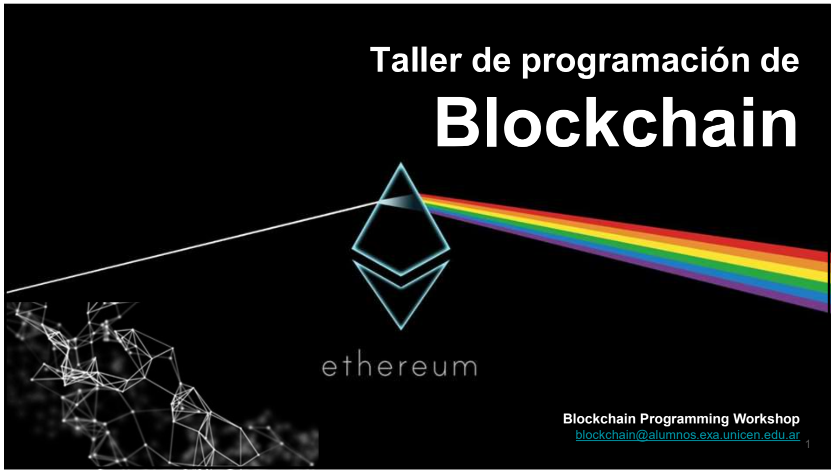
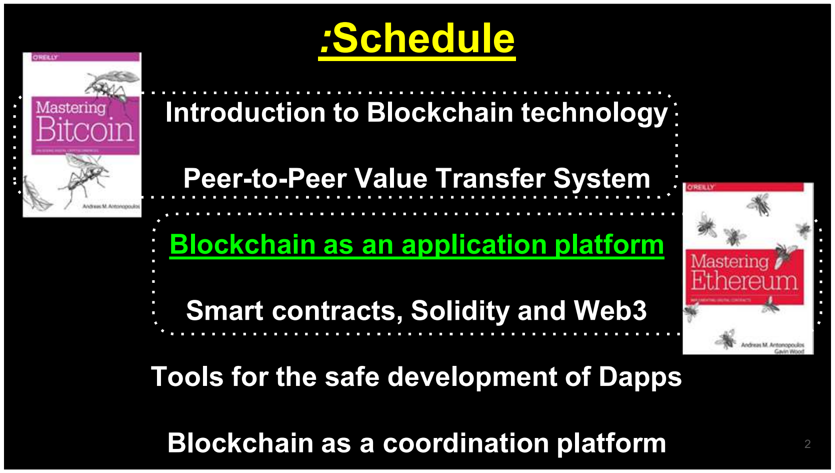


Taller de programación de **Blockchain**

Blockchain Programming Workshop
blockchain@alumnos.exa.unicen.edu.ar



:Schedule

Mastering Bitcoin
Mastering Ethereum

Introduction to Blockchain technology

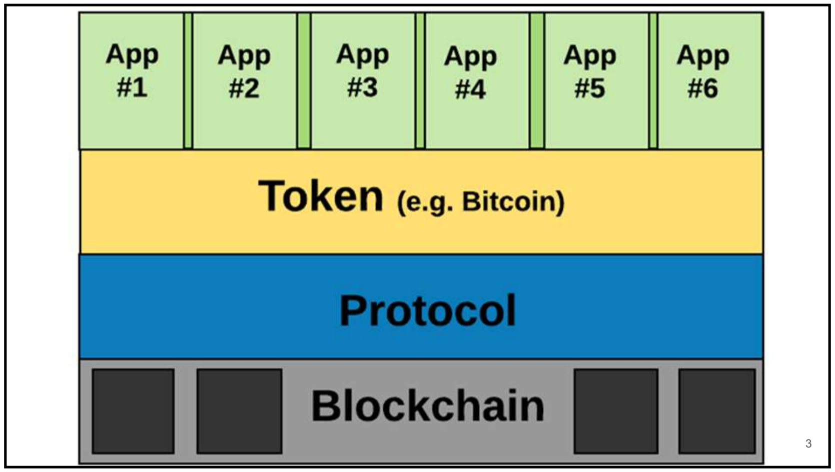
Peer-to-Peer Value Transfer System

Blockchain as an application platform

Smart contracts, Solidity and Web3

Tools for the safe development of Dapps

Blockchain as a coordination platform

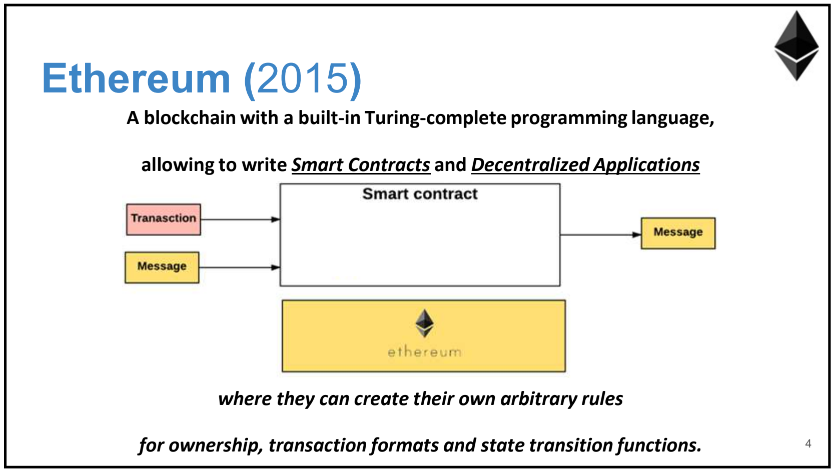


App #1 | App #2 | App #3 | App #4 | App #5 | App #6

Token (e.g. Bitcoin)

Protocol

Blockchain



Ethereum (2015)

A blockchain with a built-in Turing-complete programming language,

allowing to write *Smart Contracts* and *Decentralized Applications*

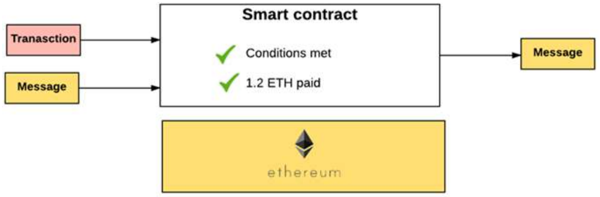
where they can create their own arbitrary rules

for ownership, transaction formats and state transition functions.

Smart Contracts

A smart contract is essentially business logic running on a blockchain.

***As simple as** a data update OR **As complex as** executing a contract with conditions attached*

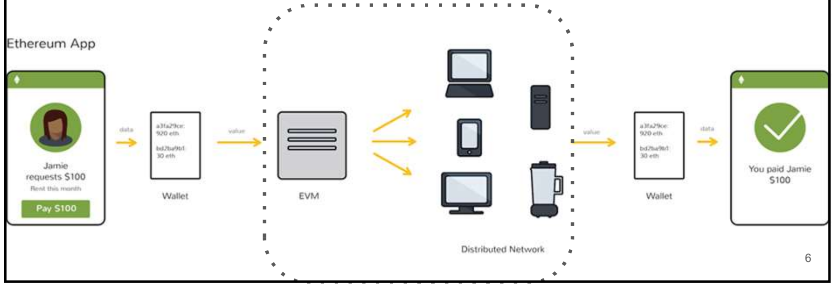


Installed smart contracts install business logic on the validators in the network before the network is launched.

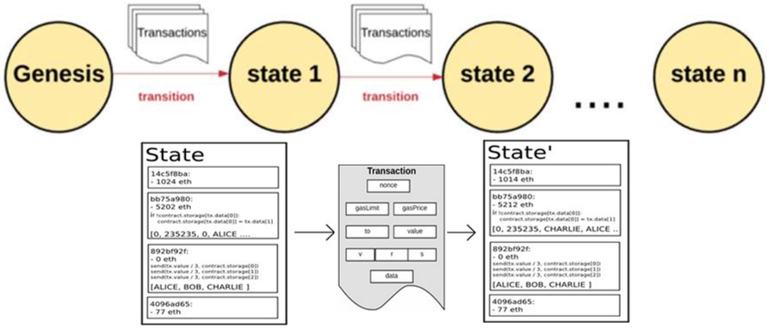
On-chain smart contracts deploy business logic as a transaction committed to the blockchain and then called by subsequent transactions. With on-chain smart contracts, the code that defines the business logic becomes part of the ledger.

Global Computer

“cryptographically secure transactional singleton machine with shared-state”

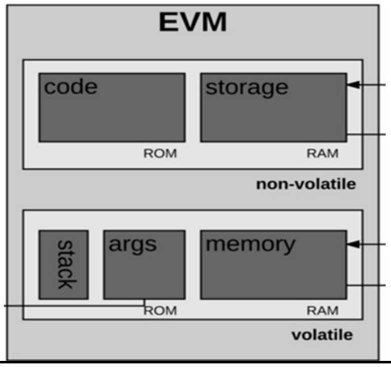


Transaction-based state machine

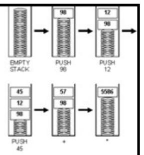

Genesis
Transactions
transition
state 1
Transactions
transition
state 2
....
state n
State
14c5f8ba:
- 1024 eth
bb75a980:
- 5202 eth
if !contract.storage[tx.data[0]]:
contract.storage[tx.data[0]] = tx.data[1]
[0, 235235, 0, ALICE ....
892bf92f:
- 0 eth
send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])
[ALICE, BOB, CHARLIE]
4096ad65:
- 77 eth
Transaction
nonce
gasLimit
gasPrice
to
value
v
r
s
data
State'
14c5f8ba:
- 1014 eth
bb75a980:
- 5212 eth
if !contract.storage[tx.data[0]]:
contract.storage[tx.data[0]] = tx.data[1]
[0, 235235, CHARLIE, ALICE ..
892bf92f:
- 0 eth
send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])
[ALICE, BOB, CHARLIE]
4096ad65:
- 77 eth

Ethereum Virtual Machine (*)

- Turing complete VM
- +Limitation by gas (https://ethgasstation.info)
- Stack-based architecture
- Stack size 1024.
- Stack item max. 256-bit

