ETHEREUM

Intro to Solidity

2018 Edition

Hudson Jameson

Hudson Jameson

Cryptocurrency/blockchain space since 2011.

USAA: 2014-2016

Ethereum Foundation: 2016-current

Oaken Innovations: 2016-current

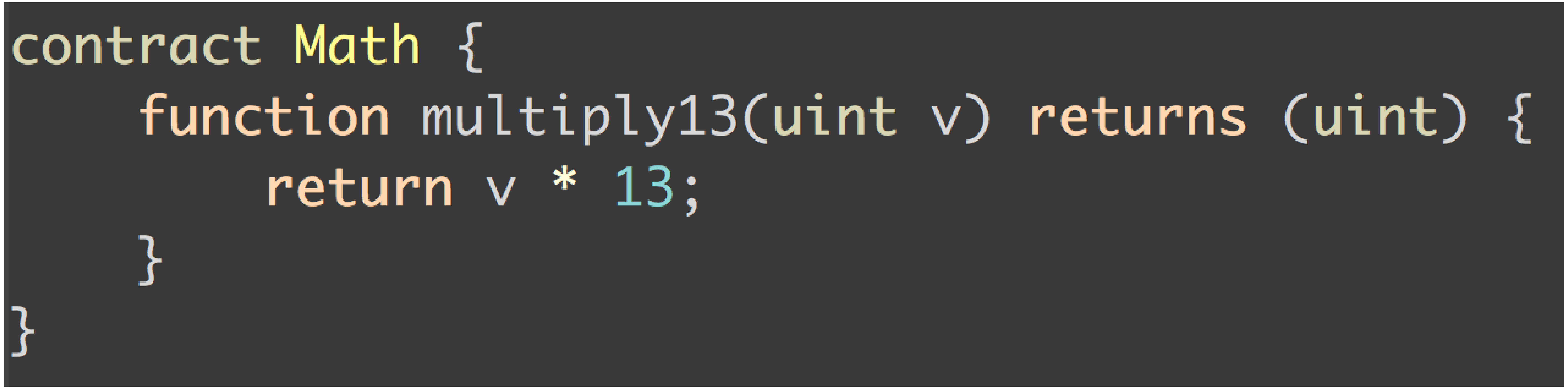
1 Wife & 3 Cats

Solidity

High level language for Ethereum contracts.

How many high level languages does Ethereum have? (Include defunct/deprecated, but not EWASM)

It looks like **Javascript** (with types).



```
contract Math {
    function multiply13(uint v) returns (uint) {
        return v * 13;
    }
}
```

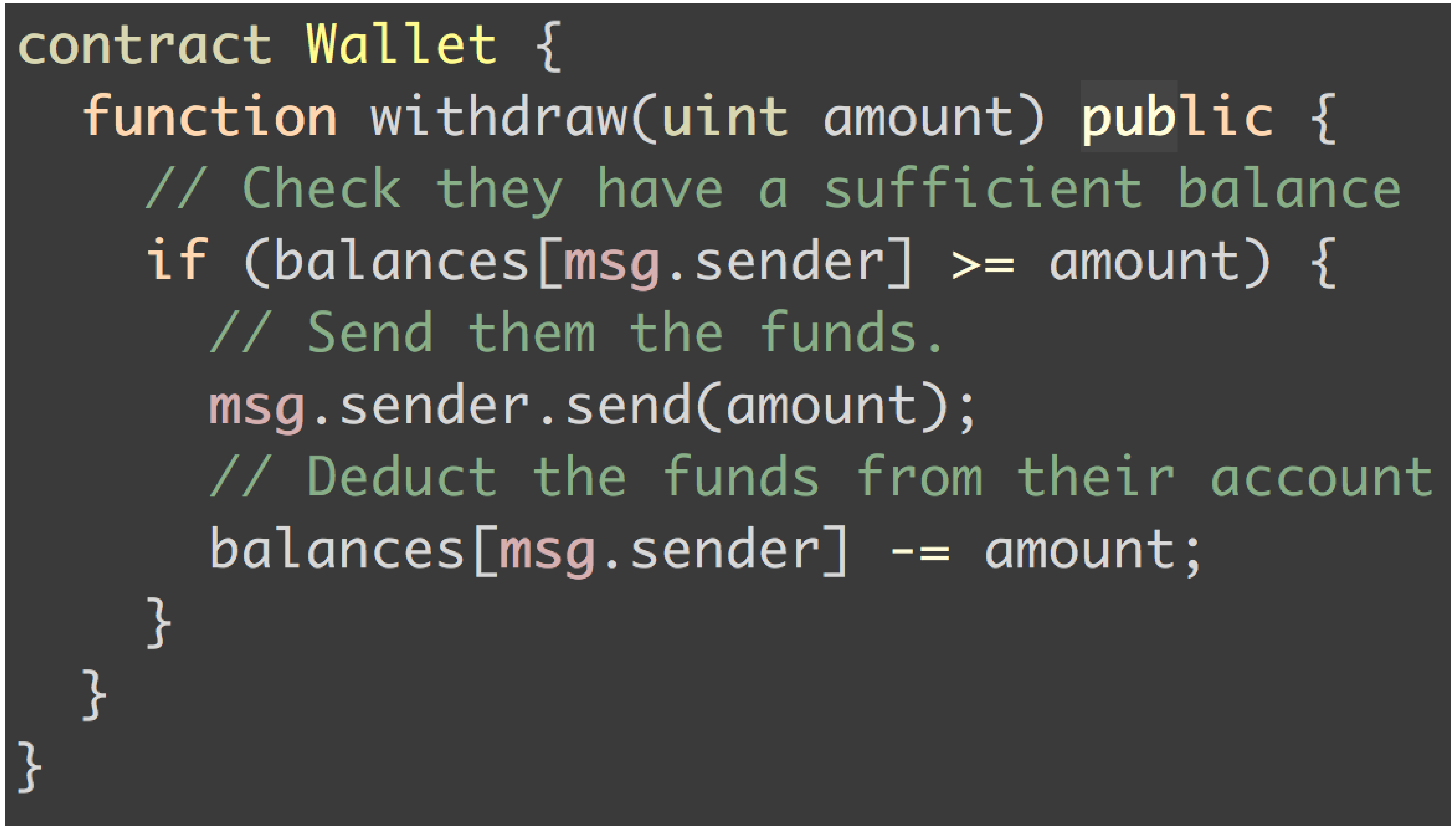
Contracts are like **classes**.

Code is compiled to the
Ethereum Virtual Machine (EVM).

EVM

Once deployed to the EVM, code is completely isolated and cannot reach outside of the EVM.

Easy to write contracts



```
contract Wallet {
  function withdraw(uint amount) public {
    // Check they have a sufficient balance
    if (balances[msg.sender] >= amount) {
      // Send them the funds.
      msg.sender.send(amount);
      // Deduct the funds from their account
      balances[msg.sender] -= amount;
    }
  }
}
```

Hard to make sure they are secure

ANSWER

How many high level languages does Ethereum have?
(Include defunct/deprecated, but not EWASM)

