dit-upm

smart contracts
solidity

José A. Mañas < http://www.dit.upm.es/~pepe/>
Dep. de Ingeniería de Sistemas Telemáticos
E.T.S. Ingenieros de Telecomunicación
Universidad Politécnica de Madrid

22.9.2018

índice

- blockchain
- ether
- smart contracts
  - solidity
- ~~ethereum wallet~~
- metamax
- remix
- ganache ?

blockchain

https://anders.com/blockchain/hash.html

SHA256 Hash

Data: man

Hash: 48b676e2b107da679512b793d5fd4cc4329f0c7c17a97cf6e0e3d1005b600b03

message digests

- *hash*, *one way*, …
  - h= H (M) where h is fixed length
- properties
  - given M, it is easy to eval H(M)
  - given h, it is hard to find M, such that H(M) = h
  - given M, it is hard to find M', such that H(M) = H(M')
    - collisions
  - it is hard to find pairs M and M', such that H (M) = H (M')
    - warn: birthday paradox

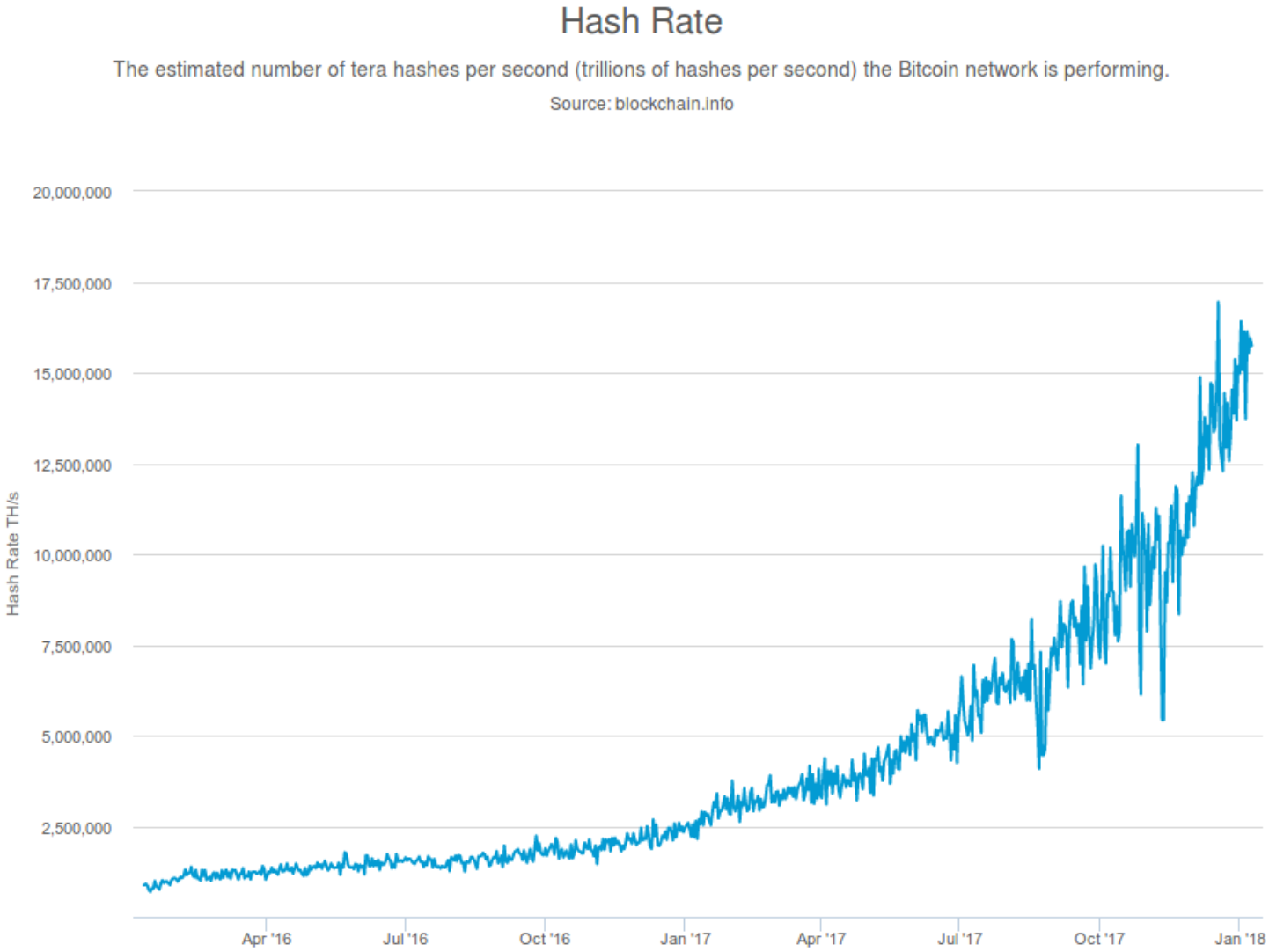
http://www.dit.upm.es/~pepe/doc/seg4/tema1/12-crypto_en_signed.pdf

dit algorithms

- message disgest
  - ~~MD2, MD4~~
  - ~~MD5: 128 bits MD2, *MD4*~~
  - SHA-1: 160 bits
  - **SHA-2: 224, 256, 384, 512 bits**
  - SHA-3: 224, 256, 384, 512 bits (a different algorithm)

  - keccak
  - https://github.com/ethereum/wiki/wiki/Ethash

bitcoin


Hash Rate
The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.
Source: blockchain.info
Hash Rate TH/s
20,000,000
17,500,000
15,000,000
12,500,000
10,000,000
7,500,000
5,000,000
2,500,000
Apr '16
Jul '16
Oct '16
Jan '17
Apr '17
Jul '17
Oct '17
Jan '18

dit

blockchain

https://anders.com/blockchain/hash.html

Block

Block:
1

Nonce:
72608

Data:

Hash:
0000f727854b50bb95

Mine

Block

Block:
1

Nonce:
72608

Data:
some data

Hash:
d8dce91d6ea7

Mine

Block

Block:
1

Nonce:
1376

Data:
some data

Hash:
0000ab22520d49b2483b44043a247f4f

Mine

s://anders.com/blockchain/distributed.html

blockchain

https://anders.com/blockchain/hash.html

Peer A

Block:	#	1			
Nonce:	139358				
Tx:	$	25.00	From:	Darcy	->	Bingle
	$	4.27	From:	Elizab	->	Jane
	$	19.22	From:	Wickha	->	Lydia
	$	106.44	From:	Lady C	->	Collin
	$	6.42	From:	Charlo	->	Elizab
Prev:	0000000000000000000000000000000000000000					
Hash:	00000c52990ee86de55ec4b9b32beefd745d71675dc					