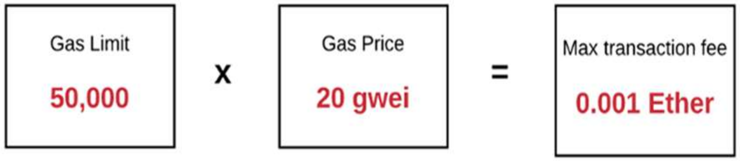


Information verification



- *System state*
- *Remaining gas* for computation
- Address of the
  - account that owns the *code that is executing*
  - *sender* of the transaction that *originated* this execution
  - account that *caused* the code to execute
- *Gas price* of the transaction that originated this execution
- *Input data* for this execution
- *Value passed* to this account as part of the current execution
- *Machine code* to be executed
- Block header of the *current block*
- *Depth* of present message call or *contract creation stack*

Gas and payment (or fee)



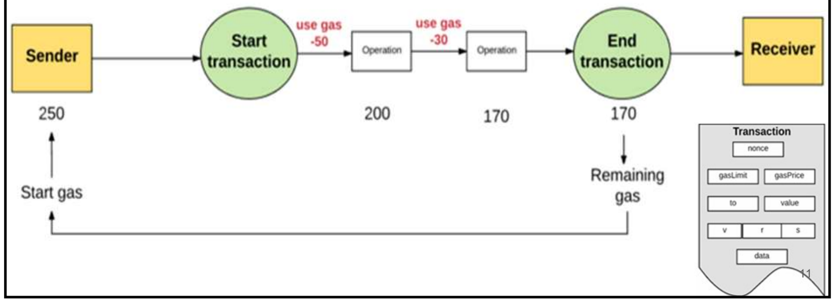
Gas Limit 50,000 x Gas Price 20 gwei = Max transaction fee 0.001 Ether

1 Ether = 1x10^{18} wei

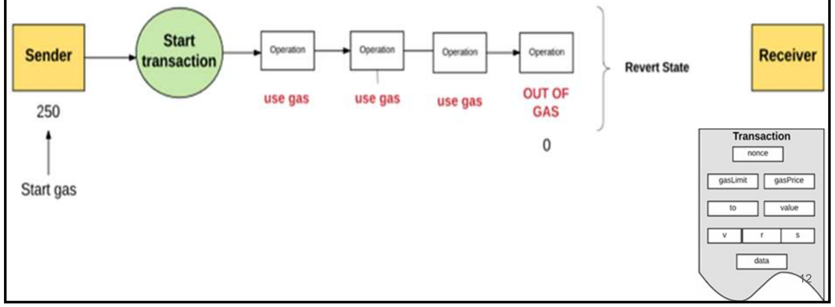
gas wei = **1,000,000,000** wei

50,000 x **20** gwei = **1,000,000,000,000,000** wei = **0.001 Ether**

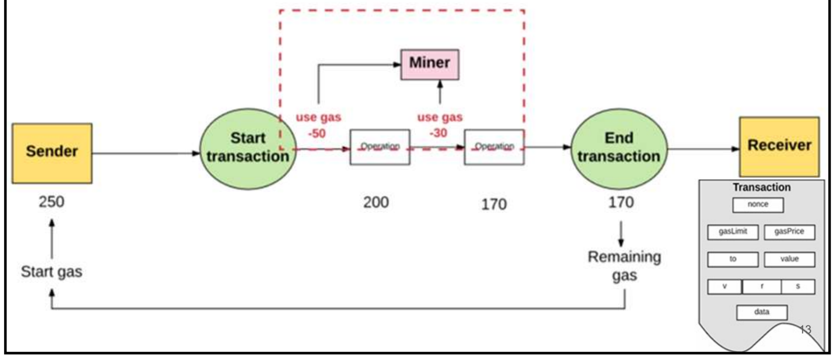
Gas and payment



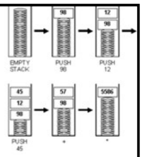
Gas and payment



Gas and payment



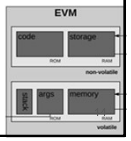
Execution Model (begin)



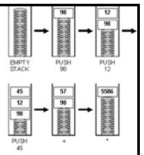
- PC: 0 STACK: [] MEM: [], ALMACENAMIENTO: {}

Machine State

- Gas available
- Program counter
- Memory contents
- Active number of words in memory
- Stack contents



Execution Model (cycle)

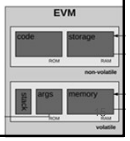


The appropriate gas amount is reduced

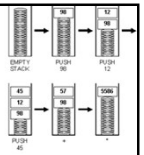
the program counter increments

1. **The machine reaches an exceptional state**
2. **The sequence continues to process into the next loop**
3. **The machine reaches a controlled halt**

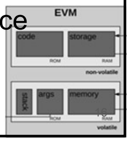
Generates the resultant state

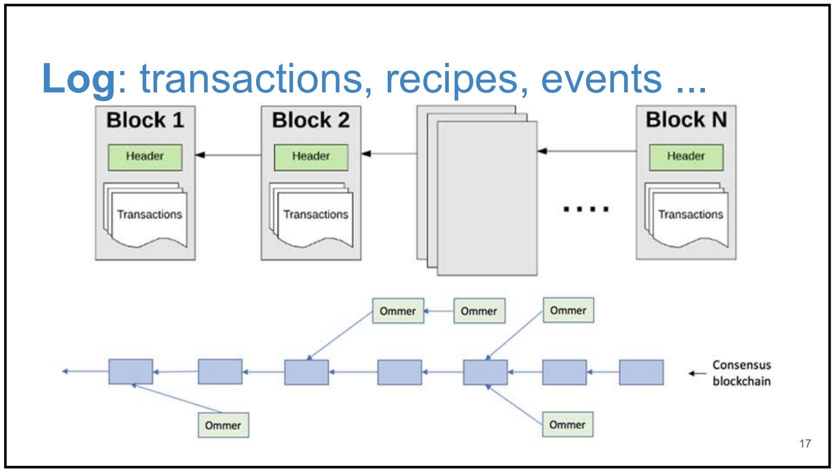


Execution Model (finally)



1. Validate (or determine) ommers
2. Validate (or determine) transactions
3. Apply rewards (only if mining)
4. Verify (or, if mining, compute a valid) state and nonce





Log: transactions, recipes, events ...

Block 1
Header
Transactions

Block 2
Header
Transactions

....

Block N
Header
Transactions

Ommer

Ommer

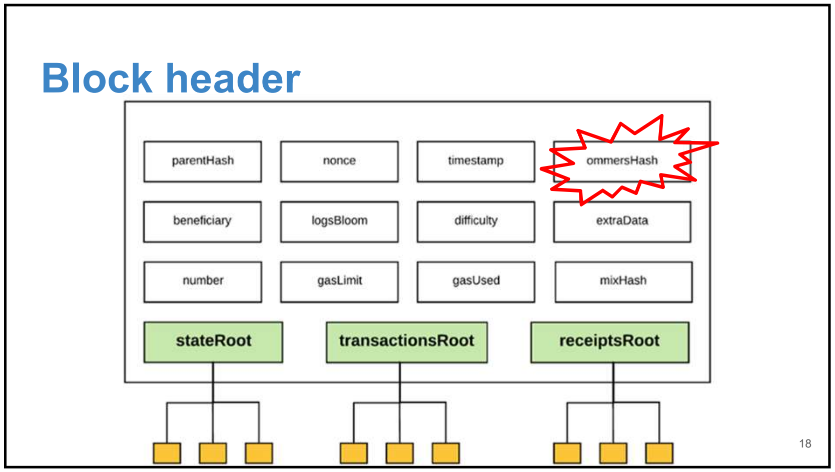
Ommer

Ommer

Ommer

Consensus blockchain

17



Block header

parentHash

nonce

timestamp

ommersHash

beneficiary

logsBloom

difficulty

extraData

number

gasLimit

gasUsed

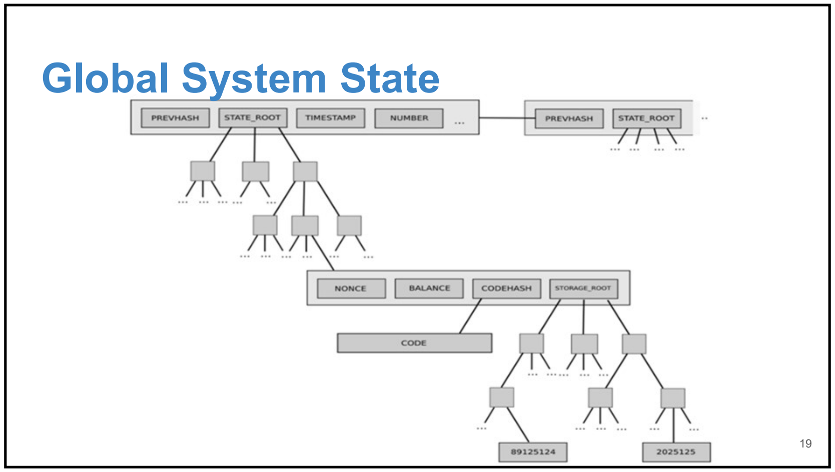
mixHash

stateRoot

transactionsRoot

receiptsRoot

18



Global System State

PREVHASH | STATE_ROOT | TIMESTAMP | NUMBER | ...

PREVHASH | STATE_ROOT | ..

