

BUILD YOUR OWN SMART CONTRACT

BY

SHRUTIRUPA BANERJEE



WHOAMI

- WAF Research @Qualys
- InfosecGirls Pune Chapter Lead
- WomenWhoCode Pune lead
- Independent Researcher

CONTACT ME

- Twitter: @freak_crypt
- Linkedin: Shrutirupa-Banerjee

<https://about.me/shrutirupa>

AGENDA

- What is Ethereum
- What are smart contracts
- Terminologies
- Demo

ETHEREUM

- Public blockchain platform
- Introduction to smart contracts

WHAT ARE SMART CONTRACTS

- Piece of code
- Satisfies certain conditions

TERMINOLOGIES

- Solidity
- Gas
- EVM
- Remix IDE
- Metamask
- ...

SOLIDITY

- Language used to write Ethereum based smart contract

GAS

- Fuel to carry on the transaction

EVM

- Works like a runtime environment for smart contracts in Ethereum
- Similar to JVM

METAMASK

- A wallet or a browser plugin
- Helps to connect to the blockchain network

REMIX IDE

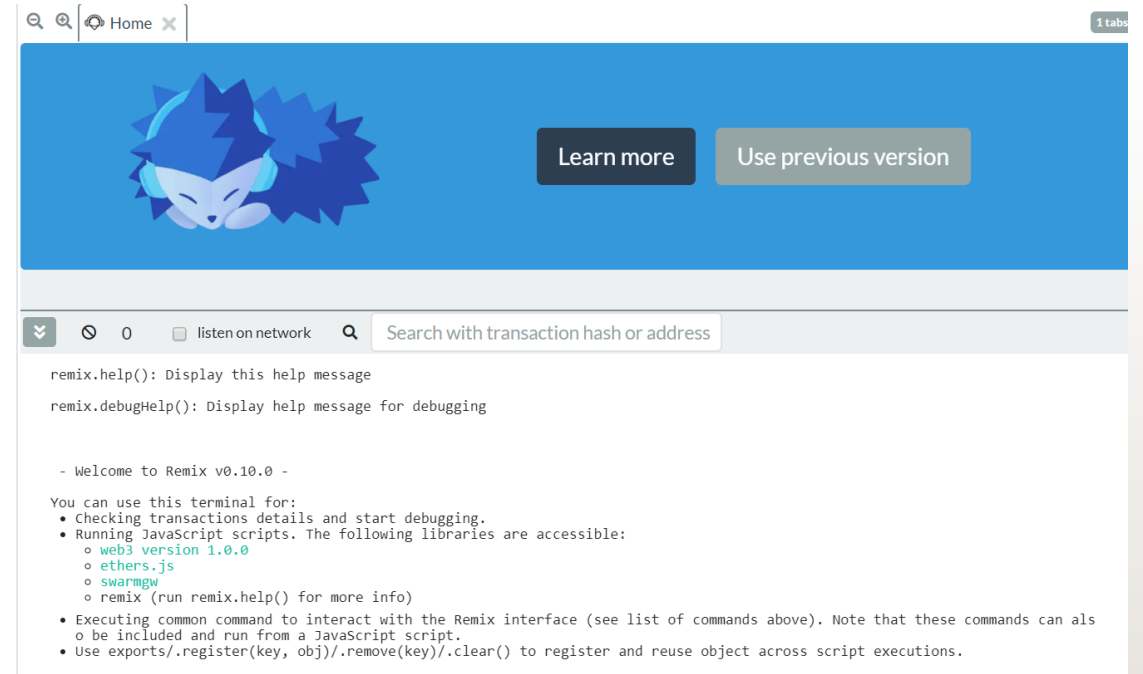
- Online IDE for writing smart contracts



FILE EXPLORERS

▼ browser + ↻ 📁

Fallout.sol
c1.sol
ballot_test.sol
sample.sol
ballot.sol
FallbackExploit.sol
Fal1out.sol



browser
config

```
1 pragma solidity >=0.4.22 <0.6.0;
2 contract Ballot {
3
4     struct Voter {
5         uint weight;
6         bool voted;
7         uint8 vote;
8         address delegate;
9     }
10    struct Proposal {
11        uint voteCount;
12    }
13
14    address chairperson;
15    mapping(address => Voter) voters;
```

[2] only remix transactions, script

Search transactions

- Welcome to Remix v0.7.7 -

You can use this terminal for:

- Checking transactions details and start debugging.
- Running JavaScript scripts. The following libraries are accessible:
 - [web3 version 1.0.0](#)
 - [ethers.js](#)
 - [swarmgw](#)
 - compilers - contains currently loaded compiler
- 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.
- Use `exports/.register(key, obj)/.remove(key)/.clear()` to register and reuse object across script executions.

CompileRunAnalysisTestingDebuggerSettingsSu

Switch to the new interface!

Current
version:0.5.1+commit.c8a2cb62.Emscripten.clang

Select new compiler version

☒ Auto compile☐ Enable Optimization

☐ Hide warnings

Start to compile (Ctrl-S)

Ballot

Swarm

DetailsABIBytecode

Static Analysis raised 3 warning(s) that requires your attention. Click here to show the warning(s).

Ballot

SAMPLE CONTRACT

The screenshot displays the Remix IDE interface. The main editor shows a Solidity contract named `SimpleStorage` with the following code:

```
1 pragma solidity >=0.4.22 <0.6.0;
2
3
4 contract SimpleStorage {
5     uint storedData;
6
7     function set(uint x) public {
8         storedData = x;
9     }
10
11     function get() public view returns (uint) {
12         return storedData;
13     }
14 }
```

The left sidebar shows a file explorer with a folder named `browser` and a file named `config`. The right sidebar contains deployment settings:

- Environment:** Injected Web3 (Ropsten (3))
- Account:** 0x547...6fe8d (5.9999956401 ether)
- Gas limit:** 3000000
- Value:** 0 wei

Below these settings, there is a dropdown menu showing `SimpleStorage` and a `Deploy` button. Below the `Deploy` button, there is an `or` label and a section for `At Address` with a text input field labeled `Load contract from Address`.

At the bottom of the right sidebar, there is a section for `Transactions recorded: 1` and a `Deployed Contracts` section with a trash icon.

The bottom of the interface shows a console with the following output:

- 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.
- Use `exports.register(key, obj).remove(key).clear()` to register and reuse object across script executions.

The console also shows the text `creation of Ballot pending...` and a large `remix` watermark.

DEMO



REFERENCES

- <https://github.com/ethereum/solidity>
- <https://solidity.readthedocs.io/en/v0.4.24/introduction-to-smart-contracts.html>
- <https://remix.ethereum.org/>
- <https://etherscan.io/>
- <https://solidity.readthedocs.io/en/v0.4.24/introduction-to-smart-contracts.html>
- <https://ropsten.etherscan.io/>
- <https://metamask.io/>