以帮助保护自己和网络。

- [关于客户端多样性的更多信息](#)
- [有关网络客户端使用情况的最新数据](#)

Geth

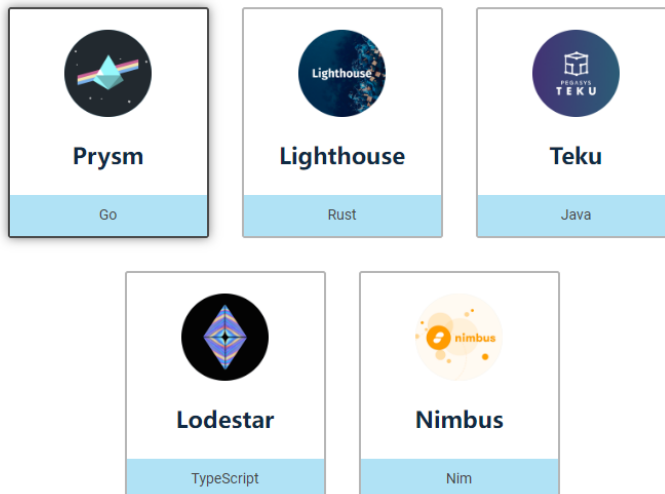
以太坊协议的三个原始实现之一。

图 3-3 共识客户端选择

选择 共识 客户端

选择您的 共识 客户端并设置节点

[阅读此文档，学习如何在 Goerli 上运行节点](#)



目前有 33% 以上的网络使用 Prysm。

客户端多样性对以太坊的网络健康至关重要：客户端内的错误占比超过 33% 会导致以太坊离线。如果这个比例占绝大多数（超过 66%），错误会导致链错误拆分，并可能造成罚没。

如果可能，此时考虑运行另一个客户端，以帮助保护自己和网络。

- [关于客户端多样性的更多信息](#)
- [有关网络客户端使用情况的最新数据](#)

Prysm

Prysm 是共识协议的一种实现，注重可用性、安全性和可靠性，它由 Prysmatic Labs 开发，后者是一家专注于客户端开发的公司。

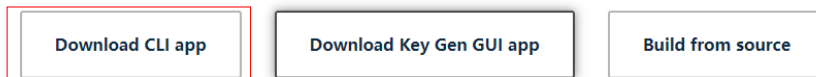
步骤3 生成密钥。

使用以太坊官方提供的[密钥生成工具](#)，生成并保存密钥文件。

采用Download CLI app方式，使用命令行工具 deposit command line interface进行创建。

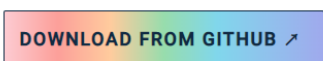
图 3-4 密钥生成工具选择

How do you want to generate your keys?

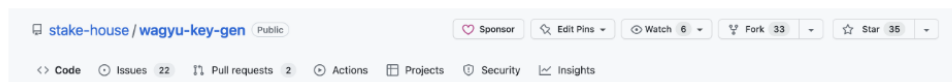
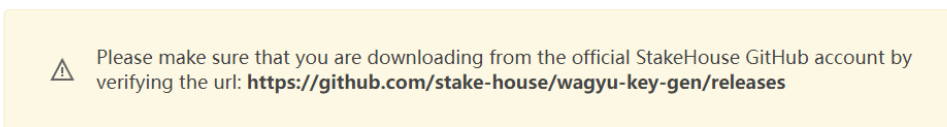


