

Myshell Testnet Smart Contract Initial Test Report

Version 0.1

David Zhang

February 21, 2024

Myshell Testnet Smart Contract Test Report

David Zhang

February 21, 2024

Myshell Testnet Smart Contract Test Report

Prepared by: David Zhang

Table of contents

See table

- 1. 合约部署与测试
- 1.1 ERC-20 合约测试
- 1.2 ERC-20 测试分析报告
- 1.3 ERC-721 合约测试
- 1.4 ERC-721 测试分析报告
- 2. Ethers 脚本测试
- 2.1 provider 测试
- 2.2 wallets & send transaction 测试
- 2.3 contract_calldata 测试
- 2.4 contract_read 测试
- 2.5 contract_write 测试
- 2.6 Etheres 测试分析报告

Environment settings

- Hardhat
- Solidity
- Openzeppelin
- ERC-20, ERC-721
- Javascript
- Myshell Testnet
- Chain ID: 202402181658
- Rollup Stack Type: OP Stack
- Settlement Chain ID: 11155111
- Settlement Layer: Sepolia Test
- Rpc url: <https://myshell-testnet.alt.technology>
- Explorer: <https://myshell-testnet-explorer.alt.technology>
- Bridge: <https://op-bridge.alt.technology/deposit?id=202402181658>

1. 合约部署与测试

1.1 ERC-20合约测试

- 合约介绍: 本智能合约名为 `TestToken`, 代币符号为“TT”。它是基于以太坊的ERC-20标准实现的一种代币合约。合约部署时, 构造函数接受一个`initialSupply`参数, 即初始供应量, 代表首次铸造代币的数量。合约使用`_mint`函数在部署时向部署者(`msg.sender`)的地址铸造初始供应量的代币。
- 部署步骤:

00-deploy-token.js

```
const { network } = require("hardhat")
const { INITIAL_SUPPLY } =
require("../helper-hardhat-config")

module.exports = async ({ getNamedAccounts, deployments })
  => {
  const { deploy, log } = deployments
  const { deployer } = await getNamedAccounts()
  const chainId = network.config.chainId

  log("Deploying TestToken On Myshell", chainId)

  const token = await deploy("TestToken", {
    from: deployer,
    log: true,
    args: [INITIAL_SUPPLY],
  })

  log("TestToken Deployed!")
  log("TestToken Address is:", token.address)

  log("-----")
}

module.exports.tags = ["all", "token"]
```

● 部署结果：

- 测试用例:[F-1] transfer功能

[F-1] TestToken::transfer

Script Code: [Github](#)

测试结果：

Transaction details

- 测试用例:[F-2] approve & transferFrom功能

[F-2] TestToken::approve & transferFrom

Script Code: [Github](#)

测试结果：

Transaction details	
Details	Token transfers
This is a testnet transaction only	
Transaction hash 0x1c4f6d938575dd31dccaf630f9f041a792fc5e6ba711cfef0d4b183deb40796 ⓘ	
Status and method	Success 0x23b872dd
Block 33555 4 Block confirmations	
Timestamp 32s ago Feb 21 2024 18:20:24 PM (+07:00 UTC) Confirmed within <= 8 secs	
From  0xA5b71068da164ECafAB295838f775Fe90764f786 ⓘ	
Interacted with contract  TestToken ⓘ ✓	
Tokens transferred 0xeb...A367 ⓘ → 0xA5...f786 ⓘ For: 25  TestToken (TT)	

1.2 ERC-20 测试分析报告

- **TestToken**合约的部署：
 - TestToken(TT) ERC-20智能合约已成功部署在Myshell测试网上。
 - 该交易在 8 秒内被挖掘并确认，表明网络健康且延迟低。
 - 总共使用了 966.013 个天然气单位，这对于合同部署来说是合理的数量。

- #### • 代币Transfer测试:

- 从一个账户向另一个账户进行了 10 TT 的代币转账, 成功。
 - 该交易使用了 35,110 个 Gas 单位, 这是 ERC-20 代币转移的典型值。
 - 传输很快就得到了确认, 不到8秒, 表明网络状况保持稳定。

- **approve和transferFrom测试:**

- 25 TT 已获得批准，并且 TransferFrom 函数已成功调用。
- 该交易使用的gas为36,573，比简单的转账略多，这是由于transferFrom函数的额外复杂性而预计的。
- 同样，交易在 8 秒内得到确认，保持了一致的性能。

总体而言，Myshell 测试网运行可靠，交易确认快速且 Gas 使用合理。这些交易为 TestToken 智能合约的部署和功能提供了信心，表明它的行为符合测试网上传输和批准等基本操作的预期。建议在任何主网部署之前进行进一步的测试，包括边缘情况和故障模式，以进行全面评估。