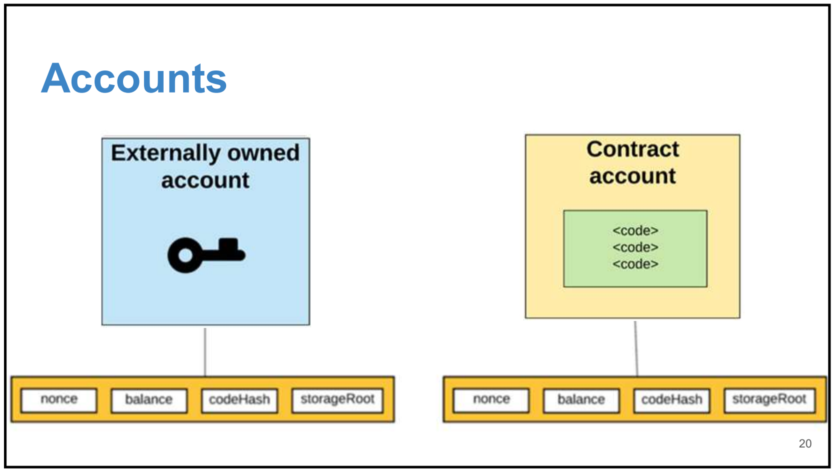
NONCE | BALANCE | CODEHASH | STORAGE_ROOT

CODE

89125124

2025125

19



Accounts

Externally owned account

Contract account

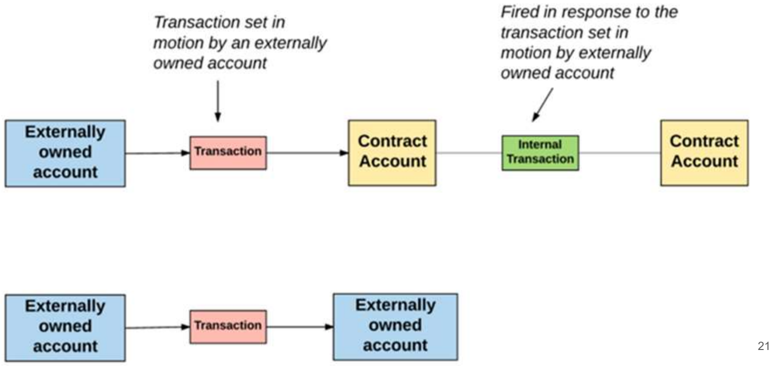
<code>
<code>
<code>

nonce | balance | codeHash | storageRoot

nonce | balance | codeHash | storageRoot

20

Externally owned accounts VS contract accounts



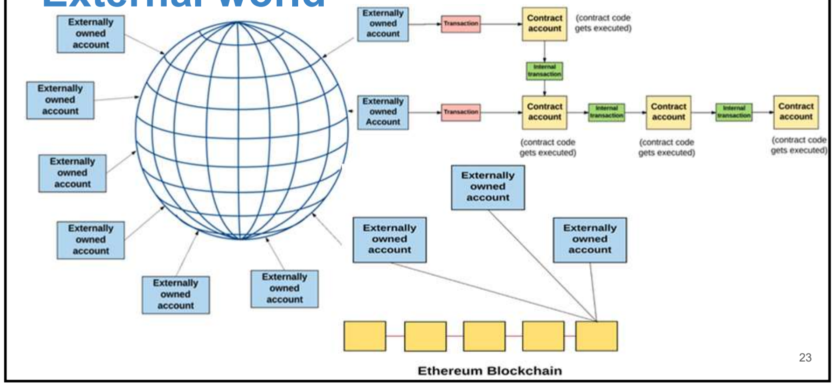
Transaction set in motion by an externally owned account

Fired in response to the transaction set in motion by externally owned account

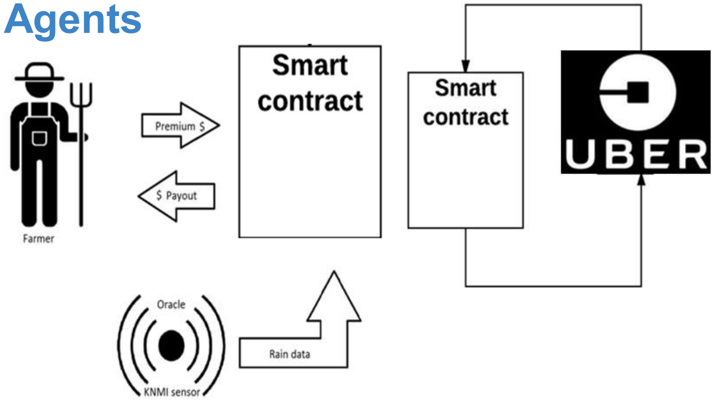
Transactions

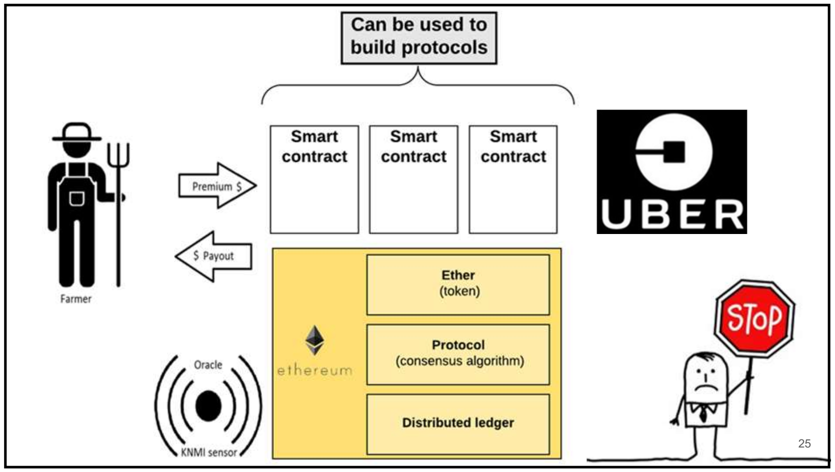
An "ordinary" transaction transferring some ether to another account	Nonce	To	Value	Signature	Gas Price	Start Gas	
A transaction creating a contract	Nonce	To	Value	Signature	Gas Price	Start Gas	Code
A transaction invoking a contract with some data	Nonce	To	Value	Signature	Gas Price	Start Gas	Data

External world



Agents





Can be used to build protocols

Smart contract

Smart contract

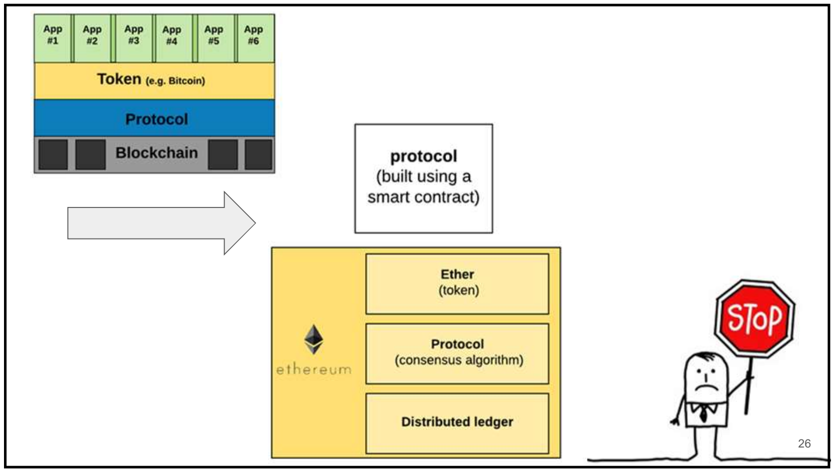
Smart contract

Ether (token)

Protocol (consensus algorithm)

Distributed ledger

25



App #1 | App #2 | App #3 | App #4 | App #5 | App #6

Token (e.g. Bitcoin)

Protocol

Blockchain

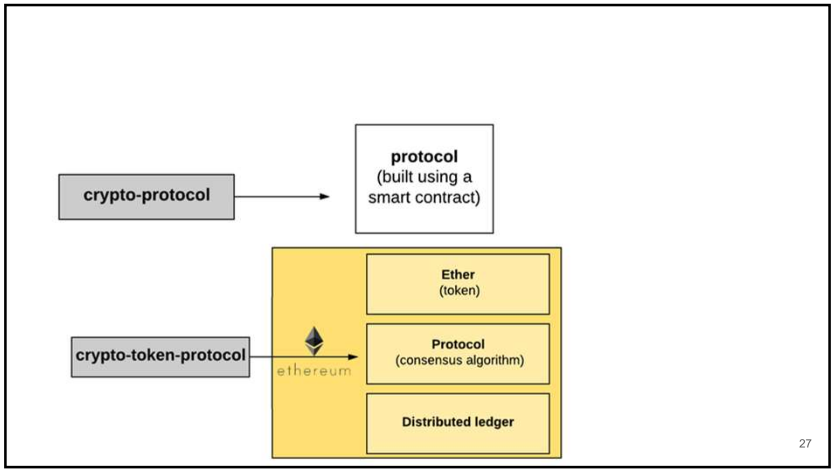
protocol (built using a smart contract)

Ether (token)

Protocol (consensus algorithm)

Distributed ledger

26



crypto-protocol

protocol (built using a smart contract)

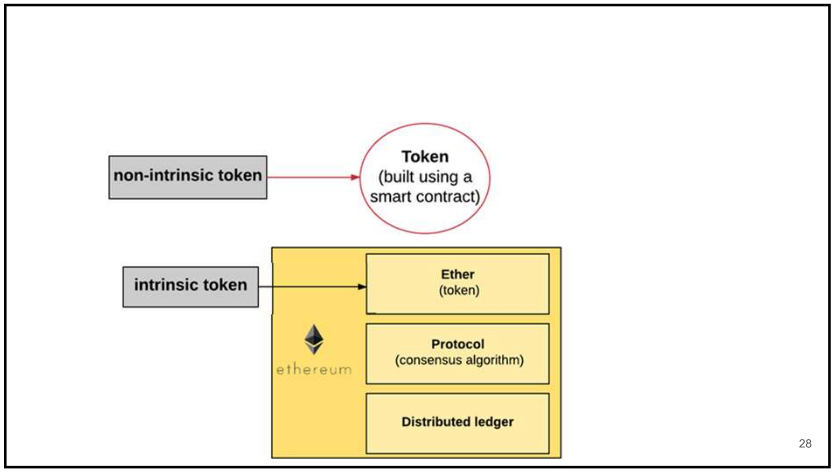
crypto-token-protocol

Ether (token)

Protocol (consensus algorithm)

Distributed ledger

27



non-intrinsic token

Token (built using a smart contract)

