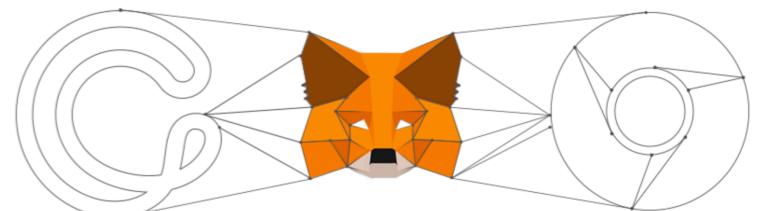


Install MetaMask

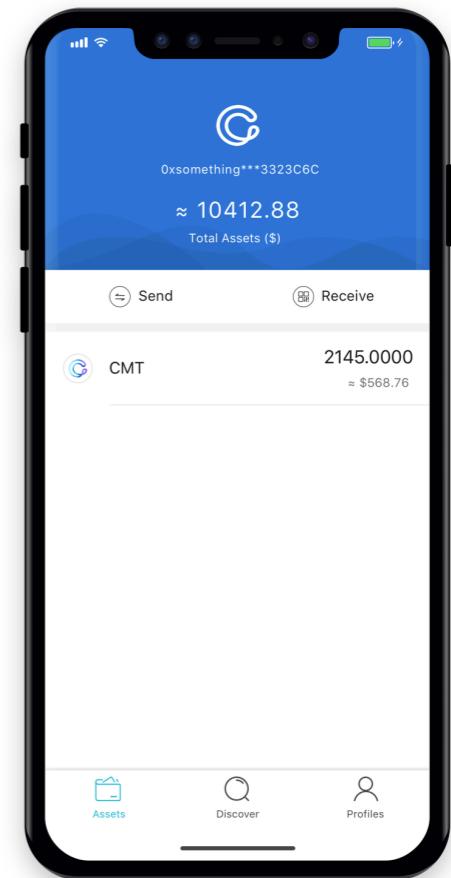
MetaMask For CMT: <https://www.cybermiles.io/metamask/>



Brings CyberMiles to your browser

Install CMT Wallet

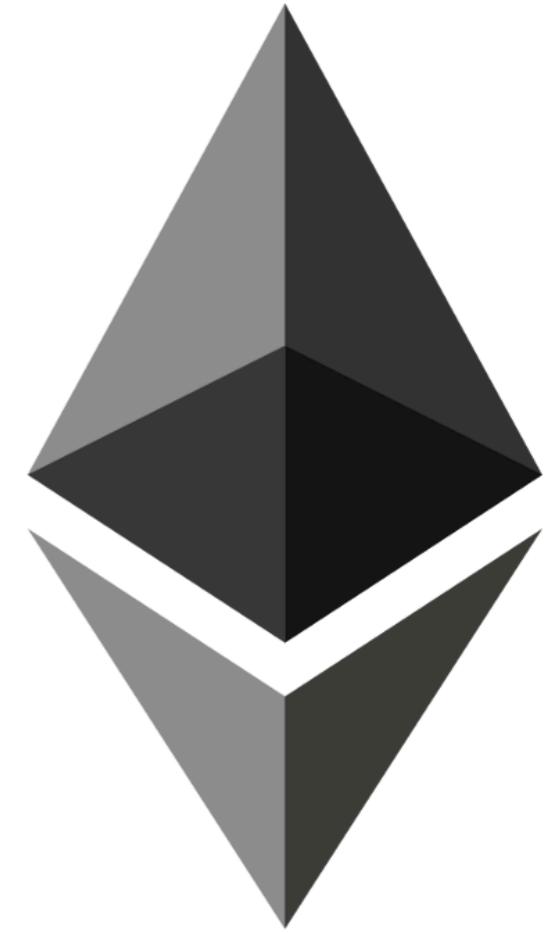
CMT Wallet: <https://www.cybermiles.io/cmt-wallet/>