Download Wagyu Key Gen app

Step 1: Download the Wagyu Key Gen app for your operating system

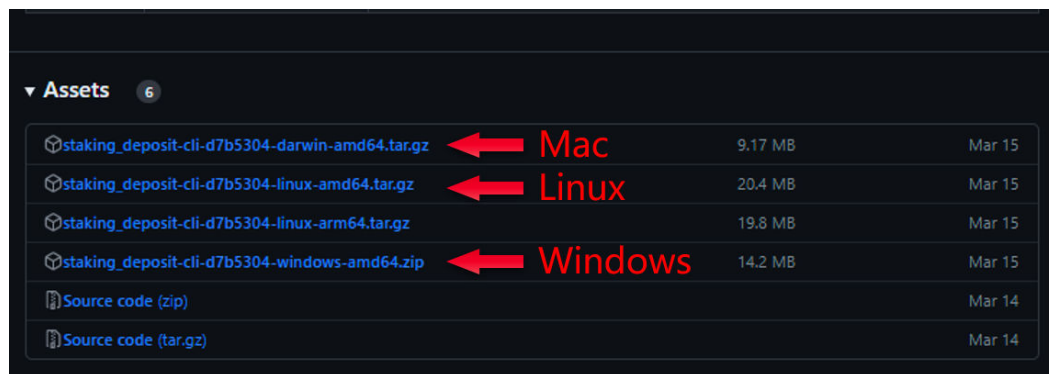


View Wagyu Key Gen audit by HashCloak ↗



首先从Github上，下载 [deposit command line interface](#)

图 3-5 下载密钥生成工具



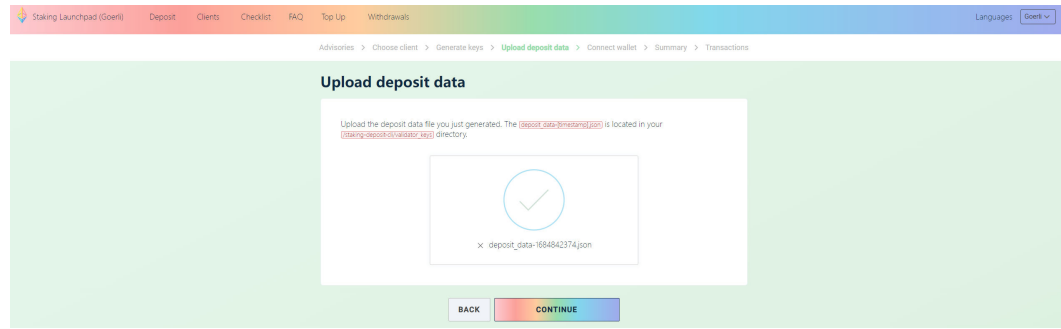
提取下载的文件到个人终端机器上。使用您的终端/Powershell 导航到工具所在文件夹。执行如下命令：

```
Linux/Mac
./deposit new-mnemonic
Windows
.\deposit.exe new-mnemonic
```

运行命令成功后，根据命令提示来执行相应操作：

```
[root@ecs-devnet01 ~]# ./deposit new-mnemonic
***Using the tool on an offline and secure device is highly recommended to keep your mnemonic safe.***
Please choose your language ['1. 2' العربية, '3. English', '4. Français', '5. Bahasa melayu', '6. Italiano', '7. 日本語', '8. 한국어', '9. Português do Brasil', '10. român', '11. Türkçe', '12. 简体中文']: [English]:
```

