Solidity

Lexie Rista, Archibald Latham, Dozie Anazia

CSC 421

Solidity

A high level object oriented language used to develop smart contracts on the Ethereum blockchain.

Influenced by C++, Python, Javascript

Turing complete language similar to the syntax of Javascript.

Inventor: Gavin Wood → Developed by Christian Reitwiessner

Runs on the Ethereum Virtual Machine (EVM)

Supports several other blockchain platforms such as Tendermint, Counterparty, Ethereum Classic, and ErisDB

Ethereum

Second largest cryptocurrency and the largest smart contract blockchain in the world.

Decentralized open-source platform

Cryptocurrency = Ether

ethereum

Ethereum (pt2)

A platform using utilitzing blockchain technology offering the functionality of smart contracts through the Ethereum Virtual Machine.

Smart contracts are written in high-level languages such as LLL, Serpent, Viper, and Solidity, but then compiled to the EVM.

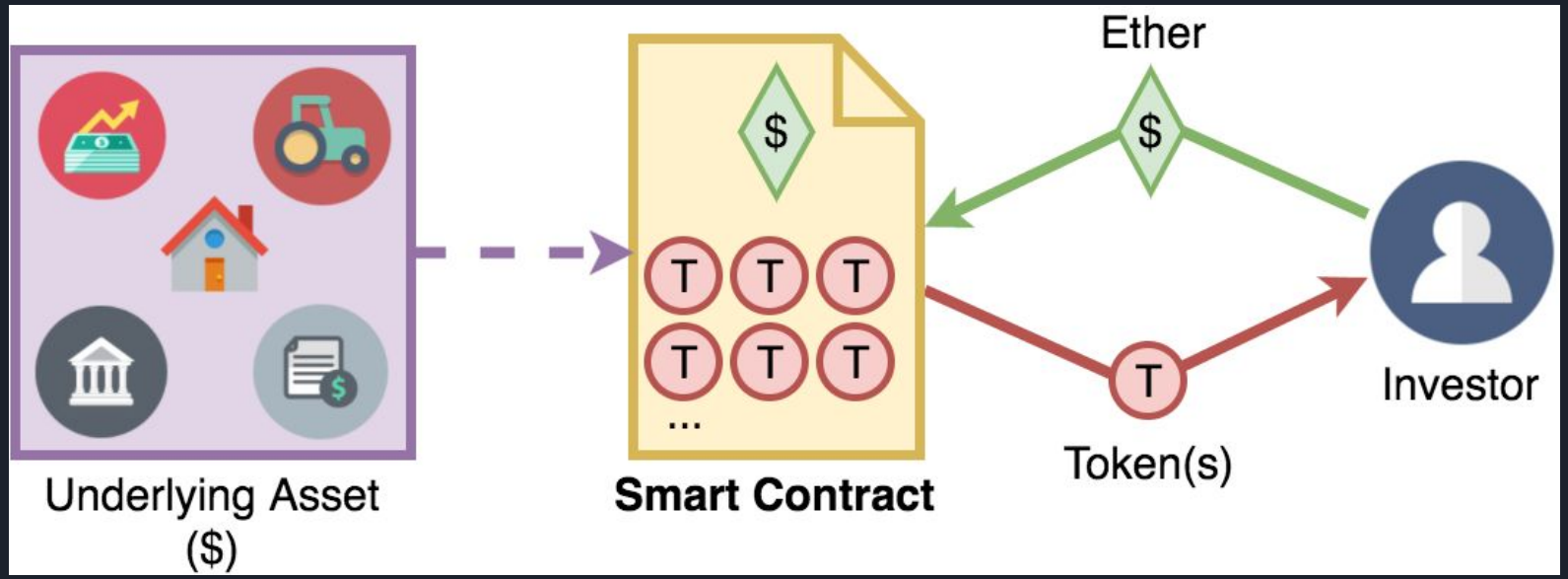
Blockchain

A Blockchain is a technology combination of cryptography, networking, and incentive mechanism supporting the verification process of the incoming transactions.

A decentralized and immutable ledger of all transactions that occur on a network.