Remix for CMT

Remix CMT: <http://remix.cybermiles.io/#version= builtin>

ERC20



Smart Contract 102

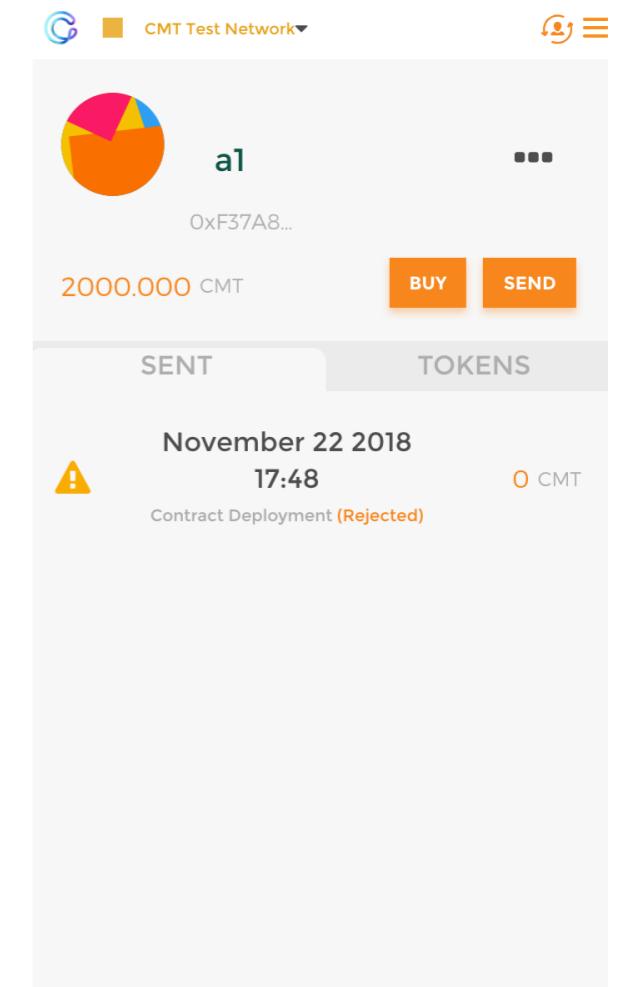
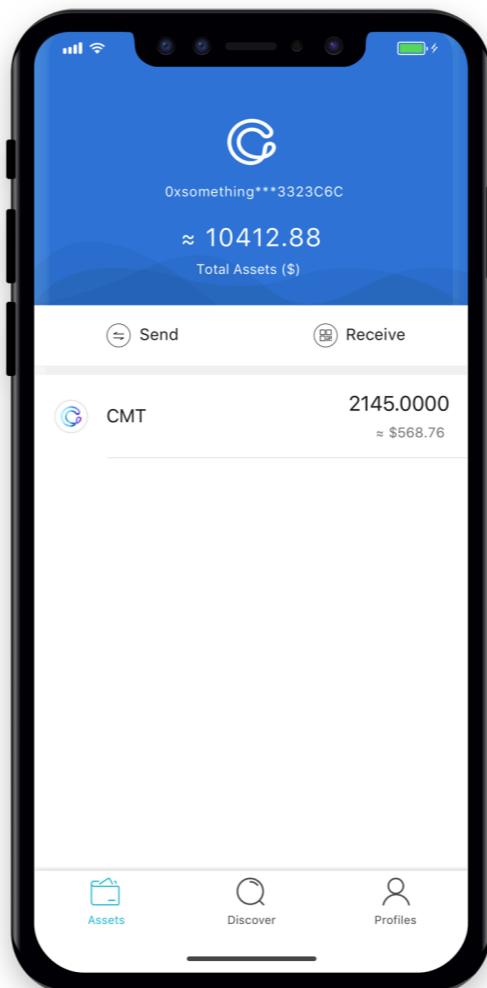
Zhun Shen, CyberMiles

Introduction

BUIDL
HODL

Wallet

- CMT Wallet
- MetaMask
- imToken
- MyEtherWallet
- ...



