
Vyper Documentation

Vitalik Buterin

Mar 12, 2019

Contents

1	Principles and Goals	3
2	Compatibility-breaking Changelog	5
3	Glossary	7
3.1	Installing Vyper	7
3.2	Compiling a Contract	11
3.3	Testing a Contract	11
3.4	Deploying a Contract	12
3.5	Structure of a Contract	12
3.6	Vyper by Example	17
3.7	Event Logging	36
3.8	Contributing	38
3.9	Frequently Asked Questions	39
3.10	Built in Functions	40
3.11	Low Level Built in Functions	45
3.12	Types	47
3.13	Release Notes	56

Vyper is a contract-oriented, pythonic programming language that targets the [Ethereum Virtual Machine \(EVM\)](#)

Principles and Goals

- **Security:** It should be possible and natural to build secure smart-contracts in Vyper.
- **Language and compiler simplicity:** The language and the compiler implementation should strive to be simple.
- **Auditability:** Vyper code should be maximally human-readable. Furthermore, it should be maximally difficult to write misleading code. Simplicity for the reader is more important than simplicity for the writer, and simplicity for readers with low prior experience with Vyper (and low prior experience with programming in general) is particularly important.

Because of this Vyper aims to provide the following features:

- **Bounds and overflow checking:** On array accesses as well as on arithmetic level.
- **Support for signed integers and decimal fixed point numbers**
- **Decidability:** It should be possible to compute a precise upper bound for the gas consumption of any function call.
- **Strong typing:** Including support for units (e.g. timestamp, timedelta, seconds, wei, wei per second, meters per second squared).
- **Small and understandable compiler code**
- **Limited support for pure functions:** Anything marked constant is not allowed to change the state.

Following the principles and goals, Vyper **does not** provide the following features:

- **Modifiers:** For example in Solidity you can define a function `foo() mod1 { ... }`, where `mod1` can be defined elsewhere in the code to include a check that is done before execution, a check that is done after execution, some state changes, or possibly other things. Vyper does not have this, because it makes it too easy to write misleading code. `mod1` just looks too innocuous for something that could add arbitrary pre-conditions, post-conditions or state changes. Also, it encourages people to write code where the execution jumps around the file, harming auditability. The usual use case for a modifier is something that performs a single check before execution of a program; our recommendation is to simply inline these checks as asserts.
- **Class inheritance:** Class inheritance requires people to jump between multiple files to understand what a program is doing, and requires people to understand the rules of precedence in case of conflicts (“Which class’s

function ‘X’ is the one that’s actually used?”). Hence, it makes code too complicated to understand which negatively impacts auditability.

- **Inline assembly:** Adding inline assembly would make it no longer possible to search for a variable name in order to find all instances where that variable is read or modified.
- **Function overloading** - This can cause lots of confusion on which function is called at any given time. Thus it’s easier to write misleading code (`foo("hello")` logs “hello” but `foo("hello", "world")` steals you funds). Another problem with function overloading is that it makes the code much harder to search through as you have to keep track on which call refers to which function.
- **Operator overloading:** Operator overloading makes writing misleading code possible. For example “+” could be overloaded so that it executes commands the are not visible at first glance, such as sending funds the user did not want to send.
- **Recursive calling:** Recursive calling makes it impossible to set an upper bound on gas limits, opening the door for gas limit attacks.
- **Infinite-length loops:** Similar to recursive calling, infinite-length loops make it impossible to set an upper bound on gas limits, opening the door for gas limit attacks.
- **Binary fixed point:** Decimal fixed point is better, because any decimal fixed point value written as a literal in code has an exact representation, whereas with binary fixed point approximations are often required (e.g. $(0.2)_{10} = (0.001100110011\dots)_2$, which needs to be truncated), leading to unintuitive results, e.g. in Python $0.3 + 0.3 + 0.3 + 0.1 \neq 1$.

Compatibility-breaking Changelog

- **2019.03.04:** *create_with_code_of* has been renamed to *create_forwarder_to*. (#1177)
- **2019.02.14:** Assigning a persistent contract address can only be done using the *bar_contact = ERC20(<address>)* syntax.
- **2019.02.12:** ERC20 interface has to be imported using *from vyper.interfaces import ERC20* to use.
- **2019.01.30:** Byte array literals need to be annotated using *b""*, strings are represented as *""*.
- **2018.12.12:** Disallow use of *None*, disallow use of *del*, implemented *clear()* built-in function.
- **2018.11.19:** Change mapping syntax to use *map()*. (VIP564)
- **2018.10.02:** Change the convert style to use types instead of string. (VIP1026)
- **2018.09.24:** Add support for custom constants.
- **2018.08.09:** Add support for default parameters.
- **2018.06.08:** Tagged first beta.
- **2018.05.23:** Changed *wei_value* to be *uint256*.
- **2018.04.03:** Changed bytes declaration from *'bytes <= n'* to *'bytes[n]'*.
- **2018.03.27:** Renaming *signed256* to *int256*.
- **2018.03.22:** Add modifiable and static keywords for external contract calls.
- **2018.03.20:** Renaming *__log__* to *event*.
- **2018.02.22:** Renaming *num* to *int128*, and *num256* to *uint256*.
- **2018.02.13:** Ban functions with payable and constant decorators.
- **2018.02.12:** Division by *num* returns decimal type.
- **2018.02.09:** Standardize type conversions.
- **2018.02.01:** Functions cannot have the same name as globals.
- **2018.01.27:** Change getter from *get_var* to *var*.

- **2018.01.11:** Change version from 0.0.2 to 0.0.3
- **2018.01.04:** Types need to be specified on assignment ([VIP545](#)).
- **2017.01.02** Change `as_wei_value` to use quotes for units.
- **2017.12.25:** Change name from Viper to Vyper.
- **2017.12.22:** Add `continue` for loops
- **2017.11.29:** `@internal` renamed to `@private`.
- **2017.11.15:** Functions require either `@internal` or `@public` decorators.
- **2017.07.25:** The `def foo() -> num(const): ...` syntax no longer works; you now need to do `def foo() -> num: ...` with a `@constant` decorator on the previous line.
- **2017.07.25:** Functions without a `@payable` decorator now fail when called with nonzero wei.
- **2017.07.25:** A function can only call functions that are declared above it (that is, A can call B only if B appears earlier in the code than A does). This was introduced to prevent infinite looping through recursion.

3.1 Installing Vyper

Don't panic if the installation fails. Vyper is still under development and undergoes constant changes. Installation will be much more simplified and optimized after a stable version release.

Take a deep breath, follow the instructions, and please [create an issue](#) if you encounter any errors.

Note: The easiest way to try out the language, experiment with examples, and compile code to `bytecode` or `LLL` is to use the online compiler at <https://vyper.online/>.

3.1.1 Prerequisites

Installing Python 3.6

Vyper can only be built using Python 3.6 and higher. If you are already running Python 3.6, skip to the next section, else follow the instructions here to make sure you have the correct Python version installed, and are using that version.

Ubuntu

16.04 and older

Start by making sure your packages are up-to-date:

```
sudo apt-get update
sudo apt-get -y upgrade
```

Install Python 3.6 and some necessary packages:

```
sudo apt-get install build-essential libssl-dev libffi-dev
wget https://www.python.org/ftp/python/3.6.2/Python-3.6.2.tgz
tar xzf Python-3.6.2.tgz
cd Python-3.6.2/
./configure --prefix /usr/local/lib/python3.6
sudo make
sudo make install
```

16.10 and newer

From Ubuntu 16.10 onwards, the Python 3.6 version is in the *universe* repository.

Run the following commands to install:

```
sudo apt-get update
sudo apt-get install python3.6
```

Note: If you get the error *Python.h: No such file or directory* you need to install the python header files for the Python C API with

```
sudo apt-get install python3-dev
```

Arch

Using your aur helper of choice ([yay](#) here).

```
yay -S vyper
```

MacOS

Make sure you have Homebrew installed. If you don't have the *brew* command available on the terminal, follow [these instructions](#) to get Homebrew on your system.

To install Python 3.6, follow the instructions here: [Installing Python 3 on Mac OS X](#)

Also, ensure the following libraries are installed using *brew*:

```
brew install gmp leveldb
```

Creating a virtual environment

It is **strongly recommended** to install Vyper in a **virtual Python environment**, so that new packages installed and dependencies built are strictly contained in your Vyper project and will not alter or affect your other development environment set-up.

To create a new virtual environment for Vyper run the following commands:

```
sudo apt install virtualenv
virtualenv -p python3.6 --no-site-packages ~/vyper-venv
source ~/vyper-venv/bin/activate
```

To find out more about virtual environments, check out: [virtualenv guide](#).

You can also create a virtual environment without virtualenv:

```
python3.6 -m venv ~/vyper-env
source ~/vyper-env/bin/activate
```

3.1.2 Installation

Again, it is **strongly recommended to install Vyper in a virtual Python environment**. This guide assumes you are in a virtual environment containing Python 3.6.

Get the latest version of Vyper by cloning the Github repository, and run the install and test commands:

```
git clone https://github.com/ethereum/vyper.git
cd vyper
make
make test
```

Additionally, you may try to compile an example contract by running:

```
vyper examples/crowdfund.vy
```

If everything works correctly, you are now able to compile your own smart contracts written in Vyper. If any unexpected errors or exceptions are encountered, please feel free to create an issue <<https://github.com/ethereum/vyper/issues/new>>.

Note: If you get the error *fatal error: openssl/aes.h: No such file or directory* in the output of *make*, then run *sudo apt-get install libssl-dev*, then run *make* again.

For MacOS users:

Apple has deprecated use of OpenSSL in favor of its own TLS and crypto libraries. This means that you will need to export some OpenSSL settings yourself, before you can install Vyper.

Use the following commands:

```
export CFLAGS="-I$(brew --prefix openssl)/include"
export LDFLAGS="-L$(brew --prefix openssl)/lib"
pip install script
```

Now you can run the install and test commands again:

```
make
make test
```

If you get the error *ld: library not found for -lyaml* in the output of *make*, make sure *libyaml* is installed using *brew info libyaml*. If it is installed, add its location to the compile flags as well:

```
export CFLAGS="-I$(brew --prefix openssl)/include -I$(brew --prefix libyaml)/include"
export LDFLAGS="-L$(brew --prefix openssl)/lib -L$(brew --prefix libyaml)/lib"
```

You can then run *make* and *make test* again.

3.1.3 PIP

Each tagged version of vyper is also uploaded to pypi, and can be installed using pip.

```
pip install vyper
```

To install a specific version use:

```
pip install vyper==0.1.0b2
```

3.1.4 Docker

Dockerhub

Vyper can be downloaded as docker image from dockerhub:

```
docker pull ethereum/vyper
```

To run the compiler use the *docker run* command:

```
docker run -v $(pwd):/code vyper /code/<contract_file.vy>
```

Alternatively you can log into the docker image and execute vyper on the prompt.

```
docker run -v $(pwd):/code/ -it --entrypoint /bin/bash vyper
root@d35252d1fb1b:/code# vyper <contract_file.vy>
```

The normal paramaters are also supported, for example:

```
docker run -v $(pwd):/code vyper -f abi /code/<contract_file.vy>
[{'name': 'test1', 'outputs': [], 'inputs': [{'type': 'uint256', 'name': 'a'}, {'type': 'bytes', 'name': 'b'}], 'constant': False, 'payable': False, 'type': 'function', 'gas': 441}, {'name': 'test2', 'outputs': [], 'inputs': [{'type': 'uint256', 'name': 'a'}], 'constant': False, 'payable': False, 'type': 'function', 'gas': 316}]
```

Dockerfile

A Dockerfile is provided in the master branch of the repository. In order to build a Docker Image please run:

```
docker build https://github.com/ethereum/vyper.git -t vyper:1
docker run -it --entrypoint /bin/bash vyper:1
```

To ensure that everything works correctly after the installtion, please run the test commands and try compiling a contract:

```
python setup.py test
vyper examples/crowdfund.vy
```

3.1.5 Snap

Vyper is published in the snap store. In any of the [supported Linux distros](#), install it with (Note that installing the above snap is the latest master):

```
sudo snap install vyper --edge --devmode
```

To install the latest beta version use:

```
sudo snap install vyper --beta --devmode
```

3.2 Compiling a Contract

To compile a contract, use:

```
vyper yourFileName.vy
```

You can also compile to other formats such as ABI using the below format:

```
vyper -f ['abi', 'bytecode', 'bytecode_runtime', 'ir', 'asm', 'source_map', 'method_
    identifiers', 'combined_json'] yourFileName.vy
```

It is also possible to use the *-f json* option, which is a legacy alias for *-f abi*.