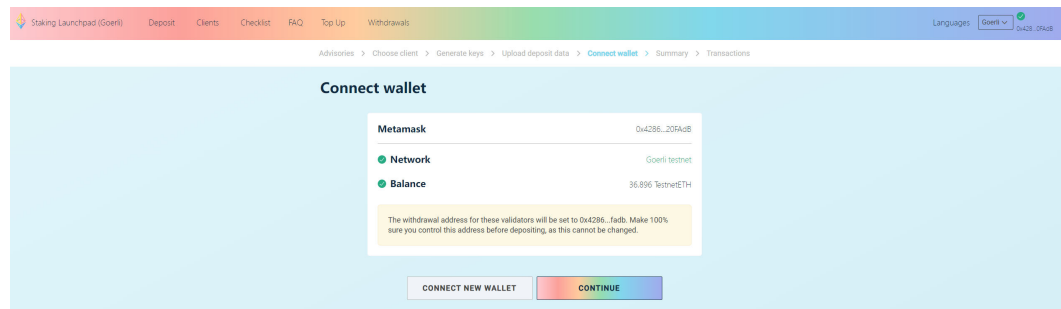

图 3-7 上传存款数据



步骤5 连接钱包。

将您的钱包连接到操作台，并确保账户中拥有32个以太币。

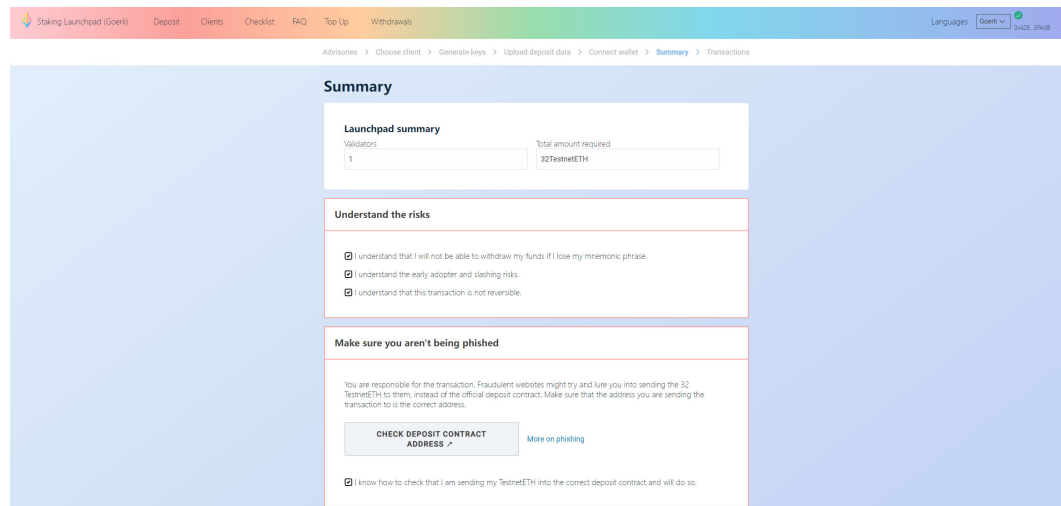
图 3-8 连接钱包



步骤6 检查质押信息。

查看选择的清单，确认信息是否正确。

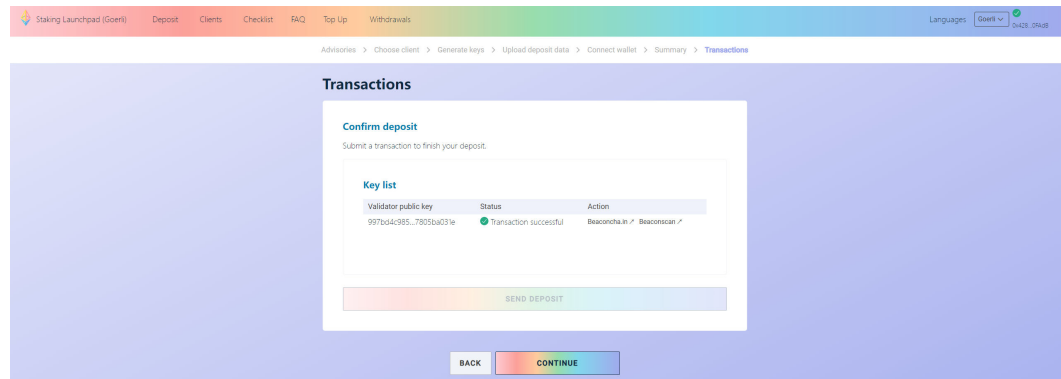
图 3-9 检查质押信息



步骤7 发送质押交易。

检查要求并单击继续，准备就绪后，交易将提交到信标链中。到这一步，就已经成功将初始存款提交到信标链中，后续则是启动客户端来完成质押操作。

图 3-10 发送质押交易



📖 说明

实践操作参考Staking Launchpad指南，更详细的操作步骤请参阅[Staking Launchpad \(Goerli\)](#)和[Staking Launchpad](#)