Mine

Block:	#	2			
Nonce:	39207				
Tx:	$	97.67	From:	Ripley	->	Lamber
	$	48.61	From:	Kane	->	Ash
	$	6.15	From:	Parker	->	Dallas
	$	10.44	From:	Hicks	->	Newt
	$	88.32	From:	Bishop	->	Burke
	$	45.00	From:	Hudson	->	Gorman
	$	92.00	From:	Vasque	->	Apone
Prev:	00000c52990ee86de55ec4b9b32beefd745d71675dc					
Hash:	000078be183417844c14a9251ca246fb15df1074019					

Mine

Block:	#	3			
Nonce:	13804				
Tx:	$	10.00	From:	Emily		
	$	5.00	From:	Madis		
	$	20.00	From:	Lucas		
Prev:	000078be183417844c14a9251ca					
Hash:	0000c2c95f54a49b4f2bee7056a					

Mine

ethereum

https://etherscan.io/

Blocks

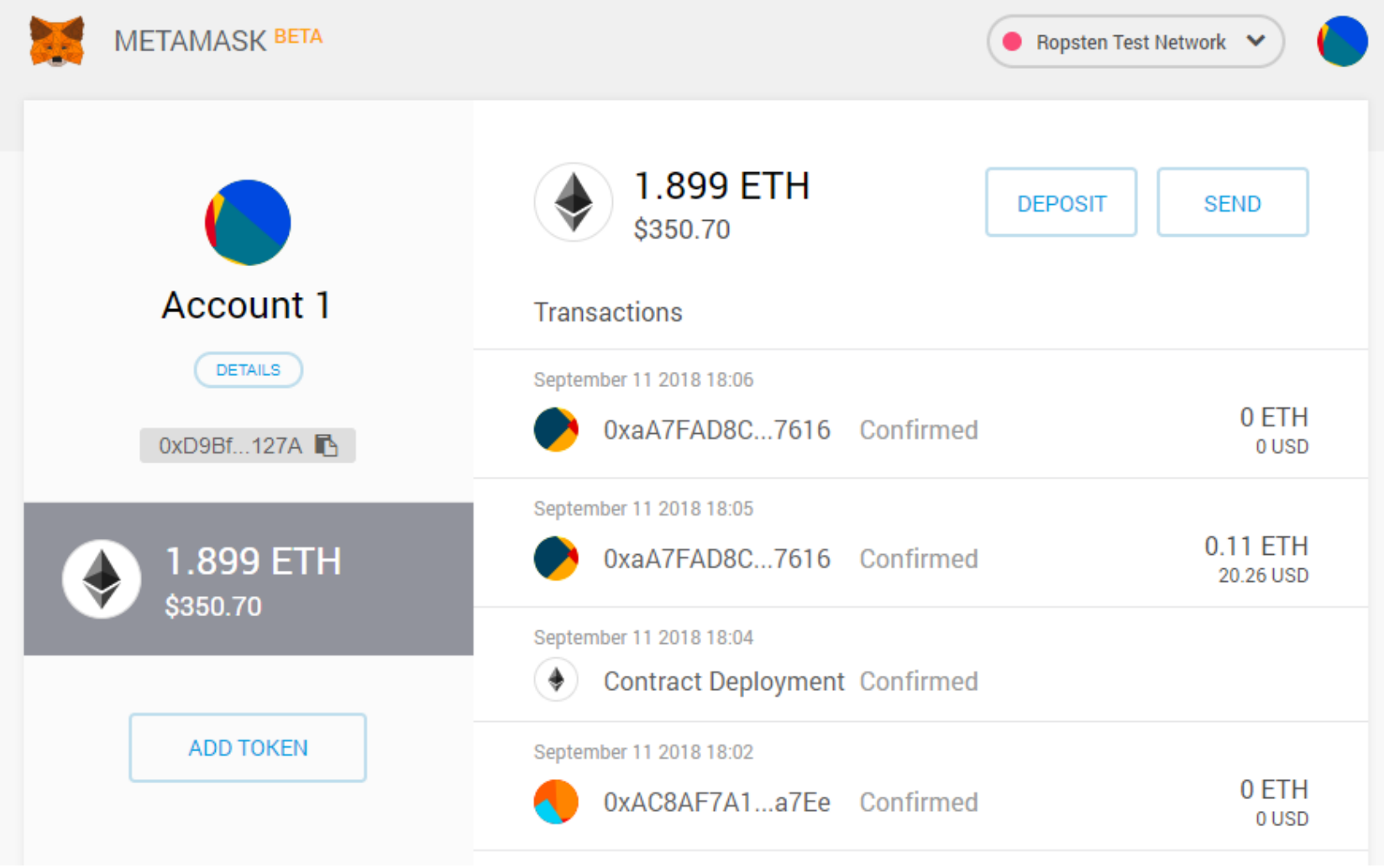
Block 6313065 >1 min 2 secs ago	Mined By BitClubPool 47 txns in 6 sec Block Reward 3.23948 Ether
Block 6313062 >53 secs ago	Mined By MiningPoolHub_1 78 txns in 19 secs Block Reward 3.08048 Ether
Block 6313061 >1 min 12 secs ago	Mined By Nanopool 75 txns in 9 secs
Block 631 >1 min 21 se	
Block 631	