Note: Since *.vy* is not officially a language supported by any syntax highlighters or linters, it is recommended to name your Vyper file ending with *.py* in order to have Python syntax highlighting.

An [online compiler](#) is available as well, which lets you experiment with the language without having to install Vyper. The online compiler allows you to compile to bytecode and/or LLL.

Note: While the vyper version of the online compiler is updated on a regular basis it might be a bit behind the latest version found in the master branch of the repository.

3.3 Testing a Contract

The following example demonstrates how to compile and deploy your vyper contract. It requires `pyethereum>=2.0.0` for the `tester` module

```
from vyper import compiler
from ethereum.tools import tester

# Get a new chain
chain = tester.Chain()
# Set the vyper compiler to run when the vyper language is requested
tester.languages['vyper'] = compiler.Compiler()

with open('my_contract.vy' 'r') as f:
    source_code = f.read()
# Compile and Deploy contract to provisioned testchain
# (e.g. run __init__ method) with given args (e.g. init_args)
# from msg.sender = t.k1 (private key of address 1 in test account)
# and supply 1000 wei to the contract
init_args = ['arg1', 'arg2', 3]
contract = chain.contract(source_code, language="vyper",
```

(continues on next page)

(continued from previous page)

```
init_args, sender=t.k1, value=1000)

contract.myMethod() # Executes myMethod on the tester "chain"
chain.mine() # Mines the above transaction (and any before it) into a block
```

Note: We are working on integration with [ethereum-tester](#), so this example will change.

3.3.1 Testing Using vyper-run Command

To allow quickly testing contracts, Vyper provides a command line tool for instantly executing a function:

```
vyper-run yourFileName.vy "yourFunction();" -i some_init_param, another_init_param
```

The vyper-run command is composed of 4 parts:

- vyper-run
- the name of the contract file you want to execute (for example: coolContract.vy)
- a string (wrapped in double quotes) with the function you want to trigger, you can trigger multiple functions by adding a semicolon at the end of each function and then call the next function (for example: "myFunction1(100,4);myFunction2()")+
- (Optional) the parameters for the `__init__` function of the contract (for example: given `__init__(a: int128, b: int128)` the syntax would be `-i 8,27`).

Putting it all together:

```
vyper-run myContract.vy "myFunction1();myFunction2()" -i 1,3
```

The vyper-run command will print out the returned value of the called functions as well as all the logged events emitted during the function's execution.

3.4 Deploying a Contract

You have several options to deploy a Vyper contract to the public testnets.

One option is to take the bytecode generated by the vyper compiler and manually deploy it through mist or geth:

```
vyper yourFileName.vy
# returns bytecode
```

Or deploy it with current browser on [myetherwallet](#) contract menu.

We are working on integration with [populus](#), this will be the preferred way of deploying vyper contracts in the future.

3.5 Structure of a Contract

Contracts in Vyper are contained within files, with each file being one smart-contract. Files in Vyper are similar to classes in object-oriented languages. Each file can contain declarations of *State Variables*, *Functions*, and structure-structs-types.

3.5.1 State Variables

State variables are values which are permanently stored in contract storage.

```
storedData: int128
```

See the [Types](#) section for valid state variable types and visibility-and-getters for possible choices for visibility.

3.5.2 Functions

Functions are the executable units of code within a contract.

```
@public
@payable
def bid(): // Function
    // ...
```

Function-calls can happen internally or externally and have different levels of visibility (visibility-and-getters) towards other contracts. Functions must be decorated with either `@public` or `@private`.

Decorators

Decorator	Description
<code>@public</code>	Can be called from external contracts.
<code>@private</code>	Can only be called within current contract.
<code>@constant</code>	Does not alter contract state.
<code>@payable</code>	The contract is open to receive ethereum.
<code>@non-reentrant(<unique_key>)</code>	Function can only be called once, both externally and internally. Used to prevent reentrancy attacks.

The visibility decorators `@public` or `@private` are mandatory on function declarations, whilst the other decorators are optional.

Default function

A contract can also have a default function, which is executed on a call to the contract if no other functions match the given function identifier (or if none was supplied at all, such as through someone sending it Eth). It is the same construct as fallback functions in [Solidity](#).

This function is always named `__default__` and must be annotated with `@public`. It cannot have arguments and cannot return anything.

If the function is annotated as `@payable`, this function is executed whenever the contract is sent Ether (without data). This is why the default function cannot accept arguments and return values - it is a design decision of Ethereum to make no differentiation between sending ether to a contract or a user address.

Example:

```
Payment: event({amount: int128, from: indexed(address)})

@public
@payable
```

(continues on next page)

(continued from previous page)

```
def __default__():  
    log.Payment(msg.value, msg.sender)
```

Considerations

Just as in Solidity, Vyper generates a default function if one isn't found, in the form of a REVERT call. Note that this still *generates an exception* and thus will not succeed in receiving funds.

Ethereum specifies that the operations will be rolled back if the contract runs out of gas in execution. `send` calls to the contract come with a free stipend of 2300 gas, which does not leave much room to perform other operations except basic logging. **However**, if the sender includes a higher gas amount through a `call` instead of `send`, then more complex functionality can be run.

It is considered a best practice to ensure your payable default function is compatible with this stipend. The following operations will consume more than 2300 gas:

- Writing to storage
- Creating a contract
- Calling an external function which consumes a large amount of gas
- Sending Ether

Lastly, although the default function receives no arguments, it can still access the `msg` global, including:

- the address of who is interacting with the contract (`msg.sender`)
- the amount of ETH sent (`msg.value`)
- the gas provided (`msg.gas`).

3.5.3 Events

Events may be logged in specially indexed data structures that allow clients, including light clients, to efficiently search for them.

```
Payment: event({amount: int128, arg2: indexed(address)})  
  
total_paid: int128  
  
@public  
@payable  
def pay():  
    self.total_paid += msg.value  
    log.Payment(msg.value, msg.sender)
```

Events must be declared before global declarations and function definitions.

3.5.4 NatSpec Metadata

Vyper supports structured documentation for state variables and functions and events.

```
carrotsEaten: int128
"""
@author Bob Clampett
@notice Number of carrots eaten
@dev Chewing does not count, carrots must pass the throat to be "eaten"
"""
```

```
@public
@payable
def doesEat(food: string):
    """
    @author Bob Clampett
    @notice Determine if Bugs will accept `food` to eat
    @dev Compares the entire string and does not rely on a hash
    @param food The name of a food to evaluate (in English)
    @return true if Bugs will eat it, false otherwise
    """

    // ...
```

```
Ate: event({food: string})
"""
@author Bob Clampett
@notice Bugs did eat `food`
@dev Chewing does not count, carrots must pass the throat to be "eaten"
@param food The name of a food that was eaten (in English)
"""
```

Additional information about Ethereum Natural Specification (NatSpec) can be found [here](#).

3.5.5 Contract Interfaces

Vyper supports exporting and importing contract interfaces, this is done using a *import* and *implements* statements.

```
import an_interface as FooBarInterface

implements: FooBarInterface
```

This will import the defined interface in vyper file at *an_interface.vy* (or *an_interface.json* if using ABI json interface type) and make sure the current contract implements all the necessary public functions. Note that all interface is valid vyper code, without the return type check. Meaning you can use a contract with code in in the function body as interface as well (but default to a function body with a *pass*).

Extracting Interfaces

Vyper has a built-in format option to allow you to make your own vyper interfaces easily.

```
vyper -f interface examples/voting/ballot.vy

# Functions

@constant
@public
def delegated(addr: address) -> bool:
```

(continues on next page)

(continued from previous page)

```
pass

# ...
```

If you want to do an external call to another contract, vyper provides an external contract extract utility as well.

```
vyper -f external_interface examples/voting/ballot.vy

# External Contracts
contract Ballot:
    def delegated(addr: address) -> bool: constant
    def directlyVoted(addr: address) -> bool: constant
    def giveRightToVote(voter: address): modifying
    def forwardWeight(delegate_with_weight_to_forward: address): modifying
    # ...
```

The output can then easily be copy-pasted to be consumed.

Built-in Interfaces

Vyper supports a few built-in interfaces such as ERC20 and ERC721. These are imported from `vyper.interfaces`:

```
from vyper.interfaces import ERC20

implements: ERC20
```

External Calls using Interfaces

To define external interfaces inline the *contract* keyword is used.

```
contract FooBar:
    def test1(): modifying
    def calculate() -> uint256: constant
```

The defined inline contract can then be use to make external calls, given a contract address.

Specifying *modifying* annoated that the call made to the external contract will be able to alter storage, were as the *constant* call will using a *STATICCALL* ensuring no storage can be altered during execution.

```
@public
def test(some_address: address):
    FooBar(some_address).calculate() # can not change storage
    FooBar(some_address).test1() # storage can be altered
```

An additional utility of storing a contract address in a contract is defined by the `<global_var>`: `FooBar` annotation. Note that assignment of and address requires the address value needs to be cast using the contract type e.g. `FooBar(<address_var>)`.

```
foobar_contract: FooBar

@public
def __init__(foobar_address: address):
    self.foobar_contract = FooBar(foobar_address)
```

(continues on next page)

(continued from previous page)

```
@public
def call_test1():
    # ...
```

To import interfaces to be used in external calls, one uses the interface just as one would use an inlined interface definition.

```
import foo_bar as FooBar

foobar_contract: FooBar

@public
def __init__(foobar_address: address):
    self.foobar_contract = FooBar(foobar_address)

@public
def test():
    self.foobar_contract.one()
```

Or alternatively

```
import foo_bar as FooBar

@public
def test(addr: address):
    FooBar(addr).one()
```

3.6 Vyper by Example

3.6.1 Simple Open Auction

As an introductory example of a smart contract written in Vyper, we will begin with a simple open auction contract. As we dive into the code, it is important to remember that all Vyper syntax is valid Python3 syntax, however not all Python3 functionality is available in Vyper.