----结束

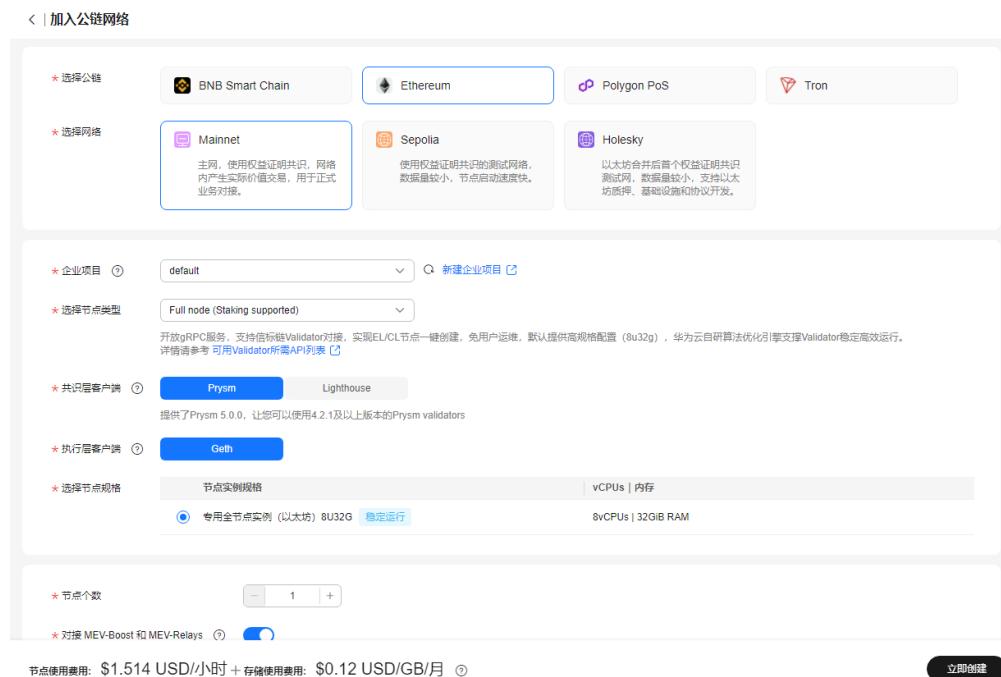
3.2 创建质押节点

步骤1 登录节点引擎服务控制台。

步骤2 在左侧导航栏中，选择“网络管理”，单击“加入公链网络”。

步骤3 在加入公链网络节点页面中，配置各参数信息。

图 3-11 Full node (Staking supported)节点



步骤4 完成后，单击“立即创建”。

步骤5 在弹出的加入公链网络节点详情页面，勾选“我已阅读并同意《华为云用户协议》和《免责声明》”后，单击“提交”。

📖 说明

- 加入公链网络节点大概需要5~8秒。
- 当前仅支持公链以太坊Mainnet、Sepolia和Holesky网络类型的质押节点。

----结束

3.3 创建并获取认证凭据

步骤1 在左侧导航栏中，选择“认证凭据”，单击“创建凭据”。

步骤2 在创建凭据页面中，填写描述信息和访问策略。

图 3-12 创建凭据

创建凭据

认证凭据可作为请求参数附加在节点访问地址尾部，以满足快速对接需求，建议仅将该凭据用于节点对接测试，如涉及正式业务，建议使用华为云Token认证。每个认证凭据仅能下载一次，为了节点安全性，建议您定期更换并妥善保存认证凭据。

★ 企业项目 [新建企业项目](#)