Block Information

Height:	6313066
TimeStamp:	45 secs ago (Sep-11-2018 04:49:15 PM +UTC)
Transactions:	61 transactions and 5 contract internal transactions in this block
Hash:	0xf210f9d5b73ad958d8a1d2ba363ec510457f4fb0a52a1a26d8d53120e9427509
Parent Hash:	0x6ffa1ab271b6ce806cd6f052de12a4dbc112549c0899b94939350a9006ada574
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
Mined By:	0xcc16e3c00dbbe76603fa833ec20a48f786dfe610 in 37 secs
Difficulty:	3,079,913,571,633,924

ethereum client

https://metamask.io/



metamask

- test blockchain: ROPSTEN
  - https://ropsten.etherscan.io/
- new account
  - pp: 0xD9Bf5d463F3462422c7e9906F60f5Cc640a0127A
- receive fake ethers
  - https://faucet.ropsten.be/
- transfer ethers between accounts, then see blockchain

transactions

https://ropsten.etherscan.io/address/0xd9bf5d463f3462422c7e9906f60f5cc640a0127a

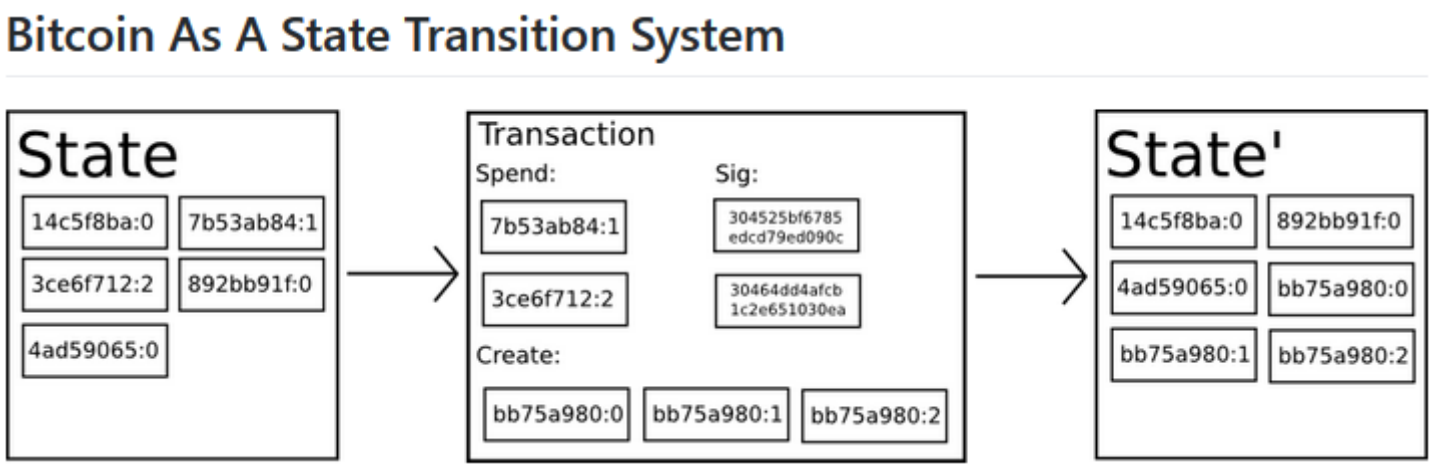
Transactions | Internal Txns

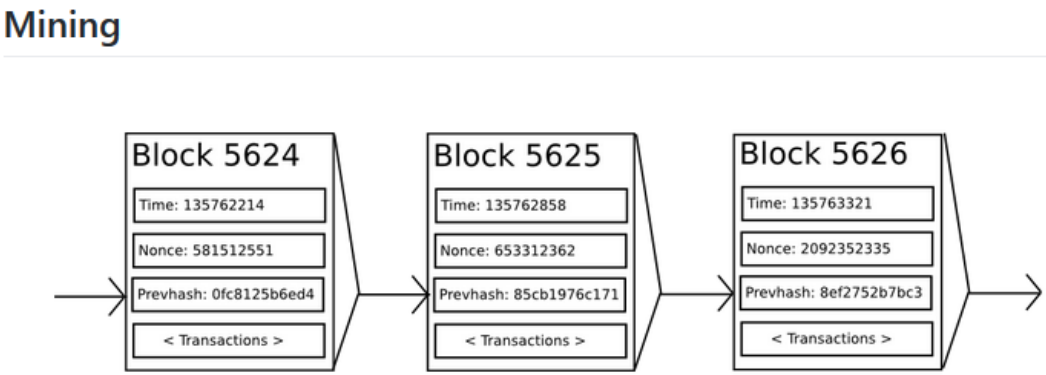
Latest 11 txns

TxHash	Block	Age	From		To	Value	[TxFee]
0x86ab1c03bb9b1d...	4019840	52 mins ago	0xd9bf5d463f34624...	OUT	0xaa7fad8ca223e54...	0 Ether	0.000029335
0xaa8e32896533e1...	4019833	53 mins ago	0xd9bf5d463f34624...	OUT	0xaa7fad8ca223e54...	0.11 Ether	0.000021361
0xd1249e9be7a627...	4019827	55 mins ago	0xd9bf5d463f34624...	OUT	Contract Creation	0 Ether	0.000142969
0xf818f39de37511e...	4019808	57 mins ago	0xd9bf5d463f34624...	OUT	0xac8af7a16bd6aec...	0 Ether	0.000019144
0xe2e824a4a13cd7...	4019806	57 mins ago	0xd9bf5d463f34624...	OUT	0xac8af7a16bd6aec...	0.11 Ether	0.000041374
0xfa9b23703c680a0...	4019797	58 mins ago	0xd9bf5d463f34624...	OUT	Contract Creation	0 Ether	0.000131415
0x9b8f4e70ff7d0759...	4019777	1 hr 3 mins ago	0xd9bf5d463f34624...	OUT	0xdf73097d2e232d7...	0 Ether	0.000020402
0x21f2b20443d29cf...	4019773	1 hr 4 mins ago	0xd9bf5d463f34624...	OUT	0xdf73097d2e232d7...	0.2 Ether	0.000053951
0x5a8624d840cc53...	4019761	1 hr 6 mins ago	0xd9bf5d463f34624...	OUT	Contract Creation	0.1 Ether	0.000380852
0x5e751eda3369a0...	4019519	1 hr 47 mins ago	0x81b7e08f65bdf56...	IN	0xd9bf5d463f34624...	1 Ether	0.000021
0x5a53d4f36abc7b0...	4010243	1 day 8 hrs ago	0x81b7e08f65bdf56...	IN	0xd9bf5d463f34624...	1 Ether	0.000021