1.3 ERC-721合约测试

- 合约介绍:本智能合约名为 TestNFT，非同质化代币符号为“DOG”。它是基于以太坊的ERC-721标准实现的一种非同质化代币合约。合约使用mint函数为用户提供NFT铸造，NFT存储在去中心化存储服务IPFS网络。
- 部署步骤:

01-deploy-nft.js

```
const { network } = require("hardhat")
module.exports = async ({ getNamedAccounts, deployments })
=> {
  const { deploy, log } = deployments
  const { deployer } = await getNamedAccounts()
  const chainId = network.config.chainId

  log("Deploying TestNFT On Myshell", chainId)

  const nft = await deploy("TestNFT", {
    from: deployer,
    log: true,
    args: [],
  })

  log("TestNFT Deployed!")
  log("TestNFT Address is:", nft.address)
```

```
    log("-----")
}
module.exports.tags = ["all", "nft"]
```

- 部署结果：

```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
● HOSANNAdeMacBook-Air:Myshell-Test hosanna$ yarn hardhat deploy --network myshell --tags nft
yarn run v1.22.19
warning package.json: No license field
$ /Users/hosanna/Myshell-Test/node_modules/.bin/hardhat deploy --network myshell --tags nft
Nothing to compile
Deploying TestNFT On Myshell 202402181658
deploying "TestNFT" (tx: 0x5804f16a846453fd697f076929e4ce801a96127dda8ead826156626e3ffdef08)...: deployed at 0x62D1b1D72D83c1caC7AD6C59FcD05A6990f5ea59
TestNFT Deployed!
TestNFT Address is: 0x62D1b1D72D83c1caC7AD6C59FcD05A6990f5ea59
'-' Done in 16.78s.
```

- 测试用例:[F-1] mint功能

[F-1] TestToken::mint

Script Code: [Github](#)

测试结果:

Transaction details

This is a testnet transaction only

Transaction hash	0x38d22fd96ac0868e7aa46df78f4204f79999688e901d1cf911dbb99986254dde
Status and method	Success 0xc2229fea
Block	34257 6 Block confirmations
Timestamp	41s ago Feb 21 2024 19:54:00 PM (+07:00 UTC) Confirmed within <= 8 secs
From	0xeb23E1a2784931A65D671DaA1235c8ae6435A367
Interacted with contract	Dogie
Tokens minted	0x00...0000 → 0xeb...A367 For token ID: 0 T Dogie (DOG)

<input type="checkbox"/> Value	0 ETH (\$0)
<input type="checkbox"/> Transaction fee	0.00000011324866215 ETH (\$0.000331832169938958)
<input type="checkbox"/> Gas price	0.000000000000100005 ETH (0.00100005 Gwei)
<input type="checkbox"/> Gas usage & limit by txn	113,243 113,243 100%
<input type="checkbox"/> Gas fees (Gwei)	Base: 0.00000005 Max: 0.001000063 Max priority: 0.001
<input type="checkbox"/> Burnt fees	0.00000000000566215 ETH (\$0.00000016590778958)
Hide details	
<input type="checkbox"/> Other	Txn type: 2 (EIP-1559) Nonce: 19 Position: 1
<input type="checkbox"/> Raw input	<div style="display: flex; align-items: center;"> Hex Raw </div> <pre>0xc2229fea</pre>

```
● HOSANNAdeMacBook-Air:Myshell-Test hosanna$ yarn hardhat run scripts/mint.js --network myshell
yarn run v1.22.19
warning package.json: No license field
$ /Users/hosanna/Myshell-Test/node_modules/.bin/hardhat run scripts/mint.js --network myshell
Minting...
Waiting for transactions to be mined...
Transaction successfully...
Transaction Hash: 0x38d22fd96ac0868e7aa46df78f4204f79999688e901d1cf911dbb99986254dde
Transaction Details: {
  hash: '0x38d22fd96ac0868e7aa46df78f4204f79999688e901d1cf911dbb99986254dde',
  type: 2,
  accessList: [],
  blockHash: '0x244be95f324ea701c0004eb5e7fb16b1becb2143061d7ee92a62a7fb04608b1c',
  blockNumber: 34257,
  transactionIndex: 1,
  confirmations: 1,
  from: '0xeb23E1a2784931A65D671DaA1235c8ae6435A367',
  gasPrice: BigNumber { _hex: '0x0f4272', _isBigNumber: true },
  maxPriorityFeePerGas: BigNumber { _hex: '0x0f4240', _isBigNumber: true },
  maxFeePerGas: BigNumber { _hex: '0x0f427f', _isBigNumber: true },
  gasLimit: BigNumber { _hex: '0x1ba5b', _isBigNumber: true },
  to: '0x6201b10720831caC7AD6C59FcD05A6900f5ea59',
  value: BigNumber { _hex: '0x00', _isBigNumber: true },
  nonce: 19,
  data: '0xc2229fea',
  r: '0x1d757a29d9dce829daa4c3f821045cb7032f4c16e1c5022f4ffdd7fdca52814',
  s: '0x594b0fa85176c5020eb12a53a4971d33e9b33401b91cd105d73162c3503455bb',
  v: 1
  creates: null,
  chainId: 202402181658,
  wait: [Function (anonymous)]
}
Block Timestamp: 2024-02-21T12:54:00.000Z
Current Token ID: 0
Token ID 0 exists: true
Token ID 0 URI: ipfs://bafybeig37ioir76s7mg5oobetncojcm3c3hxasyd4rvid4jqhy4gkaheg4/?filename=0-PUG.json
+ Done in 14.26s.
○ HOSANNAdeMacBook-Air:Myshell-Test hosanna$
```