Smart Contract

Code that can be self executed on a blockchain typically used to create an asset or facilitate the transfer of assets



ERC-20

The technical standard that a smart contract must meet to be considered a token

BNT	QNT	cDAI	Multi-collateral DAI
CVC	RCN	cSAI	KCS
EURS	REP	ENJ	LEND
GNT	RLC	OXT	LOOM
GYEN	SAI	CEL	LRC
KNC	SNT	CELR	NEXO
MANA	STORJ	cUSDC	NPXS
MATIC	sUSD	ELF	PAY
MTL	WBTC	ENG	POWR
NMR	WTC	FET	REN
OKB	ZUSD	HOT	VGX

SafeMath

```
contract SafeMath {
    function safeAdd(uint a, uint b) public pure returns (uint c) {
        c = a + b;
        require(c >= a);
    }
    function safeSub(uint a, uint b) public pure returns (uint c) {
        require(b <= a);
        c = a - b;
    }
    function safeMul(uint a, uint b) public pure returns (uint c) {
        c = a * b;
        require(a == 0 || c / a == b);
    }
    function safeDiv(uint a, uint b) public pure returns (uint c) {
        require(b > 0);
        c = a / b;
    }
}
```

ERC-20 Interface

```
abstract contract ERC20Interface {
    function totalSupply() virtual public view returns (uint);
    function balanceOf(address tokenOwner) virtual public view returns (uint balance);
    function allowance(address tokenOwner, address spender) virtual public view returns (uint remaining);
    function transfer(address to, uint tokens) virtual public returns (bool success);
    function approve(address spender, uint tokens) virtual public returns (bool success);
    function transferFrom(address from, address to, uint tokens) virtual public returns (bool success);

    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

CSC-421 Token

```
contract CSC421 is ERC20Interface, Owned, SafeMath {
    string public symbol;
    string public  name;
    uint8 public decimals;
    uint public _totalSupply;

    mapping(address => uint) balances;
    mapping(address => mapping(address => uint)) allowed;
```

Approve and Transfer

```
function approve(address spender, uint tokens) public override returns (bool success) {
    allowed[msg.sender][spender] = tokens;
    emit Approval(msg.sender, spender, tokens);
    return true;
}
```

```
function transfer(address to, uint tokens) public override returns (bool success) {
    balances[msg.sender] = safeSub(balances[msg.sender], tokens);
    balances[to] = safeAdd(balances[to], tokens);
    emit Transfer(msg.sender, to, tokens);
    return true;
}
```

Remix IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.6.6+commit.6c089d02.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Injected Web3

Ropsten (3) network

ACCOUNT

0xacE...8Eab6 (12.9768252

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

CSC421 - contracts/artifacts/CSC421.s

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

Currently you have no contract instances to interact with.

Home | CSC421.sol

```
pragma solidity 0.6.6;

// ----------------------------------------------------------------------
//
// Deployed to : 0xacE97D3EcAE07775163152A4Bad7876e1a38Eab6
// Symbol      : CSC421
// Name        : Design and Org
// Total supply: 100000000
// Decimals    : 18
//
// ----------------------------------------------------------------------


