Programming Language Survey - Solidity

Solidity

Presented by Nedurumalli Ved Varshith Reddy
CB.EN.U4CYS22045
TIFAC-CORE in Cyber Security
Amrita Vishwa Vidyapeetham, Coimbatore Campus

Feb 24, 2023

Outline

1. What is Solidity ??
2. Solidity Syntax
3. More About Solidity
4. References

Introduction

- ***Solidity*** is an ***contract-oriented*** programming language created specifically by the ***Ethereum Network*** team for constructing and designing **smart contracts** on Blockchain platforms.
- It's used to create smart contracts that implement business logic and generate a chain of transaction records in the blockchain system
- This is a **high-level** programming language which is still under development
- It is one those open source languages which are under development

Real Life Applications Of Solidity

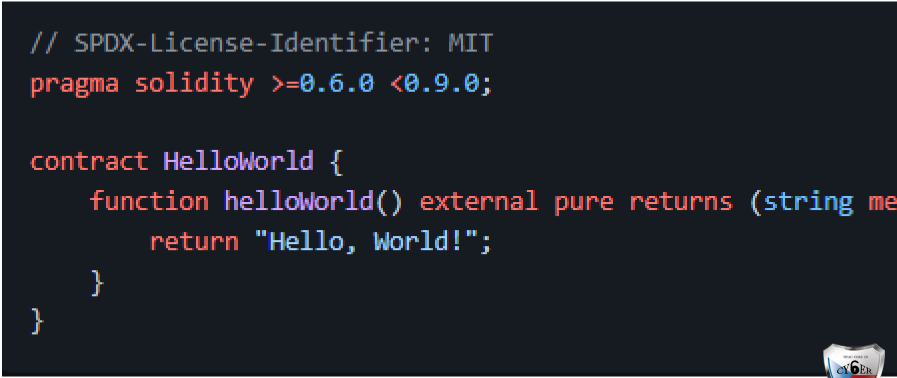
- Solidity is an contract-oriented programming language for implementing smart contracts on various blockchain platforms, most notably, Ethereum.
- Solidity can be used to creating contracts like voting, blind auctions, crowdfunding, multi-signature wallets
- ***Smart Contracts*** are computer programs published and executed in a blockchain environment. As they run on blockchains, they can be run without a central party or server.
- Solidity programs are run on **Ethereum Virtual Machines(EVM)**
- **Remix** can be used to compile Solidity online without installing any compiler

Solidity Syntax

- **Pragmas** are instructions to the compiler on how to treat the code. All solidity source code should start with a “version pragma” which is a declaration of the version of the solidity compiler this code should use.
- **A Solidity contract** is a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereumblockchain.
- A **function** is a group of reusable code which can be called anywhere in your program. This eliminates the need of writing the same code again and again. It helps programmers in writing modular codes.
- A Solidity function can have an optional **Return** statement. This is required if you want to return a value from a function.In Solidity, a function can return multiple values as well

Additional Info On Solidity

- Solidity was developed by *Christian Reitwiessner* , *Alex Beregszaszi*, and several former Ethereum core contributors on March 8 , 2018
- Solidity is the product of *Python* , *Javascript, C++*
- ***Hello World in Solidity***



```
// SPDX-License-Identifier: MIT
pragma solidity >=0.6.0 <0.9.0;

contract HelloWorld {
    function helloWorld() external pure returns (string me
        return "Hello, World!";
    }
}
```

Some of the Limitations of Solidity

- **Unchecked External Call** : The send and call function will return a Boolean Value which return a false value in terms of exceptions but will not revert the transaction
- **Costly Loops and Gas Limit** : An attacker can include infinite loops within an array to exhaust the Gas limit mimicking a DoS attack and freezing the transaction
- **Unexpected Ether** : Contracts that rely on code execution for every single Ether transaction are vulnerable because it can send Ether forcibly to another contract.
- **Overflow and Underflow** : The underflow and overflow issues happen when a user is trying to store a value that is out of the Solidity data type's range.

References

https://en.wikipedia.org/wiki/Solidity
https://101blockchains.com/solidity-issues/
https://github.com/ethereum/solidity
https://www.tutorialspoint.com/solidity/solidity_basic_syntax.htm