- 测试用例:[F-2] approve & safeTransferFrom功能

[F-2] TestToken::approve & safeTransferFrom

Script Code: [Github](#)

测试结果:

Transaction details

Details Token transfers Internal txns Logs State Raw trace

 Status and method Success 0x23b873dd

 Block 34348 | 3 Block confirmations

⌚ **Timestamp** ⌚ 20s ago | Feb 21 2024 20:06:08 PM (+07:00 UTC) | Confirmed within <= 8 secs

From 0xA5b71068da164ECafAB295838f775Fe90764f786

 Interacted with contract

④ Tokens transferred 0xeb...A367 ④ → 0xA5...f786 ④ For token ID: ⚡ 0 T Dogie (DOG)

 Value 0 ETH (\$0)

 Transaction fee 0.0000005628981435 ETH (\$0.000164935910823222)

 Gas price 0.00000000000100005 ETH (0.00100005 Gwei)

Gas usage & limit by txn 56,287 / 65,887 85.43%

 Gas fees (Gwei) Base: 0.00000005 | Max: 0.0010000003 | Max priority: 0.001

[Hide details](#)

ⓘ Other Txn type: 2 (EIP-1559) | Nonce: 1 | Position: 1

Raw Input

Hex ▾

5

1.4 ERC-721 测试分析报告

- TestNFT合约的部署：

- TestNFT(DOG)ERC-721智能合约已成功部署在Myshell测试网上。
 - 该部署消耗了大量的 Gas(1,745,536 个 Gas 单位), 这对于 ERC-721 等更复杂的合约类型来说是预计的。

- NFT 的mint测试:

- 如“代币铸造”部分所示, NFT 已成功铸造。
 - 交易在8秒内得到确认, 显示了网络效率。
 - 用于铸造的天然气用量为 113,243 单位, 在

- NFT safeTransferFrom 测试：

- NFT 已成功从原所有者转移到另一个用户。
 - 此次转账使用了 56,287 个气体单位，也在 8 秒内得到确认。
 - 这些交易的成功执行表明智能合约正在按照铸造和转移代币的预期运行。

Myshell 测试网的整体性能看起来稳定高效，所有交易都处理得很快。Gas 使用量与 ERC-721 操作的预期成本一致。该测试阶段并未表明智能合约的部署、铸造和转移功能存在任何问题。

2 Ethers 脚本测试

- 脚本介绍: 使用以太坊开发中的一个著名库 Ethers.js 编写脚本来测试 Myshell sepolia 各种功能以及与以太坊区块链的交互, 包括 provider, wallets 等测试。Ethers.js 提供了一套全面的实用程序来与以太坊及其生态系统进行交互, 使其成为开发人员编写测试、部署合约以及与区块链交互的流行选择。
- 测试用例:[F-1] provider 功能

[F-1] Provider

Script Code: [Github](#)

测试结果:

```
● HOSANNAdeMacBook-Air:myshell-test hosanna$ yarn hardhat run scripts/providers.js --network myshell
yarn run v1.22.19
warning package.json: No license field
$ /Users/hosanna/chain-test/myshell-test/node_modules/.bin/hardhat run scripts/providers.js --network myshell
Current network chainId: 202402181658
Current block number 43597
user one balance is 0.3972920926848051
1.5 ETH is 1.5
user two balance is 0.099947677388026092
userOneBalance more than userTwoBalance
user one balance has: 0.3972920926848051
user two balance has: 0.099947677388026092
userTwoBalanceAfter more than userOneBalanceBefore
user one balance has: 0.3972920926848051
user two balance has: 5000.099947677388026092
✨ Done in 4.92s.
```