state machine: bitcoin

https://github.com/ethereum/wiki/wiki/White-Paper

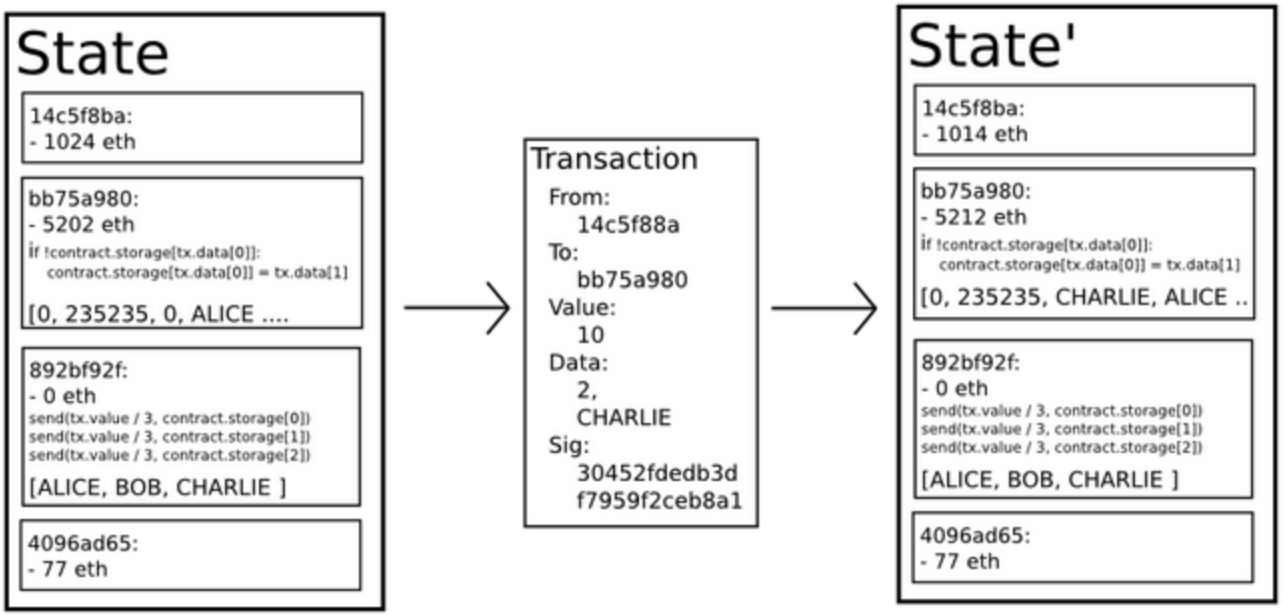




state machine: ethereum

https://github.com/ethereum/wiki/wiki/White-Paper

Ethereum State Transition Function



smart contracts

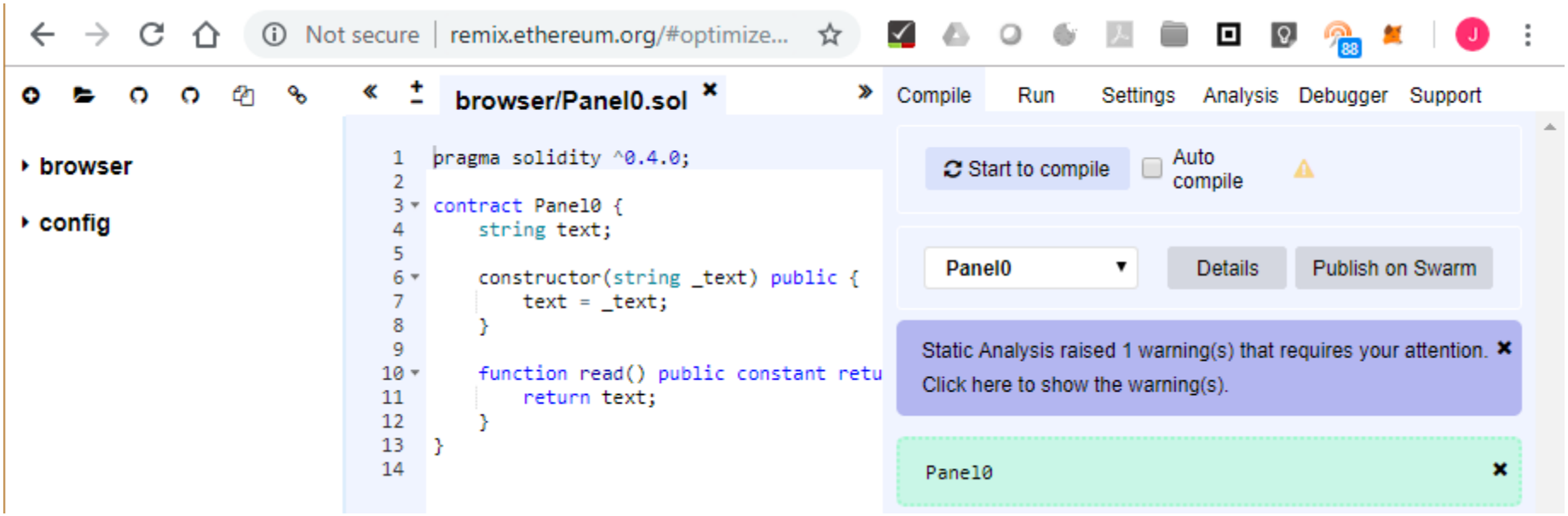
- { state i } –[contract]--> { state j }
- language to write contracts
  - solidity
  - https://solidity.readthedocs.io/en/v0.4.24/
  - gas
    - halting problem
    - repeated execution
    - pay per mining

```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

dit

online IDE

- http://remix.ethereum.org/



dit

http://remix.ethereum.org/

browser/Panel0.sol

