aws

开发人员指南

AMB 访问比特币

AMB 访问比特币: 开发人员指南

Table of Contents

什么是亚马逊托管区块链（AMB）访问比特币？

Amazon Managed Blockchain (AMB) Access 为您提供以太坊和比特币的公共区块链节点，您还可以使用 Hyperledger Fabric 框架创建私有区块链网络。从各种方法中选择与公共区块链互动，包括对公共区块链节点的完全托管、单租户（专用）和无服务器多租户 API 操作。对于访问控制很重要的用例，您可以从完全托管的私有区块链网络中进行选择。标准化的 API 操作可让您在完全托管的弹性基础设施上即时扩展，因此您可以构建区块链应用程序。

AMB Access 为您提供两种不同类型的区块链基础设施服务：多租户区块链网络访问 API 操作以及专用的区块链节点和网络。借助专用的区块链基础设施，您可以创建和使用公共的以太坊区块链节点和私有的 Hyperledger Fabric 区块链网络供自己使用。但是，基于API的多租户产品，例如AMB Access Bitcoin，由API层后面的一组比特币节点组成，在该层中，底层区块链节点基础设施由客户共享。

比特币是一个去中心化的区块链网络，可以实现以该网络的原生加密货币比特币（BTC）计价的安全价值 peer-to-peer交易。个人、金融机构、金融科技公司、政府等都在使用比特币网络。比特币网络是一种交换媒介，一种用于投资的商品，或者是用于存放刻录数据的公开可验证且不可变的账本。借助 Amazon Managed Blockchain (AMB) Access Bitcoin，您可以通过区域终端节点访问比特币主网和测试网网络池，通过这些终端节点可以写入交易、读取账本中的数据以及调用比特币核心节点客户端上可用的 JSON-RPC 请求。借助无服务器比特币终端节点，您可以专注于构建应用程序，而不必投资于无差别的工作，例如配置、维护和负载平衡比特币节点。无论您是在构建比特币钱包、建立加密货币交易所，还是分析比特币区块链数据，您只需使用AMB Access Bitcoin为通过比特币端点发出的请求付费。

你是首次使用AMB Access比特币的用户吗？

如果您是首次使用AMB Access Bitcoin的用户，我们建议您先阅读以下章节：

- 关键概念：亚马逊托管区块链 (AMB) 访问比特币
- 开始使用亚马逊托管区块链 (AMB) 访问比特币
- 亚马逊托管区块链 (AMB) 的比特币用例访问比特币
- 支持比特币 JSON-RPCs 使用亚马逊托管区块链 (AMB) 访问比特币

关键概念：亚马逊托管区块链 (AMB) 访问比特币

> **Note**
>
> 本指南假设您熟悉比特币必不可少的概念。这些概念包括去中心化、节点、交易 proof-of-work、钱包、公钥和私钥、减半等。在使用 Amazon Managed Blockchain (AMB) 访问比特币之前，我们建议您阅读比特币开发文档并掌握比特币。

Amazon Managed Blockchain (AMB) Access Bitcoin 为您提供比特币区块链的无服务器访问权限，无需您预置和管理任何比特币基础设施，包括节点。您可以使用此托管服务快速按需访问比特币网络，从而降低总体拥有成本。

AMB Access Bitcoin允许您通过运行比特币核心客户端的完整节点访问比特币网络，同时禁用钱包功能，并支持多个JSON远程程序（JSON-RPC）调用。您可以调用比特币 JSON RPCs 与托管区块链管理的比特币节点进行通信，从而与比特币网络进行交互。使用比特币 JSON-RPCs，您可以读取数据和写入交易，包括使用 Amazon Managed Blockchain 服务查询数据和向比特币网络提交交易。

> **Important**
>
> 您负责创建、维护、使用和管理您的比特币地址。您还应对您的比特币地址的内容负责。AWS 对使用亚马逊托管区块链上的比特币节点部署或调用的任何交易概不负责。

使用亚马逊托管区块链 (AMB) 的注意事项和限制访问比特币

- 支持的比特币网络

  AMB Access 比特币支持以下公共网络：

  - 主网 — 通过 proof-of-work共识保护的公共比特币区块链，比特币（BTC）加密货币是在该区块链上发行和交易的。主网上的交易具有实际价值（也就是说，它们会产生实际成本），并记录在公共区块链上。
  - Testn et —测试网是用于测试的替代比特币区块链。测试网硬币与实际的比特币（BTC）是分开的，并且通常没有任何价值。

> **Note**
>
> 不支持私有网络。

- 支持的区域

  以下是此服务支持的区域：

区域名称	代码	区域
美国东部（弗吉尼亚州北部）	IAD	us-east-1
亚太地区（东京）	NRT	ap-northeast-1
亚太地区（首尔）	ICN	ap-northeast-2
亚太地区（新加坡）	SIN	ap-southeast-1
欧洲地区（爱尔兰）	DUB	eu-west-1
欧洲地区（伦敦）	LHR	eu-west-2

- 服务终端节点

  以下是 AMB Access 比特币的服务端点。要连接服务，您必须使用包含其中一个支持的区域的终端节点。

  - `mainnet.bitcoin.managedblockchain.Region.amazonaws.com`
  - `testnet.bitcoin.managedblockchain.Region.amazonaws.com`