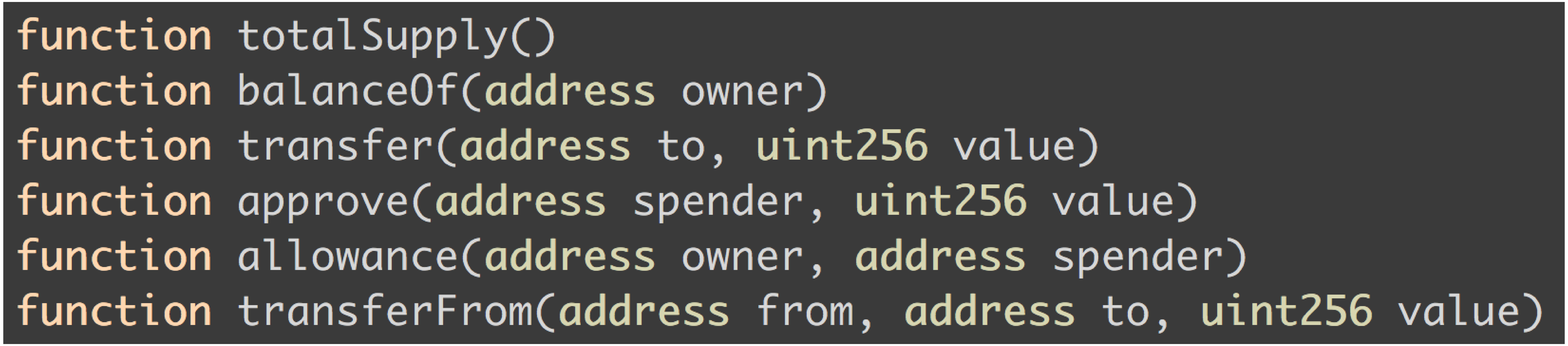
6

Mutan
Serpent
LLL
Solidity
Bamboo
Vyper

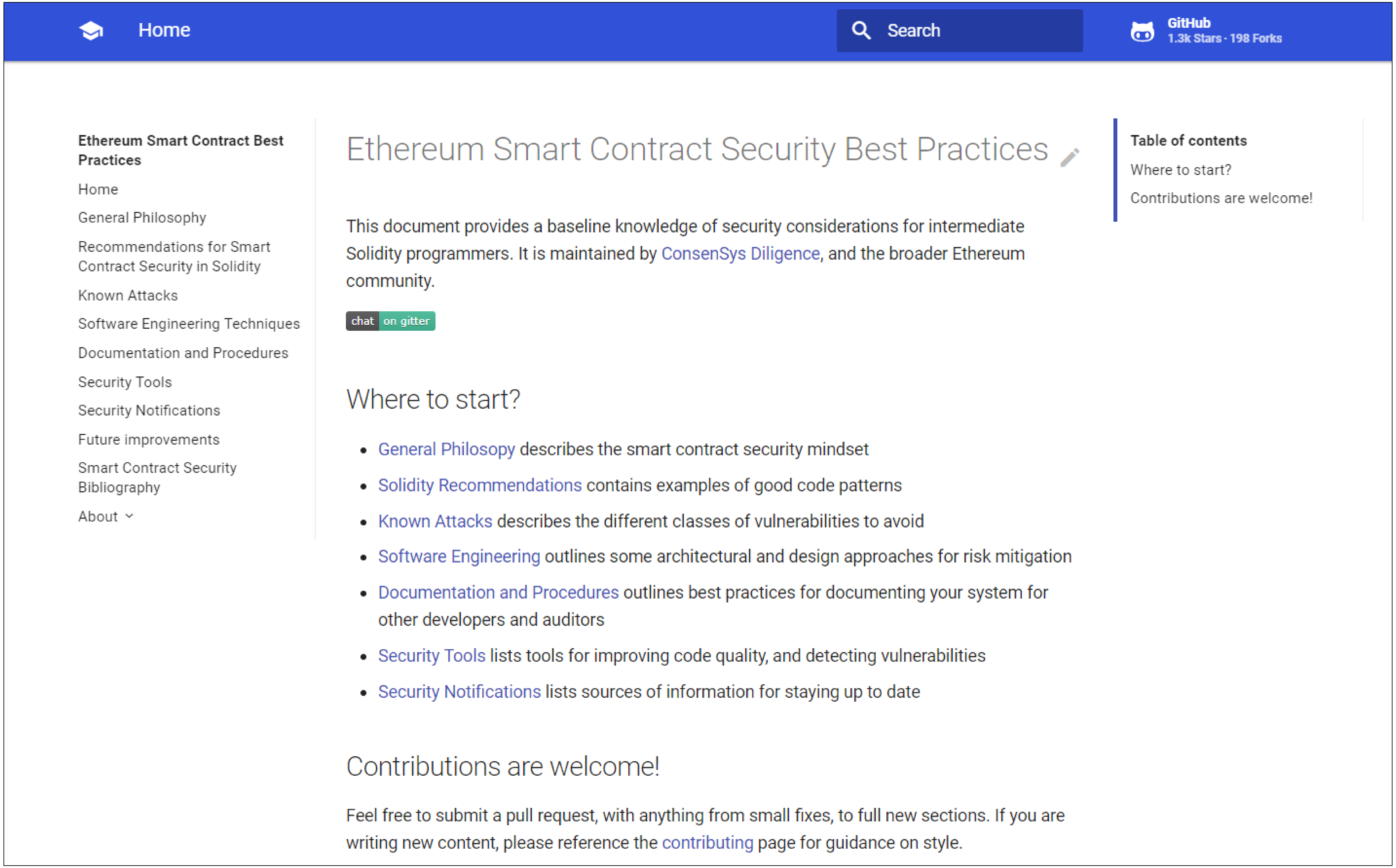
Contracts standards are beginning to emerge!

solidity

ERC20



```
function totalSupply()
function balanceOf(address owner)
function transfer(address to, uint256 value)
function approve(address spender, uint256 value)
function allowance(address owner, address spender)
function transferFrom(address from, address to, uint256 value)
```


Home
Search
GitHub
1.3k Stars · 198 Forks
Ethereum Smart Contract Best Practices
Home
General Philosophy
Recommendations for Smart Contract Security in Solidity
Known Attacks
Software Engineering Techniques
Documentation and Procedures
Security Tools
Security Notifications
Future improvements
Smart Contract Security Bibliography
About
Table of contents
Where to start?
Contributions are welcome!
chat on gitter

Ethereum Smart Contract Security Best Practices

This document provides a baseline knowledge of security considerations for intermediate Solidity programmers. It is maintained by ConsenSys Diligence, and the broader Ethereum community.

Where to start?

- General Philosopy describes the smart contract security mindset
- Solidity Recommendations contains examples of good code patterns
- Known Attacks describes the different classes of vulnerabilities to avoid
- Software Engineering outlines some architectural and design approaches for risk mitigation
- Documentation and Procedures outlines best practices for documenting your system for other developers and auditors
- Security Tools lists tools for improving code quality, and detecting vulnerabilities
- Security Notifications lists sources of information for staying up to date