```
pragma solidity ^0.4.0;

contract Panel0 {
    string text;

    constructor(string _text) public {
        text = _text;
    }

    function read() public constant returns(string) {
        return text;
    }
}
```

Compile | Run | Settings | Analysis | Debugger | Support

Environment: Injected Web3 — Ropsten (3)

Account: 0xd9b...0127a (1.899159197 ether)

Gas limit: 3000000

Value: 0 wei

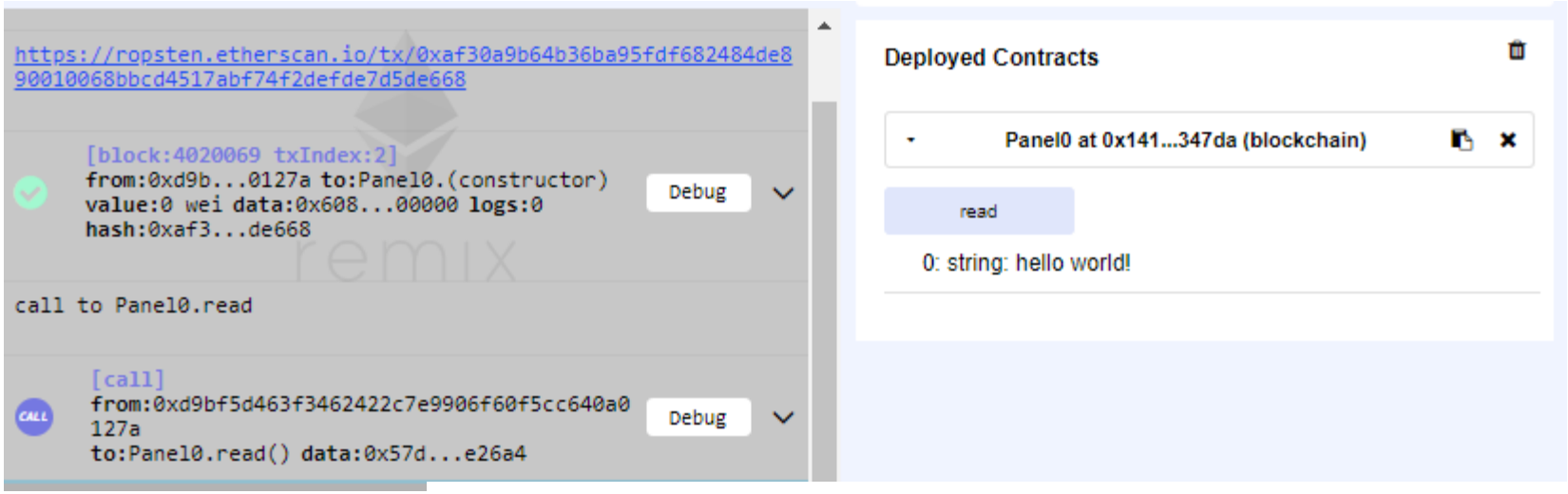
Panel0

Deploy "hello world!"

Load contract from Address | At Address

dit

http://remix.ethereum.org/



TxHash:	0xaf30a9b64b36ba95fdf682484de890010068bbcd4517abf74f2defde7d5de66
TxReceipt Status:	Success
Block Height:	4020069 (10 block confirmations)
TimeStamp:	1 min ago (Sep-11-2018 05:28:34 PM +UTC)
From:	0xd9bf5d463f3462422c7e9906f60f5cc640a0127a
To:	[Contract 0x141a6f0647d38c14cbaab3d71eed3e6c5aa347da Created]
Value:	0 Ether ($0.00)
Gas Limit:	200633
Gas Used By Txn:	200633

ethereum

solidity: data types

- bool
- int, uint
  - 8, 16, 24, 32, …, 256
  - uint8, uint256
- string
- address
  - address.balance
  - adddress.transfer(wei)
  - …
- enum
- struct
- arrays
  - fixed size
  - dynamic
- mapping
  - ~hash tables
  - “key” → value

Panel0

```
pragma solidity ^0.4.0;

contract Panel0 {
    string text;

    constructor(string _text) public {
        text = _text;
    }

    function read() public view returns(string) {
        return text;
    }
}
```


```
ABI
  0:
    constant: true
    inputs:
    name: read
    outputs:
    payable: false
    stateMutability: view
    type: function
  1:
```


deployed at
0xbeA7f7421A796E4a6bD6f0f15b100f9848850e03

dit

Panel0

ROPSTEN Etherscan
The Ethereum Block Explorer

ROPSTEN (Revival) TESTNET | Search by Address / Txhash / Block / Token / Ens | GO

HOME | BLOCKCHAIN | TOKEN | MISC

Contract 0xbeA7f7421A796E4a6bD6f0f15b100f9848850e03

Home / Accounts / Address

Contract Overview

Balance:	0 Ether
Transactions:	1 txn

Misc More Options

Contract Creator: 0xd9bf5d463f34624... at txn 0xe76fe98e7b0ffea0...

Transactions | Code | Events

Latest 1 txn

TxHash	Block	Age	From		To	Value	[TxFee]
0xe76fe98e7b0ffea0...	4026042	2 hrs 10 mins ago	0xd9bf5d463f34624...	IN	Contract Creation	0 Ether	0.000201593

[Download CSV Export]

dit

Panel1

```
pragma solidity ^0.4.0;

contract Panel1 {
    string text = "";