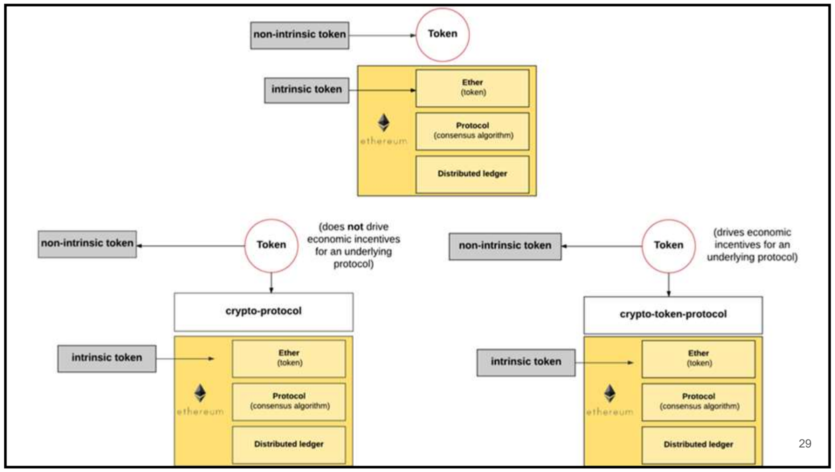
intrinsic token

Ether (token)

Protocol (consensus algorithm)

Distributed ledger

28



non-intrinsic token

Token

intrinsic token

Ether (token)

Protocol (consensus algorithm)

Distributed ledger

ethereum

non-intrinsic token

Token

(does **not** drive economic incentives for an underlying protocol)

crypto-protocol

intrinsic token

Ether (token)

Protocol (consensus algorithm)

Distributed ledger

ethereum

non-intrinsic token

Token

(drives economic incentives for an underlying protocol)

crypto-token-protocol

intrinsic token

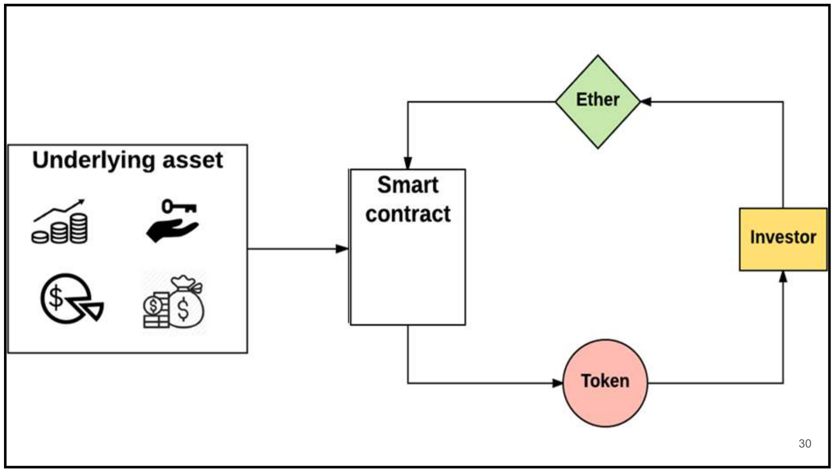
Ether (token)

Protocol (consensus algorithm)

Distributed ledger

ethereum

29



Underlying asset

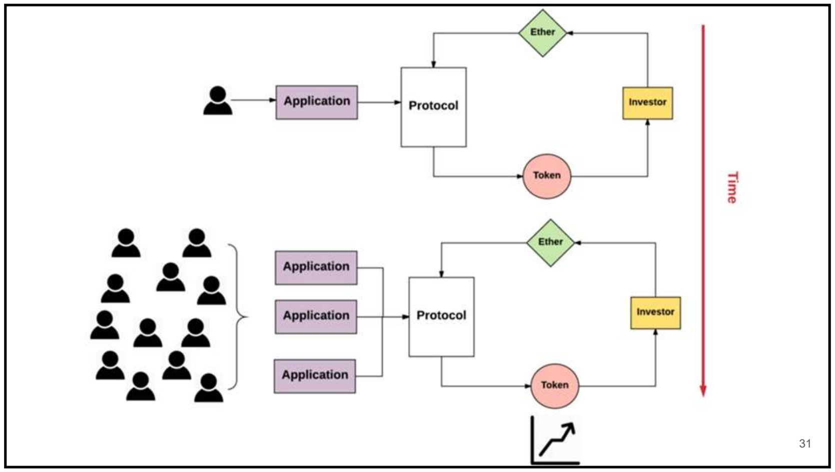
Smart contract

Ether

Investor

Token

30



Application

Protocol

Ether

Investor

Token

Application

Application

Application

Protocol

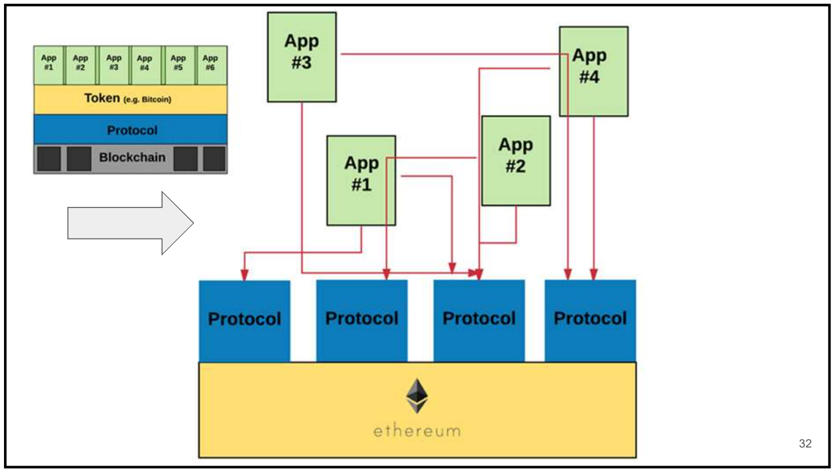
Ether

Investor

Token

Time

31



App #1

App #2

App #3

App #4

App #5

App #6

Token (e.g. Bitcoin)

Protocol

Blockchain

App #3

App #4

App #1

App #2

Protocol

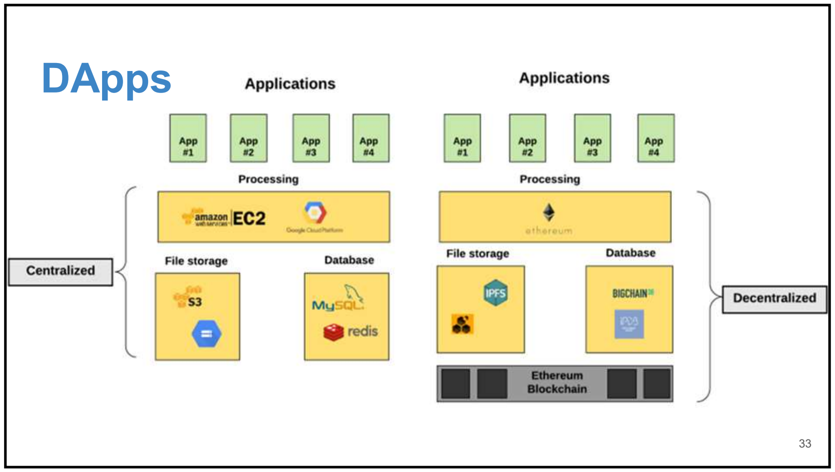
Protocol

Protocol

Protocol

ethereum

32



DApps

Applications

App #1

App #2

App #3

App #4

Processing

amazon web services EC2

Google Cloud Platform

File storage

S3

Database

MySQL

redis

Centralized

Applications

App #1

App #2

App #3

App #4

Processing

ethereum

File storage

IPFS

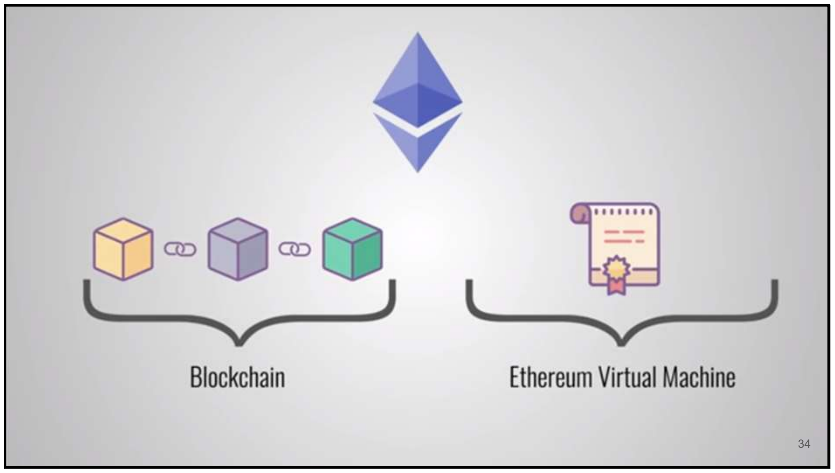
Database

BIGCHAIN DB

Ethereum Blockchain

Decentralized

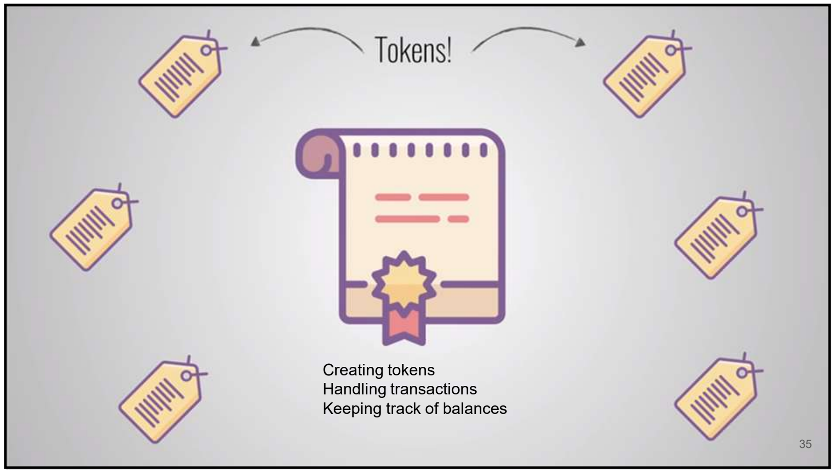
33



Blockchain

Ethereum Virtual Machine

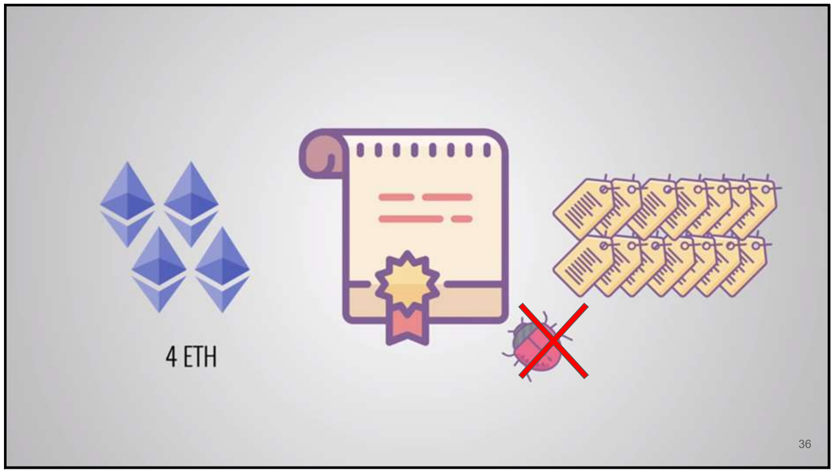
34



Tokens!