描述 0/1,000

访问策略 ^

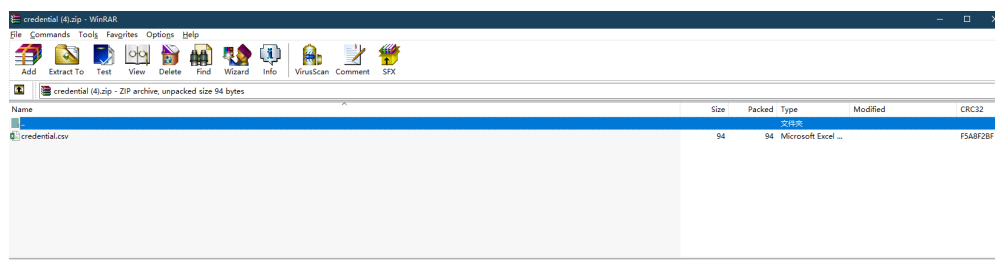
选择鉴权节点

访问策略类型 不启用 白名单 黑名单

启用此白名单设置，任何已选访问策略维度及信息不在白名单当中的请求都将被拒绝。
注：单一凭据仅能选择一种访问策略类型。

白名单	策略维度	操作
<input type="button" value="新增白名单"/>		

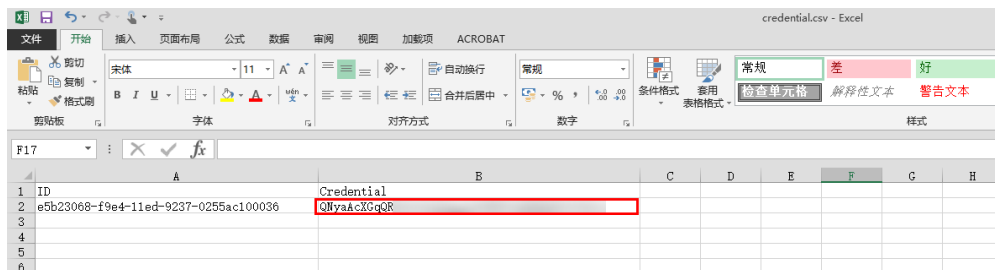
步骤3 单击“确认”，认证凭据创建完成，并自动下载认证凭据zip包。



说明

每个认证凭据仅能下载一次，为了节点安全性，建议您定期更换并妥善保存认证凭据。

步骤4 解压后，打开credential.csv文件，可获取认证凭据信息。



---结束

3.4 启动质押节点

步骤1 在左侧导航栏中，选择“网络管理”。

步骤2 在网络管理页面中，单击节点ID。

图 3-13 节点 ID

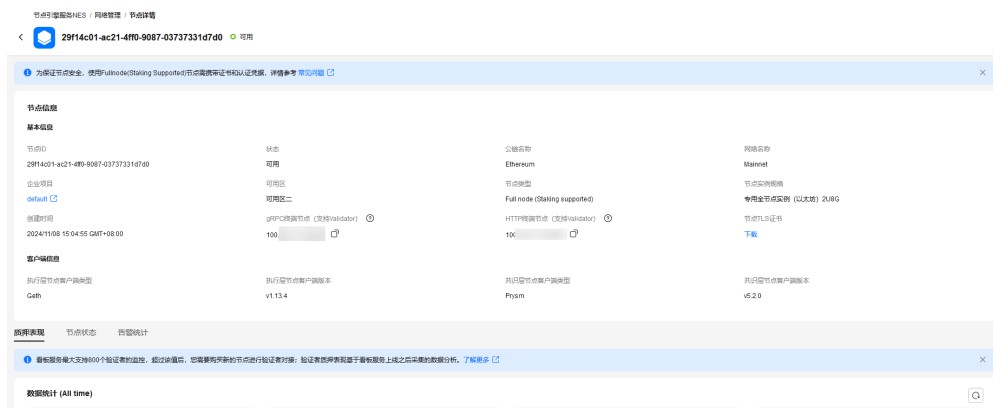


步骤3 在节点详情页面，获取节点相关信息。

当共识层客户端为Prysm，可获取gRPC终端节点、HTTP终端节点和节点TLS证书。

当共识层客户端为Lighthouse，可获取HTTP终端节点和节点TLS证书。

图 3-14 共识层客户端为 Prysm 的节点详情



步骤4 将已获取的密钥文件和节点TLS证书，复制到已安装脚本的硬件机器。

Prysm: 执行如下命令，将已获取的密钥导入密钥库：

```
./prysm.sh validator accounts import --keys-dir=<YOUR_FOLDER_PATH> --< NETWORK >
```

其中，**NETWORK** 为参与质押的网络；**YOUR_FOLDER_PATH**表示真实的密钥文件路径。

Lighthouse: 执行如下命令，将已获取的密钥导入密钥库：

```
lighthouse --network < NETWORK > account validator import --directory < YOUR_FOLDER_PATH >
```

其中，**NETWORK** 为参与质押的网络；**YOUR_FOLDER_PATH** 表示真实的密钥文件路径。

步骤5 密钥导入成功后。

执行**prysm.sh**文件，配置如下参数启动质押节点。

- beacon-rpc-provider: 值为已获取的**gRPC终端节点**。
- grpc-headers : 值为已获取的**认证凭据**。
- tls-cert: 值为已获取节点**TLS证书的相对路径**。

例如：

```
./prysm.sh validator --beacon-rpc-provider=xx.xx.xx.xx:30002 --grpc-headers=credential=xxxxxxxxxxxxxxxxxxxxxxxxx --tls-cert=ca.crt
```

