BLOCKCHAIN
COMPETENCE CENTER

Ethereum Smart Contract Security

www.blockchaincc.com

@seresistvanandras

Bp. 1139 Váci út 99.

@seresistvanandras

+36209528378

@Istvan_A_Seres

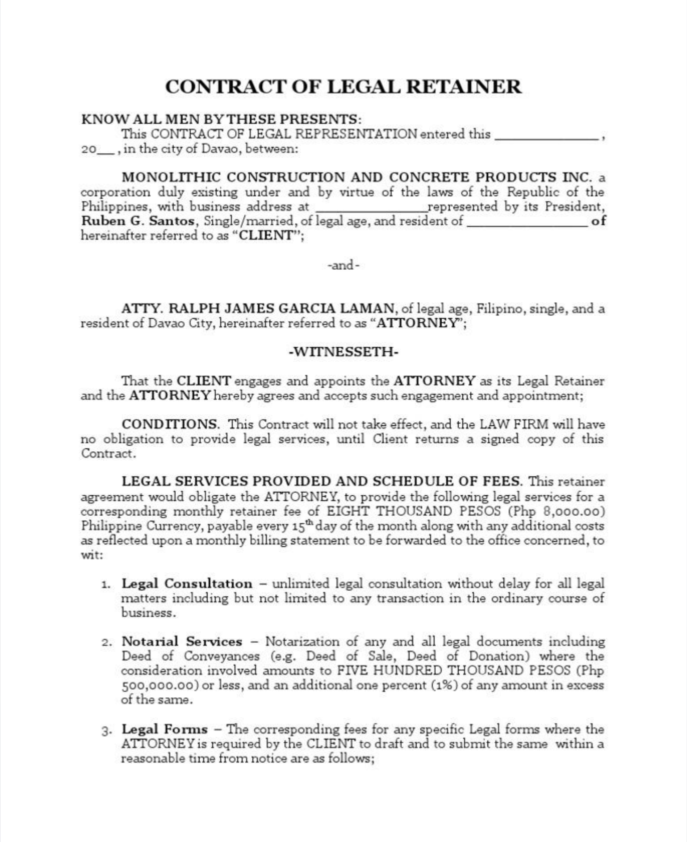
BLOCKCHAIN
COMPETENCE CENTER

BLOCKCHAIN
COMPETENCE CENTER

BLOCKCHAIN
COMPETENCE CENTER

I have a dream...

Today



CONTRACT OF LEGAL RETAINER

KNOW ALL MEN BY THESE PRESENTS:

This CONTRACT OF LEGAL REPRESENTATION entered this ______________ , 20___ , in the city of Davao, between:

MONOLITHIC CONSTRUCTION AND CONCRETE PRODUCTS INC. a corporation duly existing under and by virtue of the laws of the Republic of the Philippines, with business address at ________________represented by its President, **Ruben G. Santos**, Single/married, of legal age, and resident of __________________ **of** hereinafter referred to as "**CLIENT**";

-and-

ATTY. RALPH JAMES GARCIA LAMAN, of legal age, Filipino, single, and a resident of Davao City, hereinafter referred to as "**ATTORNEY**";

-WITNESSETH-

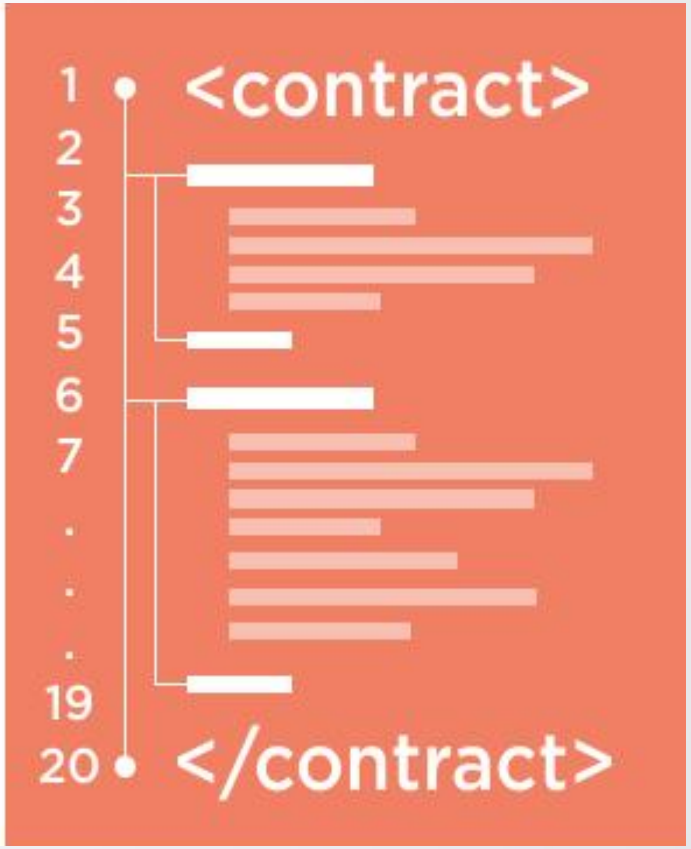
That the **CLIENT** engages and appoints the **ATTORNEY** as its Legal Retainer and the **ATTORNEY** hereby agrees and accepts such engagement and appointment;

CONDITIONS. This Contract will not take effect, and the LAW FIRM will have no obligation to provide legal services, until Client returns a signed copy of this Contract.