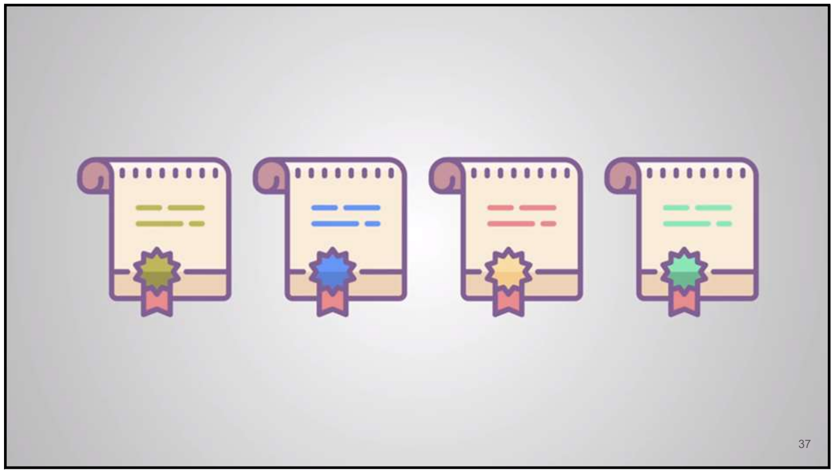
Creating tokens
Handling transactions
Keeping track of balances

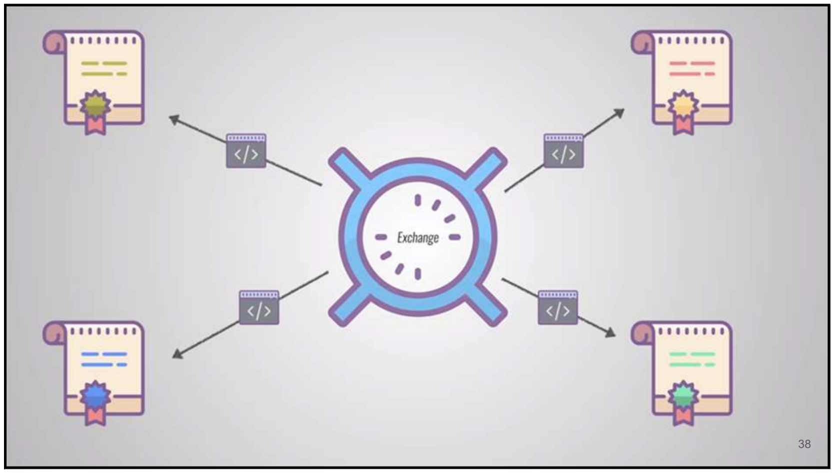
35



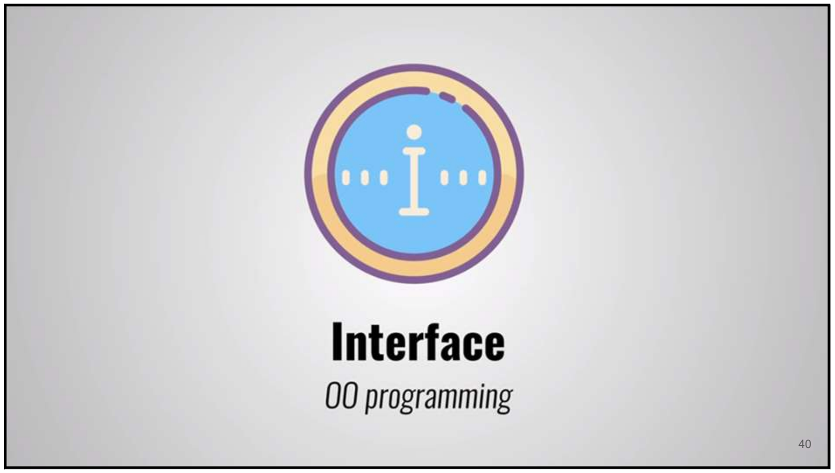
4 ETH

36

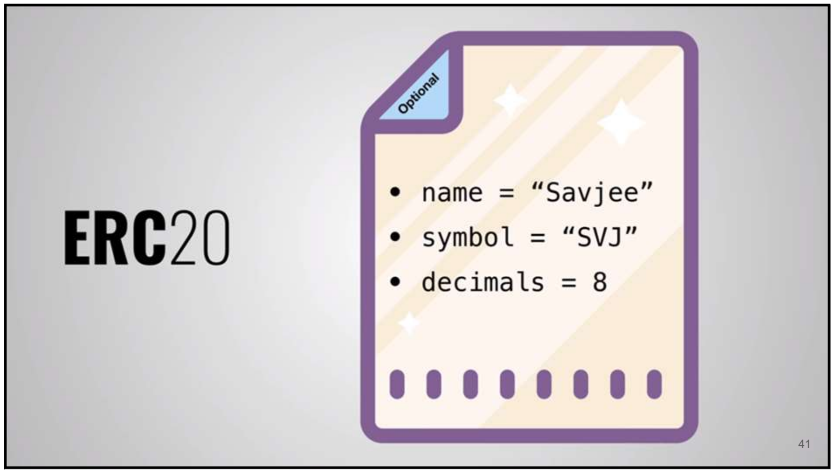




Ethereum **R**equest
for **C**omments

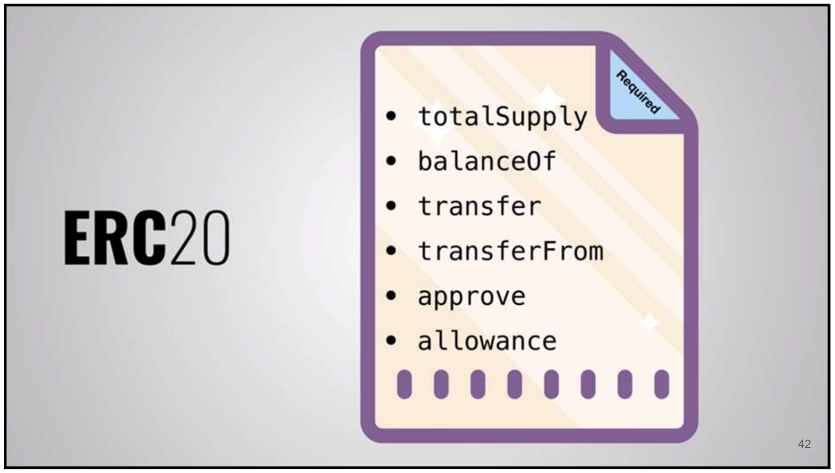

Interface

OO programming



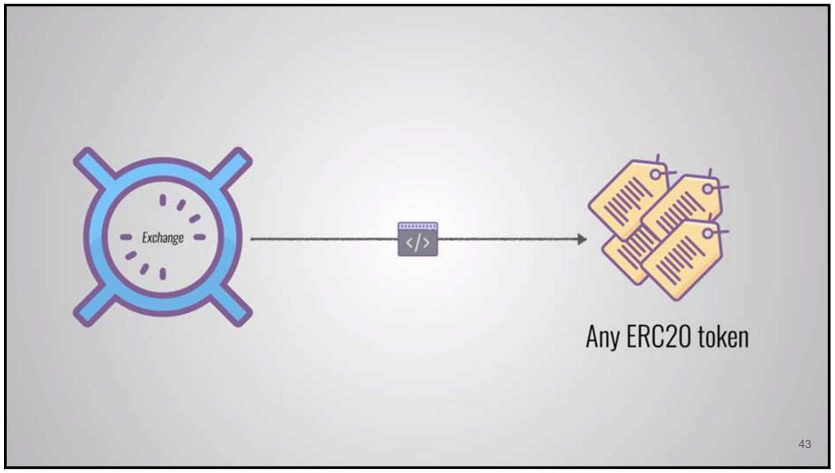
ERC20

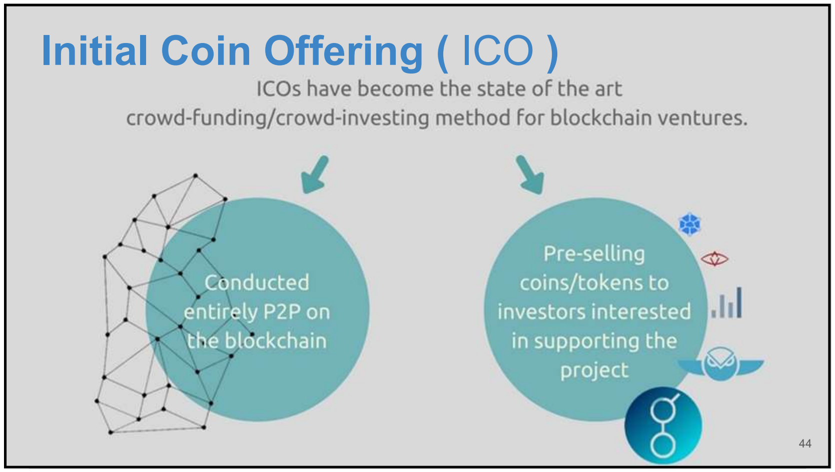
- name = “Savjee”
- symbol = “SVJ”
- decimals = 8



ERC20

- totalSupply
- balanceOf
- transfer
- transferFrom
- approve
- allowance



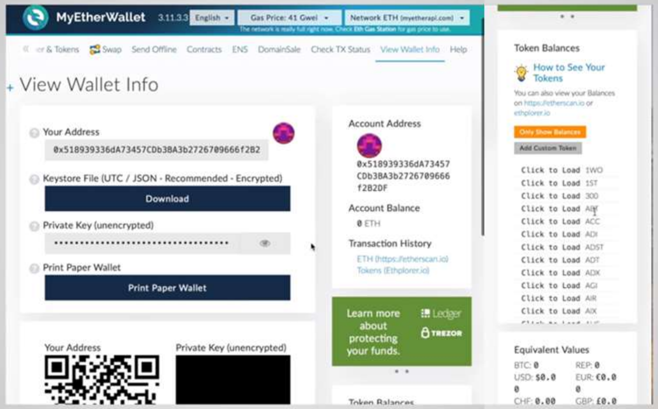


Initial Coin Offering (ICO)

ICOs have become the state of the art crowd-funding/crowd-investing method for blockchain ventures.