- 测试用例:[F-2] wallets 功能

[F-1] Wallets

Script Code: [Github](#)

测试结果:

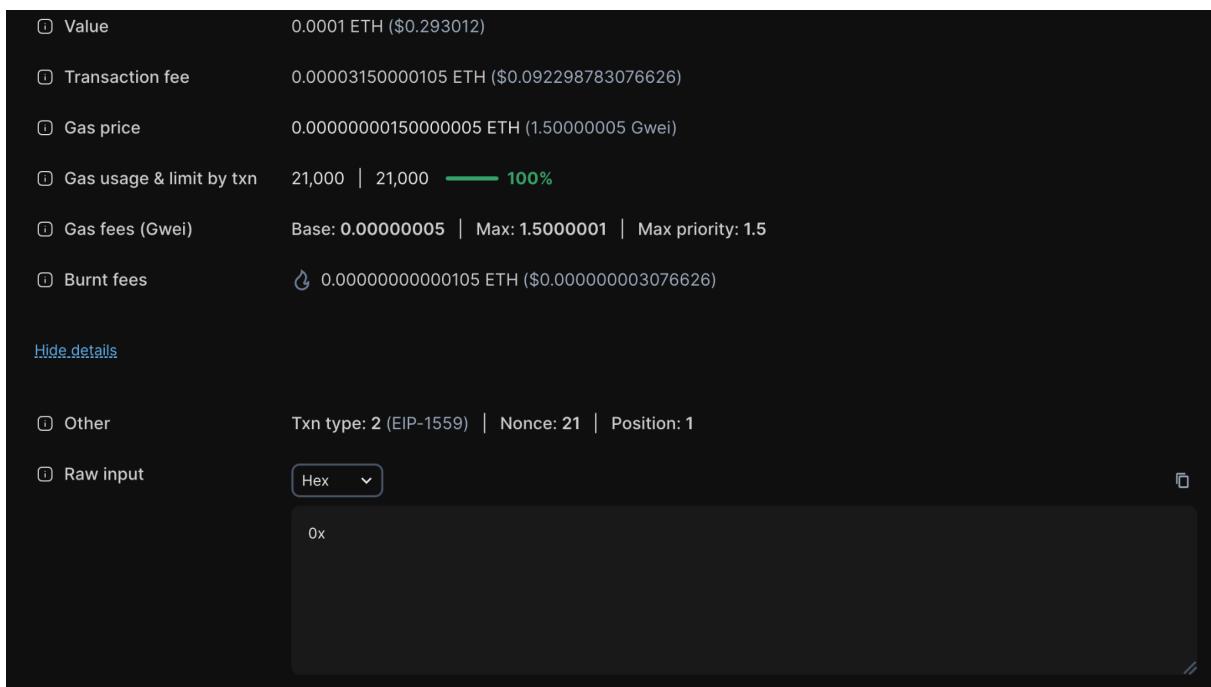
```
● HOSANNAdeMacBook-Air:myshell-test hosanna$ yarn hardhat run scripts/wallets.js --network myshell
yarn run v1.22.19
warning package.json: No license field
$ /Users/hosanna/chain-test/myshell-test/node_modules/.bin/hardhat run scripts/wallets.js --network myshell
Current network chainId: 202402181658
address: 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private Key: 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
mnemonic: impact stick sun position amount cinnamon claim nerve clarify discover custom mechanic
address: 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 1 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 1 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 2 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 2 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 3 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 3 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 4 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 4 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 5 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 5 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 6 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 6 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 7 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 7 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 8 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 8 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
address: 9 0x98740d8c00e57d8e070d23f6594a531cb089f17c1
private key: 9 0x670917599f3dc7a3decf1b8e16fe2791a3b73bffd3c8301ba22f282893fed8f
My wallet address(from private key): 0xeb23E1a2784931A65D671DaA1235c8ae6435A367
Is signer? true
Signed message 0xe0e3c3a813b1ba10e2d9899f092ca25a86b9de62c46ef631e99064eebc7612c56c07450af17d0624263d16651ea42f9409509c089f489b463c89bd53a880611c1c
signerAddress 0xeb23E1a2784931A65D671DaA1235c8ae6435A367
EOA address 0xeb23E1a2784931A65D671DaA1235c8ae6435A367
my Balance 0.397423694828158552
my Address 0xeb23E1a2784931A65D671DaA1235c8ae6435A367
user two balance is 0.099847677388026092
send transaction to user2
sending...
```

```
type: 2,
chainId: 202402181658,
nonce: 21,
maxPriorityFeePerGas: BigNumber { _hex: '0x59682f00', _isBigNumber: true },
maxFeePerGas: BigNumber { _hex: '0x59682f64', _isBigNumber: true },
gasPrice: null,
gasLimit: BigNumber { _hex: '0x5208', _isBigNumber: true },
to: '0xA5b71068da164ECafAB295838f775Fe90764f786',
value: BigNumber { _hex: '0x5af3107a4000', _isBigNumber: true },
data: '0x',
accessList: [],
hash: '0x01823b1f15b5a79b99e36f6209e994b51d4f17518b18c53ca98016ffca66a8a1',
v: 1,
r: '0x25bf2060a778badcc60b9ce33a48cc75c28c0375646731dccbf3e487f1fac05b',
s: '0x6eb210b6d9b569d9dc265a3f32ccf72526288f586d5fa32875925794082f5c11',
from: '0xeb23E1a2784931A65D671DaA1235c8ae6435A367',
confirmations: 0,
wait: [Function (anonymous)]  
}  
block confirmation...  
Transaction successfully...  
Transaction Hash: 0x01823b1f15b5a79b99e36f6209e994b51d4f17518b18c53ca98016ffca66a8a1  
Transaction Details: {  
  hash: '0x01823b1f15b5a79b99e36f6209e994b51d4f17518b18c53ca98016ffca66a8a1',  
  type: 2,  
  accessList: [],  
  blockHash: '0x594e48fe0341184163c5bfe4e1e1542ea817ab7656cab0436fd00265480a6d36',  
  blockNumber: 43492,  
  transactionIndex: 1,  
  confirmations: 3,  
  from: '0xeb23E1a2784931A65D671DaA1235c8ae6435A367',  
  gasPrice: BigNumber { _hex: '0x59682f32', _isBigNumber: true },  
  maxPriorityFeePerGas: BigNumber { _hex: '0x59682f00', _isBigNumber: true },  
  maxFeePerGas: BigNumber { _hex: '0x59682f64', _isBigNumber: true },  
  gasLimit: BigNumber { _hex: '0x5208', _isBigNumber: true },  
  to: '0xA5b71068da164ECafAB295838f775Fe90764f786',  
  value: BigNumber { _hex: '0x5af3107a4000', _isBigNumber: true },  
  nonce: 21,  
  data: '0x',  
  r: '0x25bf2060a778badcc60b9ce33a48cc75c28c0375646731dccbf3e487f1fac05b',  
  s: '0x6eb210b6d9b569d9dc265a3f32ccf72526288f586d5fa32875925794082f5c11',  
  v: 1,  
  creates: null,  
  chainId: 202402181658,  
  wait: [Function (anonymous)]  
}  
Block Timestamp: 2024-02-22T09:25:20.000Z
```