In this contract, we will be looking at a simple open auction contract where participants can submit bids during a limited time period. When the auction period ends, a predetermined beneficiary will receive the amount of the highest bid.

```
1  # Open Auction
2
3  # Auction params
4  # Beneficiary receives money from the highest bidder
5  beneficiary: public(address)
6  auctionStart: public(timestamp)
7  auctionEnd: public(timestamp)
8
9  # Current state of auction
10 highestBidder: public(address)
11 highestBid: public(wei_value)
12
13 # Set to true at the end, disallows any change
```

(continues on next page)

(continued from previous page)

```

14 ended: public(bool)
15
16 # Keep track of refunded bids so we can follow the withdraw pattern
17 pendingReturns: public(map(address, wei_value))
18
19 # Create a simple auction with `_bidding_time`
20 # seconds bidding time on behalf of the
21 # beneficiary address `_beneficiary`.
22 @public
23 def __init__(_beneficiary: address, _bidding_time: timedelta):
24     self.beneficiary = _beneficiary
25     self.auctionStart = block.timestamp
26     self.auctionEnd = self.auctionStart + _bidding_time
27
28 # Bid on the auction with the value sent
29 # together with this transaction.
30 # The value will only be refunded if the
31 # auction is not won.
32 @public
33 @payable
34 def bid():
35     # Check if bidding period is over.
36     assert block.timestamp < self.auctionEnd
37     # Check if bid is high enough
38     assert msg.value > self.highestBid
39     # Track the refund for the previous high bidder
40     self.pendingReturns[self.highestBidder] += self.highestBid
41     # Track new high bid
42     self.highestBidder = msg.sender
43     self.highestBid = msg.value
44
45 # Withdraw a previously refunded bid. The withdraw pattern is
46 # used here to avoid a security issue. If refunds were directly
47 # sent as part of bid(), a malicious bidding contract could block
48 # those refunds and thus block new higher bids from coming in.
49 @public
50 def withdraw():
51     pending_amount: wei_value = self.pendingReturns[msg.sender]
52     self.pendingReturns[msg.sender] = 0
53     send(msg.sender, pending_amount)
54
55 # End the auction and send the highest bid
56 # to the beneficiary.
57 @public
58 def endAuction():
59     # It is a good guideline to structure functions that interact
60     # with other contracts (i.e. they call functions or send Ether)
61     # into three phases:
62     # 1. checking conditions
63     # 2. performing actions (potentially changing conditions)
64     # 3. interacting with other contracts
65     # If these phases are mixed up, the other contract could call
66     # back into the current contract and modify the state or cause
67     # effects (Ether payout) to be performed multiple times.
68     # If functions called internally include interaction with external
69     # contracts, they also have to be considered interaction with
70     # external contracts.

```

(continues on next page)

(continued from previous page)

```

71
72     # 1. Conditions
73     # Check if auction endtime has been reached
74     assert block.timestamp >= self.auctionEnd
75     # Check if this function has already been called
76     assert not self.ended
77
78     # 2. Effects
79     self.ended = True
80
81     # 3. Interaction
82     send(self.beneficiary, self.highestBid)

```

As you can see, this example only has a constructor, two methods to call, and a few variables to manage the contract state. Believe it or not, this is all we need for a basic implementation of an auction smart contract.

Let's get started!

```

# Auction params
# Beneficiary receives money from the highest bidder
beneficiary: public(address)
auctionStart: public(timestamp)
auctionEnd: public(timestamp)

# Current state of auction
highestBidder: public(address)
highestBid: public(wei_value)

# Set to true at the end, disallows any change
ended: public(bool)

```

We begin by declaring a few variables to keep track of our contract state. We initialize a global variable `beneficiary` by calling `public` on the datatype `address`. The beneficiary will be the receiver of money from the highest bidder. We also initialize the variables `auctionStart` and `auctionEnd` with the datatype `timestamp` to manage the open auction period and `highestBid` with datatype `wei_value`, the smallest denomination of ether, to manage auction state. The variable `ended` is a boolean to determine whether the auction is officially over.

You may notice all of the variables being passed into the `public` function. By declaring the variable `public`, the variable is callable by external contracts. Initializing the variables without the `public` function defaults to a private declaration and thus only accessible to methods within the same contract. The `public` function additionally creates a 'getter' function for the variable, accessible through an external call such as `contract.beneficiary()`.

Now, the constructor.

The contract is initialized with two arguments: `_beneficiary` of type `address` and `_bidding_time` with type `timedelta`, the time difference between the start and end of the auction. We then store these two pieces of information into the contract variables `self.beneficiary` and `self.auctionEnd`. Notice that we have access to the current time by calling `block.timestamp`. `block` is an object available within any Vyper contract and provides information about the block at the time of calling. Similar to `block`, another important object available to us within the contract is `msg`, which provides information on the method caller as we will soon see.

With initial setup out of the way, let's look at how our users can make bids.

The `@payable` decorator will allow a user to send some ether to the contract in order to call the decorated method. In this case, a user wanting to make a bid would call the `bid()` method while sending an amount equal to their desired bid (not including gas fees). When calling any method within a contract, we are provided with a built-in variable `msg`

and we can access the public address of any method caller with `msg.sender`. Similarly, the amount of ether a user sends can be accessed by calling `msg.value`.

Warning: `msg.sender` will change between internal function calls so that if you're calling a function from the outside, it's correct for the first function call. But then, for the function calls after, `msg.sender` will reference the contract itself as opposed to the sender of the transaction.

Here, we first check whether the current time is before the auction's end time using the `assert` function which takes any boolean statement. We also check to see if the new bid is greater than the highest bid. If the two `assert` statements pass, we can safely continue to the next lines; otherwise, the `bid()` method will throw an error and revert the transaction. If the two `assert` statements and the check that the previous bid is not equal to zero pass, we can safely conclude that we have a valid new highest bid. We will send back the previous `highestBid` to the previous `highestBidder` and set our new `highestBid` and `highestBidder`.

With the `endAuction()` method, we check whether our current time is past the `auctionEnd` time we set upon initialization of the contract. We also check that `self.ended` had not previously been set to `True`. We do this to prevent any calls to the method if the auction had already ended, which could potentially be malicious if the check had not been made. We then officially end the auction by setting `self.ended` to `True` and sending the highest bid amount to the beneficiary.

And there you have it - an open auction contract. Of course, this is a simplified example with barebones functionality and can be improved. Hopefully, this has provided some insight to the possibilities of Vyper. As we move on to exploring more complex examples, we will encounter more design patterns and features of the Vyper language.

And of course, no smart contract tutorial is complete without a note on security.

Note: It's always important to keep security in mind when designing a smart contract. As any application becomes more complex, the greater the potential for introducing new risks. Thus, it's always good practice to keep contracts as readable and simple as possible.

Whenever you're ready, let's turn it up a notch in the next example.

3.6.2 Blind Auction

Before we dive into our other examples, let's briefly explore another type of auction that you can build with Vyper. Similar to its counterpart written in Solidity, this blind auction allows for an auction where there is no time pressure towards the end of the bidding period.

```
1  # Blind Auction # Adapted to Vyper from [Solidity by Example](https://github.com/
   ↳ethereum/solidity/blob/develop/docs/solidity-by-example.rst#blind-auction-1)
2
3  struct Bid:
4      blindedBid: bytes32
5      deposit: wei_value
6
7  # Note: because Vyper does not allow for dynamic arrays, we have limited the
8  # number of bids that can be placed by one address to 128 in this example
9  MAX_BIDS: constant(int128) = 128
10
11 # Event for logging that auction has ended
12 AuctionEnded: event({_highestBidder: address, _highestBid: wei_value})
13
14 # Auction parameters
```

(continues on next page)

(continued from previous page)

```

15 beneficiary: public(address)
16 biddingEnd: public(timestamp)
17 revealEnd: public(timestamp)
18
19 # Set to true at the end of auction, disallowing any new bids
20 ended: public(bool)
21
22 # Final auction state
23 highestBid: public(wei_value)
24 highestBidder: public(address)
25
26 # State of the bids
27 bids: map(address, Bid[128])
28 bidCounts: map(address, int128)
29
30 # Allowed withdrawals of previous bids
31 pendingReturns: map(address, wei_value)
32
33
34 # Create a blinded auction with `_biddingTime` seconds bidding time and
35 # `_revealTime` seconds reveal time on behalf of the beneficiary address
36 # `_beneficiary`.
37 @public
38 def __init__(_beneficiary: address, _biddingTime: timedelta, _revealTime: timedelta):
39     self.beneficiary = _beneficiary
40     self.biddingEnd = block.timestamp + _biddingTime
41     self.revealEnd = self.biddingEnd + _revealTime
42
43
44 # Place a blinded bid with:
45 #
46 # _blindedBid = sha3(concat(
47 #     convert(value, bytes32),
48 #     convert(fake, bytes32),
49 #     secret)
50 # )
51 #
52 # The sent ether is only refunded if the bid is correctly revealed in the
53 # revealing phase. The bid is valid if the ether sent together with the bid is
54 # at least "value" and "fake" is not true. Setting "fake" to true and sending
55 # not the exact amount are ways to hide the real bid but still make the
56 # required deposit. The same address can place multiple bids.
57 @public
58 @payable
59 def bid(_blindedBid: bytes32):
60     # Check if bidding period is still open
61     assert block.timestamp < self.biddingEnd
62
63     # Check that payer hasn't already placed maximum number of bids
64     numBids: int128 = self.bidCounts[msg.sender]
65     assert numBids < MAX_BIDS
66
67     # Add bid to mapping of all bids
68     self.bids[msg.sender][numBids] = Bid({
69         blindedBid: _blindedBid,
70         deposit: msg.value
71     })

```

(continues on next page)

(continued from previous page)

```

72     self.bidCounts[msg.sender] += 1
73
74
75 # Returns a boolean value, `True` if bid placed successfully, `False` otherwise.
76 @private
77 def placeBid(bidder: address, value: wei_value) -> bool:
78     # If bid is less than highest bid, bid fails
79     if (value <= self.highestBid):
80         return False
81
82     # Refund the previously highest bidder
83     if (self.highestBidder != ZERO_ADDRESS):
84         self.pendingReturns[self.highestBidder] += self.highestBid
85
86     # Place bid successfully and update auction state
87     self.highestBid = value
88     self.highestBidder = bidder
89
90     return True
91
92
93 # Reveal your blinded bids. You will get a refund for all correctly blinded
94 # invalid bids and for all bids except for the totally highest.
95 @public
96 def reveal(_numBids: int128, _values: wei_value[128], _fakes: bool[128], _secrets:
↳ bytes32[128]):
97     # Check that bidding period is over
98     assert block.timestamp > self.biddingEnd
99
100    # Check that reveal end has not passed
101    assert block.timestamp < self.revealEnd
102
103    # Check that number of bids being revealed matches log for sender
104    assert _numBids == self.bidCounts[msg.sender]
105
106    # Calculate refund for sender
107    refund: wei_value
108    for i in range(MAX_BIDS):
109        # Note that loop may break sooner than 128 iterations if i >= _numBids
110        if (i >= _numBids):
111            break
112
113        # Get bid to check
114        bidToCheck: Bid = (self.bids[msg.sender])[i]
115
116        # Check against encoded packet
117        value: wei_value = _values[i]
118        fake: bool = _fakes[i]
119        secret: bytes32 = _secrets[i]
120        blindedBid: bytes32 = sha3(concat(
121            convert(value, bytes32),
122            convert(fake, bytes32),
123            secret
124        ))
125
126        # Bid was not actually revealed
127        # Do not refund deposit

```

(continues on next page)

(continued from previous page)

```

128     if (blindedBid != bidToCheck.blindedBid):
129         assert 1 == 0
130         continue
131
132     # Add deposit to refund if bid was indeed revealed
133     refund += bidToCheck.deposit
134     if (not fake and bidToCheck.deposit >= value):
135         if (self.placeBid(msg.sender, value)):
136             refund -= value
137
138     # Make it impossible for the sender to re-claim the same deposit
139     zeroBytes32: bytes32
140     bidToCheck.blindedBid = zeroBytes32
141
142     # Send refund if non-zero
143     if (refund != 0):
144         send(msg.sender, refund)
145
146 # Withdraw a bid that was overbid.
147 @public
148 def withdraw():
149     # Check that there is an allowed pending return.
150     pendingAmount: wei_value = self.pendingReturns[msg.sender]
151     if (pendingAmount > 0):
152         # If so, set pending returns to zero to prevent recipient from calling
153         # this function again as part of the receiving call before `transfer`
154         # returns (see the remark above about conditions -> effects ->
155         # interaction).
156         self.pendingReturns[msg.sender] = 0
157
158         # Then send return
159         send(msg.sender, pendingAmount)
160
161
162 # End the auction and send the highest bid to the beneficiary.
163 @public
164 def auctionEnd():
165     # Check that reveal end has passed
166     assert block.timestamp > self.revealEnd
167
168     # Check that auction has not already been marked as ended
169     assert not self.ended
170
171     # Log auction ending and set flag
172     log.AuctionEnded(self.highestBidder, self.highestBid)
173     self.ended = True
174
175     # Transfer funds to beneficiary
176     send(self.beneficiary, self.highestBid)
177

```

While this blind auction is almost functionally identical to the blind auction implemented in Solidity, the differences in their implementations help illustrate the differences between Solidity and Vyper.

```

# Final auction state
highestBid: public(wei_value)
highestBidder: public(address)

```

One key difference is that, because Vyper does not allow for dynamic arrays, we have limited the number of bids that can be placed by one address to 128 in this example. Bidders who want to make more than this maximum number of bids would need to do so from multiple addresses.