Conducted entirely P2P on the blockchain

Pre-selling coins/tokens to investors interested in supporting the project



View Wallet Info

Your Address
0x518939336dA73457CDb3BA3b2726709666f2B2

Keystore File (UTC / JSON - Recommended - Encrypted)

Download

Private Key (unencrypted)
••••••••••••••••••••••••••••••••••

Print Paper Wallet

Print Paper Wallet

Your Address

Private Key (unencrypted)

[redacted]

Account Address
0x518939336dA73457CDb3BA3b2726709666f2B2DF

Account Balance
0 ETH

Transaction History
ETH (https://etherscan.io)
Tokens (Ethplorer.io)

Learn more about protecting your funds.

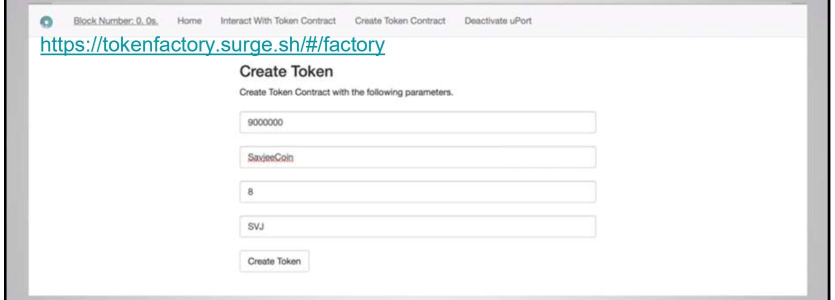
Token Balances

Token Balances
How to See Your Tokens
You can also view your Balances on https://etherscan.io or ethplorer.io

Only Show Balances
Add Custom Token

```
Click to Load 1WO
Click to Load 1ST
Click to Load 300
Click to Load AB
Click to Load ACC
Click to Load ADI
Click to Load ADST
Click to Load ADT
Click to Load ADX
Click to Load AGI
Click to Load AIR
Click to Load AIX
```

Equivalent Values
BTC: 0 REP: 0
USD: $0.00 EUR: €0.00
CHF: 0.00 GBP: £0.0



https://tokenfactory.surge.sh/#/factory

Create Token

Create Token Contract with the following parameters.

9000000

SavjeeCoin

8

SVJ

Create Token

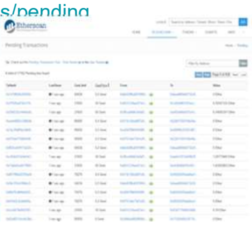
https://www.ethereum.org/token
https://etherscan.io/tokens

Exploring Blocks and Transactions

https://www.etherchain.org

https://etherscan.io/txsPending

https://www.etherchain.org/txs/pending



CryptoNetwork

https://www.ethereum.org

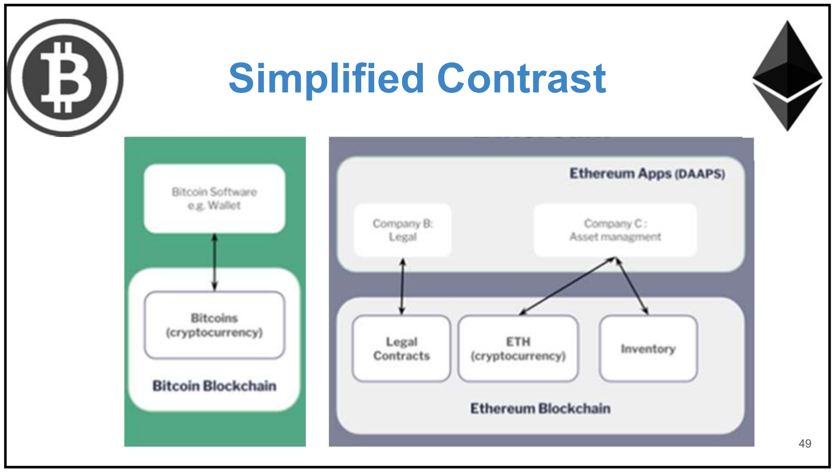
https://ethereum.org/foundation

About the Ethereum Foundation

Mission and Vision Statement

Foundation Council

VITALIK BUTERIN



Simplified Contrast

Bitcoin Software e.g. Wallet

Bitcoins (cryptocurrency)

Bitcoin Blockchain

Ethereum Apps (DAAPS)

Company B: Legal

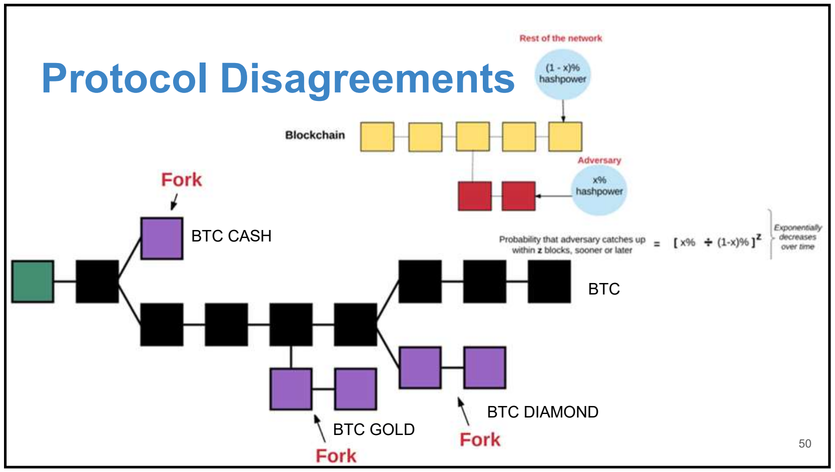
Company C : Asset managment

Legal Contracts

ETH (cryptocurrency)

Inventory

Ethereum Blockchain



Protocol Disagreements

Rest of the network

(1 - x)% hashpower

Blockchain

Adversary

x% hashpower

Probability that adversary catches up within **z** blocks, sooner or later = $[\,x\% \div (1\text{-}x)\%\,]^z$ Exponentially decreases over time

Fork

BTC CASH

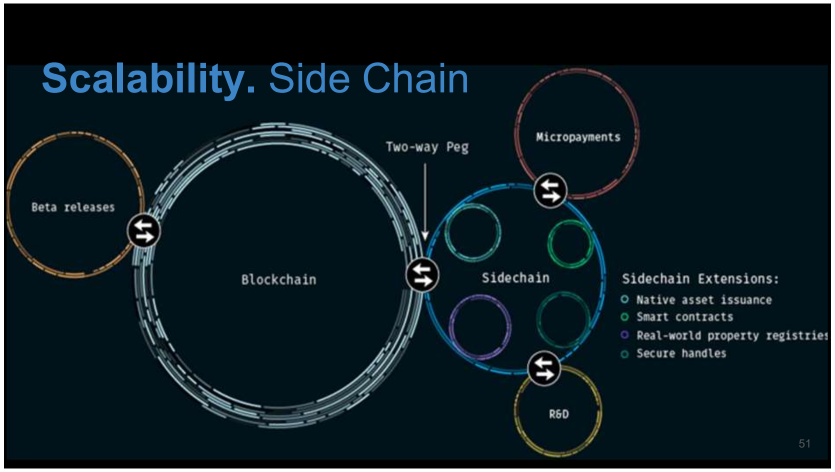
BTC

BTC GOLD

Fork

BTC DIAMOND

Fork



Scalability. Side Chain

Beta releases

Blockchain

Two-way Peg

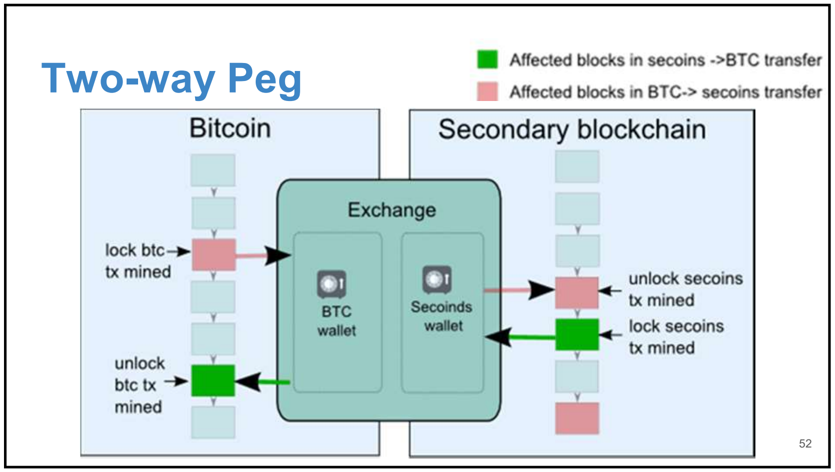
Micropayments

Sidechain

R&D

Sidechain Extensions:

- Native asset issuance
- Smart contracts
- Real-world property registries
- Secure handles