Transaction details

This is a testnet transaction only

Details	Token transfers	Internal txns	Logs	State	Raw trace
<p>ⓘ Transaction hash 0x01823b1f15b5a79b99e36f6209e994b51d4f17518b18c53ca98016ffca66a8a1 ⓘ</p> <p>ⓘ Status and method Success</p> <p>ⓘ Block 43492 72 Block confirmations</p> <p>ⓘ Timestamp ⏰ 10m ago Feb 22 2024 16:25:20 PM (+07:00 UTC) Confirmed within <= 8 secs</p> <p>ⓘ From 0xeb23E1a2784931A65D671DaA1235c8ae6435A367 ⓘ</p> <p>ⓘ To 0xA5b71068da164ECafAB295838f775Fe90764f786 ⓘ</p>					



- 合约介绍: 基于ERC721标准的NFT集合, 名为"Crypto Devs", 符号为"CD"。合约设定了NFT的最大数量为20个, 并且设定了每个NFT的价格为0.0001以太币。合约通过引入一个白名单合约, 为白名单中的地址保留了一定数量的NFT, 以确保这些地址能够优先获得NFT。合约中还包含了一个铸币函数, 允许用户根据是否在白名单中以及是否支付了足够的以太币来铸造NFT。此外, 合约拥有者可以通过提款函数将合约中积累的所有以太币提取出来。
- 部署步骤:

02-deploy-cd.js

```
const { network } = require("hardhat")

const MAX_WHITE_LISTED_ADDRESSES = 200

module.exports = async ({ getNamedAccounts, deployments }) =>
{
  const { deploy, log } = deployments
  const { deployer } = await getNamedAccounts()
  const chainId = network.config.chainId

  log("Deploying Whitelist On Myshell", chainId)

  const list = await deploy("Whitelist", {
    from: deployer,
    log: true,
```

```

        args: [MAX_WHITE_LISTED_ADDRESSES],
    }

log("Deploying CryptoDevs On Myshell", chainId)

const cd = await deploy("CryptoDevs", {
    from: deployer,
    log: true,
    args: [list.address],
})

log("CryptoDevs Deployed!")
log("CryptoDevs Address is:", cd.address)

log("-----")
}

module.exports.tags = ["all", "cd"]