// ----------------------------------------------------------------------
// Safe maths
// ----------------------------------------------------------------------
contract SafeMath {
    function safeAdd(uint a, uint b) public pure returns (uint c) {
        c = a + b;
        require(c >= a);
    }
    function safeSub(uint a, uint b) public pure returns (uint c) {
        require(b <= a);
        c = a - b;
    }
    function safeMul(uint a, uint b) public pure returns (uint c) {
        c = a * b;
        require(a == 0 || c / a == b);
```

listen on network | Search with transaction hash or address

- Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.exeCurrent()` in the comma
- Right click on a JavaScript file in the file explorer and then click `Run`

The following libraries are accessible:
- web3 version 1.0.0
- ethers.js
- swarmgw
- remix (run remix.help() for more info)

creation of CSC421 pending...

Ropsten Test Network

Account 1 → New Contract

https://remix.ethereum.org

CONTRACT DEPLOYMENT

0

DETAILS | DATA

GAS FEE 0.01415

No Conversion Rate Available

Gas Price (GWEI) 10 | Gas Limit 1414983

AMOUNT + GAS FEE

TOTAL 0.01415

No Conversion Rate Available

Reject | Confirm

Etherscan

Etherscan

Ropsten Testnet Network

All Filters | Search by Address / Txn Hash / Blo

Home

Transaction Details

Overview | Logs (1) | State

[This is a Ropsten **Testnet** transaction only]