Two-way Peg

🟩 Affected blocks in secoins ->BTC transfer

🟥 Affected blocks in BTC-> secoins transfer

Bitcoin

Secondary blockchain

Exchange

BTC wallet

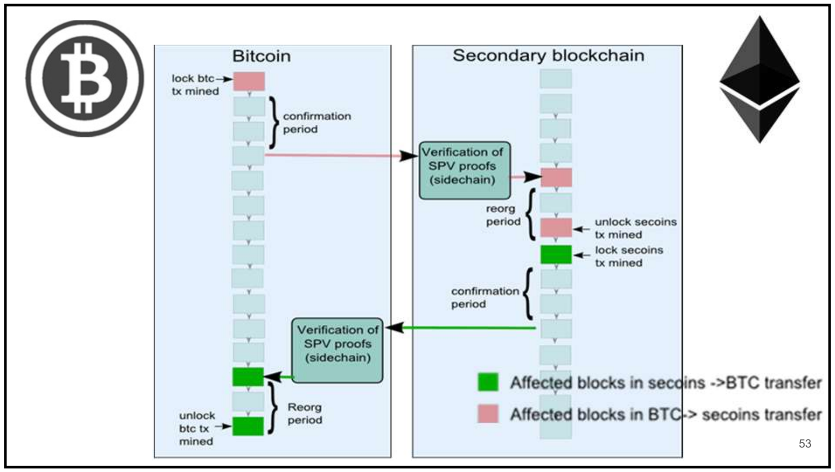
Secoinds wallet

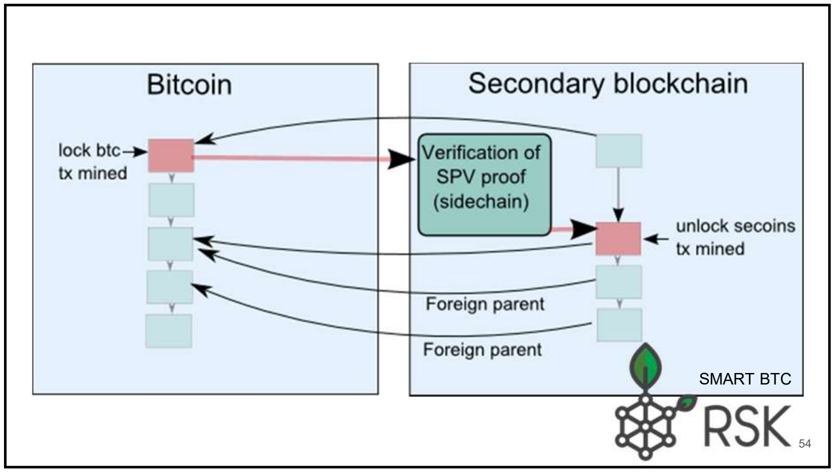
lock btc tx mined

unlock btc tx mined

unlock secoins tx mined

lock secoins tx mined





Trabajo Práctico [2] 💾

Extender el práctico 1 de modo que:

a) se de soporte a diferentes tipos de cuentas;
b) imitar una unidad de procesamiento con operaciones básicas (+costos);
c) permitir la creación de protocolos y tokens derivados;
d) desarrollar un mecanismo que administre el intercambio de tokens entre dos cadenas.

55

https://metamask.io

METAMASK

```
pragma solidity ^0.4.21;
contract HelloWorld {
    event log_string(bytes32 log); // Event
    function () public { // Fallback Function
        emit log_string("Hello World!");
        }
    }
```

http://remix.ethereum.org

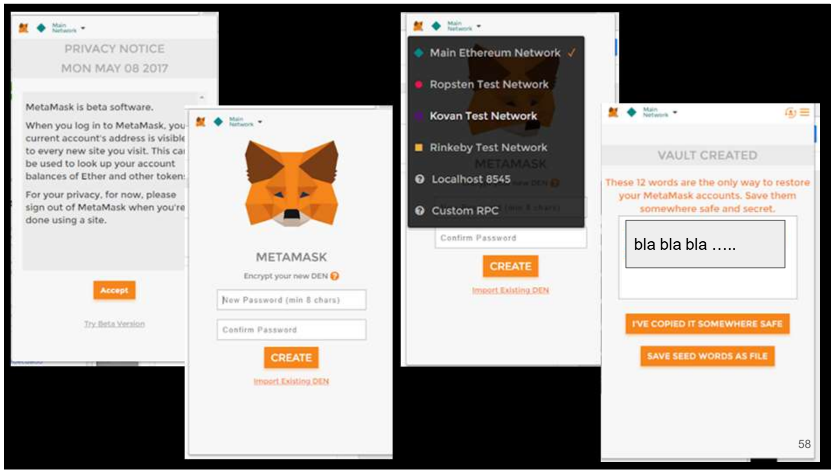
56

Starter wallets

MetaMask is a **browser extension wallet** that runs in your browser (Chrome, Firefox, Opera or Brave Browser). It is easy to use and convenient for testing, as it is able to connect to a variety of Ethereum nodes and test blockchains (see [testnets]).

Jaxx is a **multi-platform and multi-currency wallet** that runs on a variety of operating systems including Android, iOS, Windows, Mac and Linux. It is often a good choice for new users as it is designed for simplicity and ease of use.

MyEtherWallet (MEW) is a **web page-based wallet**, that runs in any browser. It has multiple sophisticated features, which we will explore in many of our examples.



MetaMask is beta software.

When you log in to MetaMask, you current account's address is visible to every new site you visit. This ca be used to look up your account balances of Ether and other token

For your privacy, for now, please sign out of MetaMask when you're done using a site.

These 12 words are the only way to restore your MetaMask accounts. Save them somewhere safe and secret.

bla bla bla …..

Switching Networks

Main Ethereum Network: The main, public, Ethereum blockchain. Real ETH, real value, real consequences.

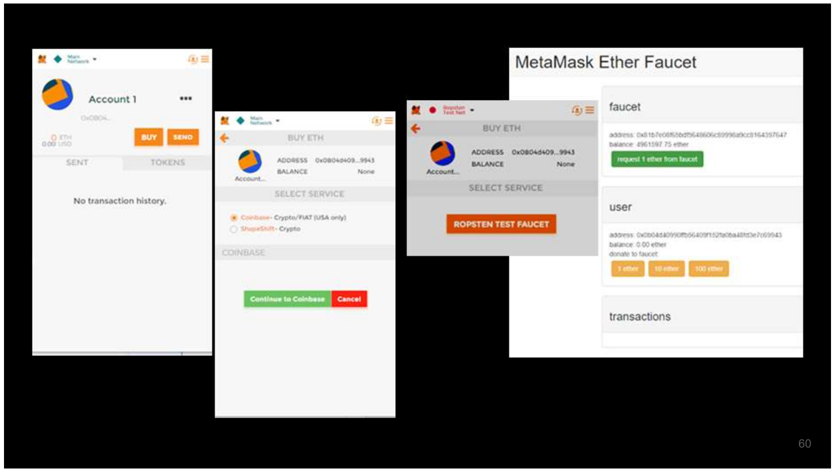
Ropsten Test Network: Ethereum public test blockchain and network, using Proof-of-Work consensus (mining). ETH on this network has no value.

Kovan Test Network: Ethereum public test blockchain and network, using Proof-of-Authority consensus (federated signing). ETH on this network has no value.

Rinkeby Test Network: Ethereum public test blockchain and network, using Proof-of-Authority consensus (federated signing). ETH on this network has no value.

Localhost 8545: Connect to a node running on the same computer as the browser. The node can be part of any public blockchain (main or testnet), or a private testnet (see [ganache]).

Custom RPC: Allows you to connect MetaMask to any node with a geth-compatible Remote Procedure Call (RPC) interface. The node can be part of any public or private blockchain.



0 ETH
0.00 USD

No transaction history.

Account...
ADDRESS 0x0804d409...9943
BALANCE None

● Coinbase- Crypto/FIAT (USA only)
○ ShapeShift- Crypto

MetaMask Ether Faucet

faucet

address: 0x81b7e08f65bdf5648606c89998a9cc8164397647
balance: 4961597.75 ether

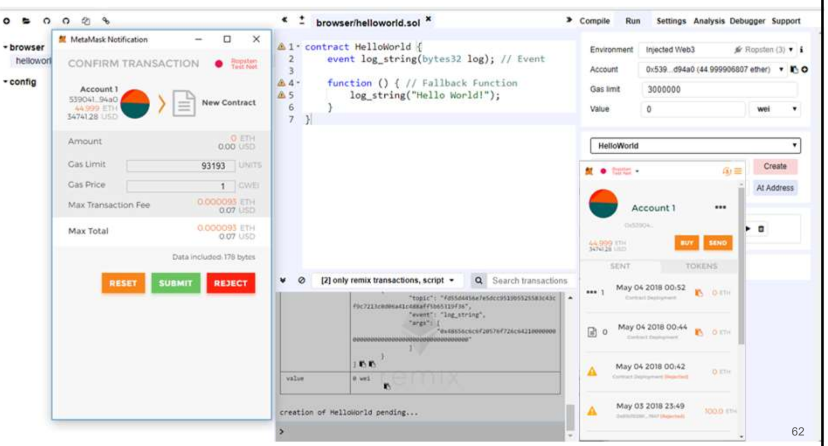
user

address: 0x0804d40990ffb56409f152fa0ba48fd3e7c69943
balance: 0.00 ether
donate to faucet:

transactions

Faucet

```
pragma solidity ^0.4.19; // Version of Solidity compiler
// Our first contract is a faucet!
contract Faucet {
        // Give out ether to anyone who asks
        function withdraw(uint withdraw_amount) public {
        // Limit withdrawal amount 1 eth
        require(withdraw_amount <= 1000000000000000000);
        // Send the amount to the address that requested it
        msg.sender.transfer(withdraw_amount);
    }
        // Accept any incoming amount
        function () public payable {}
}
```



CONFIRM TRANSACTION

Account 1
539041...94a0
44.999 ETH
3474128 USD
New Contract

Amount	0 ETH 0.00 USD
Gas Limit	93193 UNITS
Gas Price	1 GWEI
Max Transaction Fee	0.000093 ETH 0.07 USD
Max Total	0.000093 ETH 0.07 USD

Data included: 178 bytes

```
contract HelloWorld {
    event log_string(bytes32 log); // Event

    function () { // Fallback Function
        log_string("Hello World!");
    }
}
```

Environment: Injected Web3 — Ropsten (3)
Account: 0x539...d94a0 (44.999906807 ether)
Gas limit: 3000000
Value: 0 wei
HelloWorld