执行**lighthouse vc**命令，配置如下参数启动质押节点。

- network: 值为参与质押的网络。
- suggested-fee-recipient: 值为提议者费用的接收者。
- beacon-nodes-tls-certs: 值为已获取节点**TLS证书的相对路径**。
- beacon-nodes: 值为已获取的**HTTP终端节点/凭据信息**。

```
lighthouse vc --network < **NETWORK** > --suggested-fee-recipient < **YourFeeRecipient** > --beacon-nodes-tls-certs ca.pem --beacon-nodes https://xx.xx.xx.xx:30000/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

说明

以上参数仅是对接华为云节点的必选参数，其他参数配置，请参考[Prysm官方文档](#)或[Lighthouse官方文档](#)。

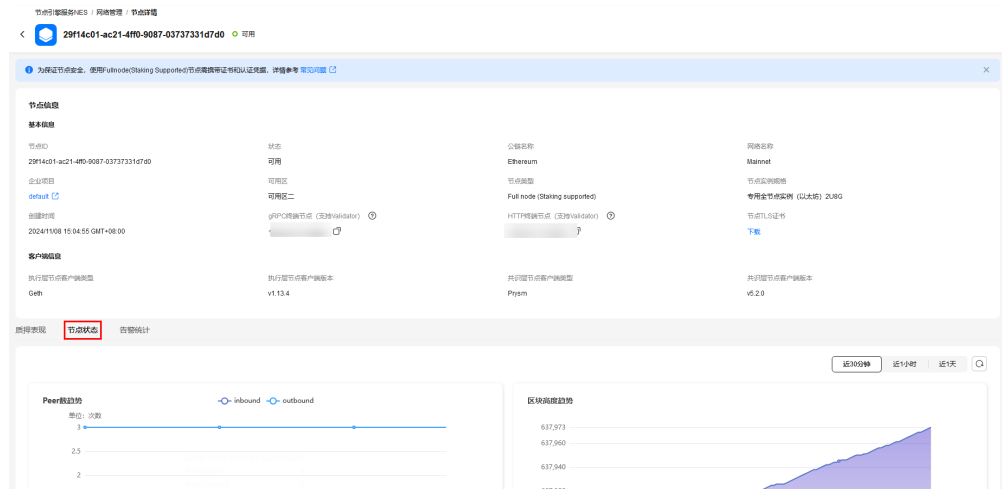
----结束

3.5 监控质押节点状态

步骤1 在左侧导航栏中，选择“网络管理”。

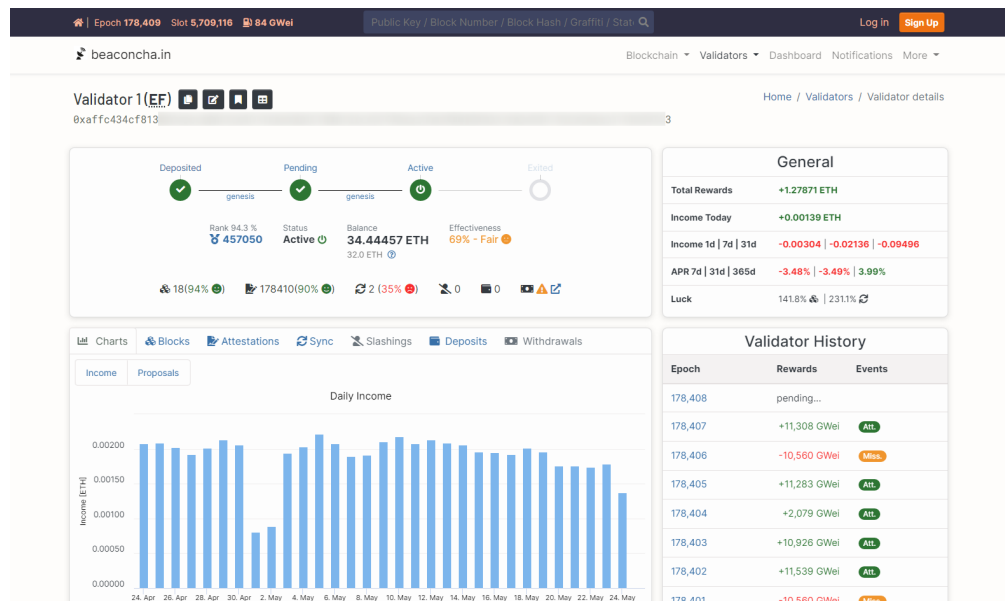
步骤2 在网络管理页面中，单击节点ID，选择“节点状态”，进行监控。

图 3-15 节点状态



说明

对于启动质押的验证客户端状态，需要您自行进行监控和运维。可在相应的网页输入公钥查看验证客户端执行情况。



---结束

4 质押节点对接 VPC 终端节点

