VYPER

19CSE100 - PROBLEM SOLVING AND ALGORITHMIC THINKING
Programming language survey

Presented by Deepak Kumar S
CB.EN.U4CYS22020
TIFAC-CORE in Cyber Security
Amrita Vishwa Vidyapeetham, Coimbatore Campus

Feb 28, 2023

Contents

1. VYPER : Creation
2. Paradigm
3. O.S supported
4. Influences
5. Example
6. Real-Time Application
7. Bibliography

VYPER : Creation

- The programming language was developed by a team led by Taylor Monahan, a software developer and co-founder of My Ether Wallet. Monahan started the project in 2016 and the Vyper team is currently actively developing and maintaining the language.
- As per GitHub, the first commit on Vyper was done by Charles cooper. Its Beta version was first released and committed on 22 August 2020. And the first commit was on March 13 2018 on version 0.0.4

Paradigm

Vyper is an

- Object-oriented
- Experimental oriented
- Statically typed oriented
- Contract-oriented programming language.
- Like objects in object-oriented programming, each contract contains state variables, functions, and common data types.

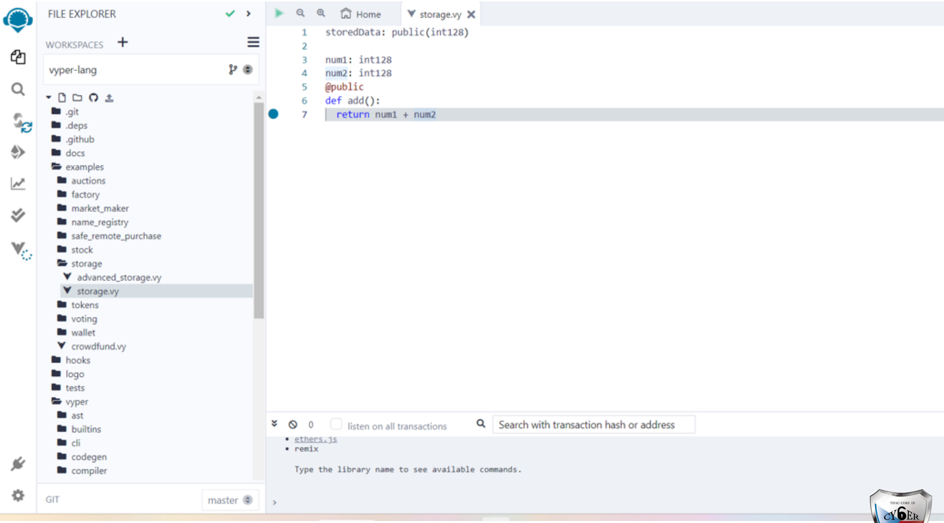
O.S supported

- Ubuntu
- Python3.6 or greater
- Mac OS

Influences

- Vyper is a relatively new, pythonic programming language used to write smart contracts. Vyper targets Ethereum Virtual Machine (EVM). After solidity vyper is the second most popular language to write smart contracts.

Program



```
storedData: public(int128)

num1: int128
num2: int128
@public
def add():
    return num1 + num2
```

```
• ethers.js
• remix

 Type the library name to see available commands.
```

Figure: Adding of two numbers

Syntax Explanation

- I used Remix – Ethereum IDE to work on Vyper. I plugged in Vyper and started my code on the addition of two numbers

  Declare two variables to hold the input numbers
- num1: int128
- num2: int128

  A function to add the two numbers and return the result
- @public
- def add():
- return num1 + num2

Real - Time Application

Vyper is the relatively new pythonic language used to write smart contracts that run on the Ethereum virtual machine.
The features of Vyper are:

- It is strongly typed.
- Has support for signed integers and decimal fixed-point numbers.
- Small and understandable code like Python.
- Has Bounds and Overflow checking.
- Decidability: With Vyper, It is possible to compute a precise upper bound for any function call's gas consumption.
- Limited support for pure functions: Any constant in Vyper cannot change state.
- Vyper omits most of the Object-Oriented Programming paradigms - perhaps requires a new paradigm definition for transactional programming.

In a study conducted in 2018, where they analyzed nearly one million deployed Ethereum smart contracts, it was found that many of these contracts had some severe vulnerabilities; the researchers divided these contracts into three categories to better identify and trace vulnerabilities:

- Suicidal Contracts - Smart contracts that arbitrary addresses can kill.
- Greedy Contracts - Sometimes, smart contracts can reach a state where they are unable to release ether, smart contracts in this phase are called Greedy contracts.
- Prodigal Contracts - Smart contracts that can be made to release ether to arbitrary adhttps://docs.vyperlang.org/en/stable/vyper-by-example.htmldresses.
- Vyper tries to eliminate this by letting users write secure code and making it difficult for programmers to write misleading or vulnerable code accidentally.

References

https://remix.ethereum.org/#optimize=false&runs=200&evmVersion=null
https://docs.vyperlang.org/en/stable/compiling-a-contract.html
https://docs.vyperlang.org/en/stable/vyper-by-example.html