  例如：`mainnet.bitcoin.managedblockchain.eu-west-2.amazonaws.com`

- 不支持挖矿

  AMB Access 比特币不支持比特币 (BTC) 挖矿。

- 签名版本 4 对比特币 JSON-RPC 通话进行签名

  RPCs 在 Amazon Managed Blockchain 上调用比特币 JSON 时，您可以通过使用签名版本 4 签名流程进行身份验证的 HTTPS 连接进行调用。这意味着只有 AWS 账户中授权的 IAM 委托人才能进行比特币 JSON-RPC 调用。为此，必须在呼叫中提供 AWS 证书（访问密钥 ID 和私有访问密钥）。

> **Important**
>
> - 不要在面向用户的应用程序中嵌入客户端凭据。
> - 您不能使用 IAM 策略来限制对单个比特币 JSON 的访问RPCs。

- 仅支持提交原始交易

  使用 `sendrawtransaction` JSON-RPC 提交更新比特币区块链状态的交易。

- AWS CloudTrail 日志支持

  您可以配置 CloudTrail 为记录您的比特币 JSON-RPCs。有关更多信息，请参阅 登录亚马逊托管区块链 (AMB) 使用访问比特币事件 AWS CloudTrail。

设置亚马逊托管区块链 (AMB) 访问比特币

在您首次使用 Amazon Managed Blockchain (AMB) 访问比特币之前，请按照本节中的步骤创建 AWS 账户。下一章讨论如何开始使用AMB Access比特币。

先决条件和注意事项

在你 AWS 第一次使用之前，你必须有一个 AWS 账户。

报名参加 AWS

当你注册时 AWS，你会自动注册所有 AWS 账户 账户 AWS 服务，包括亚马逊托管区块链 (AMB) Access Bitcoin。您只需为使用的服务付费。

如果您 AWS 账户 已经有，请转到下一步。如果您还没有 AWS 账户，请使用以下流程创建。

创建 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   注册过程的一部分涉及接听电话或短信，并在电话键盘上输入验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

创建具有适当权限的 IAM 用户

要创建和使用 AMB Access Bitcoin，您必须拥有一个 AWS Identity and Access Management (IAM) 委托人（用户或群组），该委托人必须具有允许进行必要的托管区块链操作的权限。

只有 IAM 委托人可以拨打比特币 JSON-RPC 调用。RPCs 在 Amazon Managed Blockchain 上调用比特币 JSON 时，您可以通过使用签名版本 4 签名流程进行身份验证的 HTTPS 连接进行调用。这意味着只有 AWS 账户中授权的 IAM 委托人才能进行比特币 JSON-RPC 调用。为此，必须在呼叫中提供 AWS 证书（访问密钥 ID 和私有访问密钥）。

有关如何创建 IAM 用户的信息，请参阅在您的 AWS 账户中创建 IAM 用户。有关如何向用户关联权限策略的更多信息，请参阅更改 IAM 用户的权限。有关可用于授予用户使用 AMB Access Bitcoin 的权限策略示例，请参阅Amazon Managed Blockchain (AMB) 访问比特币的基于身份的策略示例。

安装和配置 AWS Command Line Interface

如果您尚未这样做，请安装最新的 AWS 命令行界面 (CLI) 以使用来自终端的 AWS 资源。有关更多信息，请参阅安装或更新 AWS CLI的最新版本。

> **Note**
>
> 要进行 CLI 访问，您需要访问密钥 ID 和秘密访问密钥。如果可能，请使用临时凭证代替长期访问密钥。临时凭证包括访问密钥 ID、秘密访问密钥，以及一个指示凭证何时到期的安全令牌。有关更多信息，请参阅 IAM 用户指南中的将临时证书与 AWS 资源配合使用。

开始使用亚马逊托管区块链 (AMB) 访问比特币

使用本节中的 step-by-step教程来学习如何使用亚马逊托管区块链 (AMB) Access Bitcoin 来执行任务。这些示例要求您完成一些先决条件。如果您不熟悉 AMB Access Bitcoin，请查看本指南的设置部分，确保您已完成这些先决条件。有关更多信息，请参阅 设置亚马逊托管区块链 (AMB) 访问比特币。

主题

创建一个 IAM 策略来访问比特币 JSON-RPCs

要访问比特币主网和测试网的公共端点以进行 JSON-RPC 调用，您必须拥有拥有相应的 IAM 权限的用户证书（AWS_ACCESS_KEY_ID 和 AWS_SECRET _ACCESS_KEY），才能访问比特币。在 AWS CLI 安装了的终端中，运行以下命令创建用于访问两个比特币终端节点的 IAM 策略：

```
cat <<EOT > ~/amb-btc-access-policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "AMBBitcoinAccessPolicy",
            "Effect": "Allow",
            "Action": [
                "managedblockchain:InvokeRpcBitcoin*"
            ],
            "Resource": "*"
        }
    ]
}
EOT
aws iam create-policy --policy-name AmazonManagedBlockchainBitcoinAccess --policy-
document file://$HOME/amb-btc-access-policy.json
```

> **Note**
>
> 前面的示例允许您同时访问比特币主网和测试网。要访问特定端点，请使用以下Action命令：
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

创建策略后，将该策略附加到您的 IAM 用户的角色以使其生效。在中 AWS Management Console，导航到 IAM 服务，并将策略附加AmazonManagedBlockchainBitcoinAccess到分配给您的 IAM 用户的角色。有关更多信息，请参阅创建角色并分配给 IAM 用户。