LEGAL SERVICES PROVIDED AND SCHEDULE OF FEES. This retainer agreement would obligate the ATTORNEY, to provide the following legal services for a corresponding monthly retainer fee of EIGHT THOUSAND PESOS (Php 8,000.00) Philippine Currency, payable every 15th day of the month along with any additional costs as reflected upon a monthly billing statement to be forwarded to the office concerned, to wit:

1. **Legal Consultation** – unlimited legal consultation without delay for all legal matters including but not limited to any transaction in the ordinary course of business.
2. **Notarial Services** – Notarization of any and all legal documents including Deed of Conveyances (e.g. Deed of Sale, Deed of Donation) where the consideration involved amounts to FIVE HUNDRED THOUSAND PESOS (Php 500,000.00) or less, and an additional one percent (1%) of any amount in excess of the same.
3. **Legal Forms** – The corresponding fees for any specific Legal forms where the ATTORNEY is required by the CLIENT to draft and to submit the same within a reasonable time from notice are as follows;

Tomorrow?



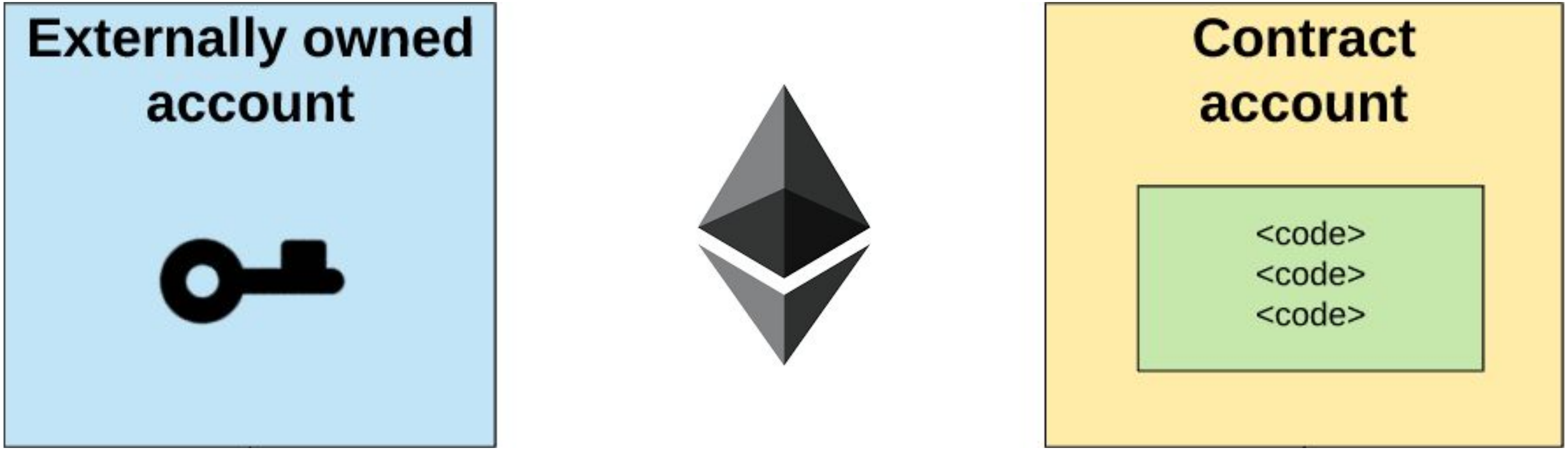
Why smart contracts?

Why should I care?