3.6.3 Safe Remote Purchases

In this example, we have an escrow contract implementing a system for a trustless transaction between a buyer and a seller. In this system, a seller posts an item for sale and makes a deposit to the contract of twice the item's value. At this moment, the contract has a balance of $2 * \text{value}$. The seller can reclaim the deposit and close the sale as long as a buyer has not yet made a purchase. If a buyer is interested in making a purchase, they would make a payment and submit an equal amount for deposit (totaling $2 * \text{value}$) into the contract and locking the contract from further modification. At this moment, the contract has a balance of $4 * \text{value}$ and the seller would send the item to buyer. Upon the buyer's receipt of the item, the buyer will mark the item as received in the contract, thereby returning the buyer's deposit (not payment), releasing the remaining funds to the seller, and completing the transaction.

There are certainly others ways of designing a secure escrow system with less overhead for both the buyer and seller, but for the purpose of this example, we want to explore one way how an escrow system can be implemented trustlessly.

Let's go!

```

1  # Safe Remote Purchase
2  # Originally from
3  # https://github.com/ethereum/solidity/blob/develop/docs/solidity-by-example.rst
4  # Ported to vyper and optimized.
5
6  # Rundown of the transaction:
7  # 1. Seller posts item for sale and posts safety deposit of double the item value.
8  #    Balance is 2*value.
9  #    (1.1. Seller can reclaim deposit and close the sale as long as nothing was_
10 ↪ purchased.)
11 # 2. Buyer purchases item (value) plus posts an additional safety deposit (Item_
12 ↪ value).
13 #    Balance is 4*value.
14 # 3. Seller ships item.
15 # 4. Buyer confirms receiving the item. Buyer's deposit (value) is returned.
16 #    Seller's deposit (2*value) + items value is returned. Balance is 0.
17
18 value: public(wei_value) #Value of the item
19 seller: public(address)
20 buyer: public(address)
21 unlocked: public(bool)
22 ended: public(bool)
23
24 @public
25 @payable
26 def __init__():
27     assert (msg.value % 2) == 0
28     self.value = msg.value / 2 # The seller initializes the contract by
29     # posting a safety deposit of 2*value of the item up for sale.
30     self.seller = msg.sender
31     self.unlocked = True
32
33 @public
34 def abort():
35     assert self.unlocked #Is the contract still refundable?
36     assert msg.sender == self.seller # Only the seller can refund
37     # his deposit before any buyer purchases the item.

```

(continues on next page)

(continued from previous page)

```

36     selfdestruct(self.seller) # Refunds the seller and deletes the contract.
37
38 @public
39 @payable
40 def purchase():
41     assert self.unlocked # Is the contract still open (is the item still up
42                          # for sale)?
43     assert msg.value == (2 * self.value) # Is the deposit the correct value?
44     self.buyer = msg.sender
45     self.unlocked = False
46
47 @public
48 def received():
49     # 1. Conditions
50     assert not self.unlocked # Is the item already purchased and pending
51                             # confirmation from the buyer?
52     assert msg.sender == self.buyer
53     assert not self.ended
54
55     # 2. Effects
56     self.ended = True
57
58     # 3. Interaction
59     send(self.buyer, self.value) # Return the buyer's deposit (=value) to the buyer.
60     selfdestruct(self.seller) # Return the seller's deposit (=2*value) and the
61                             # purchase price (=value) to the seller.

```

This is also a moderately short contract, however a little more complex in logic. Let's break down this contract bit by bit.

```

value: public(wei_value) #Value of the item
seller: public(address)
buyer: public(address)
unlocked: public(bool)

```

Like the other contracts, we begin by declaring our global variables public with their respective datatypes. Remember that the `public` function allows the variables to be *readable* by an external caller, but not *writable*.

With a `@payable` decorator on the constructor, the contract creator will be required to make an initial deposit equal to twice the item's value to initialize the contract, which will be later returned. This is in addition to the gas fees needed to deploy the contract on the blockchain, which is not returned. We `assert` that the deposit is divisible by 2 to ensure that the seller deposited a valid amount. The constructor stores the item's value in the contract variable `self.value` and saves the contract creator into `self.seller`. The contract variable `self.unlocked` is initialized to `True`.

The `abort()` method is a method only callable by the seller and while the contract is still `unlocked`—meaning it is callable only prior to any buyer making a purchase. As we will see in the `purchase()` method that when a buyer calls the `purchase()` method and sends a valid amount to the contract, the contract will be locked and the seller will no longer be able to call `abort()`.

When the seller calls `abort()` and if the `assert` statements pass, the contract will call the `selfdestruct()` function and refunds the seller and subsequently destroys the contract.

Like the constructor, the `purchase()` method has a `@payable` decorator, meaning it can be called with a payment. For the buyer to make a valid purchase, we must first `assert` that the contract's `unlocked` property is `True` and that the amount sent is equal to twice the item's value. We then set the buyer to the `msg.sender` and lock the contract. At this point, the contract has a balance equal to 4 times the item value and the seller must send the item to the buyer.

Finally, upon the buyer's receipt of the item, the buyer can confirm their receipt by calling the `received()` method to distribute the funds as intended—where the seller receives 3/4 of the contract balance and the buyer receives 1/4.

By calling `received()`, we begin by checking that the contract is indeed locked, ensuring that a buyer had previously paid. We also ensure that this method is only callable by the buyer. If these two `assert` statements pass, we refund the buyer their initial deposit and send the seller the remaining funds. The contract is finally destroyed and the transaction is complete.

Whenever we're ready, let's move on to the next example.

3.6.4 Crowdfund

Now, let's explore a straightforward example for a crowdfunding contract where prospective participants can contribute funds to a campaign. If the total contribution to the campaign reaches or surpasses a predetermined funding goal, the funds will be sent to the beneficiary at the end of the campaign deadline. Participants will be refunded their respective contributions if the total funding does not reach its target goal.

```

1  # Setup private variables (only callable from within the contract)
2
3  struct Funder :
4      sender: address
5      value: wei_value
6
7  funders: map(int128, Funder)
8  nextFunderIndex: int128
9  beneficiary: address
10 deadline: public(timestamp)
11 goal: public(wei_value)
12 refundIndex: int128
13 timelimit: public(timedelta)
14
15
16 # Setup global variables
17 @public
18 def __init__(_beneficiary: address, _goal: wei_value, _timelimit: timedelta):
19     self.beneficiary = _beneficiary
20     self.deadline = block.timestamp + _timelimit
21     self.timelimit = _timelimit
22     self.goal = _goal
23
24
25 # Participate in this crowdfunding campaign
26 @public
27 @payable
28 def participate():
29     assert block.timestamp < self.deadline, "deadline not met (yet)"
30
31     nfi: int128 = self.nextFunderIndex
32
33     self.funders[nfi] = Funder({sender: msg.sender, value: msg.value})
34     self.nextFunderIndex = nfi + 1
35
36
37 # Enough money was raised! Send funds to the beneficiary
38 @public
39 def finalize():
40     assert block.timestamp >= self.deadline, "deadline not met (yet)"

```

(continues on next page)

(continued from previous page)

```

41     assert self.balance >= self.goal, "invalid balance"
42
43     selfdestruct(self.beneficiary)
44
45     # Not enough money was raised! Refund everyone (max 30 people at a time
46     # to avoid gas limit issues)
47     @public
48     def refund():
49         assert block.timestamp >= self.deadline and self.balance < self.goal
50
51         ind: int128 = self.refundIndex
52
53         for i in range(ind, ind + 30):
54             if i >= self.nextFunderIndex:
55                 self.refundIndex = self.nextFunderIndex
56                 return
57
58             send(self.funders[i].sender, self.funders[i].value)
59             clear(self.funders[i])
60
61     self.refundIndex = ind + 30

```

Most of this code should be relatively straightforward after going through our previous examples. Let's dive right in.

```

# Setup private variables (only callable from within the contract)

struct Funder :
    sender: address
    value: wei_value

funders: map(int128, Funder)
nextFunderIndex: int128

```

Like other examples, we begin by initiating our variables - except this time, we're not calling them with the `public` function. Variables initiated this way are, by default, private.

Note: Unlike the existence of the function `public()`, there is no equivalent `private()` function. Variables simply default to private if initiated without the `public()` function.

The `funders` variable is initiated as a mapping where the key is a number, and the value is a struct representing the contribution of each participant. This struct contains each participant's public address and their respective value contributed to the fund. The key corresponding to each struct in the mapping will be represented by the variable `nextFunderIndex` which is incremented with each additional contributing participant. Variables initialized with the `int128` type without an explicit value, such as `nextFunderIndex`, defaults to 0. The `beneficiary` will be the final receiver of the funds once the crowdfunding period is over—as determined by the `deadline` and `timelimit` variables. The `goal` variable is the target total contribution of all participants. `refundIndex` is a variable for bookkeeping purposes in order to avoid gas limit issues in the scenario of a refund.

Our constructor function takes 3 arguments: the beneficiary's address, the goal in wei value, and the difference in time from start to finish of the crowdfunding. We initialize the arguments as contract variables with their corresponding names. Additionally, a `self.deadline` is initialized to set a definitive end time for the crowdfunding period.

Now let's take a look at how a person can participate in the crowdfund.

Once again, we see the `@payable` decorator on a method, which allows a person to send some ether along with a call to the method. In this case, the `participate()` method accesses the sender's address with `msg.sender` and

the corresponding amount sent with `msg.value`. This information is stored into a struct and then saved into the `funders` mapping with `self.nextFunderIndex` as the key. As more participants are added to the mapping, `self.nextFunderIndex` increments appropriately to properly index each participant.

The `finalize()` method is used to complete the crowdfunding process. However, to complete the crowdfunding, the method first checks to see if the crowdfunding period is over and that the balance has reached/passed its set goal. If those two conditions pass, the contract calls the `selfdestruct()` function and sends the collected funds to the beneficiary.

Note: Notice that we have access to the total amount sent to the contract by calling `self.balance`, a variable we never explicitly set. Similar to `msg` and `block`, `self.balance` is a built-in variable that's available in all Vyper contracts.

We can finalize the campaign if all goes well, but what happens if the crowdfunding campaign isn't successful? We're going to need a way to refund all the participants.

In the `refund()` method, we first check that the crowdfunding period is indeed over and that the total collected balance is less than the goal with the `assert` statement. If those two conditions pass, we then loop through every participant and call `send()` to send each participant their respective contribution. For the sake of gas limits, we group the number of contributors in batches of 30 and refund them one at a time. Unfortunately, if there's a large number of participants, multiple calls to `refund()` may be necessary.