    function set(string _text) public {
        text = _text;
    }

    function read() public view returns(string) {
        return text;
    }
}
```

```
ABI
▾ 0:
  ▸ constant: false
  ▸ inputs:
  ▸ name: set
  ▸ outputs:
  ▸ payable: false
  ▸ stateMutability: nonpayable
  ▸ type: function
▸ 1:
```

deployed at
0xD55d5e66383925c319e634010A6C84F9A4d2aF0C

dit

Panel1

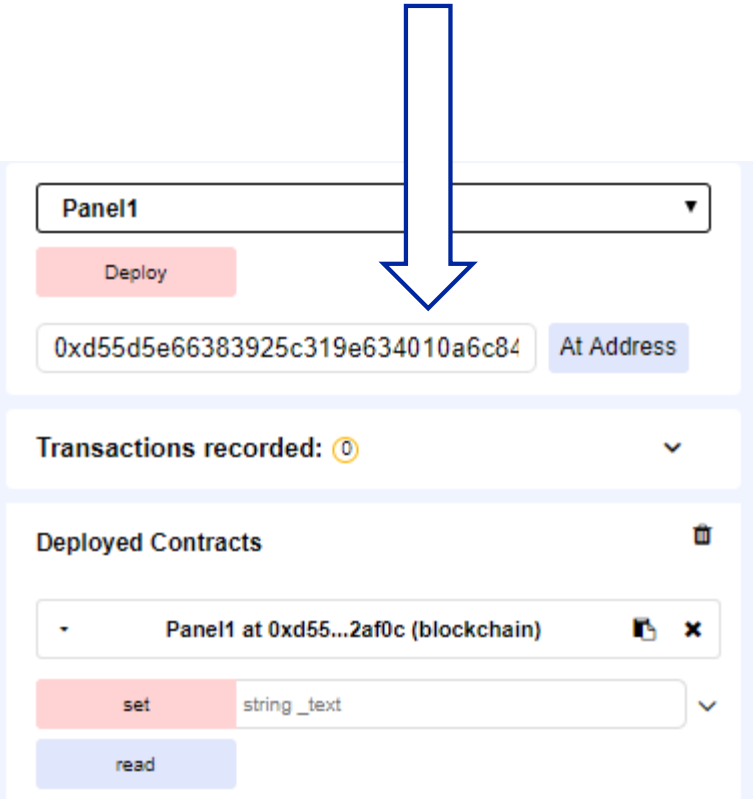
Transactions | Code | Events

Latest 5 txns

TxHash	Block	Age	From		To	Value	[TxFee]
0x924462bc883b29...	4026492	21 mins ago	0x3ae253529ba037...	IN	0xd55d5e66383925...	0 Ether	0.001353164
0xb0277a2bd77e68...	4026094	2 hrs 12 mins ago	0xd9bf5d463f34624...	IN	0xd55d5e66383925...	0 Ether	0.00003326
0x65f8e950c10f3d9...	4026094	2 hrs 12 mins ago	0xd9bf5d463f34624...	IN	0xd55d5e66383925...	0 Ether	0.000033324
0xcc77e80ecc6824...	4026091	2 hrs 14 mins ago	0xd9bf5d463f34624...	IN	0xd55d5e66383925...	0 Ether	0.000043203
0xf9f61a42662a0c3...	4026078	2 hrs 19 mins ago	0xd9bf5d463f34624...	IN	Contract Creation	0 Ether	0.000264696

acceso distribuido a Panel1

- acceso desde otro nodo
- necesitamos
  - dirección de despliegue: 0xD55d5e66383925c319e634010A6C84F9A4d2aF0C
  - ABI
- en otra instancia REMIX
  - código fuente → compila → ABI



contrato → contrato

```
pragma solidity ^0.4.0;

contract Panel1User1 {
  address panel1;
  bytes4 public function_set;

  constructor(address _at) public {
      panel1 = _at;
      // function hashes
      //    "57de26a4": "read()",
      //    "4ed3885e": "set(string)"
      function_set = bytes4(keccak256("set(string)"));
  }

  function publish(string notice) public returns(bool){
      return panel1.call(function_set, notice);
  }
}
```

dit

contrato → contrato

```
pragma solidity ^0.4.0;

contract Panel1 {
    function set(string _text) public;
}

contract Panel1User2 {
  Panel1 panel1;

  constructor(address _at) public {
      panel1 = Panel1(_at);
  }

  function publish(string notice) public {
      panel1.set(notice);
  }
}
```

testing (1/2)

```
contract Panel1 {
    string text = "";

    function set(string _text) public {
        text = _text;
    }

    function read() public view returns(string) {
        return text;
    }
}

contract TestPanel1 {
    function test() public {
        Panel1 panel = new Panel1();
        panel.set("alfa");
        assertEquals(panel.read(), "alfa", "se esperaba alfa");
        panel.set("beta");
        assertEquals(panel.read(), "beta", "se esperaba beta");
    }
```

testing (2/2)

```
function assertTrue(bool actual, string emsg) private pure {
    if ( ! actual ) { revert(emsg); }
}

function assertFalse(bool actual, string emsg) private pure {
    if ( actual ) { revert(emsg); }
}

function assertEquals(uint actual, uint expected, string emsg) private pure {
    if (actual != expected) { revert(emsg); }
}

function assertEquals(string actual, string expected, string emsg) private pure {
    if (keccak256(bytes(actual)) != keccak256(bytes(expected))) {
        revert(emsg);
    }
}
```

units and global variables

Error Handling

`assert(bool condition)`:

invalidates the transaction if the condition is not met - to be used for internal errors.

`require(bool condition)`:

reverts if the condition is not met - to be used for errors in inputs or external components.

`require(bool condition, string message)`:

reverts if the condition is not met - to be used for errors in inputs or external components. Also provides an error message.

`revert()`:

abort execution and revert state changes

`revert(string reason)`:

abort execution and revert state changes, providing an explanatory string

units and global variables

Address Related

`<address>.balance` (`uint256`):

balance of the Address in Wei

`<address>.transfer(uint256 amount)` :

send given amount of Wei to Address, throws on failure, forwards 2300 gas stipend, not adjustable

`<address>.send(uint256 amount) returns (bool)` :

send given amount of Wei to Address, returns `false` on failure, forwards 2300 gas stipend, not adjustable

`<address>.call(...) returns (bool)` :

issue low-level `CALL` , returns `false` on failure, forwards all available gas, adjustable

dit

requirements

```
contract Panel2 {
    address owner;
    string text = "";

    constructor() public {
        owner = msg.sender;
    }

    function set(string _text) public {
        if (msg.sender != owner) return;
        text = _text;
    }

    function read() public view returns(string) {
        return text;
    }
}
```

```
function set(string _text) public {
    require (msg.sender == owner);
    text = _text;
}
```

modifier

```
contract Panel3 {
    address owner;
    string text = "";

    modifier authorised(address other) {
        require(other == owner, "Sender not authorized.");
        _;
    }

    constructor() public {
        owner = msg.sender;
    }

    function set(string _text) public authorised(msg.sender) {
        text = _text;
    }

    function read() public view returns(string) {
        return text;
    }
}
```

mapping

```
contract Panel4 {
    address public owner;
    mapping(address => bool) public employees;
    string text = "";

    modifier onlyOwner() {
        require(msg.sender == owner, “...");
        _;
    }

    modifier authorised(address other) {
        require(employees[other], “...");
        _;
    }

    constructor() public {
        owner = msg.sender;
    }

}
```

```
    function authorise(address other) public
        onlyOwner {
        employees[other] = true;
    }

    function set(string _text) public
        authorised(msg.sender) {
        text = _text;
    }

    function read() public view returns(string) {
        return text;
    }
}
```

dit

logs

```
contract Panel5 {
    string text = "";

    event changed(string txt);

    function set(string _text) public {
        text = _text;
        emit changed(text);
    }

    function read() public view returns(strin
        return text;
    }
}
```

Transaction 0xc455eeae2cca858ec412c91332e348f8d4da9

Overview | Event Logs (1)

Transaction Receipt Event Logs

[12] **Address** 0xa4dc1ac30e4afc1fc6246069b8ffb15d23e44541

Topics [0] 0x91c04338d35c00f7969c979f020e4200c321cedc7b5f

Data Hex → 000000000000000000000000000000000000000

Hex → 000000000000000000000000000000000000000

Text → abcdef

logs