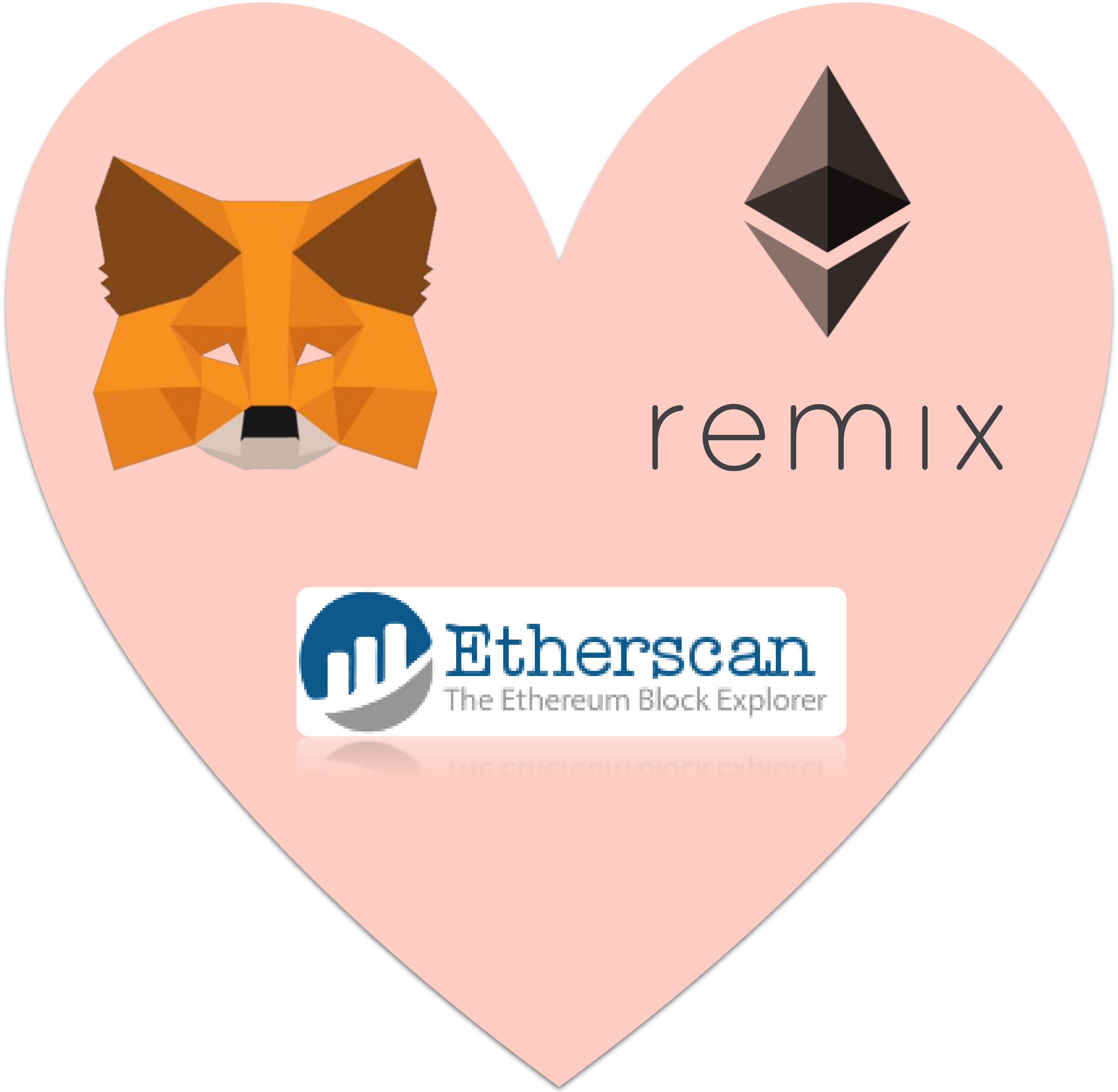
Contributions are welcome!

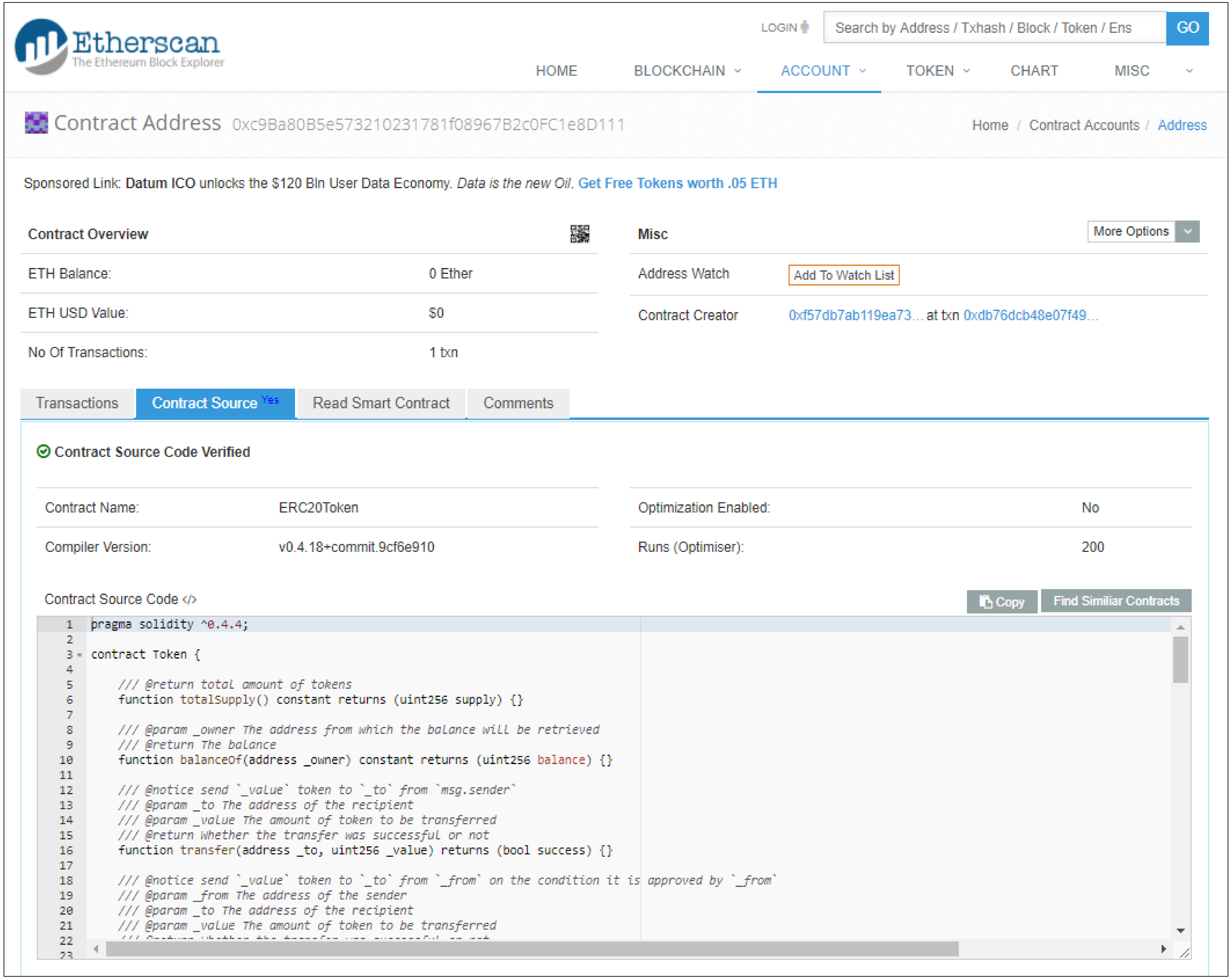
Feel free to submit a pull request, with anything from small fixes, to full new sections. If you are writing new content, please reference the contributing page for guidance on style.

https://consensys.github.io/smart-contract-best-practices/

ETHEREUM

Ultimate Software Combo




Etherscan
The Ethereum Block Explorer
LOGIN
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
ACCOUNT
TOKEN
CHART
MISC

Contract Address 0xc9Ba80B5e573210231781f08967B2c0FC1e8D111

Home / Contract Accounts / Address

Contract Overview	
ETH Balance:	0 Ether
ETH USD Value:	$0
No Of Transactions:	1 txn

Misc	More Options
Address Watch	Add To Watch List
Contract Creator	0xf57db7ab119ea73... at txn 0xdb76dcb48e07f49...

✓ Contract Source Code Verified

Contract Name:	ERC20Token	Optimization Enabled:	No
Compiler Version:	v0.4.18+commit.9cf6e910	Runs (Optimiser):	200

Contract Source Code </>

```
pragma solidity ^0.4.4;

contract Token {

    /// @return total amount of tokens
    function totalSupply() constant returns (uint256 supply) {}

    /// @param _owner The address from which the balance will be retrieved
    /// @return The balance
    function balanceOf(address _owner) constant returns (uint256 balance) {}

    /// @notice send `_value` token to `_to` from `msg.sender`
    /// @param _to The address of the recipient
    /// @param _value The amount of token to be transferred
    /// @return Whether the transfer was successful or not
    function transfer(address _to, uint256 _value) returns (bool success) {}

    /// @notice send `_value` token to `_to` from `_from` on the condition it is approved by `_from`
    /// @param _from The address of the sender
    /// @param _to The address of the recipient
    /// @param _value The amount of token to be transferred
    /// @return Whether the transfer was successful or not
```