质押节点对接VPC终端节点服务，适用于使用华为云ECS、CCE等后端资源，您可以通过华为云内网与质押节点建立快速、稳定的连接。

前提操作

已[创建质押节点](#)，且开启终端节点服务。

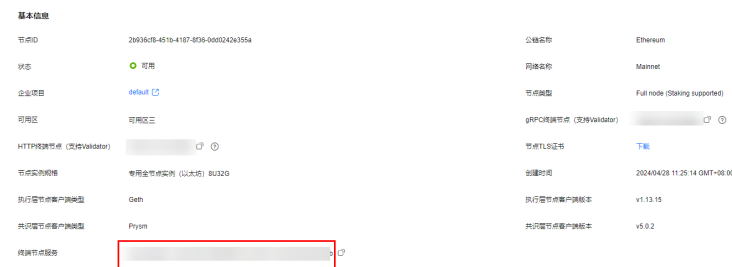
注意事项

- 质押节点、终端节点与后端资源须在**同一华为云区域**（例如：亚太-新加坡）。
- 后端资源与终端节点须在相同虚拟私有云下。

操作步骤

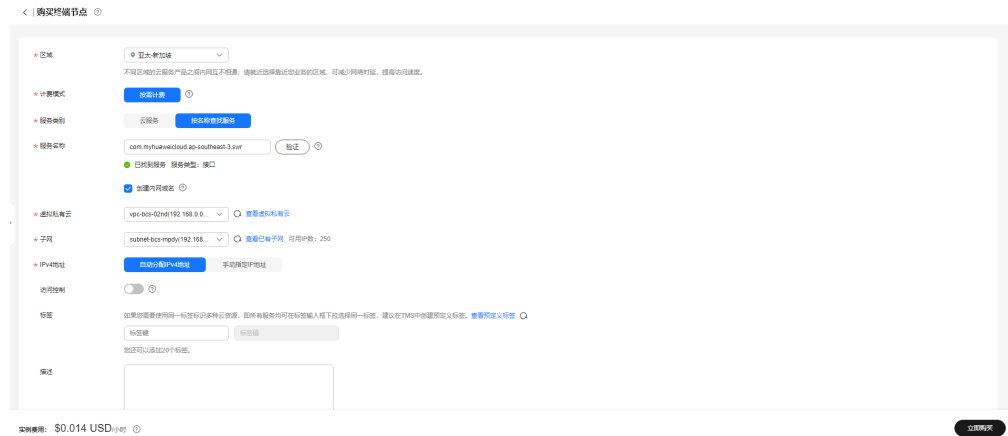
步骤1 获取终端节点服务名称

1. 登录节点引擎服务控制台。
2. 在左侧导航栏中，选择“专享版>网络管理”，进入网络管理页面。
3. 在网络管理页面，单击已创建质押节点的**节点ID**，可获取终端节点服务名称。



步骤2 创建终端节点

1. 登录VPC终端节点服务控制台。
2. 在左侧导航栏中，选择“VPC 终端节点>终端节点”，进入终端节点页面。
3. 在终端节点页面，单击“购买终端节点”，[配置各参数信息](#)。



说明

其中，服务类别选择“按名称查找服务”，服务名称填写在节点引擎服务控制台获取到的终端节点服务名称。

4. 完成后，单击“立即购买”，进行规格确认。
5. 在终端节点页面中，单击ID名称，获取内网域名。



步骤3 使用终端节点的内网域名与质押节点对应的端口号可访问质押节点。

gRPC终端节点：内网域名:端口号

HTTP终端节点：内网域名:端口号

说明

质押节点对应的端口号为节点基本信息里**gRPC终端节点（支持Validator）**和**HTTP终端节点（支持Validator）**的端口号。

----结束