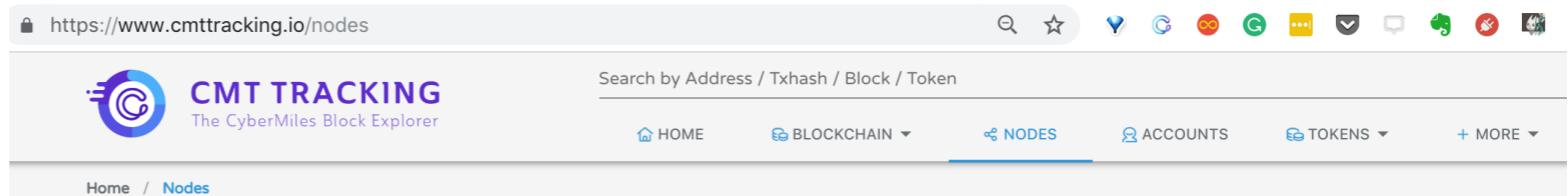
Gas



To run an application on Ethereum
YOU NEED GAS

Validator Nodes

- Validator
- Delegator



The screenshot shows a web browser displaying the CMT Tracking website at <https://www.cmtracking.io/nodes>. The page title is "CMT TRACKING - The CyberMiles Block Explorer". The navigation bar includes links for HOME, BLOCKCHAIN, NODES (which is underlined), ACCOUNTS, TOKENS, and MORE. Below the navigation is a search bar labeled "Search by Address / Txhash / Block / Token". The main content area is titled "Nodes" and displays a table of 21 validator nodes. The columns in the table are: Name, Voting Power, Rank, Owner Address, Verified, State, Location, Total Stakes, and Compensation.

Name	Voting Power	Rank	Owner Address	Verified	State	Location	Total Stakes	Compensation
Huobipool	6034201	1	0x64832de9...	Y	Validator	Beijing, China	18,697,488.86	50.00%
CyberMiles Vietnam	5950500	2	0x1b92c5bb...	Y	Validator	Sai Gon Vietnam	20,601,067.49	45.00%
SSnodes	5630576	3	0x55249a08...	Y	Validator	Shenzhen, China	26,777,865.44	30.00%
Kryptital Group	5066131	4	0x221507f2...	Y	Validator	Cayman Islands	25,456,251.53	40.00%
Noomi	3035192	5	0x70a52ff3...	Y	Validator	Malta	14,608,138.23	50.00%
Block Wonderland	2454528	6	0x858578e8...	Y	Validator	Osaka, Japan	14,269,031.43	20.00%
ArcBlock	2384371	7	0x9a3482fd...	Y	Validator	USA	7,579,880.38	50.00%
Hayek Capital	1774122	8	0x1724d4a8...	Y	Validator	Australia	7,977,886.07	50.00%
Wancloud	1613367	9	0x3af427d0...	Y	Validator	Shanghai, China	6,925,879.40	40.00%
Lvl99	1475966	10	0xcd3090e8...	Y	Validator	Jakarta, Indonesia	4,515,970.09	50.00%
COBINHOOD	1084823	11	0x89586183...	Y	Validator	Taipei, Taiwan	3,686,767.06	50.00%
TGL Capital	826364	12	0x1ac7d4f1...	Y	Validator	Beijing China	2,701,550.19	50.00%
Moon Fund	822574	13	0xeb65290b...	Y	Validator	San Francisco, USA	2,666,735.34	55.00%
Snow Eagle Group Limited	745698	14	0x0da518ec...	Y	Validator	Israel	2,470,486.03	50.00%
Hash Tower	683041	15	0xfd0e8e4c...	Y	Validator	Seoul, South Korea	2,271,780.86	50.00%
Portland Master Limited	608516	16	0x4cdaf011...	Y	Validator	Hong Kong	2,233,436.80	50.00%
LiMaGo	570972	17	0xf9a43166...	Y	Validator	Taipei Taiwan	2,167,319.76	50.00%
Ellipal	564415	18	0x77f05c29...	Y	Validator	Hongkong,China	5,743,397.18	20.00%
Seed Backup Validator	149494	19	0xe2185094...	Y	Validator	HK	508,794.86	99.00%
Seed Backup Validator	139561	20	0x04ba6cf9...	Y	Backup Validator	HK	474,990.54	99.00%
Cobo Validator	134508	21	0x73879b18...	N	Backup Validator	Beijing, China	544,234.89	50.00%