使用 AMB Access RPC 编辑器发出比特币远程过程调用 (RPC) 请求 AWS Management Console

您可以 AWS Management Console 使用 AMB Access 在上编辑和提交远程过程调用 (RPCs)。有了这些 RPCs，你就可以在比特币网络上读取数据、写入和提交交易。

Example

以下示例显示了如何使用 RPC 获取有关 00000000c983704a73af28acdec37b049d214adbda81d7e2a3dd14a3dd146f6ed09 `blockhash` 的信息。`getBlock`用您自己的输入替换突出显示的变量，或者选择列出的其他 RPC 方法之一，然后输入所需的相关输入。

1. 打开托管区块链控制台，网址为https://console.aws.amazon.com/managedblockchain/。
2. 选择 RPC 编辑器。
3. 在请求部分中，选择*`BITCOIN_MAINNET`*作为区块链网络。
4. 选择*`getblock`*作为 RPC 方法。
5. 输入*`00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09`*作为区块号并选择*`0`*作为详细程度。
6. 然后，选择提交 RPC。
7. 您将在本页的 “回复” 部分获得结果。然后，您可以复制完整的原始交易以供进一步分析或用于应用程序的业务逻辑。

欲了解更多信息，请参阅 AMB Access 比特币RPCs 支持的

使用 awscurl 发出 AMB 访问比特币 JSON-RPC 请求 AWS CLI

Example

使用签名版本 4 (Sigv4) 使用您的 IAM 用户证书签署请求，以便向 AMB Access 比特币端点进行比特币 JSON-RPC 调用。awscurl 命令行工具可以帮助您使用 Sigv4 签署对 AWS 服务的请求。有关更多信息，请参阅 awscur l README.md。

使用适合您的操作系统的方法安装 awscurl。在 macOS 上，推荐 HomeBrew使用以下应用程序：

```
brew install awscurl
```

如果您已经安装并配置了 AWS CLI，则您的 IAM 用户证书和默认 AWS 区域将在您的环境中设置并可以访问 awscurl。使用 awscurl，通过调用 RPC 向比特币主网和测试网提交请求。getblock此调用接受与您要检索其信息的区块哈希相对应的字符串参数。

以下命令使用params数组中的区块哈希来选择要检索标头的特定区块，从而从比特币主网上检索区块头数据。此示例使用us-east-1终端节点。你可以将其替换为你首选的比特币 JSON-RPC 和受亚马逊托管区块链 (AMB) 访问比特币支持的 AWS 区域。此外，您可以通过在命令中替换mainnet为，向测试网网络而不是主网发出请求。testnet

```
awscurl -X POST -d '{ "jsonrpc": "1.0", "id": "getblockheader-curltest", "method":
 "getblockheader", "params":
 ["000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0"] }' --service
 managedblockchain https://mainnet.bitcoin.managedblockchain.us-east-1.amazonaws.com
 --region us-east-1 -k
```

结果包括区块标头中的详细信息以及请求区块中包含的交易哈希列表。请参见以下示例：

```
{"result":{"hash":"000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0",
      "confirmations":2,"height":799243,"version":664485888,"versionHex":"279b4000",
      "merkleroot":"568e79752e1921ecf40c961435abb41bc5700fe2833ecadc4abfc2f615ddc1b8",
      "time":1689684290,"mediantime":1689681317,"nonce":2091174943,"bits":"17053894",
      "difficulty":53911173001054.59,
      "chainwork":"0000000000000000000000000000000000000004f375cf72ff64e2404c1589c",
      "nTx":2135,

 "previousblockhash":"00000000000000000002ffe4efe07ae74ec8b92c7696f5e12b5da506f015ba6b",
```

```
"nextblockhash":"000000000000000000038f05ddcf3f483fdcb74f4be606c022bcb673424fa4ca"},
    "error":null,"id":"curltest"}
```

在 Node.js 中发出比特币 JSON-RPC 请求

您可以使用 HTTPS 提交签名的请求来访问比特币主网和测试网端点，并使用 Node.js 中的原生 https 模块进行 JSON-RPC API 调用，也可以使用第三方库，例如 AXIOS。以下示例向您展示了如何向 AMB Access 比特币端点发出比特币 JSON-RPC 请求。

Example

要运行此示例 Node.js 脚本，请应用以下先决条件：

1. 您的计算机上必须安装节点版本管理器 (nvm) 和 Node.js。您可以在此处找到操作系统的安装说明。
2. 使用`node --version`命令并确认您使用的是 Node 版本 14 或更高版本。如果需要，您可以使用`nvm install 14`命令和`nvm use 14`命令安装版本 14。
3. 环境变量`AWS_ACCESS_KEY_ID`和`AWS_SECRET_ACCESS_KEY`必须包含与您的账户关联的证书。环境变量`AMB_HTTP_ENDPOINT`必须包含您的 AMB Access 比特币端点。

   使用以下命令将这些变量作为字符串导出到客户端。将以下字符串中突出显示的值替换为您的 IAM 用户账户中的相应值。

   ```
   export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
   export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
   ```