ETHEREUM

browser
browser/simple.sol
remix
Compile
Run
Settings
Debugger
Ana
Start to compile
☐ Auto compile
browser/simple.sol:SimpleStore
Details
[2] only remix transactions, script
☐ Listen on network
remix

```
pragma solidity ^0.4.13;

contract SimpleStore {
  uint storedData;

    event DataStored(uint data);

    function set(uint x) payable {
        storedData = x;
        DataStored(storedData);
    }

    function get() constant returns (uint retVal) {
        return storedData;
    }
    /* This is a comment. */
}
```

browser
browser/simple.sol
remix
Compile
Run
Settings
Debugger
Ana

ContractDefinition SimpleStore   0 reference(s)

```
pragma solidity ^0.4.13;

contract Simpl
  uint storedD

    event Data

    function s
        stored
        DataSt
    }

    function g
        return
    }
    /* This is
}
```

MetaMask Notification

CONFIRM TRANSACTION   Ropsten Test Net

My Account
811102...6d41
100102.992 ETH
29604458.93 USD

New Contract

Amount: 0 ETH, 0.00 USD
Gas Limit: 120187 UNITS
Gas Price: 100 GWEI
Max Transaction Fee: 0.012018 ETH, 3.55 USD
Max Total: 0.012018 ETH, 3.55 USD

Data included: 283 bytes

[2] only remix tra… …sten on network

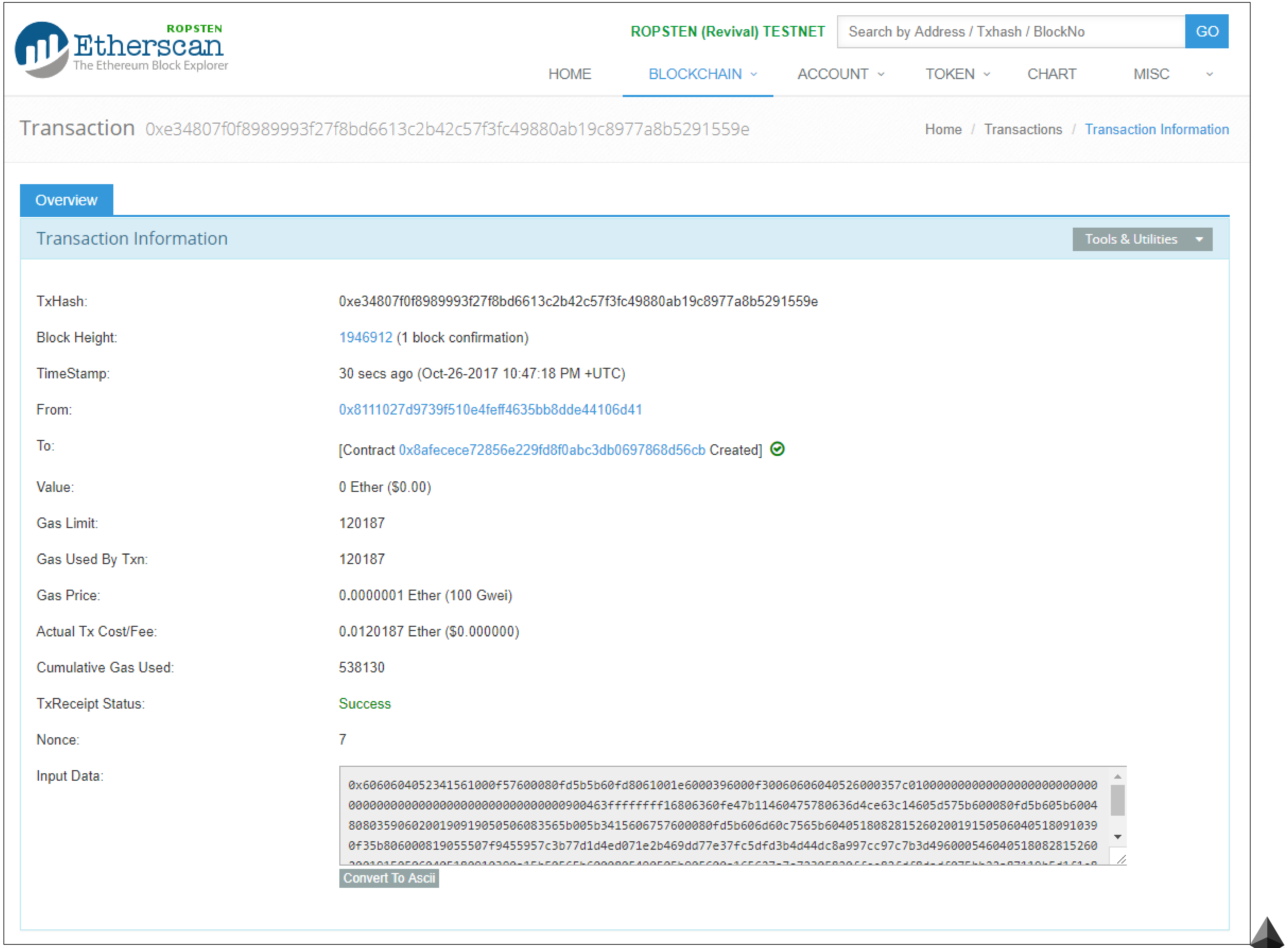
```
creation of browser/simple.sol:SimpleStore pending...
>
```

Environment: Injected Web3
Account: 0x811...06d41 (100102.99
Gas limit: 3000000
Gas Price: 0
Value: 0

browser/simple.sol:SimpleStore

1 pending transactions

0 contract Instances


ROPSTEN
Etherscan
The Ethereum Block Explorer
ROPSTEN (Revival) TESTNET
Search by Address / Txhash / BlockNo
GO
HOME
BLOCKCHAIN
ACCOUNT
TOKEN
CHART
MISC
Home / Transactions / Transaction Information
Overview
Tools & Utilities
Convert To Ascii

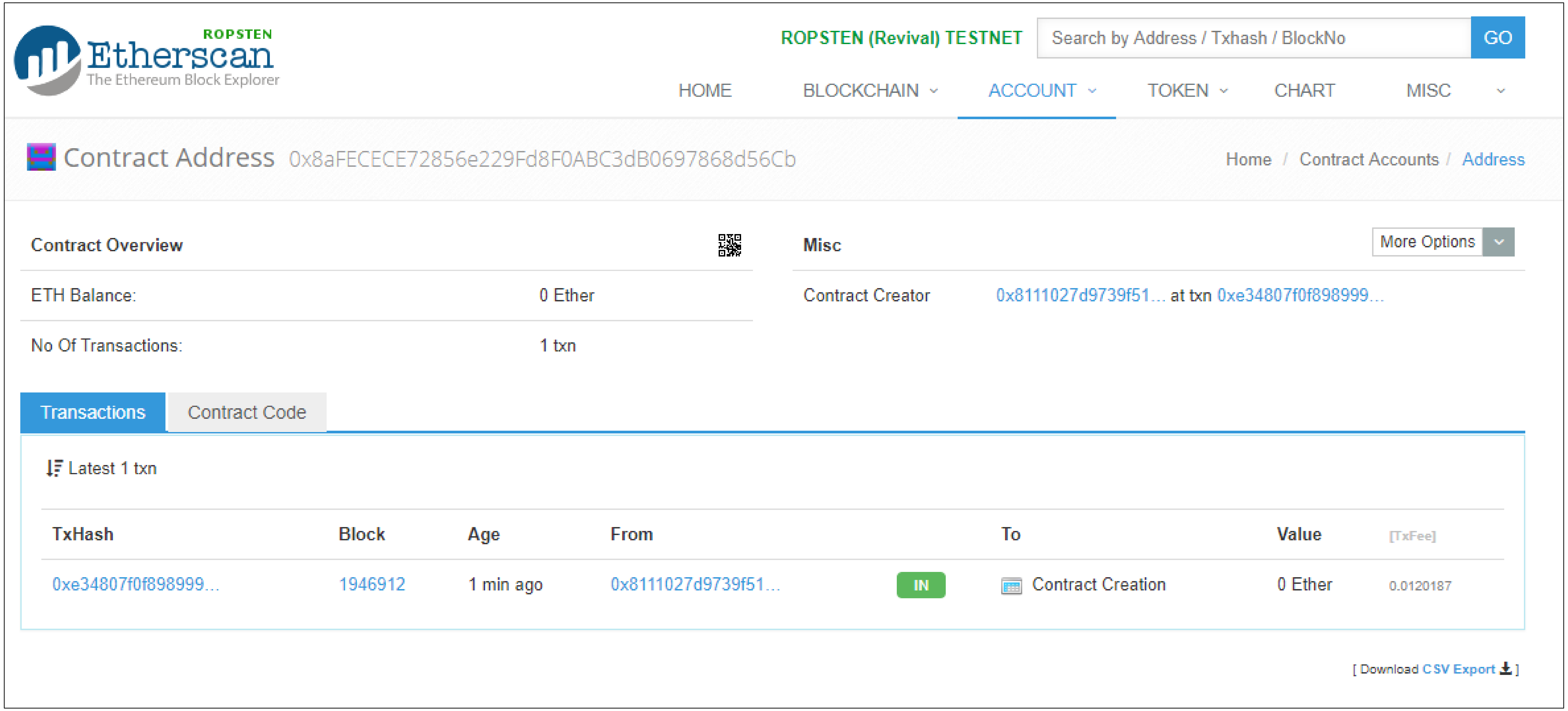
Transaction 0xe34807f0f8989993f27f8bd6613c2b42c57f3fc49880ab19c8977a8b5291559e