```
[
    {
        "from": "0xa4dc1ac30e4afc1fc6246069b8ffb15d23e44541",
        "topic": "0x91c04338d35c00f7969c979f020e4200c321cedc7b
5f55547f6b559fe848ab07",
        "event": "changed",
        "args": {
            "0": "abcdef",
            "txt": "abcdef",
            "length": 1
        }
    }
]
```

time

```
contract Panel6 {
    string text = "";
    uint mark;

    modifier ready() {
        require(now > mark);
        _;
    }

    function set(string _text, uint _mark) public {
        text = _text;
        mark = _mark;
    }

    function read() public view ready() returns(string) {
        return text;
    }
}
```

now
block.timestamp
- *last mined block*

https://www.epochconverter.com/

Yr	Mon	Day	Hr	Min	Sec		
2018	9	17	17	20	0	Local time	Human date to Timestamp

Epoch timestamp: 1537197600
Timestamp in milliseconds: 1537197600000
Human time (GMT): Monday, 17 September 2018 15:20:00
Human time (your time zone): lunes, 17 de septiembre de 2018 17:20:00 GMT+02:00

units and global variables

Time Units

Suffixes like `seconds`, `minutes`, `hours`, `days`, `weeks` and `years` after literal numbers can be used to convert between units of time where seconds are the base unit and units are considered naively in the following way:

- `1 == 1 seconds`
- `1 minutes == 60 seconds`
- `1 hours == 60 minutes`
- `1 days == 24 hours`
- `1 weeks == 7 days`
- `1 years == 365 days`

Take care if you perform calendar calculations using these units, because not every year equals 365 days and not even every day has 24 hours because of leap seconds. Due to the fact that leap seconds cannot be predicted, an exact calendar library has to be updated by an external oracle.

behind an address

Smart Contract

Ethereum Account Type (Just like User Account)

Address — *0x16E0022b17B...*

Balance — *0 Ether*

Code

State

```
contract Counter {
    uint counter;

    function Counter() public {
        counter = 0;
    }
    function count() public {
        counter = counter + 1;
    }
}
```

Gjermund Bjaanes

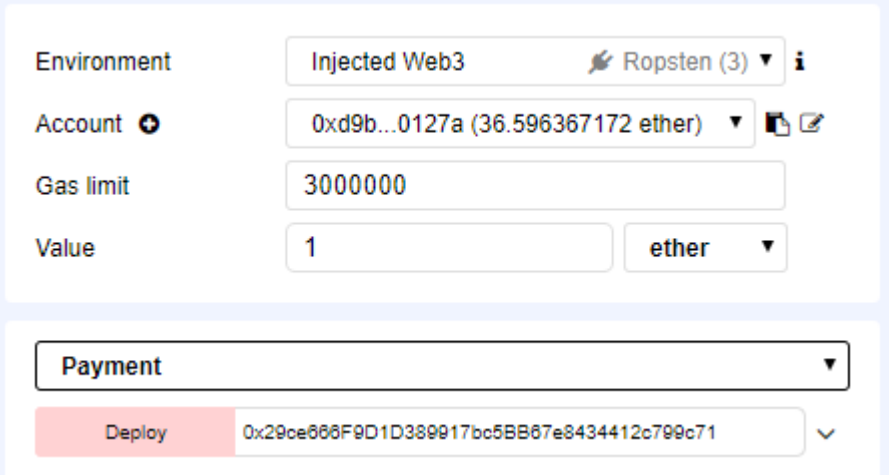
ethers

- address.balance()
- msg.value()
- msg.gasleft()
- address.send(€)
- address.transfer(€)
- address.call.value(€)
- selfdestruct(address)

- _receiver.send(value);
- _receiver.transfer(msg.value);
  _receiver.call.value(value).gas(20317)();

this . balance

```
contract Payment {
    address public owner;
    address public dst ;

    constructor(address _dst) public payable {
        owner = msg.sender;
        dst = _dst;
    }

    function getBalance() public view returns(uint) {
        return address(this).balance;
    }

    function sign() public {
            dst.transfer(address(this).balance);
    }

    function terminate() public {
        selfdestruct(owner);
    }
}
```



n signers

- constructor
  - msg.sender pays msg.value to dst address
  - requiring N signatures
- termination foreseen
- no need to
  - register signers
  - sign

```
contract Nsigners1 {
    address public owner ;
    address public dst ;
    uint public needed ;

    modifier onlyOwner() {
        require(msg.sender == owner);
        _;
    }

    constructor(uint _needed, address _dst) public
                payable {
        needed = _needed;
        dst = _dst;
        owner = msg.sender;
    }

    function terminate() public
                onlyOwner {
        selfdestruct(owner);
    }
```

n signers

```
enum State {Init, Registered, Signed}
mapping(address => State) public authoriserMap ;

function register(address signer) onlyOwner() public {
    require(msg.sender != signer);
    require(authoriserMap[signer] == State.Init);
    authoriserMap[signer] = State.Registered;
}

function sign() public {
    require(authoriserMap[msg.sender] == State.Registered);
    authoriserMap[msg.sender] = State.Signed;
    needed--;
    if (needed <= 0) {
        dst.transfer(address(this).balance);
    }
}
```

fallback functions

- 1 per contract
  - no name
  - no argument
- called if no other
- send() specifies a blank function signature and thus it will always trigger the fallback function if it exists.