完成所有先决条件后，使用编辑器将以下`package.json`文件和`index.js`脚本复制到本地环境中：

包裹.json

```
{
  "name": "bitcoin-rpc",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
```

```
  "license": "ISC",
  "dependencies": {
    "@aws-crypto/sha256-js": "^4.0.0",
    "@aws-sdk/credential-provider-node": "^3.360.0",
    "@aws-sdk/protocol-http": "^3.357.0",
    "@aws-sdk/signature-v4": "^3.357.0",
    "axios": "^1.4.0"
  }
}
```

index.js

```
const axios = require('axios');
const SHA256 = require('@aws-crypto/sha256-js').Sha256
const defaultProvider = require('@aws-sdk/credential-provider-node').defaultProvider
const HttpRequest = require('@aws-sdk/protocol-http').HttpRequest
const SignatureV4 = require('@aws-sdk/signature-v4').SignatureV4

// define a signer object with AWS service name, credentials, and region
const signer = new SignatureV4({
  credentials: defaultProvider(),
  service: 'managedblockchain',
  region: 'us-east-1',
  sha256: SHA256,
});


const rpcRequest = async () => {

  // create a remote procedure call (RPC) request object definig the method, input
 params
  let rpc = {
    jsonrpc: "1.0",
    id: "1001",
    method: 'getblock',
    params: ["00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09"]
  }

  //bitcoin endpoint
  let bitcoinURL = 'https://mainnet.bitcoin.managedblockchain.us-
east-1.amazonaws.com/';

  // parse the URL into its component parts (e.g. host, path)
```

```
  const url = new URL(bitcoinURL);

  // create an HTTP Request object
  const req = new HttpRequest({
    hostname: url.hostname.toString(),
    path: url.pathname.toString(),
    body: JSON.stringify(rpc),
    method: 'POST',
    headers: {
      'Content-Type': 'application/json',
      'Accept-Encoding': 'gzip',
      host: url.hostname,
    }
  });


  // use AWS SignatureV4 utility to sign the request, extract headers and body
  const signedRequest = await signer.sign(req, { signingDate: new Date() });

  try {
    //make the request using axios
    const response = await axios({...signedRequest, url: bitcoinURL, data: req.body})

    console.log(response.data)
  } catch (error) {
    console.error('Something went wrong: ', error)
    throw error
  }


}

rpcRequest();
```

前面的示例代码使用 Axios 向比特币端点发出 RPC 请求，并使用官方的 SDK v3 工具，使用相应的签名版本 4 (Sigv4) 标头对这些请求进行签名。 AWS 要运行代码，请在文件所在目录下打开终端，然后运行以下命令：

```
npm i
node index.js
```

生成的结果将类似于以下内容：

```
{"hash":"00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09","
    confirmations":784126,"height":1000, "version":1,"versionHex":"00000001",
    "merkleroot":"fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33",
    "time":1232346882,
    "mediantime":1232344831,"nonce":2595206198,"bits":"1d00ffff","difficulty":1,
    "chainwork":"0000000000000000000000000000000000000000000000000000000000000003e903e903e9",
    "nTx":1,

 "previousblockhash":"0000000008e647742775a230787d66fdf92c46a48c896bfbc85cdc8acc67e87d",
    "nextblockhash":"00000000a2887344f8db859e372e7e4bc26b23b9de340f725afbf2edb265b4c6",
    "strippedsize":216,"size":216,"weight":864,
    "tx":["fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33"]},
    "error":null,"id":"1001"}
```


> **Note**
>
> 前一个脚本中的示例请求使用与使用 awscurl 发出 AMB 访问比特币 JSON-RPC 请求 AWS CLI示例相同的输入参数区块哈希进行`getblock`调用。要进行其他调用，请使用不同的比特币 JSON-RPC 修改脚本中的`rpc`对象。您可以将主机属性选项更改为比特币，`testnet`以便在该端点上拨打电话。

使用 AMB 访问比特币 AWS PrivateLink

AWS PrivateLink 是一种高度可用、可扩展的技术，您可以使用它来私下连接您的 VPC 和服务，就像这些服务位于您的 VPC 中一样。您不必使用互联网网关、NAT 设备、公有 IP 地址、 AWS Direct Connect 连接或 AWS 站点到站点 VPN 连接即可从您的私有子网与服务通信。有关 AWS PrivateLink 或要设置的更多信息 AWS PrivateLink，请参阅什么是 AWS PrivateLink？

您可以 AWS PrivateLink 使用 VPC 终端节点向 AMB Access Bitcoin 发送比特币 JSON-RPC 请求。对该私有端点的请求不会通过开放的互联网传递，因此您可以使用相同的 SigV4 身份验证将请求直接发送到比特币端点。有关更多信息，请参阅通过访问 AWS 服务 AWS PrivateLink。

要查看服务名称，请在AWS 服务栏中查找 Amazon Managed Blockch ain。有关更多信息，请参阅与集成的AWS 服务 AWS PrivateLink。终端节点的服务名称将采用以下格式：`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*。

例如：`com.amazonaws.`*`us-east-1`*`.managedblockchain.bitcoin.`*`testnet`*。

亚马逊托管区块链 (AMB) 的比特币用例访问比特币

本主题提供了 AMB Access 比特币用例列表

主题

创建一个比特币 (BTC) 钱包来发送和接收比特币

比特币是比特币网络上的原生加密货币，是网络安全模型的重要组成部分。它还充当商品和交换媒介，被机构、企业和个人广泛使用。因此，许多钱包应用程序依赖比特币节点与比特币区块链进行交互。这些应用程序计算给定地址组的未用输出余额 (UTXOs)，签署交易并将其发送到比特币网络，并检索有关历史交易的数据。

