



Moonbeam开发进阶课程

许可预编译

PureStake开发者关系团队



课程导航

EIP-2612许可
概述

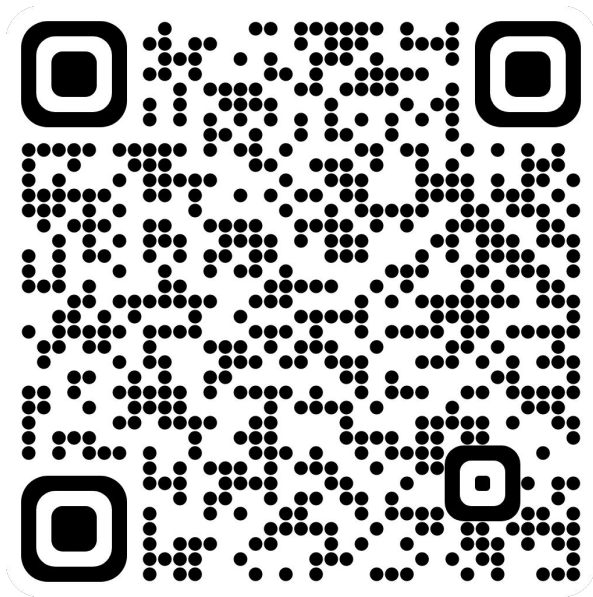
Moonbeam
许可预编译

示例
:xcUNITBridge (3)

生成
secp256k1
签名

课程资源GitHub Repo

<https://github.com/PureStake/moonbuilders-academy/tree/main/chinese/advanced-course>





EIP-2612许可概述

EIP-2612: 许可 (EIP-712 签署授权)


- 是对ERC-20标准授权 (Approve) 功能的延伸
- ERC-20授权设计的局限性：
 - 用户需要签署两笔交易：1. 授权 2. 智能合约上调用包含TransferFrom的方法（比如各类DEX）
 - 用户必须持有ETH才可以调用ERC-20授权等方法，包括简单转帐
- EIP-2612为ERC-20标准添加一个新方法：许可 (Permit)，允许定义另外一个地址来支付调用授权的Gas
- 签署交易的格式按照 EIP-721中的定义格式

EIP-712: 类型化数据结构哈希和签名


- 对类型化数据结构哈希和签名的标准, 优化可读性, 而不仅是字节串

```
{
  type: 'object',
  properties: {
    types: {
      type: 'object',
      properties: {
        EIP712Domain: {type: 'array'},
      }
      required: ['EIP712Domain']
    },
    primaryType: {type: 'string'},
    domain: {type: 'object'},
    message: {type: 'object'}
  },
  required: ['types', 'primaryType', 'domain', 'message']
}
```

MetaMask Notification

CONFIRM TRANSACTION 

Sign Message


 Account...

ADDRESS 0x5409ED02...A631

BALANCE 0.10 ETH

DOMAIN Ether Mail version 1


URL ✓ https://ether-mail.eth

CONTRACT  0xCcCCccccCCCCcC...cccC

Mail


from Person

name "Alice"

wallet  0xaAaAaaAa...aaAa

to Person

name "Bob"

wallet  0xbBbBBBBbbB...BBbB

contents "Hello, Bob!"

CANCEL SIGN



Moonbeam许可预编译

许可预编译: 交易许可的执行条件

- 当前的系统时间小于或等于许可截止时间
- owner 不是零地址
- nonces[owner] (在状态更新之前) 等于 nonce
- r、s 和 v 是来自消息所有者的有效 secp256k1 签名



主要使用场景: Gasless交易

- 让用户没有原生代币也可以与智能合约交互, 只需要签署交易的许可
- 可以应用于Gasless Swap, 铸造, 转帐等
- Biconomy协议提供这个功能的集成



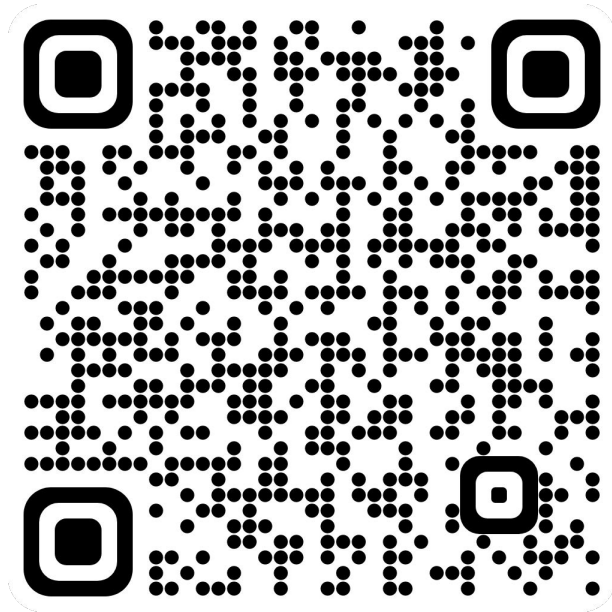
许可预编译接口定义

方法:

- **dispatch**(*address from, address to, uint256 value, bytes data, uint64[] gaslimit, uint256 deadline, uint8 v, bytes32 r, bytes32 s*) — 代表其他用户调用EIP-712许可。
 - *from* - 此许可的签名者, 调用将会代表此地址被调度
 - *to* - 接收调度的调用地址
 - *value* - 从*from*账户转移的数值
 - *data* - 调用所需的数据, 或是要执行的操作
 - *gasLimit* - 调度此调用所需的Gas限制。开发者能够为此参数提供一个参数以防止调度人操纵Gas限制
 - *deadline* - 许可截止时间, 以UNIX系统时间为单位
 - *v* - 签名的恢复ID, 整个签名串的最后一个字节
 - *r* - 签名串的首32个字节
 - *s* - 签名串的第二个32个字节
- **nonces**(*address owner*) - 返回参数钱包的Nonce
- **DOMAIN_SEPARATOR**() - 返回用于避免重复攻击的EIP-712域名分隔器, 跟随[EIP-2612](#)实现

CallPermit.sol

<https://github.com/PureStake/moonbeam/blob/master/precompiles/call-permit/CallPermit.sol>





许可预编译示例： xcUNITBridge示例(3)

实现Gasless一键式跨链转帐流程

1. 使用签署者账户签署执行批处理交易的许可
2. 批处理交易的内容为：
 - 子调用 1: 在xcUNIT ERC20合约上授权 X 数额
 - 子调用 2: 在xcUNITBridge合约上调用
send_tokens方法
3. 使用交易付费账户调用许可预编译的Dispatch方法
执行许可

- [illegible]



生成secp256k1签名 (r,s,v)