10% GDP

Smart contract platforms

Ethereum Accounts

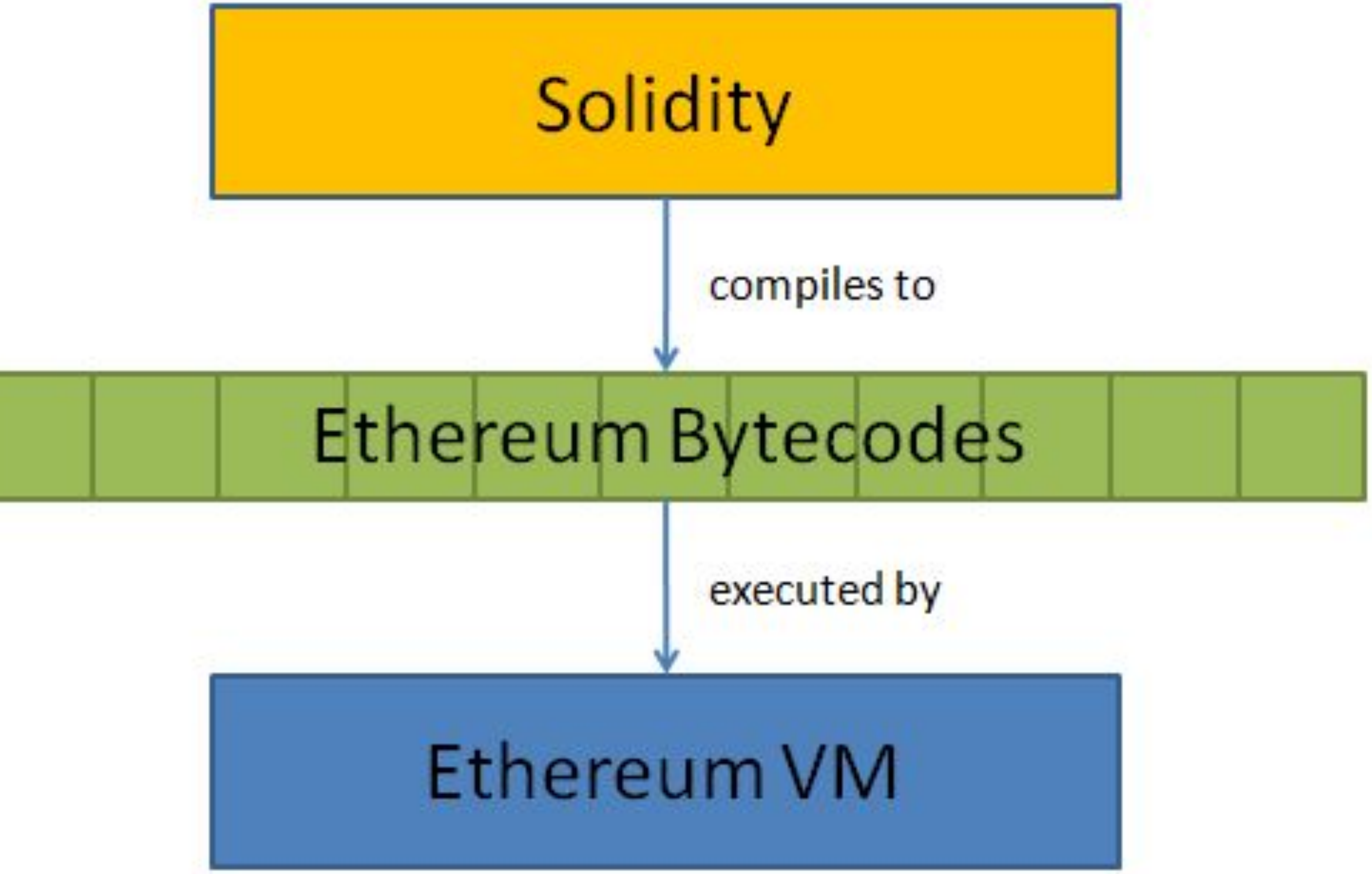


Externally owned account

Contract account

<code>
<code>
<code>

EVM crash-course



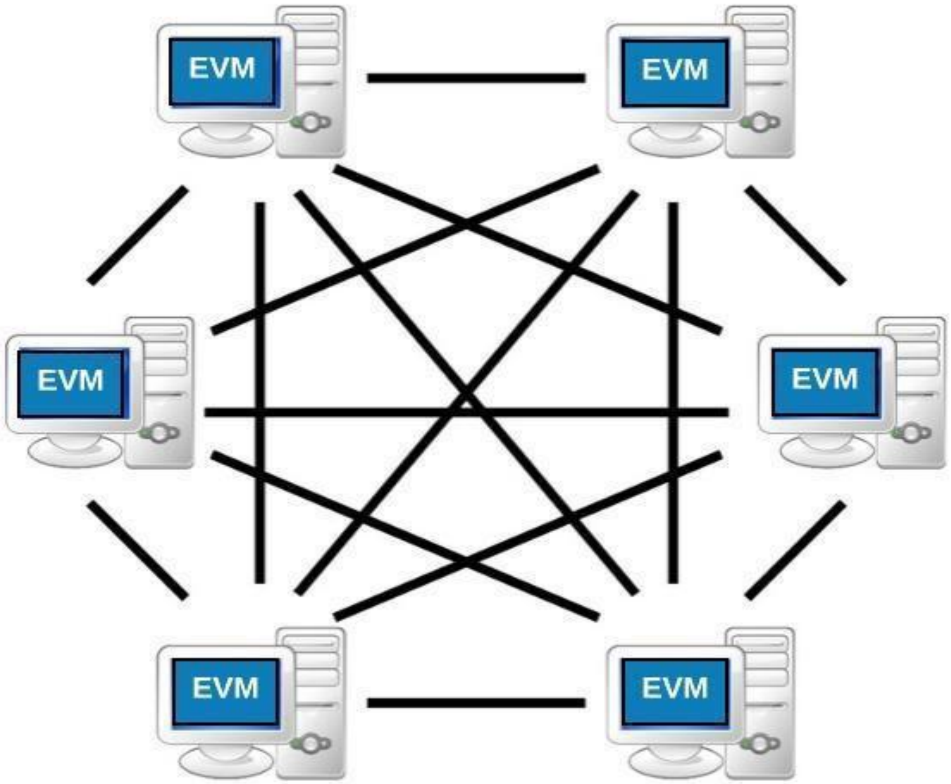
Solidity

compiles to

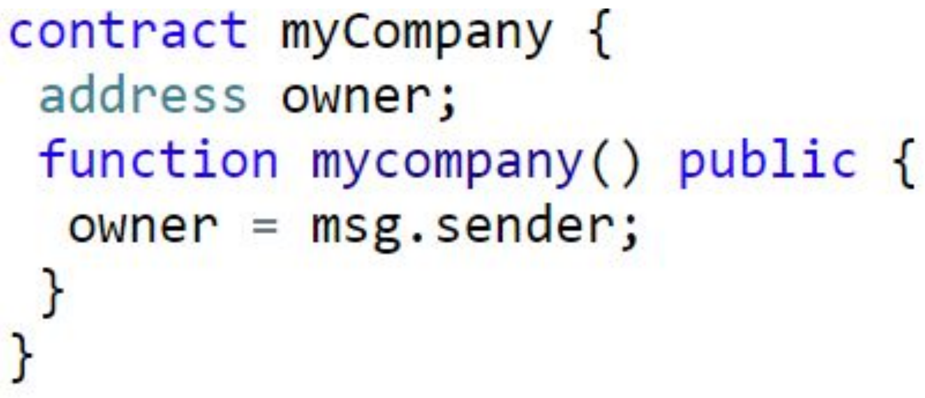
Ethereum Bytecodes

executed by

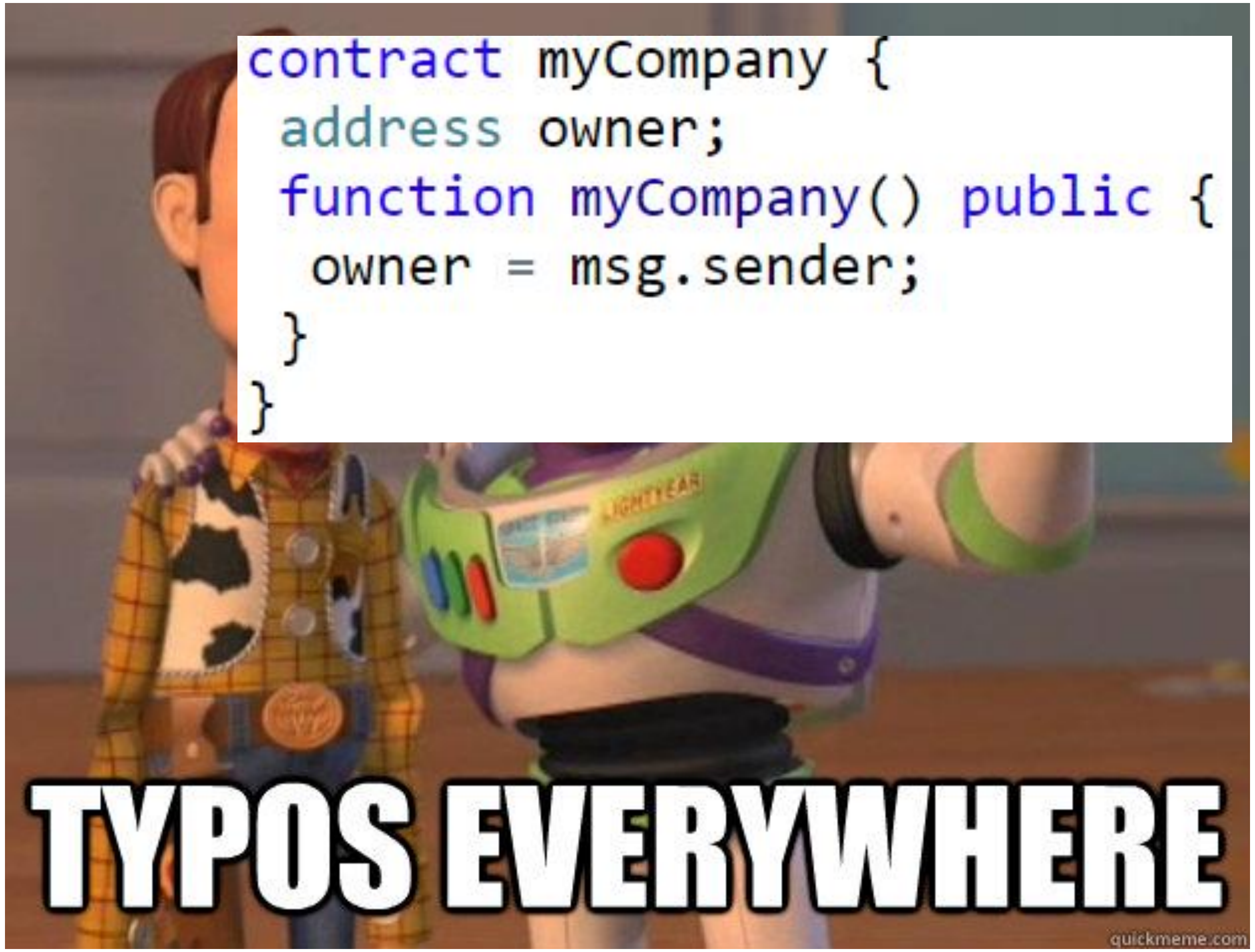