Transaction Information

TxHash:	0xe34807f0f8989993f27f8bd6613c2b42c57f3fc49880ab19c8977a8b5291559e
Block Height:	1946912 (1 block confirmation)
TimeStamp:	30 secs ago (Oct-26-2017 10:47:18 PM +UTC)
From:	0x8111027d9739f510e4feff4635bb8dde44106d41
To:	[Contract 0x8afecece72856e229fd8f0abc3db0697868d56cb Created] ✓
Value:	0 Ether ($0.00)
Gas Limit:	120187
Gas Used By Txn:	120187
Gas Price:	0.0000001 Ether (100 Gwei)
Actual Tx Cost/Fee:	0.0120187 Ether ($0.000000)
Cumulative Gas Used:	538130
TxReceipt Status:	Success
Nonce:	7

Input Data:

```
0x6060604052341561000f57600080fd5b5b60fd8061001e6000396000f300606060405260003557c010000000000000000000000000
0000000000000000000000000000000900463ffffffff16806360fe47b11460475780636d4ce63c14605d575b600080fd5b605b6004
8080359060200190919050506083565b005b3415606757600080fd5b606d60c7565b604051808281526020019150506040518091039
0f35b806000819055507f9455957c3b77d1d4ed071e2b469dd77e37fc5dfd3b4d44dc8a997cc97c7b3d49600054604051808281526 0
```



ROPSTEN
Etherscan
The Ethereum Block Explorer
ROPSTEN (Revival) TESTNET
Search by Address / Txhash / BlockNo
GO
HOME
BLOCKCHAIN
ACCOUNT
TOKEN
CHART
MISC

Contract Address 0x8aFECECE72856e229Fd8F0ABC3dB0697868d56Cb

Home / Contract Accounts / Address

Contract Overview

ETH Balance:	0 Ether
No Of Transactions:	1 txn

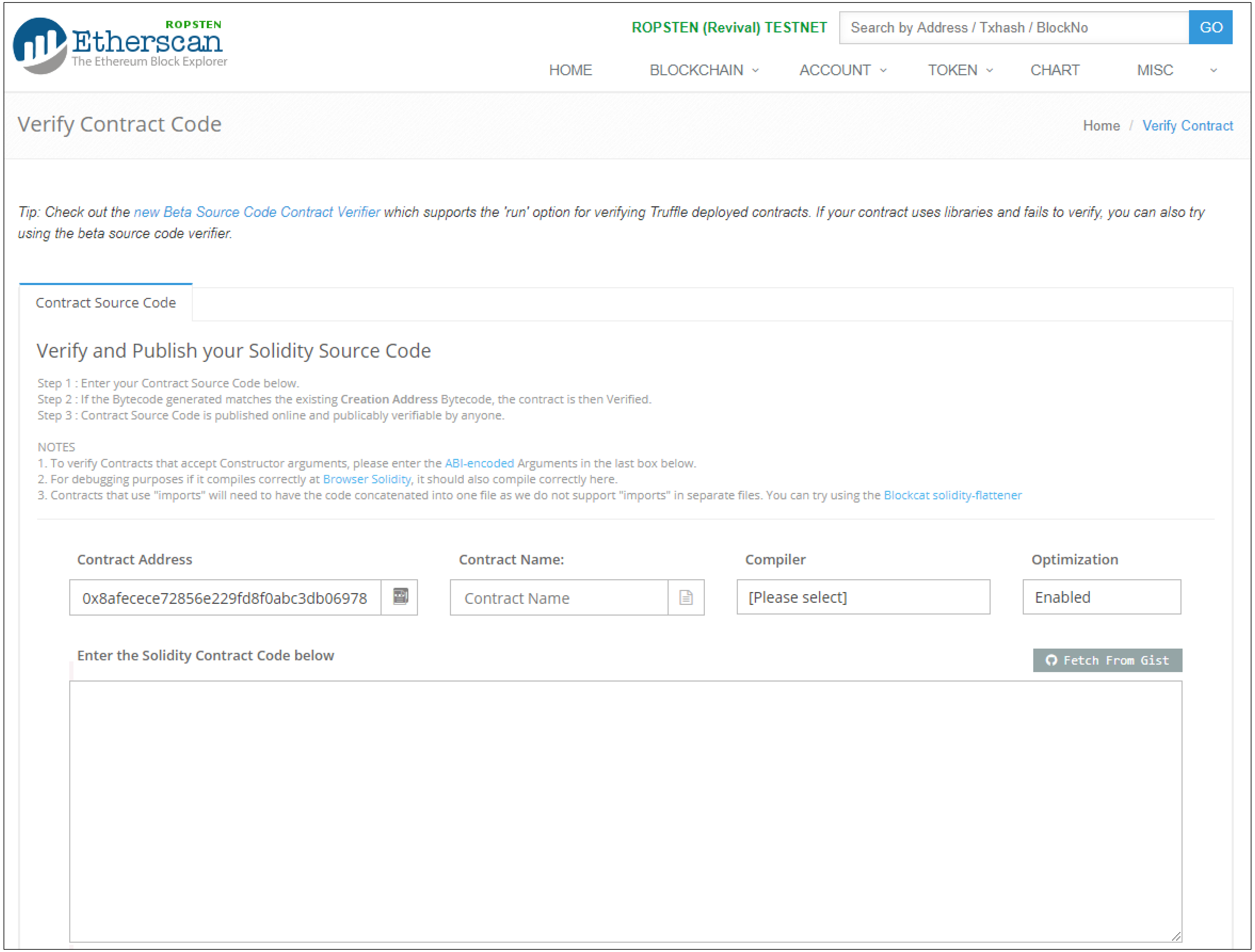
Misc

Contract Creator	0x8111027d9739f51... at txn 0xe34807f0f898999...

Latest 1 txn

TxHash	Block	Age	From		To	Value	[TxFee]
0xe34807f0f898999...	1946912	1 min ago	0x8111027d9739f51...	IN	Contract Creation	0 Ether	0.0120187

[Download CSV Export]



ROPSTEN
Etherscan
The Ethereum Block Explorer
ROPSTEN (Revival) TESTNET
Search by Address / Txhash / BlockNo
GO
HOME
BLOCKCHAIN
ACCOUNT
TOKEN
CHART
MISC
Home / Verify Contract

Verify Contract Code

Tip: Check out the new Beta Source Code Contract Verifier which supports the 'run' option for verifying Truffle deployed contracts. If your contract uses libraries and fails to verify, you can also try using the beta source code verifier.