<https://www.cmtracking.io/>

DApp

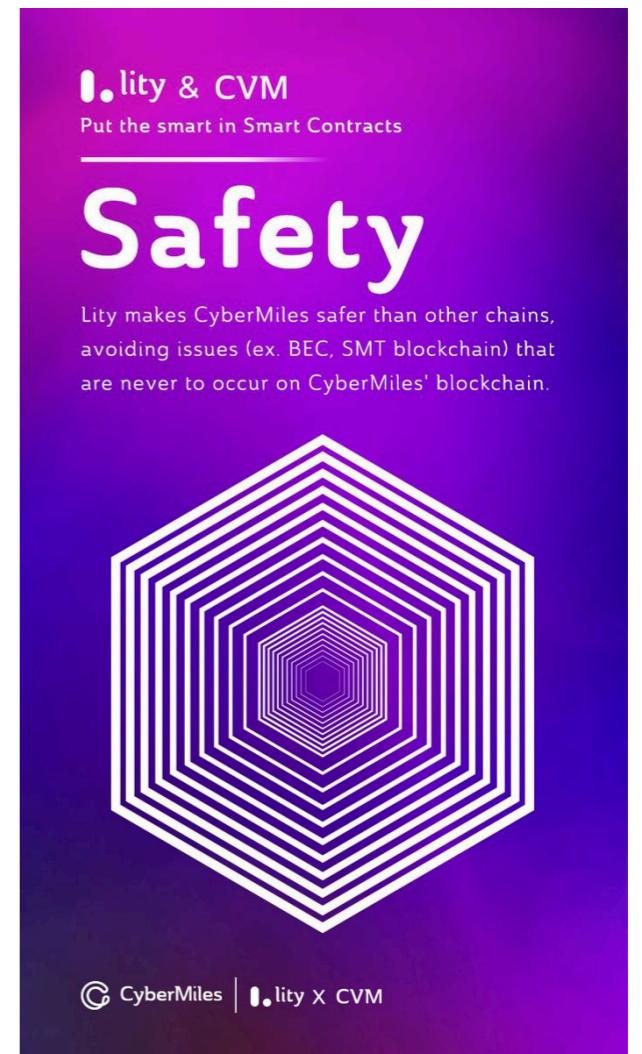


What is CryptoKitties?

CryptoKitties is a game centered around breedable, collectible, and oh-so-adorable creatures we call CryptoKitties! Each cat is one-of-a-kind and 100% owned by you; it cannot be replicated, taken away, or destroyed.

Language & Compiler

- Lity (powerful)
- Solidity
- ...



<https://www.litylang.org/>

Consensus Mechanism

- Proof of Work (POW)
- Delegated Proof of Stake (DPOS)
- ...

Warm-up

Hello World

```
pragma lity ^1.2.4;

contract HelloWorld {

    string helloMessage;
    address owner;

    modifier onlyOwner() {
        assert(msg.sender == owner);
        _;
    }

    constructor () public {
        helloMessage = "Hello world";
        owner = msg.sender;
    }

    function updateMessage (string _new_msg) public {
        helloMessage = _new_msg;
    }

    function sayHello() public view returns (string) {
        return helloMessage;
    }

    function terminate() external onlyOwner {
        selfdestruct(owner);
    }
}
```

ERC-20

What's a token contract

An application that

- keeps a record of all account balances
- allows transfer of tokens between accounts via signed transactions
- has trusted records due to the underlying blockchain

Coin vs Token

- Bitcoin operates and functions on the Bitcoin blockchain
- Ether operates and functions on the Ethereum blockchain
- CMT operates and functions on the CyberMiles blockchain
- ...



What's ERC20?

ERC: Token standard · Issue #20 · ethereum/EIPs

ERC: 20 Title: Token standard Status: Draft Type: Informational Created: 19–11.2015 Resolution: [https://github.com...](https://github.com/)

github.com



<https://github.com/ethereum/EIPs/issues/20>

Methods and Events

The ERC20 Token Standard Interface

Following is an interface contract declaring the required functions and events to meet the ERC20 standard:

```
1 // -----
2 // ERC Token Standard #20 Interface
3 // https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md
4 // -----
5 contract ERC20Interface {
6     function totalSupply() public constant returns (uint);
7     function balanceOf(address tokenOwner) public constant returns (uint balance);
8     function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
9     function transfer(address to, uint tokens) public returns (bool success);
10    function approve(address spender, uint tokens) public returns (bool success);
11    function transferFrom(address from, address to, uint tokens) public returns (bool success);
12
13    event Transfer(address indexed from, address indexed to, uint tokens);
14    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
15 }
```

Functions

Events

Most of the major tokens on the Ethereum blockchain are ERC20-compliant. The GNT Golem Network Token is only partially-ERC20-compliant as it does not implement the `approve(...)`, `allowance(...)` and `transferFrom(...)` functions, and the `Approval(...)` event.