Ethereum VM



Ownership, constructors

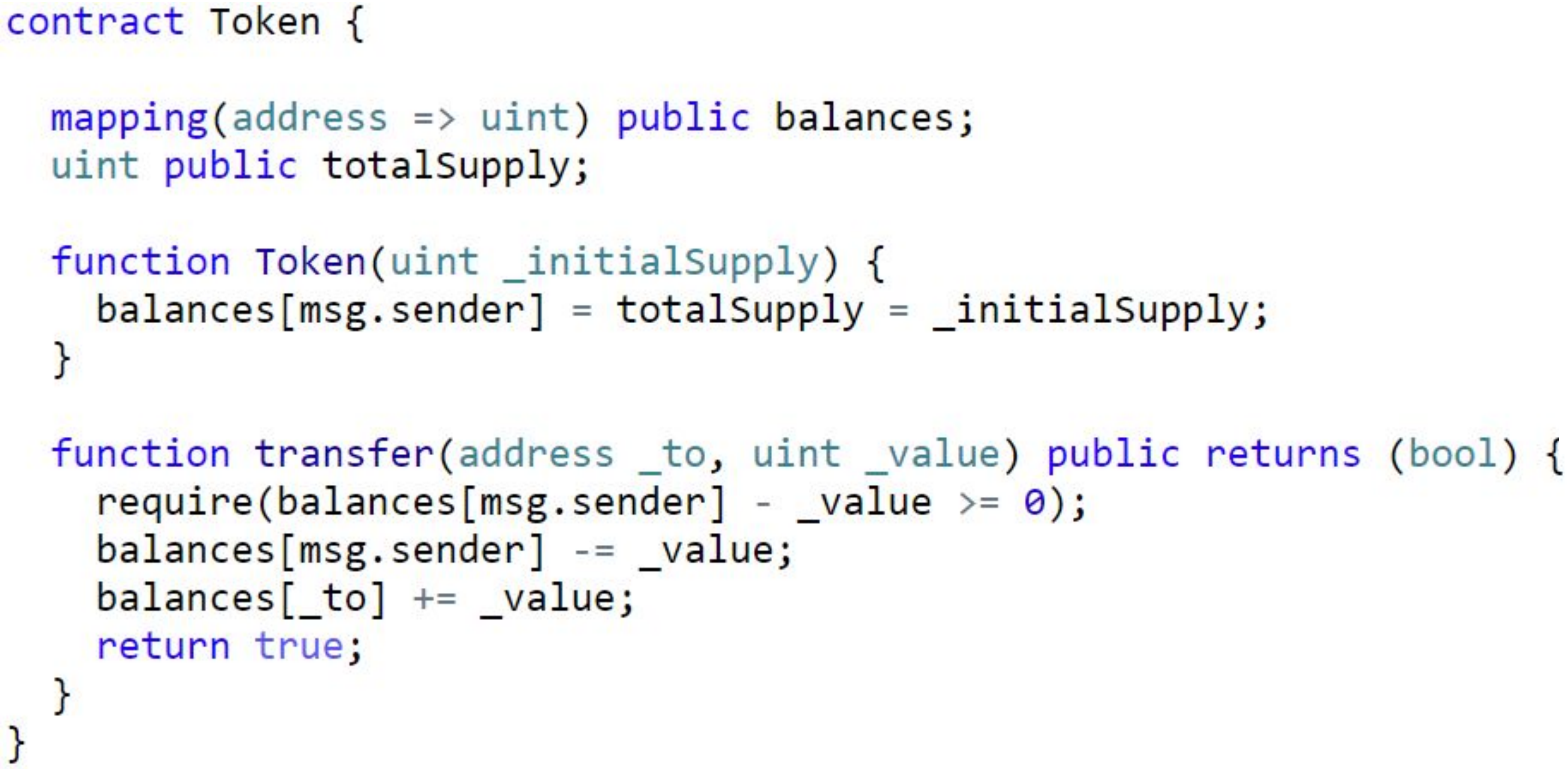


```
contract myCompany {
 address owner;
 function mycompany() public {
  owner = msg.sender;
 }
}
```



```
contract myCompany {
 address owner;
 function myCompany() public {
  owner = msg.sender;
 }
}
```

The classical ones



```
contract Token {

  mapping(address => uint) public balances;
  uint public totalSupply;

  function Token(uint _initialSupply) {
    balances[msg.sender] = totalSupply = _initialSupply;
  }

  function transfer(address _to, uint _value) public returns (bool) {
    require(balances[msg.sender] - _value >= 0);
    balances[msg.sender] -= _value;
    balances[_to] += _value;
    return true;
  }
}
```