```

● 部署结果:

```

HOSANNAdeMacBook-Air:myshell-test hosanna$ yarn hardhat deploy --network myshell --tags cd
yarn run v1.22.19
warning package.json: No license field
$ /Users/hosanna/chain-test/myshell-test/node_modules/.bin/hardhat deploy --network myshell --tags cd
Compiled 1 Solidity file successfully (evm target: paris).
Deploying Whitelist On Myshell 202402181658
reusing "Whitelist" at 0x75621FC47aaaf29bd7BD0bbdB77b0203E7684F776
Deploying CryptoDevs On Myshell 202402181658
deploying "CryptoDevs" (tx: 0xc4de0574b974e2b20beaf47d2be35a5020e0fd290761f3a69804d194cc3c33f5)...: deployed at 0x080849A3dee93E16C
e12bDe9B27b99ceC3EbbaC with 2722547 gas
CryptoDevs Deployed!
CryptoDevs Address is: 0x080849A3dee93E16Ce12bDe9B27b99ceC3EbbaC
: Done in 13.28s.

```

Whitelist.sol

Transaction details

- [Details](#) [Token transfers](#) [Internal txns](#) [Logs](#) [State](#) [Raw trace](#)

This is a testnet transaction only

<input type="checkbox"/> Transaction hash	0x98c5dbe4c2ca4975591d98e4d2a2069490588e5807a0d3df88414fc47f1c700e	
<input type="checkbox"/> Status and method	Success	
<input type="checkbox"/> Block	43932 19 Block confirmations	
<input type="checkbox"/> Timestamp	2m ago Feb 22 2024 17:24:00 PM (+07:00 UTC) Confirmed within <= 8 secs	
<input type="checkbox"/> From	0xeb23E1a2784931A65D671DaA1235c8ae6435A367	
<input type="checkbox"/> To	[Contract 0x75621FC47aaaf29bd7BD0bbdB77b0203E7684F776 created]	

<input type="checkbox"/> Value	0 ETH (\$0)
<input type="checkbox"/> Transaction fee	0.0000003719305956 ETH (\$0.001089801276779472)
<input type="checkbox"/> Gas price	0.00000000000100005 ETH (0.00100005 Gwei)
<input type="checkbox"/> Gas usage & limit by txn	371,912 371,912 100%
<input type="checkbox"/> Gas fees (Gwei)	Base: 0.00000005 Max: 0.001000063 Max priority: 0.001
<input type="checkbox"/> Burnt fees	⚡ 0.0000000000185956 ETH (\$0.000000054487339472)
Hide details	
<input type="checkbox"/> Other	Txn type: 2 (EIP-1559) Nonce: 22 Position: 1
<input type="checkbox"/> Raw input	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Hex Raw </div> <pre>0x608060405234801561001057600080fd5b506040516106243803806106248339818101604052810190610032919061 0090565b806000806101000a81548160ff021916908360ff160217905550506100bd565b600080fd5b600060ff82169050 919050565b61006d81610057565b811461007857600080fd5b50565b60008151905061008a81610064565b9291505056 5b6000602082840312156100a6576100a5610052565b5b60006100b48482850161007b565b91505092915050565b6105 58806100cc6000396000f3fe608060405234801561001057600080fd5b506004361061004c5760003560e01c806306c9 33d81461005157806331a72188146100815780634011d7cd1461009f5780638e7314d9146100bd575b600080fd5b61006b 600480360381019061006691906102ef565b6100c7565b6040516100789190610337565b60405180910390f35b610089</pre>

CryptoDevs.sol

Transaction details	
	Details Token transfers Internal txns Logs State Raw trace
This is a testnet transaction only	
<input type="checkbox"/> Transaction hash	0xc4de0574b974e2b20beaf47d2be35a5020e0fd290761f3a69804d194cc3c33f5 Raw
<input type="checkbox"/> Status and method	Success
<input type="checkbox"/> Block	44185 43 Block confirmations
<input type="checkbox"/> Timestamp	⌚ 6m ago Feb 22 2024 17:57:44 PM (+07:00 UTC) Confirmed within <= 8 secs
<input type="checkbox"/> From	0xeb23E1a2784931A65D671DaA1235c8ae6435A367 Raw
<input type="checkbox"/> To	[Contract Crypto Devs created] ✓

- 测试用例:[F-3] contract calldata 功能

[F-3] contract calldata

Script Code: [Github](#)