Contract Source Code

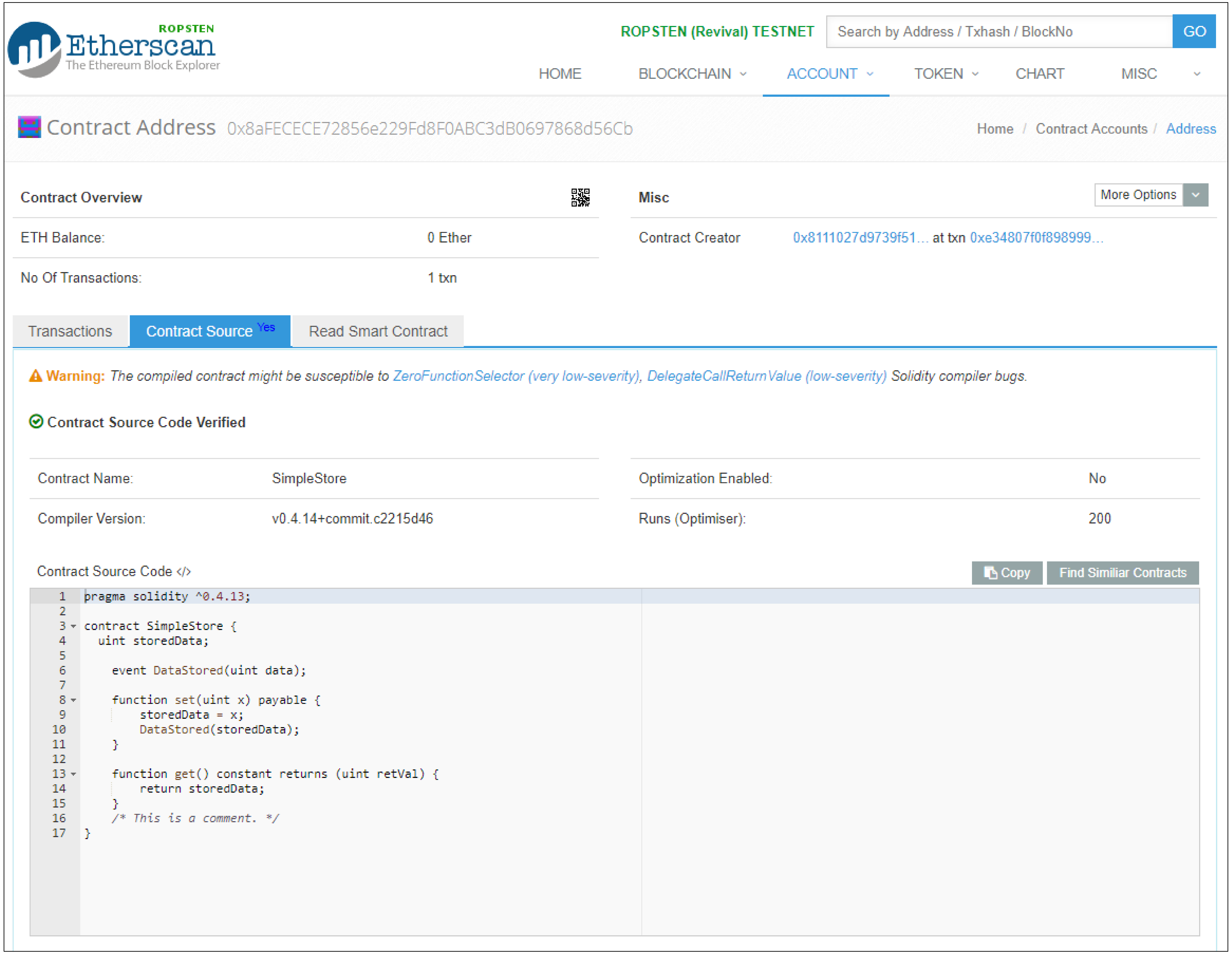
Verify and Publish your Solidity Source Code

Step 1 : Enter your Contract Source Code below.
Step 2 : If the Bytecode generated matches the existing **Creation Address** Bytecode, the contract is then Verified.
Step 3 : Contract Source Code is published online and publicably verifiable by anyone.

NOTES
1. To verify Contracts that accept Constructor arguments, please enter the ABI-encoded Arguments in the last box below.
2. For debugging purposes if it compiles correctly at Browser Solidity, it should also compile correctly here.
3. Contracts that use "imports" will need to have the code concatenated into one file as we do not support "imports" in separate files. You can try using the Blockcat solidity-flattener

Contract Address	Contract Name:	Compiler	Optimization
0x8afecece72856e229fd8f0abc3db06978	Contract Name	[Please select]	Enabled

Enter the Solidity Contract Code below



Contract Address 0x8aFECECE72856e229Fd8F0ABC3dB0697868d56Cb

Contract Overview

ETH Balance:	0 Ether
No Of Transactions:	1 txn

Misc

Contract Creator 0x8111027d9739f51... at txn 0xe34807f0f898999...

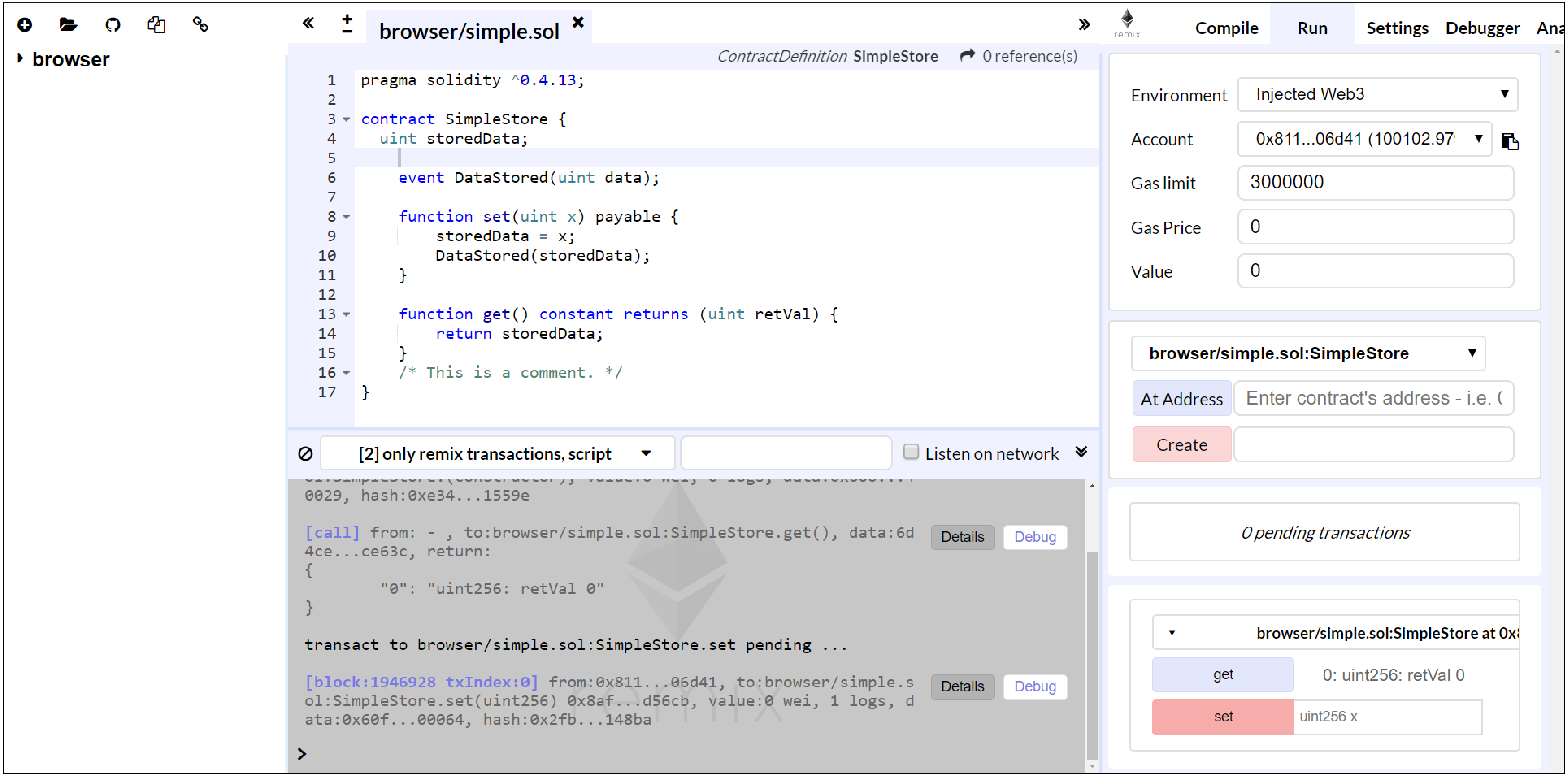
⚠ **Warning:** *The compiled contract might be susceptible to ZeroFunctionSelector (very low-severity), DelegateCallReturnValue (low-severity) Solidity compiler bugs.*