Transaction Hash:	0x3cc27b995a90fe01889b9017bff897305c16a7faa6645da531259742048b1357
Status:	Success
Block:	10113443 3 Block Confirmations
Timestamp:	35 secs ago (Apr-26-2021 01:28:52 AM +UTC)
From:	0xace97d3ecae07775163152a4bad7876e1a38eab6
To:	[Contract 0x4af1cd46b87cea2bf5f7c890ae8ded4871e109ce Created]
Value:	0 Ether ($0.00)
Transaction Fee:	0.01414983 Ether ($0.00)
Gas Price:	0.00000001 Ether (10 Gwei)

Ropsten Test Network

Not connected

Account 1

0xacE9...Eab6

12.9627 ETH

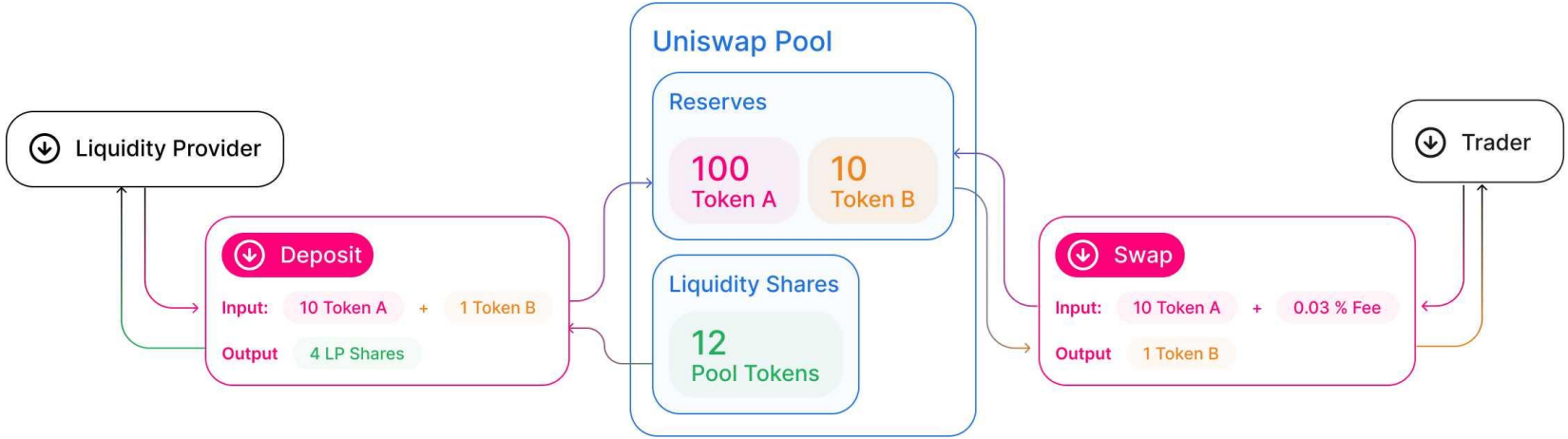
Buy | Send | Swap

Assets | Activity

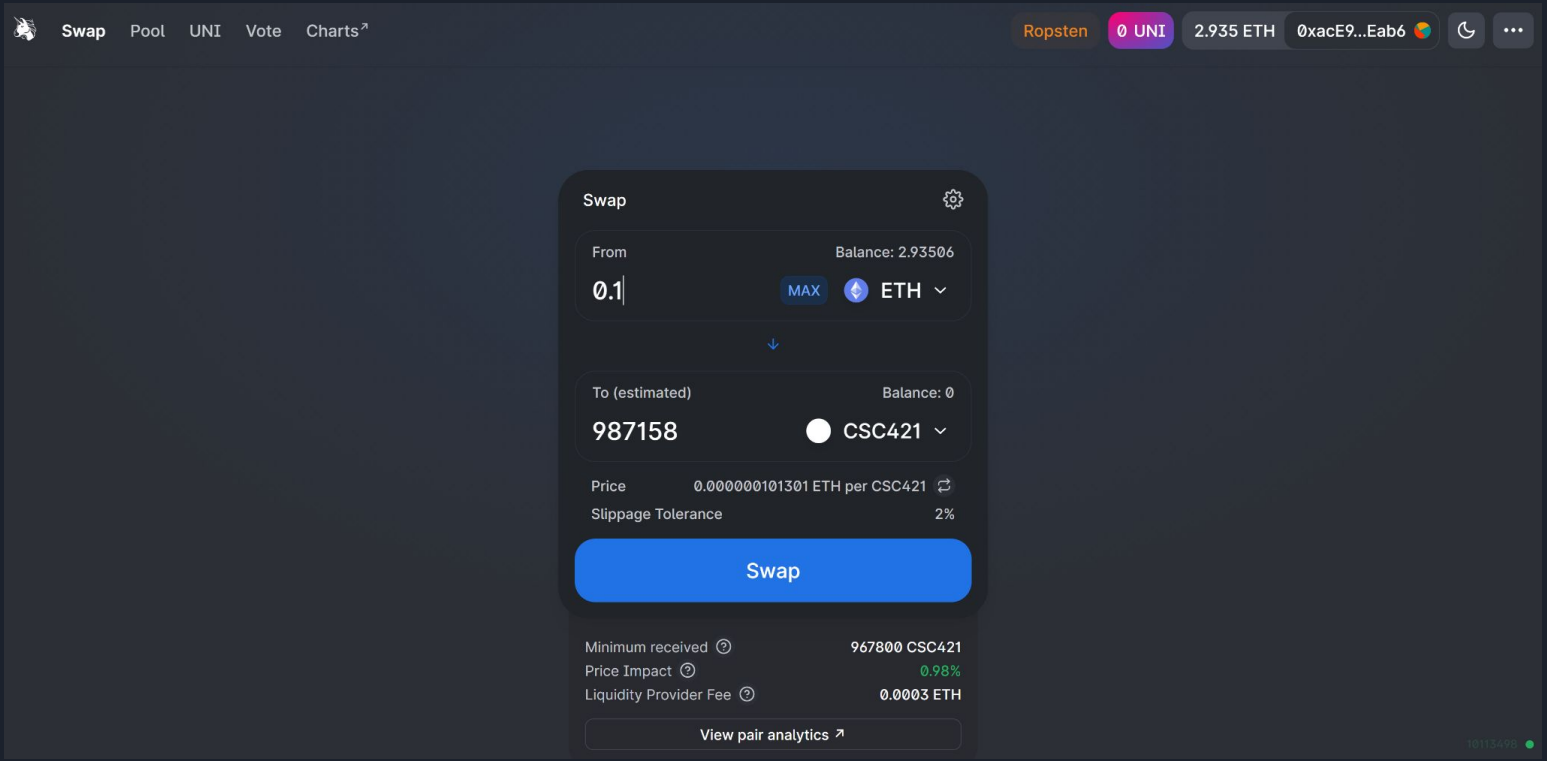
12.9627 ETH

100000000 CSC421

Decentralized Exchange (DEX)



app.uniswap.org



0x4af1CD46b87Cea2Bf5f7c890Ae8ded4871e109CE

Contract 0x4af1CD46b87Cea2Bf5f7c890Ae8ded4871e109CE

Contract Overview

Balance: 0 Ether

More Info More

My Name Tag: Not Available

Contract Creator: 0xace97d3ecae0777516… at txn 0x3cc27b995a90fe0188…

Token Tracker: DesignAndOrg (CSC421)

Transactions | Internal Txns | Contract | Events

Latest 3 from a total of 3 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0x9e0d1b37b9c1102f0a…	Approve	10113477	6 mins ago	0xace97d3ecae0777516…	IN	0x4af1cd46b87cea2bf5f…	0 Ether	0.00026558
0xb0a360898c6340a754…	Approve	10113473	7 mins ago	0xace97d3ecae0777516…	IN	0x4af1cd46b87cea2bf5f…	0 Ether	0.00046458
0x3cc27b995a90fe0188…	0x60806040	10113443	13 mins ago	0xace97d3ecae0777516…	IN	Contract Creation	0 Ether	0.01414983

Questions?