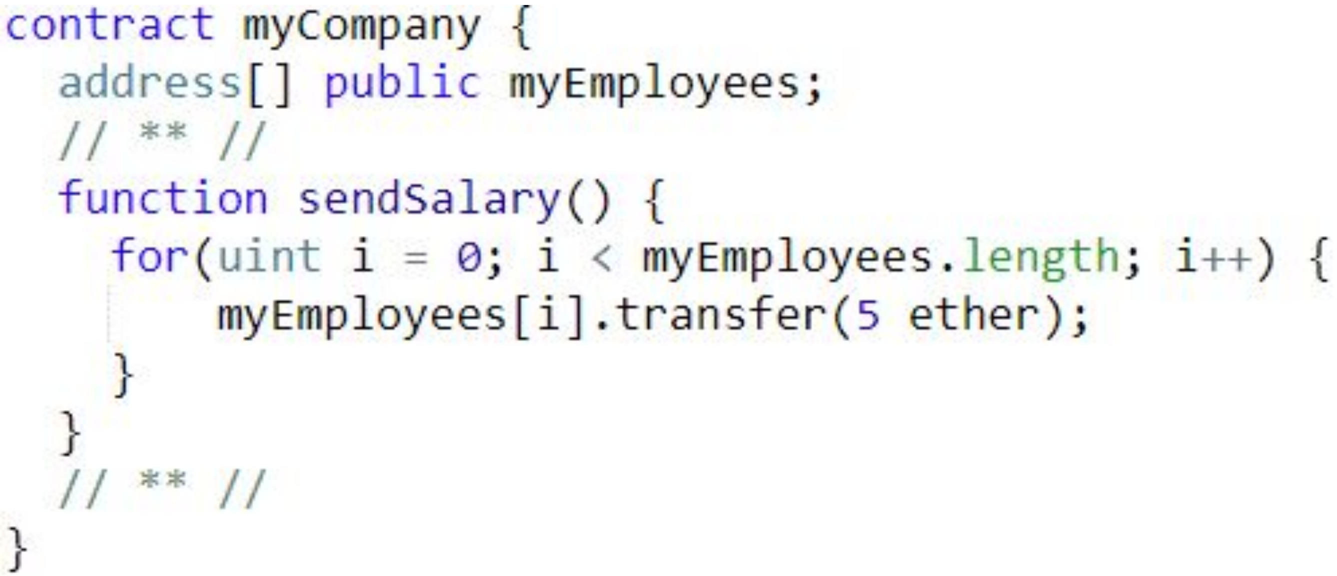
John: 20 Jim: 0

transfer(Jim, 2^256-1)

John: 21 Jim: 2^256-1

JIM: 115792089237316195423570985008687907853269984665640564039457584007913129639935

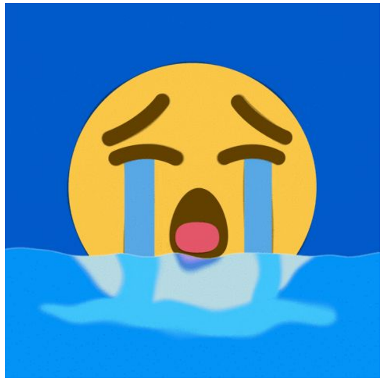
Looooooping 😮



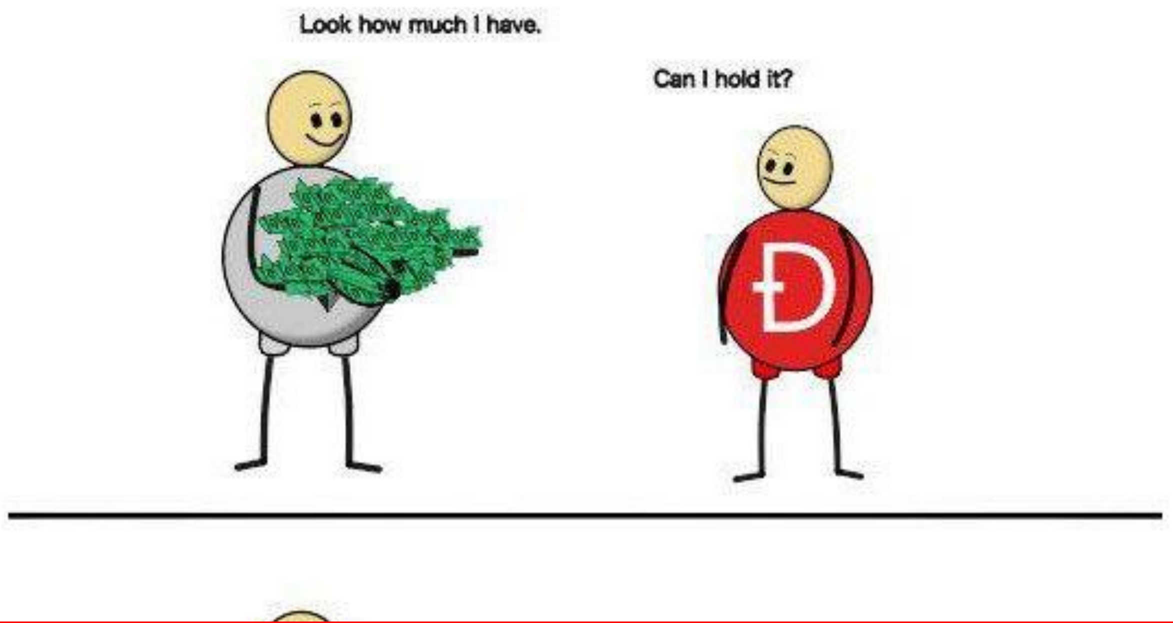
```
contract myCompany {
  address[] public myEmployees;
  // ** //
  function sendSalary() {
    for(uint i = 0; i < myEmployees.length; i++) {
        myEmployees[i].transfer(5 ether);
    }
  }
  // ** //
}
```

BLOCK GAS LIMIT !!!