```
contract Fallback1 {
    uint public x = 1;

    function () public {
        x *= 2;
    }
}

contract Tester {
    address addr;

    constructor (address _addr) public {
        addr = _addr;
    }

    function test() public returns(bool) {
        return addr.call(0x0);
    }
}
```

fallback functions

```
contract Payment2 {
    address public owner;
    address public dst ;

    constructor(address _dst) public payable {
        owner = msg.sender;
        dst = _dst;
    }

    function getBalance() public view
                returns(uint) {
        return address(this).balance;
    }

    function() public payable { }

    function sign() public {
            dst.transfer(address(this).balance);
    }

    function terminate() public {
        selfdestruct(owner);
    }
}
```

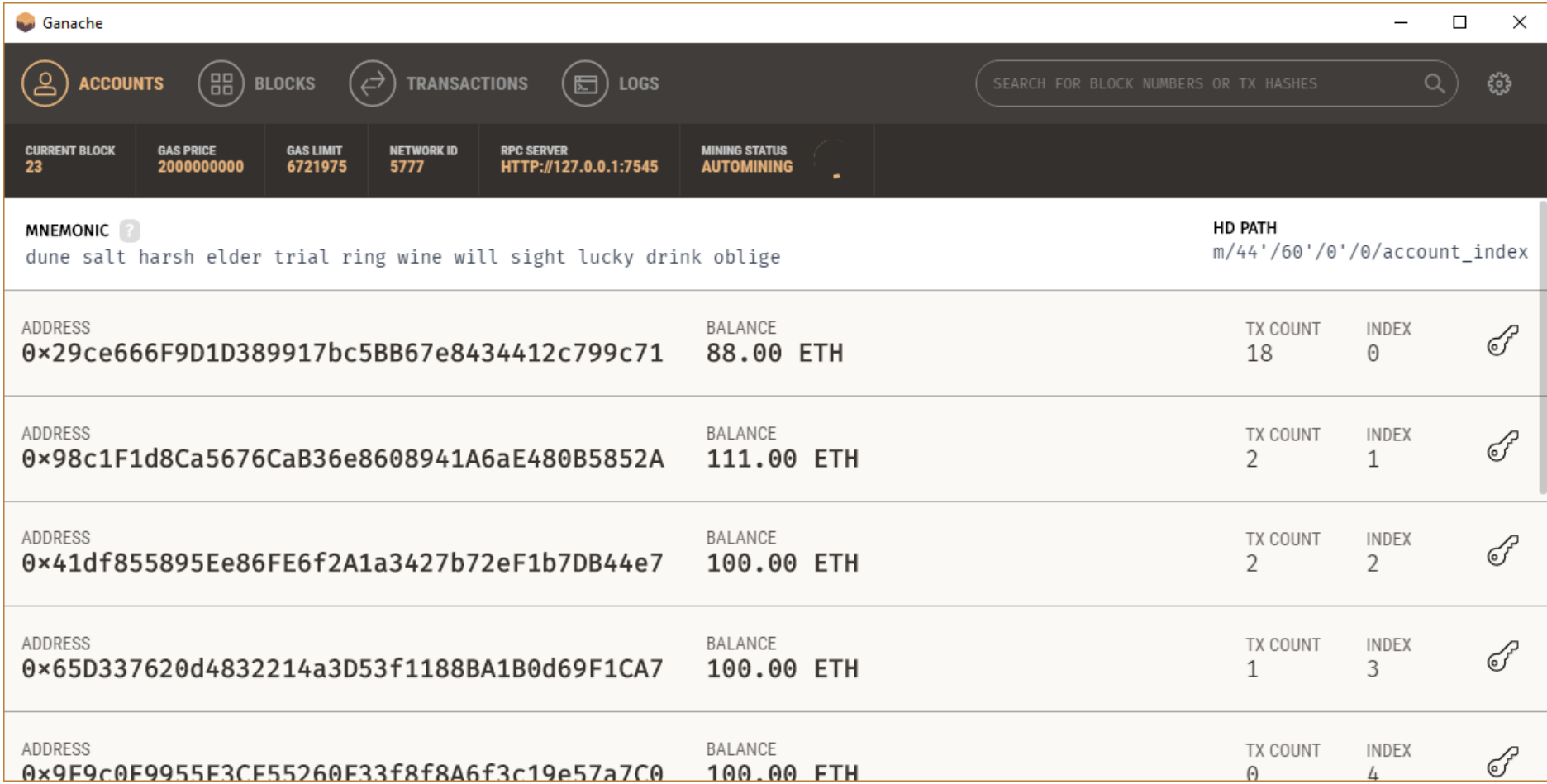
```
contract Test {
    address addr;
    Payment2 p;

    constructor(address _addr) public {
        addr = _addr;
        p = Payment2(_addr);
    }

    function test1() public payable {
        uint value = 1 ether;
        uint b0 = p.getBalance();
        require(addr.send(value));
        uint b2 = p.getBalance();
        require(b2 == b0 + 1, "b2 != b0 + value");
    }
}
```

dit

local blockchain

- 1 node
- “mining”

https://truffleframework.com/ganache



accounts

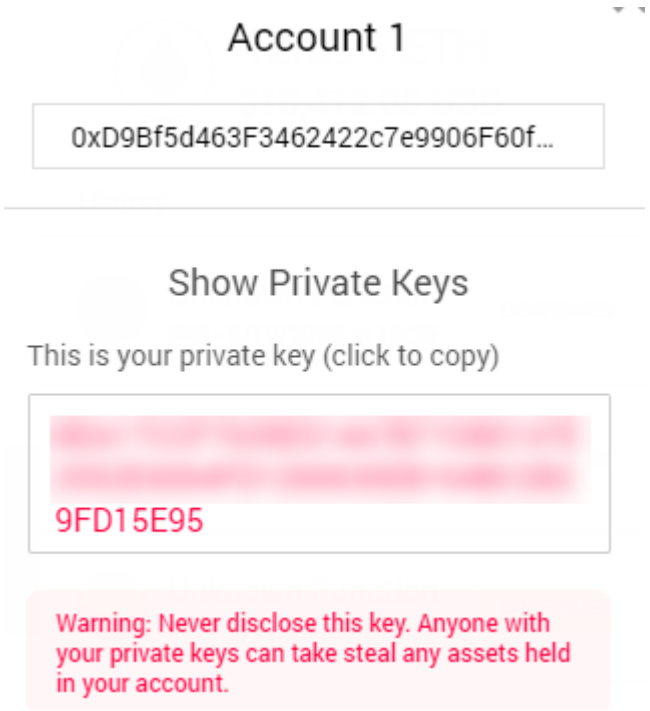
EOA

- con su balance
- pueden mandar y recibir transacciones
- controladas por clave privada (firma)
- sin código ejecutable

Contract

- con su balance
- con código asociado (funciones)
  - activado por llamadas
  - activado por eventos
- las funciones modifican el estado persistente

EOA: user account



public
- to address transactions to
- to verify signatures

private
- to sign transactions