Some of the tokens include further information describing the token contract:

```
1     string public constant name = "Token Name";
2     string public constant symbol = "SYM";
3     uint8 public constant decimals = 18; // 18 is the most common number of decimal places
```

Optional

Example(1)

Holder address	Balance
0x0000...0000	0
0x1f59...3492	100
0x2299...3ab7	100
0x4ba5...ae22	100
0x4919...413d	100
0x93f1...1b09	100
0xd8f0...c028	100
0xe20b...93b6	100
Total supply	700

Example(2)

Holder address	Balance
0x0000...0000	0
0x1f59...3492	110
0x2299...3ab7	90
0x4ba5...ae22	100
0x4919...413d	100
0x93f1...1b09	100
0xd8f0...c028	100
0xe20b...93b6	100

Total supply 700

Let's create your own token

CMT Wallet Dapp

A screenshot of a mobile application form titled 'Issue Token'. It has three input fields: 'Token Name *' with placeholder 'Please enter the token name', 'Token Abbreviation *' with placeholder 'less than 5 characters', and 'Total Supply *' with placeholder 'Please enter the Total Supply'. Below the fields, a note says 'Your wallet balance need to be greater than 1000 CMT'. A large grey 'Submit' button is at the bottom.

- Dapps
- Issue Token >
One-step issue your token
 - BlockTonic >
Free shopping:Pay CMT,100% Cashback
 - CMT Tracking >
CyberMiles block explorer

- News
- Celebrating a year of success thanks to YOU
[cybermiles.io](#)
 - CyberMiles Mainnet Launch & Migration Notice
[cybermiles.io](#)
 - Validator Program
[cybermiles.io](#)

Don't have 1000 CMT?

<http://remix.cybermiles.io/#version= builtin>

Types of Addresses

- Regular Address (you own private key)
- Smart Contract Address (you don't)
- ...

**Do not send ETH/CMT directly to
an Ethereum/CyberMiles contract**

Play with methods

The screenshot shows the Remix Ethereum IDE interface. On the left, there is a code editor window titled "browser/erc20_demo.sol" containing Solidity code. The code includes imports for `ERC20Basic` and `SafeMath`, and defines a `SafeMath` library. The `ERC20Basic` contract has functions for `totalSupply`, `balanceOf`, `transfer`, and an event `Transfer`. The `SafeMath` library contains various mathematical operations with safety checks.

At the top right, there are buttons for "Compile", "Run", and "Settings". Below these, the "Deployed Contracts" section shows a single contract named "TTT at 0x0d4...c8f6a (blockchain)". A red box highlights the list of methods for this contract:

- approve address_spender, uint256 _value
- decreaseApproval address_spender, uint256 _subtractedValue
- increaseApproval address_spender, uint256 _addedValue
- pause
- transfer address_to, uint256 _value
- transferFrom address_from, address_to, uint256 _value
- transferOwnership address newOwner
- unpause
- allowance address_owner, address_spender
- balanceOf address_owner
- decimals
- name
- owner
- paused
- symbol
- totalSupply

At the bottom left, there is a sidebar with sections for "webs-CMT.js" and "Metamask for CMT". A note in the sidebar says: "Executing common command to interact with the Remix interface (see list of commands above). Note that these commands can also be included and run from a JavaScript script."

Problems of ERC20

- “Do not send to exchange addresses!”
- ”I send some tokens to the contract address! Help!”
- ”My tokens are locked in an inactive smart contract!”
- Very difficult to do KYC
- Very hard to raise funding in other ERC 20 tokens
- Unsafe from hacking

Why Lity

<https://www.litylang.org/security/#erc-checker>

Use Cases

- credits
- coupon
- money/time
- ...



Q&A