Reentrancy



```
contract myCompany {
 mapping (address => uint) salaries;
 //**//
 function withdrawSalary() {
  uint amountToWithdraw = salaries[msg.sender]
```

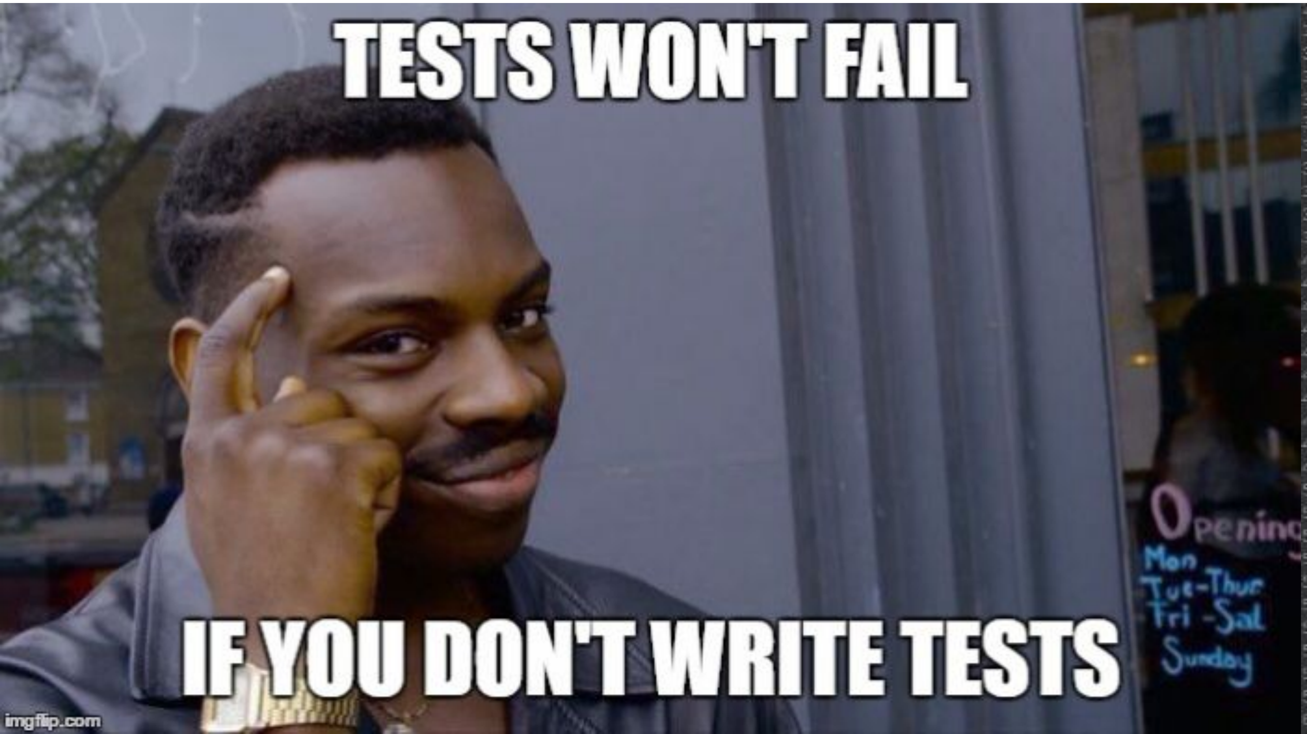


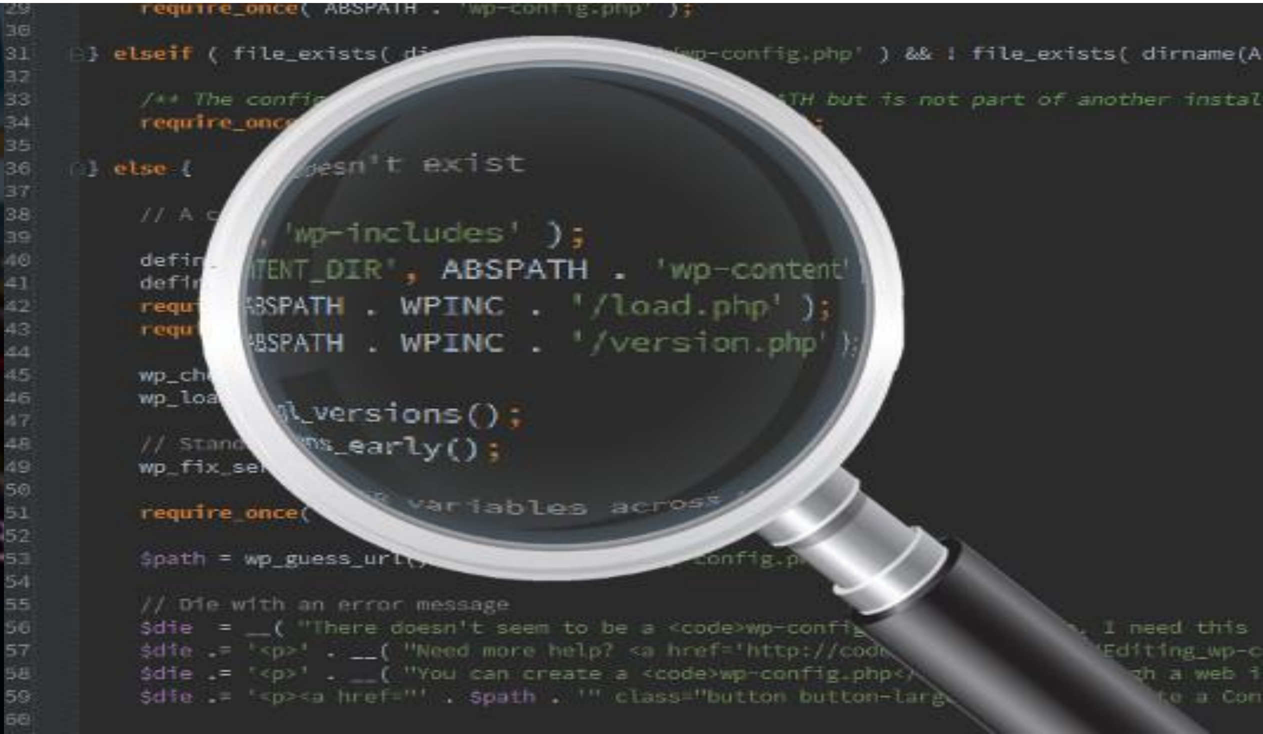
300,000,000 USD lost

```
      function () {
       myCompany.withdrawSalary();
      }
     }
```

