

# Project A: Smart Contract 報告

資工所 R08922156 黃劍韜

## (a) Code

```
pragma solidity ^0.4.24;

// -----
// 'R08922156Coin' token contract
//
// Symbol      : R08922156
// Name        : R08922156Coin
// Total supply: 1000000000000000000
// Decimals    : 18
// -----

contract Token{
    uint256 public totalSupply;

    function totalSupply() public constant returns (uint);
    function balanceOf(address _owner) public constant returns (uint256 balance);
    function transfer(address _to, uint256 _value) public returns (bool success);
    function transferFrom(address _from, address _to, uint256 _value) public returns (bool success);
    function approve(address _spender, uint256 _value) public returns (bool success);
    function allowance(address _owner, address _spender) public constant returns (uint256 remaining);
    event Transfer(address indexed _from, address indexed _to, uint256 _value);
    event Approval(address indexed _owner, address indexed _spender, uint256 _value);
}

contract TokenDemo is Token {

    string public name;
    uint8 public decimals;
    string public symbol;

    function TokenDemo(uint256 _initialAmount, string _tokenName, uint8 _decimalUnits, string _tokenSymbol) public {
        totalSupply = _initialAmount * 10 ** uint256(_decimalUnits);
        balances[msg.sender] = totalSupply;

        name = _tokenName;
        decimals = _decimalUnits;
        symbol = _tokenSymbol;
    }

    function transfer(address _to, uint256 _value) public returns (bool success) {
        require(balances[msg.sender] >= _value && balances[_to] + _value > balances[_to]);
        require(_to != 0x0);
        balances[msg.sender] -= _value;
        balances[_to] += _value;
        Transfer(msg.sender, _to, _value);
        return true;
    }

    function transferFrom(address _from, address _to, uint256 _value) public returns (bool success) {
        require(balances[_from] >= _value && allowed[_from][msg.sender] >= _value);
        balances[_to] += _value;
        balances[_from] -= _value;
        allowed[_from][msg.sender] -= _value;
        Transfer(_from, _to, _value);
        return true;
    }

    function balanceOf(address _owner) public constant returns (uint256 balance) {
        return balances[_owner];
    }

    function approve(address _spender, uint256 _value) public returns (bool success) {
        allowed[msg.sender][_spender] = _value;
        Approval(msg.sender, _spender, _value);
        return true;
    }

    function allowance(address _owner, address _spender) public constant returns (uint256 remaining) {
        return allowed[_owner][_spender];
    }

    mapping (address => uint256) balances;
    mapping (address => mapping (address => uint256)) allowed;
}
```

## (b) The address of contract

The address of contract: 0x0e796c04838852af1fe82a3a3c18514f626adf8f

This screenshot shows the 'Transaction Details' page on Etherscan for the Ropsten Testnet. The transaction is successful and has 198 block confirmations. The 'Interacted With (To):' field is highlighted with a red box, showing the contract address 0x0e796c04838852af1fe82a3a3c18514f626adf8f. The transaction value is 0 Ether, and the fee is 0.0012907237 Ether.

Field	Value
Transaction Hash	0x026baa94aa8ecb31eaa3fbf175ae17695b2d96a5c9606c2cd24a166209c1e8
Status	Success
Block	897925 (198 Block Confirmations)
Timestamp	1 hr 47 mins ago (Oct-31-2020 09:28:02 AM +UTC)
From	0x378ecc6607dc5dca7b97d2b2a06b06169874da8
Interacted With (To)	Contract 0x0e796c04838852af1fe82a3a3c18514f626adf8f
Tokens Transferred	From 0x378ecc6607dc5d... To 0xd2448ac204465a... For 1,000 "R08922156Coin" ("R0892...")
Value	0 Ether (\$0.00)
Transaction Fee	0.0012907237 Ether (\$0.000000)
Gas Price	0.0000000241 Ether (24.1 Gwei)

## (c) Screenshot of transaction on Etherscan

This screenshot shows the 'Contract Overview' page for the address 0x0e796c04838852af1fe82a3a3c18514f626adf8f. The balance is 0 Ether. The 'Transactions' tab is active, showing a list of transactions. The first transaction is highlighted with a red box, showing it was sent from 0x378ecc6607dc5dca7b97d2b2a06b06169874da8 to the contract address for 0 Ether.

Txn Hash	Block	Age	From	To	Value	[Txn Fee]
0x026baa94aa8ecb31...	897925	1 hr 51 mins ago	0x378ecc6607dc5dca...	0x0e796c04838852af1...	0 Ether	0.0012907237
0x96bb5d7700c0629...	897984	2 hrs 14 mins ago	0x378ecc6607dc5dca...	Contract Creation	0 Ether	0.003299716

This screenshot shows the 'Address Overview' page for the address 0xd2448ac204465ab30e20652421fa70b5da8f8d15. The balance is 11.466050339035 Ether. The 'Transactions' tab is active, showing a list of transactions. The first transaction is highlighted with a red box, showing it was sent from 0x378ecc6607dc5dca7b97d2b2a06b06169874da8 to the address for 1,000 tokens.

Txn Hash	Age	From	To	Value	Token
0x026baa94aa8ecb31...	1 hr 54 mins ago	0x378ecc6607dc5dca...	0xd2448ac204465ab3...	1,000	"R08922156Coin" ("R0892...")
0xd53dded2cd19238...	2 hrs 3 mins ago	0x160d24845489ce9a...	0xd2448ac204465ab3...	999	R08922112 (YIWEI)
0x9ddc110590f114d40...	4 days 3 hrs ago	0x6e061eb9c81da31f8...	0xd2448ac204465ab3...	1,000	R08922159Col... (SIYUE)