3.6.5 Voting

In this contract, we will implement a system for participants to vote on a list of proposals. The chairperson of the contract will be able to give each participant the right to vote, and each participant may choose to vote, or delegate their vote to another voter. Finally, a winning proposal will be determined upon calling the `winningProposals()` method, which iterates through all the proposals and returns the one with the greatest number of votes.

```

1  # Voting with delegation.
2
3  # Information about voters
4  struct Voter:
5      # weight is accumulated by delegation
6      weight: int128
7      # if true, that person already voted (which includes voting by delegating)
8      voted: bool
9      # person delegated to
10     delegate: address
11     # index of the voted proposal, which is not meaningful unless `voted` is True.
12     vote: int128
13
14  # Users can create proposals
15  struct Proposal:
16      # short name (up to 32 bytes)
17      name: bytes32
18      # number of accumulated votes
19      voteCount: int128
20
21  voters: public(map(address, Voter))
22  proposals: public(map(int128, Proposal))
23  voterCount: public(int128)
24  chairperson: public(address)
25  int128Proposals: public(int128)
26

```

(continues on next page)

(continued from previous page)

```

27
28 @public
29 @constant
30 def delegated(addr: address) -> bool:
31     return self.voters[addr].delegate != ZERO_ADDRESS
32
33
34 @public
35 @constant
36 def directlyVoted(addr: address) -> bool:
37     return self.voters[addr].voted and (self.voters[addr].delegate == ZERO_ADDRESS)
38
39
40 # Setup global variables
41 @public
42 def __init__(_proposalNames: bytes32[2]):
43     self.chairperson = msg.sender
44     self.voterCount = 0
45     for i in range(2):
46         self.proposals[i] = Proposal({
47             name: _proposalNames[i],
48             voteCount: 0
49         })
50     self.int128Proposals += 1
51
52 # Give a `voter` the right to vote on this ballot.
53 # This may only be called by the `chairperson`.
54 @public
55 def giveRightToVote(voter: address):
56     # Throws if the sender is not the chairperson.
57     assert msg.sender == self.chairperson
58     # Throws if the voter has already voted.
59     assert not self.voters[voter].voted
60     # Throws if the voter's voting weight isn't 0.
61     assert self.voters[voter].weight == 0
62     self.voters[voter].weight = 1
63     self.voterCount += 1
64
65 # Used by `delegate` below, and can be called by anyone.
66 @public
67 def forwardWeight(delegate_with_weight_to_forward: address):
68     assert self.delegated(delegate_with_weight_to_forward)
69     # Throw if there is nothing to do:
70     assert self.voters[delegate_with_weight_to_forward].weight > 0
71
72     target: address = self.voters[delegate_with_weight_to_forward].delegate
73     for i in range(4):
74         if self.delegated(target):
75             target = self.voters[target].delegate
76             # The following effectively detects cycles of length <= 5,
77             # in which the delegation is given back to the delegator.
78             # This could be done for any int128ber of loops,
79             # or even infinitely with a while loop.
80             # However, cycles aren't actually problematic for correctness;
81             # they just result in spoiled votes.
82             # So, in the production version, this should instead be
83             # the responsibility of the contract's client, and this

```

(continues on next page)

(continued from previous page)

```

84         # check should be removed.
85         assert target != delegate_with_weight_to_forward
86     else:
87         # Weight will be moved to someone who directly voted or
88         # hasn't voted.
89         break
90
91     weight_to_forward: int128 = self.voters[delegate_with_weight_to_forward].weight
92     self.voters[delegate_with_weight_to_forward].weight = 0
93     self.voters[target].weight += weight_to_forward
94
95     if self.directlyVoted(target):
96         self.proposals[self.voters[target].vote].voteCount += weight_to_forward
97         self.voters[target].weight = 0
98
99     # To reiterate: if target is also a delegate, this function will need
100    # to be called again, similarly to as above.
101
102    # Delegate your vote to the voter `to`.
103    @public
104    def delegate(to: address):
105        # Throws if the sender has already voted
106        assert not self.voters[msg.sender].voted
107        # Throws if the sender tries to delegate their vote to themselves or to
108        # the default address value of 0x0000000000000000000000000000000000000000
109        # (the latter might not be problematic, but I don't want to think about it).
110        assert to != msg.sender
111        assert to != ZERO_ADDRESS
112
113        self.voters[msg.sender].voted = True
114        self.voters[msg.sender].delegate = to
115
116        # This call will throw if and only if this delegation would cause a loop
117        # of length <= 5 that ends up delegating back to the delegator.
118        self.forwardWeight(msg.sender)
119
120    # Give your vote (including votes delegated to you)
121    # to proposal `proposals[proposal].name`.
122    @public
123    def vote(proposal: int128):
124        # can't vote twice
125        assert not self.voters[msg.sender].voted
126        # can only vote on legitimate proposals
127        assert proposal < self.int128Proposals
128
129        self.voters[msg.sender].vote = proposal
130        self.voters[msg.sender].voted = True
131
132        # transfer msg.sender's weight to proposal
133        self.proposals[proposal].voteCount += self.voters[msg.sender].weight
134        self.voters[msg.sender].weight = 0
135
136    # Computes the winning proposal taking all
137    # previous votes into account.
138    @public
139    @constant
140    def winningProposal() -> int128:

```

(continues on next page)

(continued from previous page)

```

141 winning_vote_count: int128 = 0
142 winning_proposal: int128 = 0
143 for i in range(2):
144     if self.proposals[i].voteCount > winning_vote_count:
145         winning_vote_count = self.proposals[i].voteCount
146         winning_proposal = i
147     return winning_proposal
148
149 # Calls winningProposal() function to get the index
150 # of the winner contained in the proposals array and then
151 # returns the name of the winner
152 @public
153 @constant
154 def winnerName() -> bytes32:
155     return self.proposals[self.winningProposal()].name

```

As we can see, this is contract of moderate length which we will dissect section by section. Let's begin!

```

# Information about voters
struct Voter:
    # weight is accumulated by delegation
    weight: int128
    # if true, that person already voted (which includes voting by delegating)
    voted: bool
    # person delegated to
    delegate: address
    # index of the voted proposal, which is not meaningful unless `voted` is True.
    vote: int128

# Users can create proposals
struct Proposal:
    # short name (up to 32 bytes)
    name: bytes32
    # number of accumulated votes
    voteCount: int128

voters: public(map(address, Voter))
proposals: public(map(int128, Proposal))
voterCount: public(int128)
chairperson: public(address)
int128Proposals: public(int128)

```

The variable `voters` is initialized as a mapping where the key is the voter's public address and the value is a struct describing the voter's properties: `weight`, `voted`, `delegate`, and `vote`, along with their respective datatypes.

Similarly, the `proposals` variable is initialized as a public mapping with `int128` as the key's datatype and a struct to represent each proposal with the properties `name` and `vote_count`. Like our last example, we can access any value by key'ing into the mapping with a number just as one would with an index in an array.

Then, `voterCount` and `chairperson` are initialized as public with their respective datatypes.

Let's move onto the constructor.

Warning: Both `msg.sender` and `msg.balance` change between internal function calls so that if you're calling a function from the outside, it's correct for the first function call. But then, for the function calls after, `msg.sender` and `msg.balance` reference the contract itself as opposed to the sender of the transaction.

In the constructor, we hard-coded the contract to accept an array argument of exactly two proposal names of type `bytes32` for the contracts initialization. Because upon initialization, the `__init__()` method is called by the contract creator, we have access to the contract creator's address with `msg.sender` and store it in the contract variable `self.chairperson`. We also initialize the contract variable `self.voter_count` to zero to initially represent the number of votes allowed. This value will be incremented as each participant in the contract is given the right to vote by the method `giveRightToVote()`, which we will explore next. We loop through the two proposals from the argument and insert them into `proposals` mapping with their respective index in the original array as its key.

Now that the initial setup is done, lets take a look at the functionality.

We need a way to control who has the ability to vote. The method `giveRightToVote()` is a method callable by only the chairperson by taking a voter address and granting it the right to vote by incrementing the voter's `weight` property. We sequentially check for 3 conditions using `assert`. The `assert not` function will check for falsy boolean values - in this case, we want to know that the voter has not already voted. To represent voting power, we will set their `weight` to 1 and we will keep track of the total number of voters by incrementing `voterCount`.

In the method `delegate`, firstly, we check to see that `msg.sender` has not already voted and secondly, that the target `delegate` and the `msg.sender` are not the same. Voters shouldn't be able to delegate votes to themselves. We, then, loop through all the voters to determine whether the person `delegate` to had further delegated their vote to someone else in order to follow the chain of delegation. We then mark the `msg.sender` as having voted if they delegated their vote. We increment the proposal's `voterCount` directly if the `delegate` had already voted or increase the `delegate's` vote `weight` if the `delegate` has not yet voted.

Now, let's take a look at the logic inside the `vote()` method, which is surprisingly simple. The method takes the key of the proposal in the `proposals` mapping as an argument, check that the method caller had not already voted, sets the voter's `vote` property to the proposal key, and increments the `proposals` `voteCount` by the voter's `weight`.

With all the basic functionality complete, what's left is simply returning the winning proposal. To do this, we have two methods: `winningProposal()`, which returns the key of the proposal, and `winnerName()`, returning the name of the proposal. Notice the `@constant` decorator on these two methods. We do this because the two methods only read the blockchain state and do not modify it. Remember, reading the blockchain state is free; modifying the state costs gas. By having the `@constant` decorator, we let the EVM know that this is a read-only function and we benefit by saving gas fees.

The `winningProposal()` method returns the key of proposal in the `proposals` mapping. We will keep track of greatest number of votes and the winning proposal with the variables `winningVoteCount` and `winningProposal`, respectively by looping through all the proposals.

And finally, the `winnerName()` method returns the name of the proposal by key'ing into the `proposals` mapping with the return result of the `winningProposal()` method.

And there you have it - a voting contract. Currently, many transactions are needed to assign the rights to vote to all participants. As an exercise, can we try to optimize this?

Now that we're familiar with basic contracts. Let's step up the difficulty.

3.6.6 Company Stock

This contract is just a tad bit more thorough than the ones we've previously encountered. In this example, we are going to look at a comprehensive contract that manages the holdings of all shares of a company. The contract allows for a person to buy, sell, and transfer shares of a company as well as allowing for the company to pay a person in ether. The company, upon initialization of the contract, holds all shares of the company at first but can sell them all.

Let's get started.

```

1 units: {
2     currency_value: "Currency Value"
3 }
4
5 # Financial events the contract logs
6 Transfer: event({_from: indexed(address), _to: indexed(address), _value: _
7     ↳ uint256(currency_value)})
8 Buy: event({_buyer: indexed(address), _buy_order: uint256(currency_value)})
9 Sell: event({_seller: indexed(address), _sell_order: uint256(currency_value)})
10 Pay: event({_vendor: indexed(address), _amount: wei_value})
11
12 # Initiate the variables for the company and it's own shares.
13 company: public(address)
14 totalShares: public(uint256(currency_value))
15 price: public(uint256(wei / currency_value))
16
17 # Store a ledger of stockholder holdings.
18 holdings: map(address, uint256(currency_value))
19
20 # Set up the company.
21 @public
22 def __init__(_company: address, _total_shares: uint256(currency_value),
23     initial_price: uint256(wei / currency_value) ):
24     assert _total_shares > 0
25     assert initial_price > 0
26
27     self.company = _company
28     self.totalShares = _total_shares
29     self.price = initial_price
30
31     # The company holds all the shares at first, but can sell them all.
32     self.holdings[self.company] = _total_shares
33
34 @public
35 @constant
36 def stockAvailable() -> uint256(currency_value):
37     return self.holdings[self.company]
38
39 # Give some value to the company and get stock in return.
40 @public
41 @payable
42 def buyStock():
43     # Note: full amount is given to company (no fractional shares),
44     # so be sure to send exact amount to buy shares
45     buy_order: uint256(currency_value) = msg.value / self.price # rounds down
46
47     # Check that there are enough shares to buy.
48     assert self.stockAvailable() >= buy_order
49
50     # Take the shares off the market and give them to the stockholder.
51     self.holdings[self.company] -= buy_order
52     self.holdings[msg.sender] += buy_order
53
54     # Log the buy event.
55     log.Buy(msg.sender, buy_order)
56
57 # Find out how much stock any address (that's owned by someone) has.