以下是亚马逊托管区块链 (AMB) Access Bitcoin 支持比特币钱包交易的一些比特币 JSON 示例：RPCs

- `estimatesmartfee`
- `createmultisig`
- `createrawtransaction`
- `sendrawtransaction`

有关更多信息，请参阅 支持的 JSON-RPCs。

分析比特币区块链上的活动

您可以使用 `getchaintxstats` JSON-RPC 方法分析比特币区块链上的交易活动量。此 JSON-RPC 允许您访问诸如每秒平均交易速率、总交易数、区块数等指标。如果需要，您还可以将区块编号窗口或区块哈希定义为分隔符，以计算网络中一组特定区块的统计数据。

有关更多信息，请参阅 支持的 JSON-RPCs。

验证使用比特币 key pair 签名的消息

比特币钱包有一个私钥和一个构成密钥对的公钥。这些密钥用于签署交易，并在区块链上用作用户的身份。公钥用于创建地址，这些地址是标准化的字母数字标识符（长 27 到 34 个字符）。这些地址用于接收 BTC 输出和处理交易或消息。

使用比特币钱包，用户还可以通过加密方式对消息进行签名和验证。此过程通常用于证明特定钱包地址以及与之相关的比特币的所有权。通过使用`verifymessage`比特币 JSON-RPC，您可以检查由另一个钱包签名的消息的真实性和有效性。具体而言，比特币节点可用于验证消息是否已使用与签名消息本身中提供的公钥派生地址相对应的私钥进行签名。

有关更多信息，请参阅 支持的 JSON-RPCs。

查看比特币内存池

许多应用程序需要访问内存池来跟踪待处理的交易、获取所有待处理交易的列表或找出交易的来源。为此，有RPCs 类似比特币 JSON 的`getmempoolancestors`、`getmempoolentry`、、支持`getrawmempool`这项活动。这些比特币 JSON-RPCs 帮助应用程序从内存池中获取所需的信息。

Amazon Managed Blockchain (AMB) Access Bitcoin 还支持`testmempoolaccept`比特币 JSON-RPCs，它允许您在提交之前验证交易是否符合协议规则并且是否会被节点接受。钱包、交易所和任何其他直接向比特币区块链提交交易的实体都使用这些比特币 JSON-RPCs。

有关更多信息，请参阅 支持的 JSON-RPCs。

支持比特币 JSON-RPCs 使用亚马逊托管区块链 (AMB) 访问比特币

本主题提供了托管区块链支持的比特币 JSON 列表和参考文献。RPCs 每个支持的 JSON-RPC 都有其用法的简要描述。

Note

- 您可以使用签名版本 4 (Sigv4) 签名流程RPCs 在托管区块链上对比特币 JSON 进行身份验证。这意味着只有账户中获得授权的 IAM 委托人才能使用比特币 JSON-RPCs 与 AWS 账户进行交互。在呼叫中提供 AWS 凭证（访问密钥 ID 和私有访问密钥）。
- 如果您的 HTTP 响应大于 10 MB，则会出现错误。要更正此问题，必须将压缩标头设置为`Accept-Encoding:gzip`。您的客户端随后收到的压缩响应包含以下标头：`Content-Type: application/json`和`Content-Encoding: gzip`。
- Amazon Managed Blockchain (AMB) Access Bitcoin 会为格式错误的 JSON-RPC 请求生成一个 400 错误。
- 使用 `sendrawtransaction` JSON-RPC 提交更新比特币区块链状态的交易。
- AMB Access Bitcoin 的默认请求限制为每个地区每秒 100 个请求 (RPS)。`NETWORK_TYPE` AWS

  要增加配额，您必须联系AWS 支持人员。要联系 AWS 支持人员，请登录 Support AWS Center 控制台。选择创建案例。选择 “技术”。选择托管区块链作为您的服务。选择 Access: Bitcoin 作为您的类别，选择一般指导作为您的严重性。在主题和描述文本框中输入 RPC 配额，并按每个区域每个比特币网络的 RPS 列出适用于您需求的配额限制。提交您的案例。

支持的 JSON-RPCs

AMB Access 比特币支持以下比特币 JSON-RPCs。每个支持的呼叫都有其用法的简要说明。

类别	JSON-RPC	描述
区块链 RPCs	获取最佳区块哈希	返回工作量最大、经过全面验证的链中最佳（提示）区块的哈希值。

类别	JSON-RPC	描述
	获取区块	如果 verbosity 为 0，则返回一个字符串，该字符串是块 “哈希” 的序列化十六进制编码数据。如果 verbosity 为 1，则返回一个包含有关方块 “哈希” 信息的对象。如果 verbosity 为 2，则返回一个 Object，其中包含有关区块 “哈希” 的信息以及有关每笔交易的信息。如果 verbosity 为 3，则返回一个 Object，其中包含有关区块 “哈希” 的信息以及有关每笔交易的信息，包括`prevout`输入信息。
	获取区块链信息	返回一个包含有关区块链处理的各种状态信息的对象。
	获取区块数	返回工作量最大、经过全面验证的链的高度。创世区块的高度为 0。
	获取区块过滤器	使用区块哈希检索特定区块的 BIP 157 内容过滤器。
	获取区块哈希	返回在提供的高度 best-block-chain处的区块哈希值。
	获取区块标头	如果 verbose 为 false，则返回一个字符串，该字符串是区块标头 “哈希” 的序列化十六进制编码数据。如果 verbose 为真，则返回一个包含有关区块标头 “哈希” 信息的对象。
	获取区块统计信息	计算给定窗口的每个区块的统计信息。所有金额均以中本聪为单位。在某些高度修剪时它不起作用。
	获取链条小贴士	返回有关区块树中所有已知提示的信息，包括主链和孤立分支。
	getchaintxstats	计算有关链中交易总数和交易率的统计数据。
	获得难度	以最低 proof-of-work难度的倍数返回难度。