测试结果：

Transaction details	
Details	Token transfers
This is a testnet transaction only	
Transaction hash	0xf4413ecadd7f35b08788f296f98db4bfb2626a641ebf56cd2318dceaf7404af8
Status and method	Success 0x1249c58b
Block	44194 7 Block confirmations
Timestamp	54s ago Feb 22 2024 17:58:56 PM (+07:00 UTC) Confirmed within <= 8 secs
From	 0xeb23E1a2784931A65D671DaA1235c8ae6435A367
Interacted with contract	 Crypto Devs 
Tokens minted	0x00...0000  → 0xeb...A367  For token ID:  0  Crypto Devs (CD)

Value 0.0001 ETH (\$0.293012)

Transaction fee 0.0109111 ETH (\$31.970832332)

Gas price 0.0000001 ETH (100 Gwei)

Gas usage & limit by txn 109,111 | 1,000,000 • 10.91%

Gas fees (Gwei) Base: 0.00000005

[Hide details](#)

Other Txn type: 0 |Nonce: 27 |Position: 1

Raw input Hex Raw

```
0x1249c58b
```

```
● HOSANNAd MacBook-Air:myshell-test hosanna$ yarn hardhat run scripts/calldata.js --network myshell
yarn run v1.22.19
warning package.json: No license field
$ /Users/hosanna/chain-test/myshell-test/node_modules/.bin/hardhat run scripts/calldata.js --network myshell
mint price is: 0.0001
current transaction nonce is 27
block confirmation...
Transaction successfully...
Transaction Hash: 0xf4413ecadd7f35b08788f296f98db4bfb2626a641ebf56cd2318dceaf7404af8
Transaction Details: {
  hash: '0xf4413ecadd7f35b08788f296f98db4bfb2626a641ebf56cd2318dceaf7404af8',
  type: 0,
  accessList: null,
  blockHash: '0xe3522afa2c6a43a4bd5241bb06d56489d045ca960eb662d4701ba61d31e41ca7',
  blockNumber: 44194,
  transactionIndex: 1,
  confirmations: 1,
  from: '0xeb023e1a2784931a65d671daA1235c8ae6435a367',
  gasPrice: BigNumber { _hex: '0x174876e800', _isBigNumber: true },
  gasLimit: BigNumber { _hex: '0x0f4240', _isBigNumber: true },
  to: '0x000849A3dee93E16Ce12b0e9B27b99c0c3EbbbaC',
  value: BigNumber { _hex: '0x5af3107a4000', _isBigNumber: true },
  nonce: 27,
  data: '0x1249c58b',
  r: '0xb47cbe8e1f01ef499c93940a9811d1471c249dd0829deb4822f92e3ab51f7944',
  s: '0x6f29e3d8af96fc3c90446a1ad17d4fb20e82b8cb234160a7dc54c925e08eeb66e',
  v: 404804363352,
  creates: null,
  chainId: 202402181658,
  wait: [Function (anonymous)]
}
+ Done in 14.41s.
```

- 测试用例:[F-4] contract_read功能

[F-3] contract_read

Script Code: [Github](#)

测试结果:

```
● HOSANNAd MacBook-Air:myshell-test hosanna$ yarn hardhat run scripts/contract_read.js --network myshell
yarn run v1.22.19
warning package.json: No license field
$ /Users/hosanna/chain-test/myshell-test/node_modules/.bin/hardhat run scripts/contract_read.js --network myshell
mint price: 0.0001
+ Done in 3.51s.
```

- 测试用例:[F-5] contract_write功能

[F-3] contract_write

Script Code: [Github](#)

测试结果:

Transaction details

This is a testnet transaction only

Transaction hash	0xaeceae1bca7ffe87ec3885c84455cd392722155dfab366f4a9433f89162993fb
Status and method	Success 0x1249c58b
Block	44368 2 Block confirmations
Timestamp	15s ago Feb 22 2024 18:22:08 PM (+07:00 UTC) Confirmed within <= 8 secs
From	0xeb23E1a2784931A65D671DaA1235c8ae6435A367
Interacted with contract	Crypto Devs
Tokens minted	0x00...0000 → 0xeb...A367 For token ID: 1 Crypto Devs (CD)

Value	0.0001 ETH (\$0.293012)
Transaction fee	0.00000015451872555 ETH (\$0.000452758408108566)
Gas price	0.0000000000100005 ETH (0.00100005 Gwei)
Gas usage & limit by txn	154,511 154,511 100%
Gas fees (Gwei)	Base: 0.00000005 Max: 0.001000063 Max priority: 0.001
Burnt fees	0.00000000000772555 ETH (\$0.00000022636788566)

[Hide details](#)

Other	Txn type: 2 (EIP-1559) Nonce: 28 Position: 1
Raw input	Hex <input type="button" value="Copy"/>