```

(continues on next page)

(continued from previous page)

```

57 @public
58 @constant
59 def getHolding(_stockholder: address) -> uint256(currency_value):
60     return self.holdings[_stockholder]
61
62 # Return the amount the company has on hand in cash.
63 @public
64 @constant
65 def cash() -> wei_value:
66     return self.balance
67
68 # Give stock back to the company and get money back as ETH.
69 @public
70 def sellStock(sell_order: uint256(currency_value)):
71     assert sell_order > 0 # Otherwise, this would fail at send() below,
72         # due to an OOG error (there would be zero value available for gas).
73     # You can only sell as much stock as you own.
74     assert self.getHolding(msg.sender) >= sell_order
75     # Check that the company can pay you.
76     assert self.cash() >= (sell_order * self.price)
77
78     # Sell the stock, send the proceeds to the user
79     # and put the stock back on the market.
80     self.holdings[msg.sender] -= sell_order
81     self.holdings[self.company] += sell_order
82     send(msg.sender, sell_order * self.price)
83
84     # Log the sell event.
85     log.Sell(msg.sender, sell_order)
86
87 # Transfer stock from one stockholder to another. (Assume that the
88 # receiver is given some compensation, but this is not enforced.)
89 @public
90 def transferStock(receiver: address, transfer_order: uint256(currency_value)):
91     assert transfer_order > 0 # This is similar to sellStock above.
92     # Similarly, you can only trade as much stock as you own.
93     assert self.getHolding(msg.sender) >= transfer_order
94
95     # Debit the sender's stock and add to the receiver's address.
96     self.holdings[msg.sender] -= transfer_order
97     self.holdings[receiver] += transfer_order
98
99     # Log the transfer event.
100     log.Transfer(msg.sender, receiver, transfer_order)
101
102 # Allow the company to pay someone for services rendered.
103 @public
104 def payBill(vendor: address, amount: wei_value):
105     # Only the company can pay people.
106     assert msg.sender == self.company
107     # Also, it can pay only if there's enough to pay them with.
108     assert self.cash() >= amount
109
110     # Pay the bill!
111     send(vendor, amount)
112
113     # Log the payment event.

```

(continues on next page)

(continued from previous page)

```

114     log.Pay(vendor, amount)
115
116     # Return the amount in wei that a company has raised in stock offerings.
117     @public
118     @constant
119     def debt() -> wei_value:
120         return (self.totalShares - self.holdings[self.company]) * self.price
121
122     # Return the cash holdings minus the debt of the company.
123     # The share debt or liability only is included here,
124     # but of course all other liabilities can be included.
125     @public
126     @constant
127     def worth() -> wei_value:
128         return self.cash() - self.debt()

```

The contract contains a number of methods that modify the contract state as well as a few ‘getter’ methods to read it. We first declare several events that the contract logs. We then declare our global variables, followed by function definitions.

```

Buy: event({_buyer: indexed(address), _buy_order: uint256(currency_value)})
Sell: event({_seller: indexed(address), _sell_order: uint256(currency_value)})
Pay: event({_vendor: indexed(address), _amount: wei_value})

# Initiate the variables for the company and it's own shares.
company: public(address)
totalShares: public(uint256(currency_value))

```

We initiate the `company` variable to be of type `address` that’s `public`. The `totalShares` variable is of type `currency_value`, which in this case represents the total available shares of the company. The `price` variable represents the wei value of a share and `holdings` is a mapping that maps an address to the number of shares the address owns.

In the constructor, we set up the contract to check for valid inputs during the initialization of the contract via the two `assert` statements. If the inputs are valid, the contract variables are set accordingly and the company’s address is initialized to hold all shares of the company in the `holdings` mapping.

We will be seeing a few `@constant` decorators in this contract—which is used to decorate methods that simply read the contract state or return a simple calculation on the contract state without modifying it. Remember, reading the blockchain is free, writing on it is not. Since Vyper is a statically typed language, we see an arrow following the definition of the `stockAvailable()` method, which simply represents the data type which the function is expected to return. In the method, we simply key into `self.holdings` with the company’s address and check it’s holdings.

Now, lets take a look at a method that lets a person buy stock from the company’s holding.

The `buyStock()` method is a `@payable` method which takes an amount of ether sent and calculates the `buyOrder` (the stock value equivalence at the time of call). The number of shares is deducted from the company’s holdings and transferred to the sender’s in the `holdings` mapping.

Now that people can buy shares, how do we check someone’s holdings?

The `getHolding()` is another `@constant` method that takes an address and returns its corresponding stock holdings by keying into `self.holdings`.

To check the ether balance of the company, we can simply call the getter method `cash()`.

To sell a stock, we have the `sellStock()` method which takes a number of stocks a person wishes to sell, and sends the equivalent value in ether to the seller’s address. We first `assert` that the number of stocks the person wishes to sell is a value greater than 0. We also `assert` to see that the user can only sell as much as the user owns and that the

company has enough ether to complete the sale. If all conditions are met, the holdings are deducted from the seller and given to the company. The ethers are then sent to the seller.

A stockholder can also transfer their stock to another stockholder with the `transferStock()` method. The method takes a receiver address and the number of shares to send. It first `asserts` that the amount being sent is greater than 0 and `asserts` whether the sender has enough stocks to send. If both conditions are satisfied, the transfer is made.

The company is also allowed to pay out an amount in ether to an address by calling the `payBill()` method. This method should only be callable by the company and thus first checks whether the method caller's address matches that of the company. Another important condition to check is that the company has enough funds to pay the amount. If both conditions satisfy, the contract sends its ether to an address.

We can also check how much the company has raised by multiplying the number of shares the company has sold and the price of each share. We can get this value by calling the `debt()` method.

Finally, in this `worth()` method, we can check the worth of a company by subtracting its debt from its ether balance.

This contract has been the most thorough example so far in terms of its functionality and features. Yet despite the thoroughness of such a contract, the logic remained simple. Hopefully, by now, the Vyper language has convinced you of its capabilities and readability in writing smart contracts.

3.7 Event Logging

Like Solidity and other EVM languages, Vyper can log events to be caught and displayed by user interfaces.

3.7.1 Example of Logging

This example is taken from the [sample ERC20 contract](#) and shows the basic flow of event logging.

```
# Events of the token.
Transfer: event({_from: indexed(address), _to: indexed(address), _value: uint256})
Approval: event({_owner: indexed(address), _spender: indexed(address), _value:
    uint256})

# Transfer some tokens from message sender to another address
def transfer(_to : address, _value : uint256) -> bool:

    ... Logic here to do the real work ...

    # All done, log the event for listeners
    log.Transfer(msg.sender, _to, _amount)
```

Let's look at what this is doing. First, we declare two event types to log. The two events are similar in that they contain two indexed address fields. Indexed fields do not make up part of the event data itself, but can be searched by clients that want to catch the event. Also, each event contains one single data field, in each case called `_value`. Events can contain several arguments with any names desired.

Next, in the `transfer` function, after we do whatever work is necessary, we log the event. We pass three arguments, corresponding with the three arguments of the `Transfer` event declaration.

Clients listening to the events will declare and handle the events they are interested in using a [library such as web3.js](#):

```
var abi = /* abi as generated by the compiler */;
var MyToken = web3.eth.contract(abi);
var myToken = MyToken.at("0x1234...ab67" /* address */);
```

(continues on next page)

(continued from previous page)

```
// watch for changes in the callback
var event = myToken.Transfer(function(error, result) {
    if (!error) {
        var args = result.args;
        console.log('value transferred = ', args._amount);
    }
});
```

In this example, the listening client declares the event to listen for. Any time the contract sends this log event, the callback will be invoked.

3.7.2 Declaring Events

Let's look at an event declaration in more detail.

```
Transfer: event({_from: indexed(address), _to: indexed(address), _value: uint256})
```

Event declarations look like state variable declarations but use the special keyword `event`. `event` takes a as its argument that consist of all the arguments to be passed as part of the event. Typical events will contain two kinds of arguments:

- Indexed arguments, which can be searched for by listeners. Each indexed argument is identifier by the *indexed* keyword. Here, each indexed argument is an address. You can have any number of indexed arguments, but indexed arguments are not passed directly to listeners, although some of this information (such as the sender) may be available in the listener's *results* object.
- Value arguments, which are passed through to listeners. You can have any number of value arguments and they can have arbitrary names, but each is limited by the EVM to be no more than 32 bytes.

Note that while the argument definition syntax looks like a Python dictionary, it's actually an order-sensitive definition. (Python dictionaries [maintain order starting with 3.7.](#)) Thus, the first element (`_from`) will be matched up with the first argument passed in the `log.Transfer` call.

3.7.3 Logging Events

Once an event is declared, you can log (send) events. You can send events as many times as you want to. Please note that events sent do not take state storage and thus do not cost gas: this makes events a good way to save some information. However, the drawback is that events are not available to contracts, only to clients.

Logging events is done using the magic keyword `log`:

```
log.Transfer(msg.sender, _to, _amount)
```

The order and types of arguments sent needs to match up with the order of declarations in the dictionary.

3.7.4 Listening for Events

In the example listener above, the *result* arg actually passes a [large amount of information](#). Here we're most interested in *result.args*. This is an object with properties that match the properties declared in the event. Note that this object does not contain the indexed properties, which can only be searched in the original *myToken.Transfer* that created the callback.

3.8 Contributing

Help is always appreciated!

To get started, you can try [installing Vyper](#) in order to familiarize yourself with the components of Vyper and the build process. Also, it may be useful to become well-versed at writing smart-contracts in Vyper.

3.8.1 Types of Contributions

In particular, we need help in the following areas:

- Improving the documentation
- Responding to questions from other users on [StackExchange](#) and the [Vyper Gitter](#)
- Suggesting Improvements
- Fixing and responding to [Vyper's GitHub issues](#)

3.8.2 How to Suggest Improvements

To suggest an improvement, please create a Vyper Improvement Proposal (VIP for short) using the [VIP Template](#).

3.8.3 How to Report Issues

To report an issue, please use the [GitHub issues tracker](#). When reporting issues, please mention the following details:

- Which version of Vyper you are using
- What was the source code (if applicable)
- Which platform are you running on
- Your operating system name and version
- Detailed steps to reproduce the issue
- What was the result of the issue
- What the expected behaviour is

Reducing the source code that caused the issue to a bare minimum is always very helpful and sometimes even clarifies a misunderstanding.

3.8.4 Fix Bugs

Find or report bugs at our [issues page](#). Anything tagged with “bug” is open to whoever wants to implement it.

3.8.5 Workflow for Pull Requests

In order to contribute, please fork off of the `master` branch and make your changes there. Your commit messages should detail *why* you made your change in addition to *what* you did (unless it is a tiny change).

If you need to pull in any changes from `master` after making your fork (for example, to resolve potential merge conflicts), please avoid using `git merge` and instead, `git rebase` your branch.