类别	JSON-RPC	描述
	getmempool 祖先	如果 txid 在内存池中，则返回内存池中的所有祖先。
	获取 mempool 后代	如果 txid 在内存池中，则返回内存池中的所有后代。
	获取内存池条目	返回给定交易的内存池数据。
	获取内存池信息	返回有关 TX 内存池活动状态的详细信息。
	getrawmempool	以字符串事务的 JSON 数组形式返回内存池 IDs 中的所有事务 IDs。 **Note** 不支持 `verbose = true`。
	gettxout	返回有关未使用的交易输出的详细信息。
	gettxoutproof	返回一个十六进制编码的证据，证明区块中包含“txid”。
原始交易 RPCs	创建原始交易	创建使用给定输入并创建新输出的交易。
	decoderaw交易	返回一个表示序列化的十六进制编码交易的 JSON 对象。
	decodescri	解码十六进制编码的脚本。
	获取原始交易	返回原始交易数据。
	发送交易	向本地节点和网络提交原始交易（序列化、十六进制编码）。

类别	JSON-RPC	描述
	测试内存池接受	返回内存池验收测试的结果，该结果表明 mempool 是否接受原始交易（序列化、十六进制编码）。这将检查交易是否违反共识规则或政策规则。
Util RPCs	创建多重签名	创建一个多重签名地址，其中包含 n 个必需的 m 个密钥的签名。
	估算智能费用	如果可能，估算在 conf_target 区块内开始确认交易所需的每千字节的大致费用，并返回该估算值有效的区块数。使用 BIP 141 中定义的虚拟交易规模（见证数据已打折）。
	验证地址	返回有关给定比特币地址的信息。
	验证消息	验证已签名的消息。

亚马逊托管区块链 (AMB) 中的安全访问比特币

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模型将其描述为既是云端的安全性，又是云端的安全：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于Amazon Managed Blockchain (AMB) 访问比特币的合规计划，请参阅按合规计划划分的范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

为了提供数据保护、身份验证和访问控制，Amazon Managed Blockchain 使用了在托管区块链中运行的开源框架的功能和 AWS 功能。

本文档可帮助您了解在使用AMB Access比特币时如何应用分担责任模型。以下主题向您展示如何配置 AMB Access Bitcoin 以满足您的安全与合规目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AMB Access 比特币资源。

主题

亚马逊托管区块链 (AMB) 中的数据保护访问比特币

AWS 分担责任模型分适用于亚马逊托管区块链（AMB）Access Bitcoin中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括当你使用控制台、API 或 AMB Access Bitcoin 或其他 AWS 服务 方式使用时 AWS CLI。 AWS SDKs在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

数据加密

数据加密有助于防止未经授权的用户从区块链网络和相关的数据存储系统读取数据。这包括在网络中传输时可能被拦截的数据，即传输中的数据。

传输中加密

默认情况下，托管区块链使用 HTTPS/TLS 连接来加密从运行的客户端计算机传输到服务端点的所有数据。 AWS CLI AWS

您无需执行任何操作即可使用 HTTPS/TLS。除非您使用命令为单个 AWS CLI 命令明确禁用它，否则它始终处于启用状态。`--no-verify-ssl`

Amazon Managed Blockchain (AMB) 的身份和访问管理访问比特币

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 AMB Access 比特币资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在AMB Access Bitcoin中所做的工作。

服务用户 — 如果您使用 AMB Access Bitcoin 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多的 AMB Access Bitcoin 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 AMB Access Bitcoin 中的某项功能，请参阅Amazon Managed Blockchain (AMB) 访问比特币身份和访问权限疑难解答。

服务管理员 — 如果您负责公司的 AMB Access 比特币资源，那么您可能拥有对 AMB Access Bitcoin 的完全访问权限。你的工作是确定你的服务用户应该访问哪些AMB Access比特币功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何将 IAM 与 AMB Access 比特币结合使用，请参阅亚马逊托管区块链 (AMB) 访问比特币如何与 IAM 配合使用。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 AMB Access Bitcoin 的访问权限。要查看您可以在 IAM 中使用的基于身份的 AMB Access 比特币策略示例，请参阅。Amazon Managed Blockchain (AMB) 访问比特币的基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的AWS 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的 IAM 中的AWS 多重身份验证。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅 AWS IAM Identity Center 用户指南中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括

AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)- SCPs 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。