0x1249c58b

```
● HOSANNAdeMacBook-Air:myshell-test hosanna$ yarn hardhat run scripts/contract_write.js --network myshell
yarn run v1.22.19
warning package.json: No license field
$ /Users/hosanna/chain-test/myshell-test/node_modules/.bin/hardhat run scripts/contract_write.js --network myshell
Minting...
mint price is: 0.0001
block confirmation...
Transaction successfully...
Transaction Hash: 0xaeceae1bca7ffe87ec3885c84455cd392722155dfab366f4a9433f89162993fb
Transaction Details: {
  hash: '0xaeceae1bca7ffe87ec3885c84455cd392722155dfab366f4a9433f89162993fb',
  type: 2,
  accessList: [],
  blockHash: '0xb371b5236d1f3ce063c0983ae8cf9da0e6bdf89decc78d836fab434289a2dac1',
  blockNumber: 44368,
  transactionIndex: 1,
  confirmations: 1,
  from: '0xeb23E1a2784931A65D671DaA1235c8ae6435A367',
  gasPrice: BigNumber { _hex: '0x0f4272', _isBigNumber: true },
  maxPriorityFeePerGas: BigNumber { _hex: '0x0f4240', _isBigNumber: true },
  maxFeePerGas: BigNumber { _hex: '0x0f427f', _isBigNumber: true },
  gasLimit: BigNumber { _hex: '0x25b8f', _isBigNumber: true },
  to: '0x000849A3dee93E16Ce12b0e9827b99ce3EbbbaC',
  value: BigNumber { _hex: '0x5af3107a4000', _isBigNumber: true },
  nonce: 28,
  data: '0x1249c58b',
  r: '0x999bb095c924b23a045c4ecfb1ae75b6df7aff370e8ce842b93f6506779151e2',
  s: '0x6b14b3c1c3450117d7073c586d2b15a9f3060d681e356d2d007914af5da57',
  v: 0,
  creates: null,
  chainId: 202402181658,
  wait: [Function (anonymous)]
}
+ Done in 16.10s.
```

2.6 Ethers 测试分析报告

- **wallets** 的测试:

- 成功在Myshell测试网络上创建随机钱包，生成了10个账户，每个账户均由助记词派生，钱包地址和私钥正确显示。
- 使用环境变量中的私钥创建了签名者(signer)，成功签名了消息“hello web3”并验证了签名者地址。
- 查询了签名者和第二个用户的余额，向第二个用户发送了0.0001 ETH的交易，交易回执被成功捕获并等待了3个区块确认，从交易费用来看，资源使用合理。

- **contract_calldata** 的测试:

- 获取签名者钱包实例，获取“CryptoDevs”智能合约实例。
- 执行铸造操作，通过提供`calldata`和交易价值。
- 109,111 Gas 使用，设置的Gas限制为1,000,000，交易费用0.0109111 ETH，对应于高Gas价格100 Gwei，在此类操作的预期范围内。
- Gas消耗：交易Gas消耗占用了设置的Gas上限的10.91%，表明交易复杂性中等。
- 交易速度：交易在8秒内得到确认，显示出测试网络的高效性能。
- 费用：交易费用较高，可能由于设置的Gas价格较市场价格高。

- **contract_write** 的测试:

- Gas消耗: 交易的Gas消耗量占用了其Gas上限的全部, 这对于铸造NFT的操作是正常的, 考虑到该操作的复杂性。
- 交易确认速度: 交易在8秒内得到确认, 显示出测试网络的高响应速度。
- 交易费用: 相比之前的测试, 此次交易的费用显著较低, 这可能是因为Gas价格设置得更为合理。

在一系列的测试中, 我们成功在Myshell测试网络上执行了不同的智能合约和钱包相关操作。创建了一个随机钱包并从助记词派生了10个账户, 每个账户的地址和私钥都得到了正确的显示。我们还进行了签名操作, 其中使用私钥签名了消息, 并验证了签名者地址。余额查询和交易发送表明网络资源使用合理, 其中包括向另一用户发送ETH并成功捕获交易回执。

在与CryptoDevs智能合约的交互中, 铸造操作通过提供适当的calldata和交易价值完成。这些测试显示了中等的Gas消耗和较高的交易确认速度, 尽管费用相对较高, 但仍在预期范围内。此外, 通过write脚本的测试, 我们观察到铸造NFT时Gas消耗量占用了Gas上限的全部, 且交易速度快, 费用低, 表明了对Gas价格策略的合理优化。

总体而言, 这些测试反映出Myshell测试网络在处理智能合约操作时的高效性和稳定性, 同时也突显了代码的健壮性和交易成本的合理性。这为未来的智能合约开发和部署提供了信心, 同时也强调了持续监控和优化Gas策略的重要性。