Implement Features

If you are writing a new feature, please ensure you write appropriate Boost test cases and place them under `tests/`.

If you are making a larger change, please consult first with the Gitter channel.

Although we do CI testing, please make sure that the tests pass for supported Python version and ensure that it builds locally before submitting a pull request.

Thank you for your help!

3.9 Frequently Asked Questions

3.9.1 Basic Questions

What is Vyper?

Vyper is a smart contract development language. Vyper aims to be auditable, secure, and human-readable. Being simple to read is more important than being simple to write.

Vyper or Solidity?

For the majority of use-cases, this is personal preference. To support the aims of being secure, auditable, and human-readable, a number of programming constructs included in Solidity are not included in Vyper. If your use-case requires these, use Solidity not Vyper.

What is not included in Vyper?

The following constructs are not included because their use can lead to misleading or difficult to understand code:

- Modifiers
- Class inheritance
- Inline assembly
- Function overloading
- Operator overloading
- Binary fixed point.

Recursive calling and infinite-length loops are not included because they cannot set an upper bound on gas limits. An upper bound is required to prevent gas limit attacks and ensure the security of smart contracts built in Vyper.

How do for loops work?

Like Python for loops but with one significant difference. Vyper does not allow looping over variable lengths. Looping over variables introduces the possibility of infinite-length loops which make gas limit attacks possible.

How do structs work?

Structs group variables and are accessed using `struct.argname`. They are similar to Python classes:

```
# define the struct
struct MyStruct:
    arg1: int128
    arg2: decimal
struct: MyStruct

#access arg1 in struct
struct.arg1 = 1
```

3.9.2 Advanced Questions

3.10 Built in Functions

Vyper contains a set amount of built in functions that would be timely and/or unachievable to write in Vyper.

3.10.1 Functions

floor

```
def floor(a) -> b:
    """
    :param a: value to round down
    :type a: decimal

    :output b: int128
    """
```

Rounds a decimal down to the nearest integer.

ceil

```
def ceil(a) -> b:
    """
    :param a: value to round up
    :type a: decimal

    :output b: int128
    """
```

Rounds a decimal up to the nearest integer.

convert

```
def convert(a, b) -> c:
    """
    :param a: value to convert
    :type a: either bool, decimal, int128, uint256 or bytes32
    :param b: the destination type to convert to
    :type b: type of either decimal, int128, uint256 or bytes32

    :output c: either decimal, int128, uint256 or bytes32
    """
```

Converts a variable/ literal from one type to another.

clear

```
def clear(a):
    """
    :param a: variable to reset to its default value
    :type a: all types
    """
```

Clears a variable's contents to the default value of its type.

as_wei_value

```
def as_wei_value(a, b) -> c:
    """
    :param a: value for the ether unit
    :type a: uint256 or int128 or decimal
    :param b: ether unit name (e.g. ``"wei"``)
    :type b: str_literal

    :output c: wei_value
    """
```

The value of the input number as wei, converted based on the specified unit.

as_unitless_number

```
def as_unitless_number(a) -> b:
    """
    :param a: value to remove units from
    :type a: either decimal or int128

    :output b: either decimal or int128
    """
```

Turns a int128, uint256, decimal with units into one without units (used for assignment and math).

slice

```
def slice(a, start=b, len=c) -> d:
    """
    :param a: bytes to be sliced
    :type a: either bytes or bytes32
    :param b: start position of the slice
    :type b: int128
    :param c: length of the slice
    :type c: int128

    :output d: bytes
    """
```

Takes a list of bytes and copies, then returns a specified chunk.

len

```
def len(a) -> b:
    """
    :param a: value to get the length of
    :type a: bytes

    :output b: int128
    """
```

Returns the length of a given list of bytes.

concat

```
def concat(a, b, ...) -> c:
    """
    :param a: value to combine
    :type a: bytes, bytes32
    :param b: value to combine
    :type b: bytes, bytes32

    :output b: bytes
    """
```

Takes 2 or more bytes arrays of type bytes32 or bytes and combines them into one.

sha3/ keccak256

```
def sha3(a) -> b:
    """
    :param a: value to hash
    :type a: either str_literal, bytes, bytes32

    :output b: bytes32
    """
```

Returns keccak256 (Ethereum's sha3) hash of input. Note that it can be called either by using sha3 or keccak256.

sha256

```
def sha256(a) -> b:
    """
    :param a: value to hash
    :type a: either str_literal, bytes, bytes32

    :output b: bytes32
    """
```

Returns sha256 (SHA2 256bit output) hash of input.

method_id

```
def method_id(a, b) -> c:
    """
    :param a: method declaration
    :type a: str_literal
    :param b: type of output
    :type b: either bytes32 or bytes[4]

    :output c: either bytes32 or bytes[4]
    """
```

Takes a function declaration and returns its method_id (used in data field to call it).

ecrecover

```
def ecrecover(hash, v, r, s) -> b:
    """
    :param hash: a signed hash
    :type hash: bytes32
    :param v:
    :type v: uint256
    :param r: elliptic curve point
    :type r: uint256
    :param s: elliptic curve point
    :type s: uint256

    :output b: address
    """
```

Takes a signed hash and vrs and returns the public key of the signer.

ecadd

```
def ecadd(a, b) -> sum:
    """
    :param a: pair to be added
    :type a: uint256[2]
    :param b: pair to be added
    :type b: uint256[2]
```

(continues on next page)

(continued from previous page)

```
:output sum: uint256[2]
"""
```

Takes two elliptical curves and adds them together.

ecmul

```
def ecmul(a, b) -> product:
    """
    :param a: pair to be multiplied
    :type a: uint256[2]
    :param b: number to be multiplied
    :type b: uint256

    :output product: uint256[2]
    """
```

Takes two elliptical curves and multiplies them together.

extract32

```
def extract32(a, b, type=c) -> d:
    """
    :param a: where 32 bytes are extracted from
    :type a: bytes
    :param b: start point of bytes to be extracted
    :type b: int128
    :param c: type of output (Optional, default: bytes32)
    :type c: either bytes32, int128, or address

    :output d: either bytes32, int128, or address
    """
```

RLPList

```
def _RLPList(a, b) -> c:
    """
    :param a: encoded data
    :type a: bytes
    :param b: RLP list
    :type b: list

    :output c: LLLnode
    """
```

Takes encoded RLP data and an unencoded list of types. Usage:

```
vote_msg: bytes <= 1024 = ...

values = RLPList(vote_msg, [int128, int128, bytes32, bytes, bytes])

var1: int128 = values[0]
```

(continues on next page)

1. send 6270960000000000 wei to 0xd2c560282c9C02465C2dAcDEF3E859E730848761
2. Publish this tx to create the contract:

```
0xf90237808506fc23ac00830330888080b902246102128061000e60003961022056600060007f01000000000000000000
```

3. This is the contract address: 0xCb969cAAad21A78a24083164ffa81604317Ab603

3.11 Low Level Built in Functions

Vyper contains a set of built in functions which executes unique OPCODES such as send or selfdestruct.

3.11.1 Low Level Functions

send

```
def send(a, b):
    """
    :param a: the destination address to send ether to
    :type a: address
    :param b: the wei value to send to the address
    :type b: uint256(wei)
    """
```

Sends ether from the contract to the specified Ethereum address. Note that the amount to send should be specified in wei.

raw_call

```
def raw_call(a, b, outsize=c, gas=d, value=e, delegate_call=f) -> g:
    """
    :param a: the destination address to call to
    :type a: address
    :param b: the data to send the called address
    :type b: bytes
    :param c: the max-length for the bytes array returned from the call.
    :type c: fixed literal value
    :param d: the gas amount to attach to the call.
    :type d: uint256
    :param e: the wei value to send to the address (Optional, default: 0)
    :type e: uint256
    :param f: the bool of whether or not to use DELEGATECALL (Optional, default: False)
    :type f: bool
```

(continues on next page)

(continued from previous page)

```
:output g: bytes[outsized]
"""
```

Calls to the specified Ethereum address. The call should pass data and may optionally send eth value (specified in wei) as well. The call must specify a gas amount to attach the call and the outsized. Returns the data returned by the call as a bytes array with the outsized as the max length.

selfdestruct

```
def selfdestruct(a):
    """
    :param a: the address to send the contracts left ether to
    :type a: address
    """
```

Causes a self destruction of the contract, triggers the SELFDESTRUCT opcode (0xff). CAUTION! This method will delete the contract from the Ethereum blockchain. All none ether assets associated with this contract will be “burned” and the contract will be inaccessible.

assert

```
def assert(a):
    """
    :param a: the boolean condition to assert
    :type a: bool
    """
```

Asserts the specified condition, if the condition is equals to true the code will continue to run. Otherwise, the OPCODE REVERT (0xfd) will be triggered, the code will stop it’s operation, the contract’s state will be reverted to the state before the transaction took place and the remaining gas will be returned to the transaction’s sender.

Note: To give it a more Python like syntax, the assert function can be called without parenthesis, the syntax would be `assert your_bool_condition`. Even though both options will compile, it’s recommended to use the Pythonic version without parenthesis.

raw_log

```
def raw_log(a, b):
    """
    :param a: the address of the contract to duplicate.
    :type a: * (any input)
    :param b: the name of the logged event.
    :type b: bytes
    """
```

Emits a log without specifying the abi type, with the arguments entered as the first input.

create_forwarder_to

```
def create_forwarder_to(a, value=b):
    """
    :param a: the address of the contract to duplicate.
    :type a: address
    :param b: the wei value to send to the new contract instance (Optional, default: 0)
    :type b: uint256(wei)
    """
```

Duplicates a contract's code and deploys it as a new instance, by means of a DELEGATECALL. You can also specify wei value to send to the new contract as `value=the_value`.

blockhash

```
def blockhash(a) -> hash:
    """
    :param a: the number of the block to get
    :type a: uint256

    :output hash: bytes32
    """
```

Returns the hash of the block at the specified height.

Note: The EVM only provides access to the most 256 blocks. This function will return 0 if the block number is greater than or equal to the current block number or more than 256 blocks behind the current block.

3.12 Types

Vyper is a statically typed language, which means that the type of each variable (state and local) needs to be specified or at least known at compile-time. Vyper provides several elementary types which can be combined to form complex types.

In addition, types can interact with each other in expressions containing operators.

3.12.1 Value Types

The following types are also called value types because variables of these types will always be passed by value, i.e. they are always copied when they are used as function arguments or in assignments.

Boolean

Keyword: `bool`

A boolean is a type to store a logical/truth value.

Values

The only possible values are the constants `True` and `False`.

Operators

Operator	Description
<code>x not y</code>	Logical negation
<code>x and y</code>	Logical conjunction
<code>x or y</code>	Logical disjunction
<code>x == y</code>	Equality
<code>x != y</code>	Inequality

The operators `or` and `and` apply the common short-circuiting rules.

Signed Integer (128 bit)

Keyword: `int128`

A signed integer (128 bit) is a type to store positive and negative integers.

Values

Signed integer values between -2^{127} and $(2^{127} - 1)$, inclusive.

Operators

Comparisons

Comparisons return a boolean value.

Operator	Description
<code>x < y</code>	Less than
<code>x <= y</code>	Less than or equal to
<code>x == y</code>	Equals
<code>x != y</code>	Does not equal
<code>x >= y</code>	Greater than or equal to
<code>x > y</code>	Greater than

`x` and `y` must be of the type `int128`.

Arithmetic Operators

Operator	Description
<code>x + y</code>	Addition
<code>x - y</code>	Subtraction
<code>-x</code>	Unary minus/Negation
<code>x * y</code>	Multiplication
<code>x / y</code>	Division
<code>x**y</code>	Exponentiation
<code>x % y</code>	Modulo
<code>min(x, y)</code>	Minimum
<code>max(x, y)</code>	Maximum

`x` and `y` must be of the type `int128`.