How can we do better?

openzeppelin

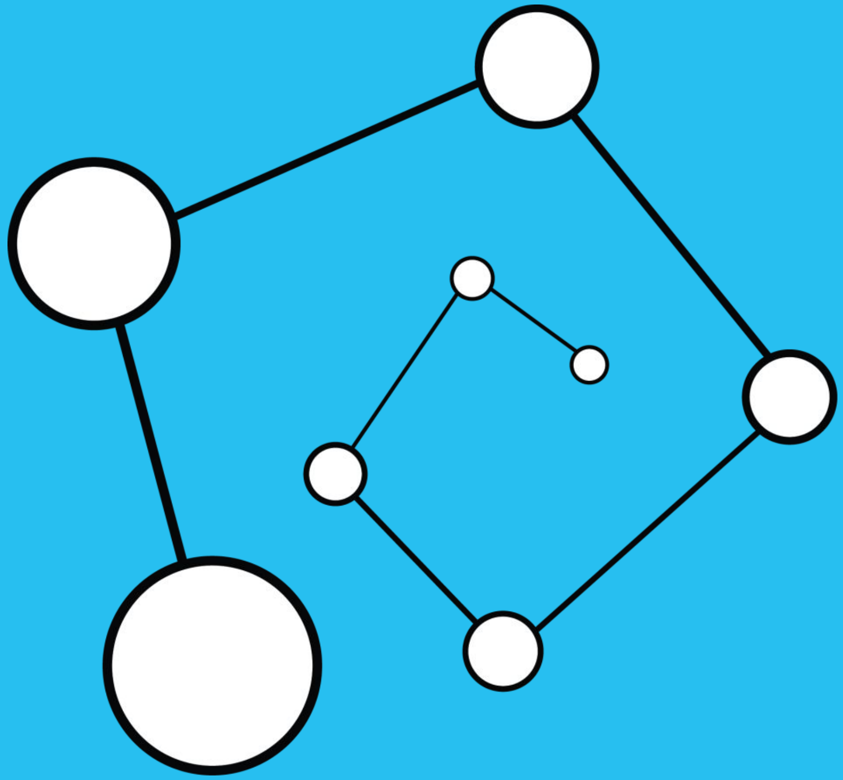




```
    require_once( ABSPATH . 'wp-config.php' );

} elseif ( file_exists( di                    wp-config.php' ) && ! file_exists( dirname(A

    /** The confi                           TH but is not part of another instal
    require_once

} else {                    esn't exist

    // A c          'wp-includes' );

    defi           TENT_DIR', ABSPATH . 'wp-content'
    defi          BSPATH . WPINC . '/load.php' );
    requ          BSPATH . WPINC . '/version.php' );
    requ

    wp_ch
    wp_loa           l_versions();

    // Stand        ns_early();
    wp_fix_se

    require_once(        variables across

    $path = wp_guess_url(                    config.p

    // Die with an error message
    $die  = __( "There doesn't seem to be a <code>wp-config              . I need this
    $die .= '<p>' . __( "Need more help? <a href='http://code              Editing_wp-c
    $die .= '<p>' . __( "You can create a <code>wp-config.php</              h a web i
    $die .= '<p><a href="' . $path . '" class="button button-larg              e a Con
```

References

1. Szilágyi Péter: https://ethereum.karalabe.com/talks/2016-hackethon.html#1
2. Christian Reitweissner: https://blog.ethereum.org/2016/06/10/smart-contract-security/
3. Vitalik Buterin: https://blog.ethereum.org/2016/06/19/thinking-smart-contract-security/
4. Loi Luu et al.: https://eprint.iacr.org/2016/633.pdf
5. Consensys: https://consensys.github.io/smart-contract-best-practices/
6. OpenZeppelin: https://github.com/OpenZeppelin/zeppelin-solidity
7. https://blog.zeppelin.solutions/onward-with-ethereum-smart-contract-security-97a827e47702
8. Peter Vessenes: http://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/
9. Emin Gün Sirer: http://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/
10. Arseny Reutov: https://blog.positive.com/predicting-random-numbers-in-ethereum-smart-contracts-e5358c6b8620
11. Break them all: https://ethernaut.zeppelin.solutions/
12. Securify: https://securify.ch/



THANK YOU!

WWW.BLOCKCHAINCC.COM