✓ **Contract Source Code Verified**

Contract Name:	SimpleStore	Optimization Enabled:	No
Compiler Version:	v0.4.14+commit.c2215d46	Runs (Optimiser):	200

Contract Source Code </>

```
pragma solidity ^0.4.13;

contract SimpleStore {
  uint storedData;

    event DataStored(uint data);

    function set(uint x) payable {
        storedData = x;
        DataStored(storedData);
    }

    function get() constant returns (uint retVal) {
        return storedData;
    }
    /* This is a comment. */
}
```



```
pragma solidity ^0.4.13;

contract SimpleStore {
  uint storedData;

    event DataStored(uint data);

    function set(uint x) payable {
        storedData = x;
        DataStored(storedData);
    }

    function get() constant returns (uint retVal) {
        return storedData;
    }
    /* This is a comment. */
}
```

Environment: Injected Web3

Account: 0x811...06d41 (100102.97

Gas limit: 3000000

Gas Price: 0

Value: 0

browser/simple.sol:SimpleStore

At Address: Enter contract's address - i.e. (

Create

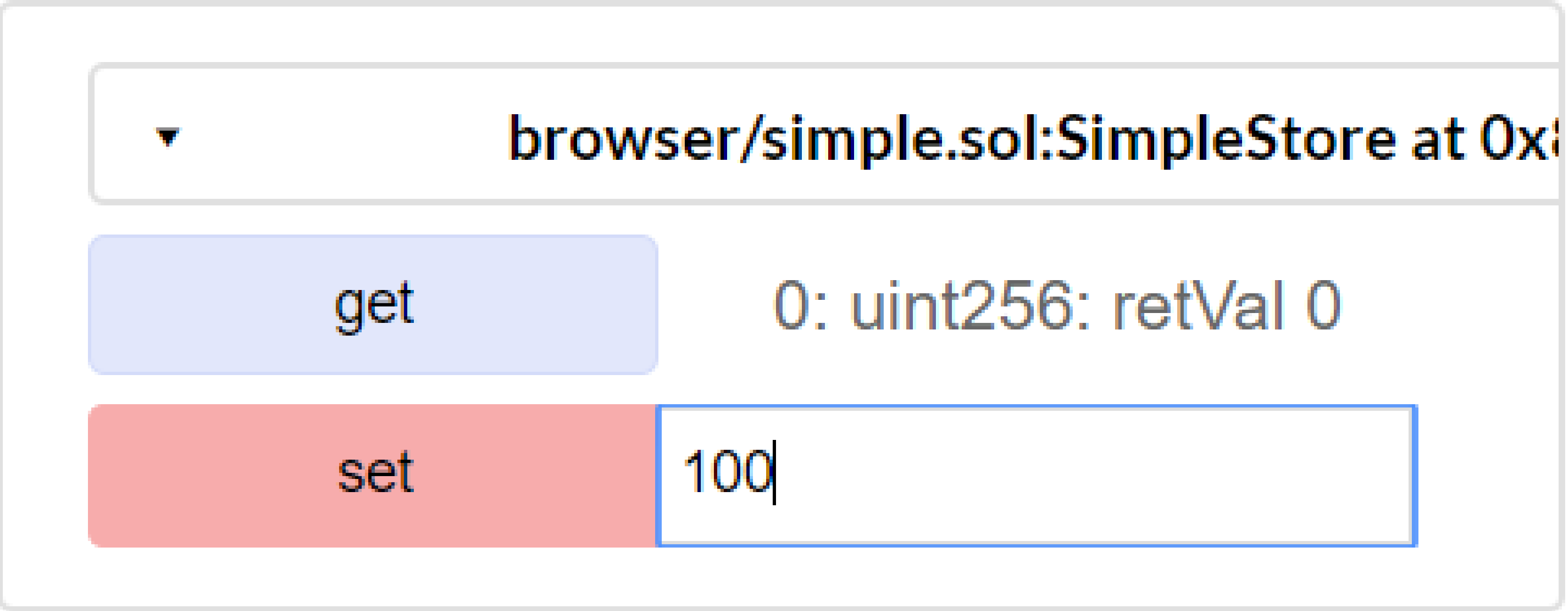
0 pending transactions

browser/simple.sol:SimpleStore at 0x

get: 0: uint256: retVal 0

set: uint256 x

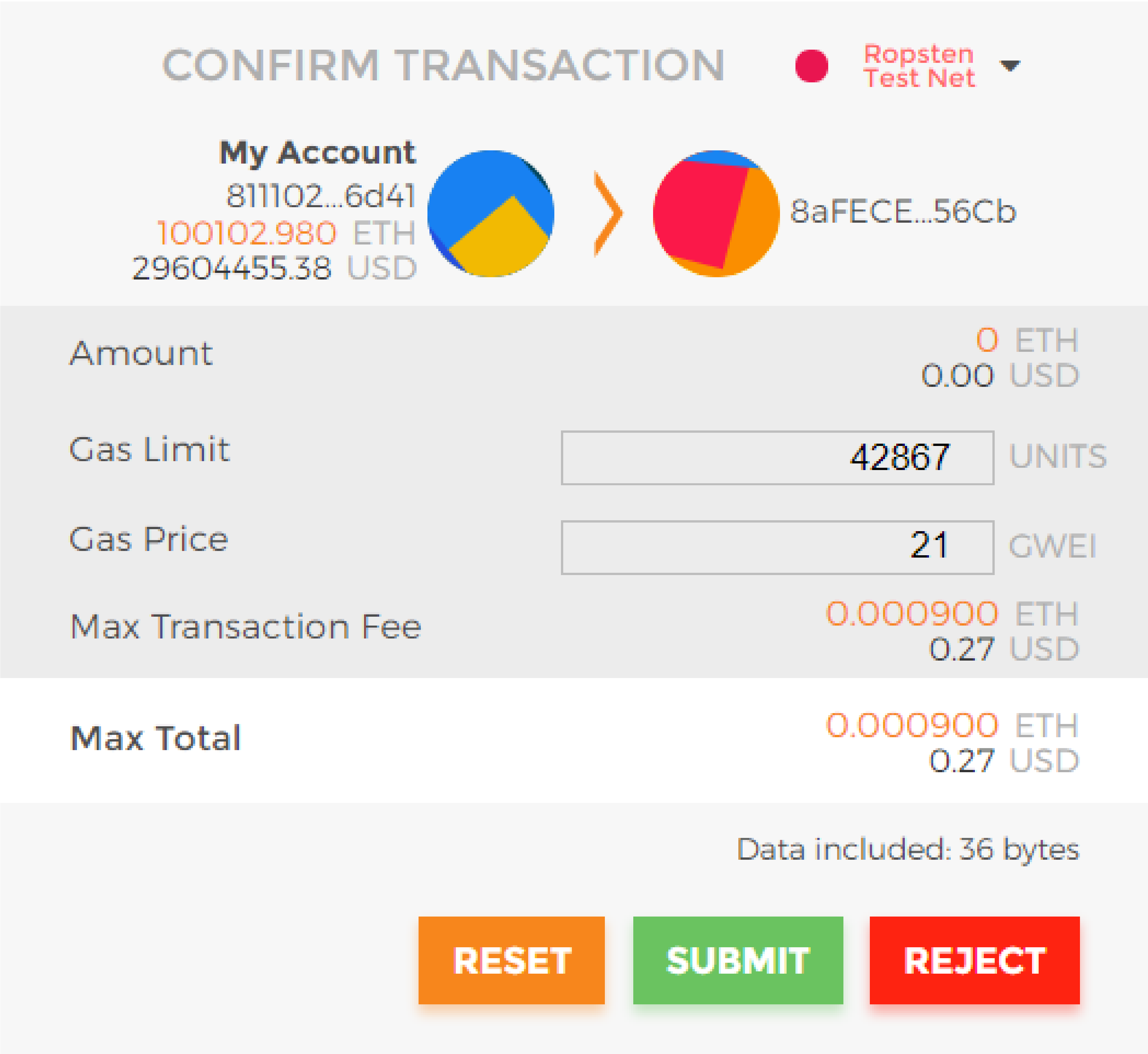
```
ol:SimpleStore.(constructor), value:0 wei, 0 logs, data:0x606...4
0029, hash:0xe34...1559e

[call] from: - , to:browser/simple.sol:SimpleStore.get(), data:6d
4ce...ce63c, return:
{
        "0": "uint256: retVal 0"
}

transact to browser/simple.sol:SimpleStore.set pending ...

[block:1946928 txIndex:0] from:0x811...06d41, to:browser/simple.s
ol:SimpleStore.set(uint256) 0x8af...d56cb, value:0 wei, 1 logs, d
ata:0x60f...00064, hash:0x2fb...148ba

>
```