有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。

- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

亚马逊托管区块链 (AMB) 访问比特币如何与 IAM 配合使用

在使用 IAM 管理 AMB Access Bitcoin 的访问权限之前，请先了解有哪些 IAM 功能可用于 AMB Access Bitcoin。

您可以在亚马逊托管区块链 (AMB) 上使用的 IAM 功能访问比特币

IAM 特征	AMB 访问比特币支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	否
策略条件密钥	否
ACLs	否
ABAC（策略中的标签）	否
临时凭证	否
主体权限	否
服务角色	否

IAM 特征	AMB 访问比特币支持
服务相关角色	否

要全面了解 AMB Access 比特币和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

AMB Access 比特币基于身份的政策

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

AMB Access 比特币基于身份的策略示例

要查看 AMB Access 比特币基于身份的策略示例，请参阅。Amazon Managed Blockchain (AMB) 访问比特币的基于身份的策略示例

AMB Access Bitcoin 内部基于资源的政策

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予

访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

AMB Access Bitcoin 的政策行动

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 AMB Access 比特币操作列表，请参阅《服务授权参考》中的 Amazon Managed Blockchain (AMB) 定义的访问比特币的操作。

AMB Access Bitcoin 中的策略操作在操作前使用以下前缀：

```
managedblockchain:
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "managedblockchain::action1",
      "managedblockchain::action2"
         ]
```

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 `InvokeRpcBitcoin` 开头的所有操作，包括以下操作：

```
"Action": "managedblockchain::InvokeRpcBitcoin*"
```

要查看 AMB Access 比特币基于身份的策略示例，请参阅。Amazon Managed Blockchain (AMB) 访问比特币的基于身份的策略示例

AMB Access Bitcoin 的政策资源

支持策略资源：否

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 AMB Access 比特币资源类型及其列表 ARNs，请参阅《服务授权参考》中的 Amazon Managed Blockchain (AMB) 定义的资源访问比特币。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 A mazon Managed Blockchain (AMB) 定义的操作访问比特币。

要查看 AMB Access 比特币基于身份的策略示例，请参阅。Amazon Managed Blockchain (AMB) 访问比特币的基于身份的策略示例

AMB Access 比特币的政策条件密钥

支持特定于服务的策略条件键：否

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 AMB Access 比特币条件密钥列表，请参阅《服务授权参考》中的 Amazon Managed Blockchain (AMB) 访问比特币的条件密钥。要了解您可以使用哪些操作和资源使用条件密钥，请参阅 Amazon Managed Blockchain (AMB) 定义的操作访问比特币。

要查看 AMB Access 比特币基于身份的策略示例，请参阅。Amazon Managed Blockchain (AMB) 访问比特币的基于身份的策略示例

ACLs 在 AMB 中访问比特币

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC 拥有 AMB 访问比特币

支持 ABAC（策略中的标签）：否

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在 AMB Access Bitcoin 上使用临时证书

支持临时凭证：否

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

AMB Access 比特币的跨服务主体权限

支持转发访问会话（FAS）：否

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

AMB Access Bitcoin 的服务职位

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 AMB Access Bitcoin 的功能。只有在 AMB Access Bitcoin 提供相关指导时才编辑服务角色。

AMB Access Bitcoin 的服务相关角色

支持服务相关角色：否

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

Amazon Managed Blockchain (AMB) 访问比特币的基于身份的策略示例

默认情况下，用户和角色无权创建或修改 AMB Access 比特币资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 AMB Access Bitcoin 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的 Amazon Managed Blockchain (AMB) 访问比特币的操作、资源和条件密钥。ARNs

主题

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除AMB Access比特币资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管式策略或工作职能的AWS 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服

务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 AMB Access 比特币控制台

要访问亚马逊托管区块链 (AMB) Access Bitcoin 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看您 AWS 账户的 AMB Access 比特币资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 AMB Access Bitcoin 控制台，还要将 AMB Access Bitcoin *ConsoleAccess* 或*ReadOnly* AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

访问比特币网络

> **Note**
>
> 为了访问比特币的公共终端节点`mainnet`和`testnet`进行 JSON-RPC 调用，您需要具有 AMB Access Bitcoin 的相应 IAM 权限的用户证书（`AWS_ACCESS_KEY_ID`和`AWS_SECRET_ACCESS_KEY`）。

Example 访问所有比特币网络的 IAM 政策

此示例授予您中的一个 IAM 用户 AWS 账户 访问所有比特币网络的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AccessAllBitcoinNetworks",
            "Effect": "Allow",
```