Unsigned Integer (256 bit)

Keyword: `uint256`

An unsigned integer (256 bit) is a type to store non-negative integers.

Values

Integer values between 0 and $(2^{256}-1)$.

Note: Integer literals are interpreted as `int128` by default. In cases where `uint256` is more appropriate, such as assignment, the literal might be interpreted as `uint256`. Example: `_variable: uint256 = _literal`. In order to explicitly cast a literal to a `uint256` use `convert(_literal, uint256)`.

Operators

Comparisons

Comparisons return a boolean value.

Operator	Description
<code>x < y</code>	Less than
<code>x <= y</code>	Less than or equal to
<code>x == y</code>	Equals
<code>x != y</code>	Does not equal
<code>x >= y</code>	Greater than or equal to
<code>x > y</code>	Greater than

`x` and `y` must be of the type `uint256`.

Arithmetic Operators

Operator	Description
<code>x + y</code>	Addition
<code>x - y</code>	Subtraction
<code>uint256_addmod(x, y, z)</code>	Addition modulo <code>z</code>
<code>x * y</code>	Multiplication
<code>uint256_mulmod(x, y, z)</code>	Multiplication modulo <code>z</code>
<code>x / y</code>	Division
<code>x**y</code>	Exponentiation
<code>x % y</code>	Modulo
<code>min(x, y)</code>	Minimum
<code>max(x, y)</code>	Maximum

`x`, `y` and `z` must be of the type `uint256`.

Bitwise Operators

Operator	Description
<code>bitwise_and(x, y)</code>	AND
<code>bitwise_not(x, y)</code>	NOT
<code>bitwise_or(x, y)</code>	OR
<code>bitwise_xor(x, y)</code>	XOR
<code>shift(x, _shift)</code>	Bitwise Shift

`x` and `y` must be of the type `uint256`. `_shift` must be of the type `int128`.

Note: Positive `_shift` equals a left shift; negative `_shift` equals a right shift. Values shifted above/below the most/least significant bit get discarded.

Decimals

Keyword: `decimal`

A decimal is a type to store a decimal fixed point value.

Values

A value with a precision of 10 decimal places between -2^{127} and $(2^{127} - 1)$.

Operators

Comparisons

Comparisons return a boolean value.

Operator	Description
<code>x < y</code>	Less than
<code>x <= y</code>	Less or equal
<code>x == y</code>	Equals
<code>x != y</code>	Does not equal
<code>x >= y</code>	Greater or equal
<code>x > y</code>	Greater than

`x` and `y` must be of the type `decimal`.

Arithmetic Operators

Operator	Description
<code>x + y</code>	Addition
<code>x - y</code>	Subtraction
<code>-x</code>	Unary minus/Negation
<code>x * y</code>	Multiplication
<code>x / y</code>	Divison
<code>x % y</code>	Modulo
<code>min(x, y)</code>	Minimum
<code>max(x, y)</code>	Maximum
<code>floor(x)</code>	Largest integer $\leq x$. Returns <code>int128</code> .
<code>ceil(x)</code>	Smallest integer $\geq x$. Returns <code>int128</code> .

`x` and `y` must be of the type `decimal`.

Address

Keyword: `address`

The `address` type holds an Ethereum address.

Values

An `address` type can hold an Ethereum address which equates to 20 bytes or 160 bits. It returns in hexadecimal notation with a leading `0x`.

Members

Member	Description
<code>balance</code>	Query the balance of an address. Returns <code>wei_value</code> .
<code>codesize</code>	Query the code size of an address. Returns <code>int128</code> .
<code>is_contract</code>	Query whether it is a contract address. Returns <code>bool</code> .

Syntax as follows: `_address.<member>`, where `_address` is of the type `address` and `<member>` is one of the above keywords.

Unit Types

Vyper allows the definition of types with discrete units e.g. meters, seconds, wei, These types may only be based on either `uint256`, `int128` or `decimal`. Vyper has 3 unit types built in, which are the following:

Time

Keyword	Unit	Base type	Description
<code>timestamp</code>	1 sec	<code>uint256</code>	This represents a point in time.
<code>timedelta</code>	1 sec	<code>uint256</code>	This is a number of seconds.

Note: Two `timedelta` can be added together, as can a `timedelta` and a `timestamp`, but not two `timestamps`.

Wei

Keyword	Unit	Base type	Description
<code>wei_value</code>	1 wei	<code>uint256</code>	This is an amount of Ether in wei.

Custom Unit Types

Vyper allows you to add additional not-provided unit label to either `uint256`, `int128` or `decimal`.

Custom units example:

```
# specify units used in the contract.
units: {
    cm: "centimeter",
    km: "kilometer"
}
```

Having defined the units they can be defined on variables as follows.

Custom units usage:

```
a: int128(cm)
b: uint256(km)
```

32-bit-wide Byte Array

Keyword: `bytes32` This is a 32-bit-wide byte array that is otherwise similar to byte arrays.

Example:

```
# Declaration
hash: bytes32
# Assignment
self.hash = _hash
```


Operators

Keyword	Description
<code>sha3(x)</code>	Return the sha3 hash as bytes32.
<code>concat(x, ...)</code>	Concatenate multiple inputs.
<code>slice(x, start=_start, len=_len)</code>	Return a slice of <code>_len</code> starting at <code>_start</code> .

Where `x` is a byte array and `_start` as well as `_len` are integer values.

Fixed-size Byte Arrays

Keyword: `bytes`

A byte array with a fixed size. The syntax being `bytes[maxLen]`, where `maxLen` is an integer which denotes the maximum number of bytes. On the ABI level the Fixed-size bytes array is annotated as `bytes`.

Example:

```
example_bytes: bytes[100] = b"\x01\x02\x03"
```

Fixed-size Strings

Keyword: `string` Fixed-size strings can hold strings with equal or fewer characters than the maximum length of the string. On the ABI level the Fixed-size bytes array is annotated as `string`.

Example:

```
example_str: string[100] = "Test String"
```

Operators

Keyword	Description
<code>len(x)</code>	Return the length as an integer.
<code>sha3(x)</code>	Return the sha3 hash as bytes32.
<code>concat(x, ...)</code>	Concatenate multiple inputs.
<code>slice(x, start=_start, len=_len)</code>	Return a slice of <code>_len</code> starting at <code>_start</code> .

Where `x` is a byte array or string while `_start` and `_len` are integers. The `len`, `sha3`, `concat`, `slice` operators can be used with `string` and `bytes` types.

3.12.2 Reference Types

Reference types do not fit into 32 bytes. Because of this, copying their value is not as feasible as with value types. Therefore only the location, i.e. the reference, of the data is passed.

Fixed-size Lists

Fixed-size lists hold a finite number of elements which belong to a specified type.

Syntax

Lists can be declared with `_name: _ValueType[_Integer]`. Multidimensional lists are also possible.

Example:

```
#Defining a list
exampleList: int128[3]
#Setting values
exampleList = [10, 11, 12]
exampleList[2] = 42
#Returning a value
return exampleList[0]
```

Structs

Structs are custom defined types that can group several variables.

Syntax

Structs can be accessed via `struct.argname`. **Example:**

```
#Defining a struct
struct MyStruct:
    value1: int128
    value2: decimal
exampleStruct: MyStruct
#Constructing a struct
exampleStruct = MyStruct({value1: 1, value2: 2})
#Accessing a value
exampleStruct.value1 = 1
```

Mappings

Mappings in Vyper can be seen as [hash tables](#) which are virtually initialized such that every possible key exists and is mapped to a value whose byte-representation is all zeros: a type's default value. The similarity ends here, though: The key data is not actually stored in a mapping, only its `keccak256` hash used to look up the value. Because of this, mappings do not have a length or a concept of a key or value being “set”.

It is possible to mark mappings `public` and have Vyper create a getter. The `_KeyType` will become a required parameter for the getter and it will return `_ValueType`.

Note: Mappings are only allowed as state variables.

Syntax

Mapping types are declared as `map(_KeyType, _ValueType)`. Here `_KeyType` can be any base or bytes type. Mappings, contract or structs are not support as key types. `_ValueType` can actually be any type, including mappings.

Example:

```
#Defining a mapping
exampleMapping: map(int128, decimal)
#Accessing a value
exampleMapping[0] = 10.1
```

Note: Mappings can only be accessed, not iterated over.

3.12.3 Builtin Constants

Vyper has a few convenience constants builtin.

Type	Name	Value
address	ZERO_ADDRESS	0x00000000000000000000000000000000
bytes32	EMPTY_BYTES32	0x00
int128	MAX_INT128	2**127 - 1
int128	MIN_INT128	-2**127
decimal	MAX_DECIMAL	(2**127 - 1)
decimal	MIN_DECIMAL	(-2**127)
uint256	MAX_UINT256	2**256 - 1

3.12.4 Custom Constants

Custom constants can be defined at a global level in Vyper. To define a constant make use of the *constant* keyword.

Example:

```
TOTAL_SUPPLY: constant(uint256) = 10000000
total_supply: public(uint256)

@public
def __init__():
    self.total_supply = TOTAL_SUPPLY
```

Advanced Example:

```
units: {
    share: "Share unit"
}

MAX_SHARES: constant(uint256(share)) = 1000
SHARE_PRICE: constant(uint256(wei/share)) = 5

@public
def market_cap() -> uint256(wei):
    return MAX_SHARES * SHARE_PRICE
```

3.12.5 Initial Values

In Vyper, there is no `null` option like most programming languages have. Thus, every variable type has a default value. In order to check if a variable is empty, you will need to compare it to its type's default value. If you would like to reset a variable to its type's default value, use the built-in `clear()` function.

Here you can find a list of all types and default values:

Table 1: Default Variable Values

Type	Default Value
<code>bool</code>	<code>False</code>
<code>int128</code>	<code>0</code>
<code>uint256</code>	<code>0</code>
<code>decimal</code>	<code>1.0</code>
<code>address</code>	<code>0x00</code>
<code>bytes32</code>	<code>0x00</code>

Note: In `bytes` the array starts with the bytes all set to `'\x00'`

Note: In reference types all the type's members are set to their initial values.

3.13 Release Notes

3.13.1 v0.1.0-beta.9

Date released: 12-03-2019

- Add support for list constants ([#1211](#))
- Add sha256 function ([#1327](#))
- Renamed `create_with_code_of` to `create_forwarder_to` ([#1177](#))
- `@nonreentrant` Decorator ([#1204](#))
- Add opcodes and opcodes_runtime flags to compiler ([#1255](#))
- Improved External contract call interfaces ([#885](#))

A

arrays, [53](#)
auction
 blind, [20](#)
 open, [17](#)

B

ballot, [28](#)
blind auction, [20](#)
bool, [47](#)
built-in, [40](#)
bytes, [53](#)
bytes32, [52](#)

C

company stock, [32](#)
contract, [12](#)
conversion, [56](#)
crowdfund, [26](#)

F

false, [47](#)
function, [12](#), [40](#)

I

initial, [55](#)
int, [48](#)
int128, [48](#)
integer, [48](#)

M

mapping, [54](#)
metadata, [12](#)

O

open auction, [17](#)

P

purchases, [24](#)

R

reference, [53](#)

S

state variable, [12](#)
stock
 company, [32](#)
string, [53](#)
structs, [54](#)

T

testing, [11](#)
 deploying, [11](#)
true, [47](#)
type, [47](#)

U

uint256, [49](#)
unit, [49](#)

V

value, [47](#)
voting, [28](#)