BUILD YOUR OWN SMART CONTRACT

BY

SHRUTIRUPA BANERJIEE

WHOAMI

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

CONTACT ME

- Twitter: @freak_crypt
- Linkedin: Shrutirupa-Banerjiee

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

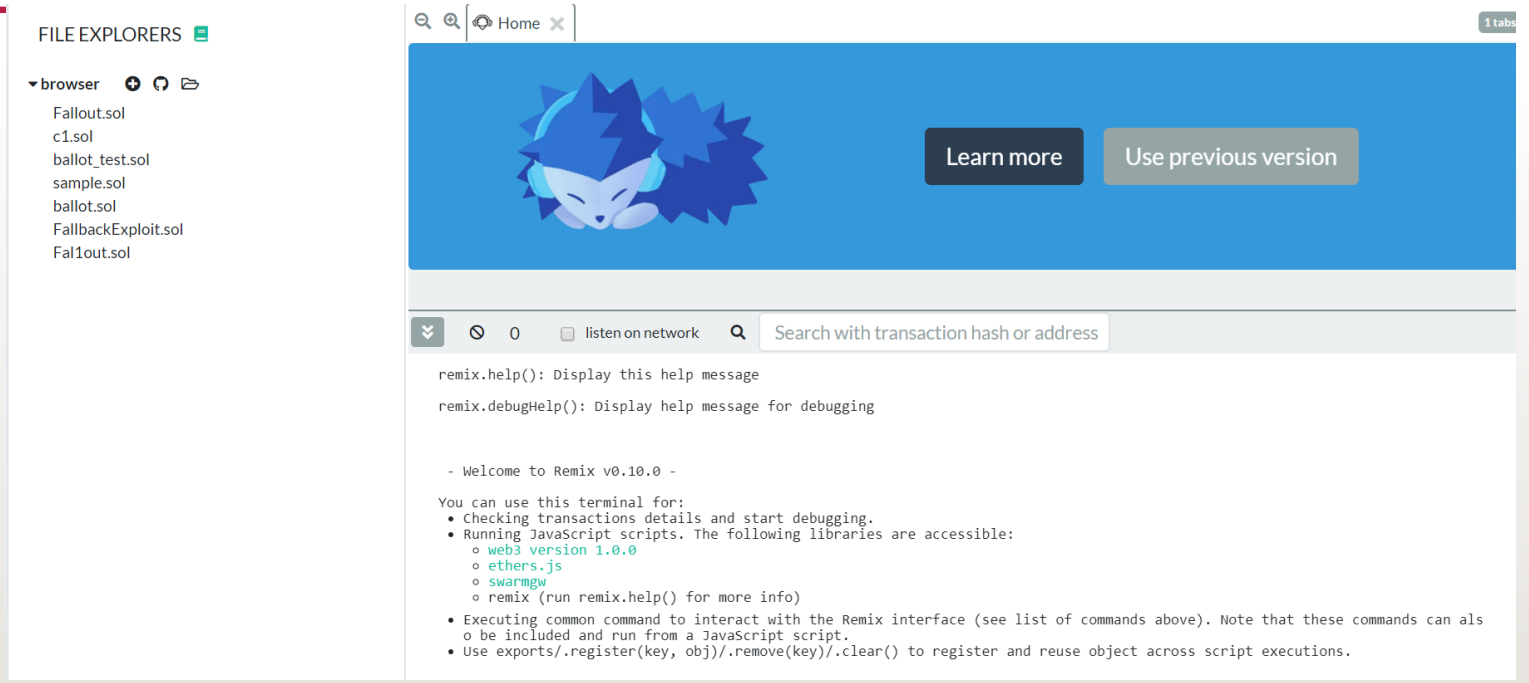
METAMASK

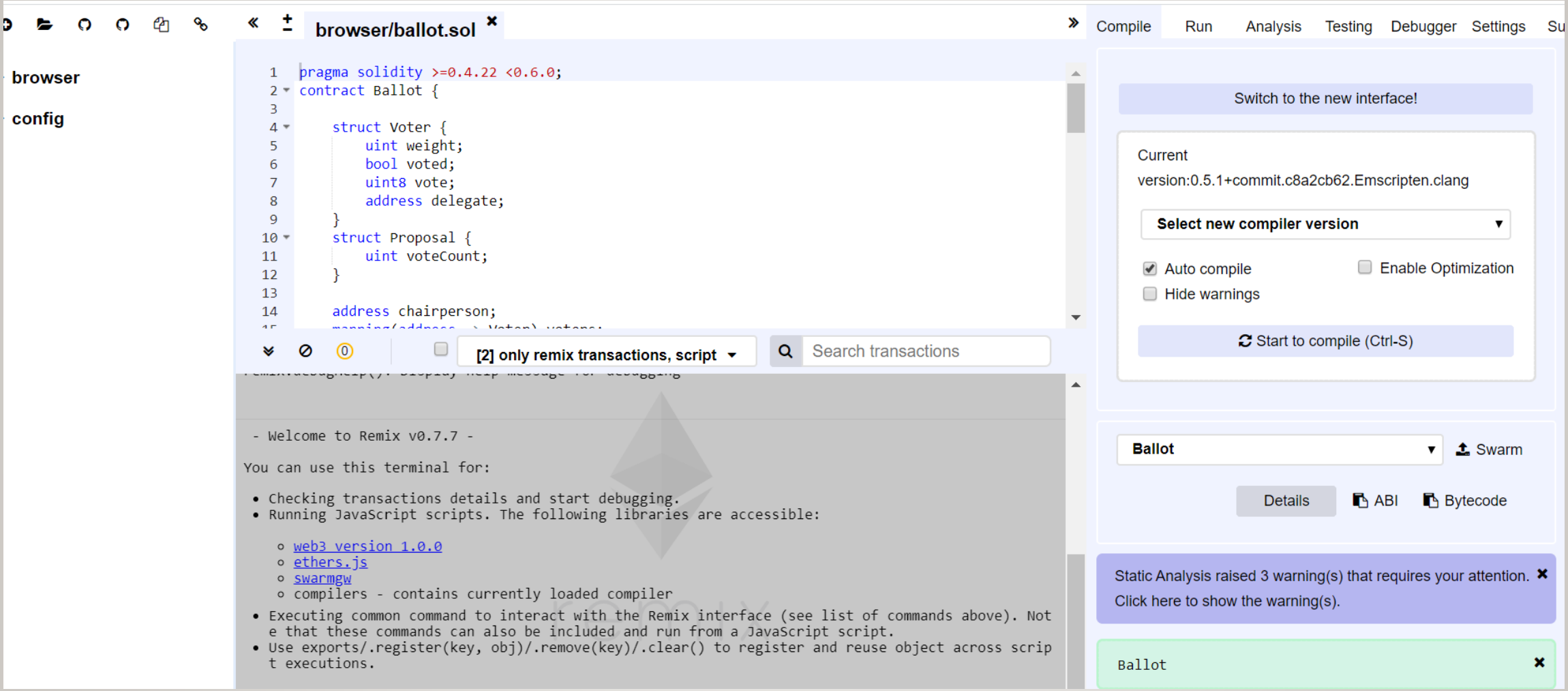
- A wallet or a browser plugin
- Helps to connect to the blockchain network

REMIX IDE

- Online IDE for writing smart contracts

REMIX IDE


FILE EXPLORERS
browser
Fallout.sol
c1.sol
ballot_test.sol
sample.sol
ballot.sol
FallbackExploit.sol
Fal1out.sol
Home
1 tabs
Learn more
Use previous version
0
listen on network
Search with transaction hash or address
remix.help(): Display this help message
remix.debugHelp(): Display help message for debugging
- Welcome to Remix v0.10.0 -
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
remix (run remix.help() for more info)
• Executing common command to interact with the Remix interface (see list of commands above). Note that these commands can als o be included and run from a JavaScript script.
• Use exports/.register(key, obj)/.remove(key)/.clear() to register and reuse object across script executions.


browser
config
browser/ballot.sol
pragma solidity >=0.4.22 <0.6.0;
contract Ballot {
struct Voter {
uint weight;
bool voted;
uint8 vote;
address delegate;
}
struct Proposal {
uint voteCount;
}
address chairperson;
[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.
Compile
Run
Analysis
Testing
Debugger
Settings
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
Details
ABI
Bytecode
Static Analysis raised 3 warning(s) that requires your attention.
Click here to show the warning(s).
Ballot

SAMPLE CONTRACT

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/