```
            "Action": [
                "managedblockchain:InvokeRpcBitcoin*"
            ],
            "Resource": "*"
        }
    ]
}
```

Example 访问比特币测试网网络的 IAM 政策

此示例授予您中的 IAM 用户 AWS 账户 访问比特币`testnet`网络的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AccessBitcoinTestnet",
            "Effect": "Allow",
            "Action": [
                "managedblockchain:InvokeRpcBitcoinTestnet"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon Managed Blockchain (AMB) 访问比特币身份和访问权限疑难解答

使用以下信息来帮助您诊断和修复在使用 AMB Access 比特币和 IAM 时可能遇到的常见问题。

主题

- 我无权在 AMB Access Bitcoin 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人访问我 AWS 账户 的 AMB Access 比特币资源

我无权在 AMB Access Bitcoin 中执行操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 managedblockchain::*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 managedblockchain::GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 managedblockchain::*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到错误消息，说您无权执行该iam:PassRole操作，则必须更新您的政策，以允许您将角色传递给AMB Access Bitcoin。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在 AMB Access Bitcoin 中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我 AWS 账户 的 AMB Access 比特币资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 AMB Access Bitcoin 是否支持这些功能，请参阅亚马逊托管区块链 (AMB) 访问比特币如何与 IAM 配合使用。

- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

登录亚马逊托管区块链 (AMB) 使用访问比特币事件 AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain (AMB) Access Bitcoin 不支持管理事件。

Amazon Manage AWS CloudTrail d Blockchain 与一项服务集成，可记录用户、角色或 AWS 服务在托管区块链中采取的操作。 CloudTrail 捕获谁调用了托管区块链的 AMB Access 比特币端点作为数据平面事件。

如果您创建了经过正确配置的跟踪以接收所需的数据平面事件，则可以连续接收与 AMB Access Bitcoin 相关的事件发送到 Amazon CloudTrail S3 存储桶。使用收集的信息 CloudTrail，您可以确定是否向其中一个 AMB Access Bitcoin 端点发出了请求、请求来自哪个 IP 地址、谁发出了请求、发出请求的时间以及其他详细信息。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail 用户指南。

AMB 访问比特币信息 CloudTrail

AWS CloudTrail 创建时默认处于启用状态 AWS 账户。但是，要查看谁调用了 AMB Access 比特币端点，您必须配置 CloudTrail 为记录数据平面事件。

要持续记录您的事件 AWS 账户，包括AMB Access Bitcoin的数据平面事件，您必须创建跟踪。跟踪可以 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在中创建跟踪时 AWS Management Console，该跟踪将应用于所有跟踪 AWS 区域。跟踪记录 AWS 分区中所有受支持区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务以进一步分析这些数据并对 CloudTrail 日志中收集的事件数据采取行动。有关更多信息，请参阅下列内容：

- 用于 CloudTrail 追踪比特币 JSON-RPCs
- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

通过分析 CloudTrail 数据事件，您可以监控谁调用了 AMB Access 比特币端点。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 AMB Access 比特币日志文件条目

对于数据平面事件，跟踪是一种配置，允许将事件作为日志文件传送到指定的 S3 存储桶。每个 CloudTrail 日志文件都包含一个或多个日志条目，这些条目代表来自任何来源的单个请求。这些条目提供有关请求操作的详细信息，包括操作的日期和时间以及任何相关的请求参数。

> **Note**
>
> CloudTrail 日志文件中的数据事件不是 AMB Access Bitcoin API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

用于 CloudTrail 追踪比特币 JSON-RPCs

您可以使用 CloudTrail 来跟踪您的账户中谁调用了 AMB Access 比特币端点，以及调用了哪些 JSON-RPC 作为数据事件。默认情况下，当您创建跟踪时，不会记录数据事件。要记录谁将 AMB Access Bitcoin 端点调用为 CloudTrail 数据事件，您必须明确添加要为其收集活动的支持的资源或资源类型。Amazon Managed Blockchain 支持使用 AWS Management Console、 AWS 软件开发工具包和来添加数据事件 AWS CLI。有关更多信息，请参阅AWS CloudTrail 用户指南中的使用高级选择器记录事件。

要在跟踪中记录数据事件，请在创建跟踪后使用put-event-selectors操作。使用该`--advanced-event-selectors`选项指定`AWS::ManagedBlockchain::Network`资源类型，以便开始记录数据事件，从而确定谁调用了 AMB Access Bitcoin 端点。

Example 所有账户的 AMB Access 比特币端点请求的数据事件日志条目

以下示例演示了如何使用该`put-event-selectors`操作来记录您账户`us-east-1`在该区域跟踪`my-bitcoin-trail`的所有AMB Access Bitcoin终端节点请求。

```
aws cloudtrail put-event-selectors \

--region us-east-1 \
--trail-name my-bitcoin-trail  \
--advanced-event-selectors '[{
    "Name": "Test",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::ManagedBlockchain::Network"] } ]}]'
```

订阅后，您可以跟踪连接到上一个示例中指定的跟踪的 S3 存储桶中的使用情况。

以下结果显示了由收集的信息 CloudTrail 的数据事件日志条目 CloudTrail。您可以确定比特币 JSON-RPC 请求是向其中一个 AMB Access Bitcoin 端点发出的，请求来自哪个 IP 地址，谁发出了请求，何时发出请求，以及其他详细信息。


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROA554UO62RJ7KSB7FAX:777777777777",
            "arn": "arn:aws:sts::111122223333:assumed-role/Admin/777777777777",
            "accountId": "111122223333"
        },
        "eventTime": "2023-04-12T19:00:22Z",
        "eventSource": "managedblockchain.amazonaws.com",
        "eventName": "getblock",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "111.222.333.444",
        "userAgent": "python-requests/2.28.1",
        "errorCode": "-",
        "errorMessage": "-",
        "requestParameters": {
            "jsonrpc": "2.0",
            "method": "getblock",
            "params": [],
            "id": 1
        },
        "responseElements": null,
        "requestID": "DRznHHEjIAMFSzA=",
        "eventID": "baeb232d-2c6b-46cd-992c-0e4033aace86",
        "readOnly": true,
        "resources": [{
```

```
            "type": "AWS::ManagedBlockchain::Network",
            "ARN": "arn:aws:managedblockchain:::networks/n-bitcoin-mainnet"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data"
}
```

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。