▾ browser/simple.sol:SimpleStore at 0x

get 0: uint256: retVal 0

set 100



CONFIRM TRANSACTION ● Ropsten Test Net ▾

My Account
811102...6d41
100102.980 ETH
29604455.38 USD

8aFECE...56Cb

Amount 0 ETH 0.00 USD

Gas Limit 42867 UNITS

Gas Price 21 GWEI

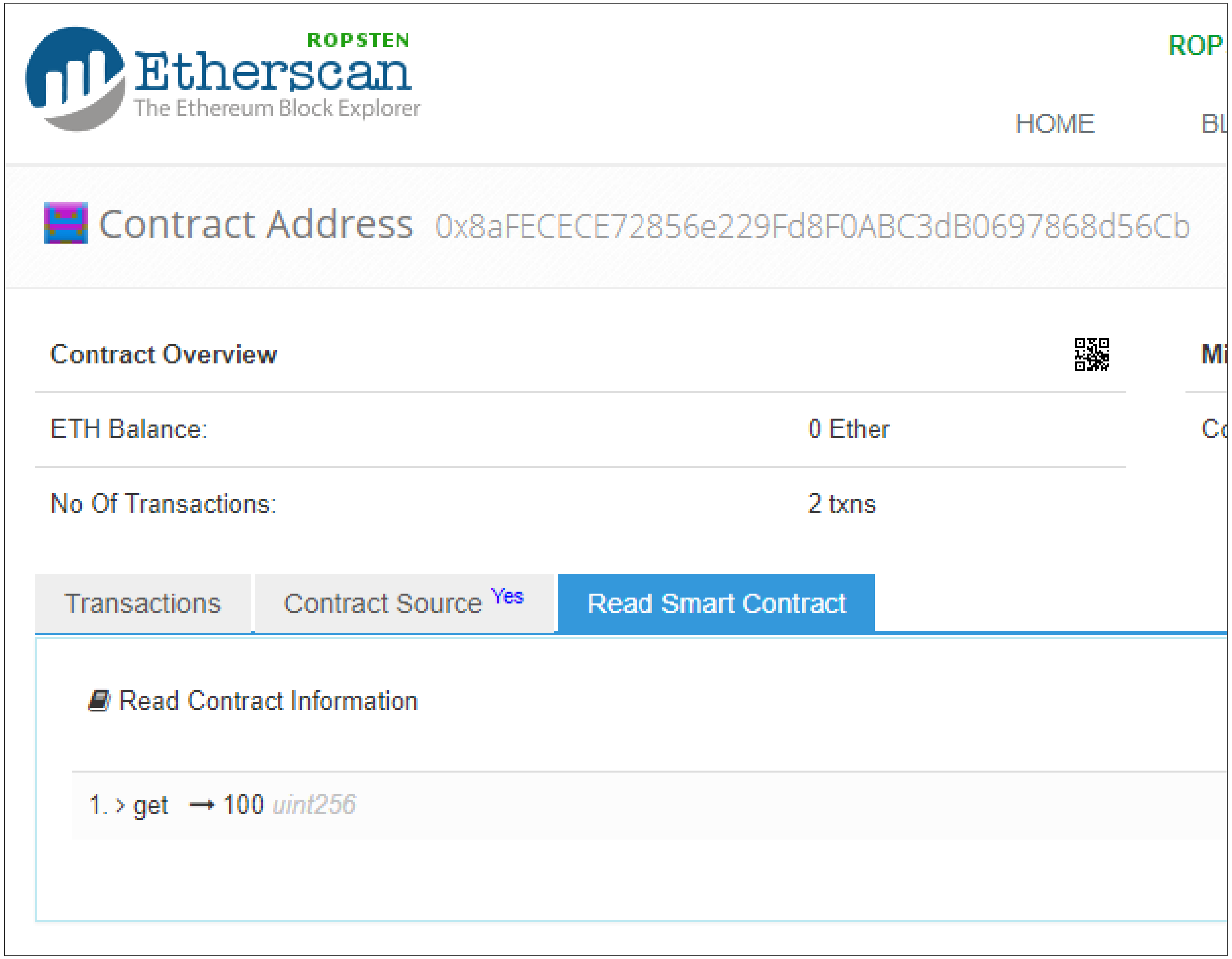
Max Transaction Fee 0.000900 ETH 0.27 USD

Max Total 0.000900 ETH 0.27 USD

Data included: 36 bytes

RESET SUBMIT REJECT

ETHEREUM



Contract Address 0x8aFECECE72856e229Fd8F0ABC3dB0697868d56Cb

Contract Overview

ETH Balance: 0 Ether

No Of Transactions: 2 txns

Read Contract Information

1. › get → 100 *uint256*

IDEs & Integrations

remix

Visual Studio

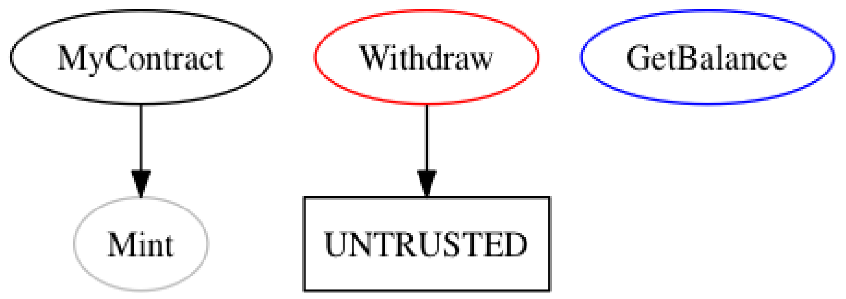
IJ

Vim

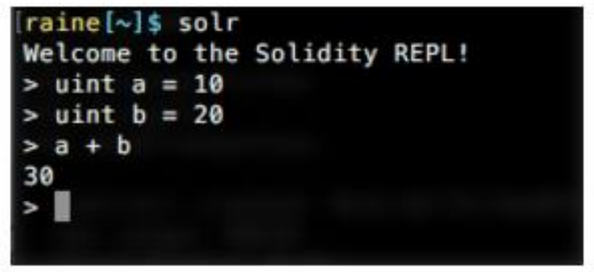
Emacs

Tools

solgraph



solidity repl



```
[raine[~]$ solr
Welcome to the Solidity REPL!
> uint a = 10
> uint b = 20
> a + b
30
> 
```

Solium

evmdis
(EVM Disassembler)

Embark

TRUFFLE

Ethereum Package Management

Populus
(Dapp framework)

Get Started Today!

<3 solidity

Site: **hudsonjameson.com**

Twitter: **@hudsonjameson**

Reddit: **/u/souptacular**