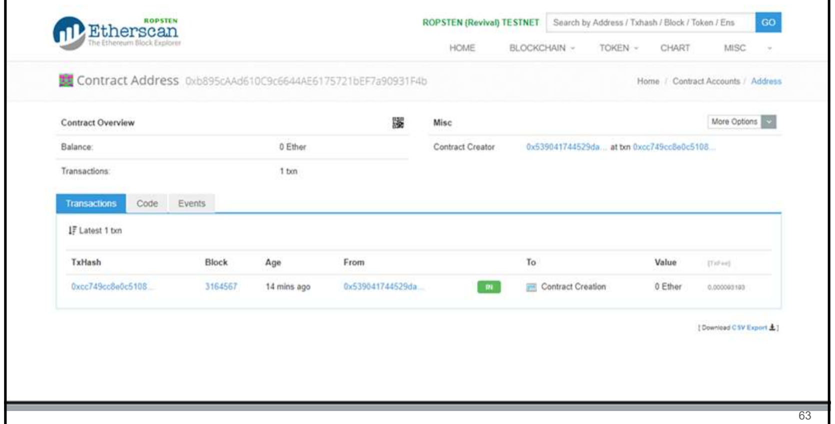
[2] only remix transactions, script

```
                "topic": "0xd5d4456e7e5dcc95190552558 3c43c
f9c7213c0d06a41c488aff5b65319f36",
                "event": "log_string",
                "args": [
                        "0x48656c6c6f20576f726c6421000000
000000000000000000000000000000000"
                ]
        }
]
value        0 wei

creation of HelloWorld pending...
```

Account 1
44.999 ETH
3474128 USD

1	May 04 2018 00:52	Contract Deployment	0 ETH
0	May 04 2018 00:44	Contract Deployment	0 ETH
	May 04 2018 00:42	Contract Deployment (Rejected)	0 ETH
	May 03 2018 23:49	(Rejected)	100.0 ETH


ROPSTEN
Etherscan
The Ethereum Block Explorer
ROPSTEN (Revival) TESTNET
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKEN
CHART
MISC
Home / Contract Accounts / Address
More Options
Transactions
Code
Events
[Download CSV Export]

Contract Address 0xb895cAAd610C9c6644AE6175721bEF7a90931F4b

Contract Overview

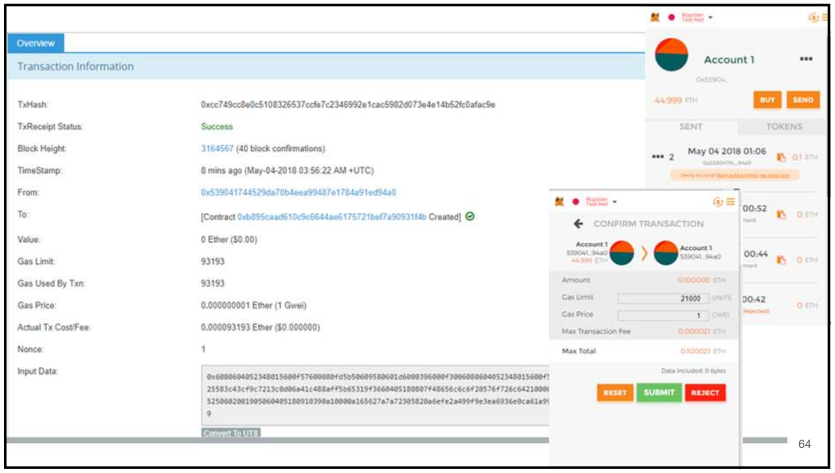
Balance: 0 Ether
Transactions: 1 txn

Misc

Contract Creator: 0x539041744529da... at txn 0xcc749cc8e0c5108...

Latest 1 txn

TxHash	Block	Age	From		To	Value	[TxFee]
0xcc749cc8e0c5108...	3164567	14 mins ago	0x539041744529da...	IN	Contract Creation	0 Ether	0.000093193



Transaction Information

TxHash:	0xcc749cc8e0c5108326537ccfe7c2346992e1cac5982d073e4e14b52fc0afac9e
TxReceipt Status:	Success
Block Height:	3164567 (40 block confirmations)
TimeStamp:	8 mins ago (May-04-2018 03:56:22 AM +UTC)
From:	0x539041744529da70b4eea99487e1784a91ed94a0
To:	[Contract 0xb895caad610c9c6644ae6175721bef7a90931f4b Created]
Value:	0 Ether ($0.00)
Gas Limit:	93193
Gas Used By Txn:	93193
Gas Price:	0.000000001 Ether (1 Gwei)
Actual Tx Cost/Fee:	0.000093193 Ether ($0.000000)
Nonce:	1
Input Data:	0x6080604052348015600f57600080fd5b50609580601d6000396000f3006080604052348015600f 25583c43cf9c7213c0d06a41c488aff5b65319f3660405180807f48656c6c6f20576f726c6421000 525060200190506040518091039 0a10000a165627a7a72305820a6efe2a499f9e3ea6936e0ca61a9 9

Account 1
0x53904...
44.999 ETH

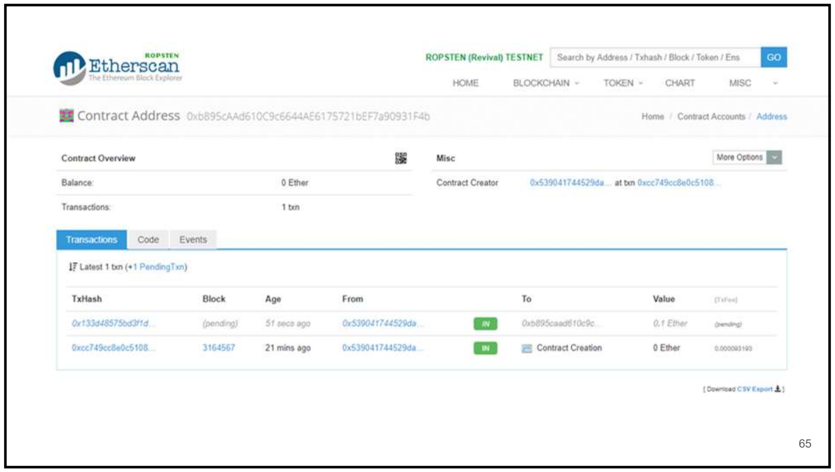
2	May 04 2018 01:06	0x539041... 94a0	0.1 ETH
	00:52		0 ETH
	00:44		0 ETH
	00:42	(Rejected)	0 ETH

CONFIRM TRANSACTION

Account 1
539041...94a0
44.999 ETH
Account 1
539041...94a0

Amount	0.100000 ETH
Gas Limit	21000 UNITS
Gas Price	1 GWEI
Max Transaction Fee	0.000021 ETH
Max Total	0.100021 ETH

Data included: 0 bytes


ROPSTEN Etherscan
The Ethereum Block Explorer
ROPSTEN (Revival) TESTNET
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKEN
CHART
MISC
Home / Contract Accounts / Address
More Options
Transactions
Code
Events
[Download CSV Export]

Contract Address 0xb895cAAd610C9c6644AE6175721bEF7a90931F4b

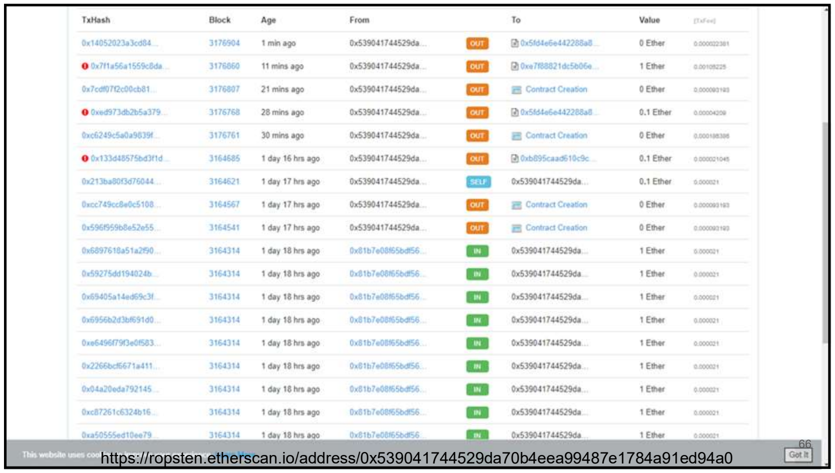
Contract Overview	
Balance:	0 Ether
Transactions:	1 txn

Misc	
Contract Creator	0x539041744529da... at txn 0xcc749cc8e0c5108...

Latest 1 txn (+1 PendingTxn)

TxHash	Block	Age	From		To	Value	[TxFee]
0x133d48575bd3f1d...	(pending)	51 secs ago	0x539041744529da...	IN	0xb895caad610c9c...	0.1 Ether	(pending)
0xcc749cc8e0c5108...	3164567	21 mins ago	0x539041744529da...	IN	Contract Creation	0 Ether	0.000093193

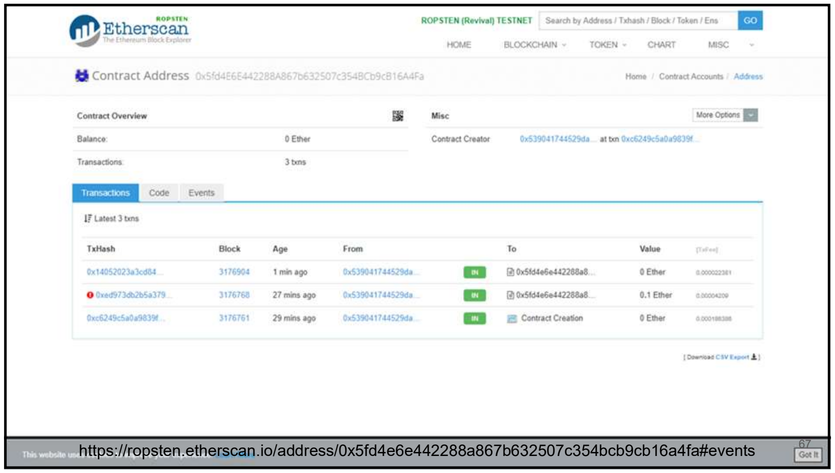
65



TxHash	Block	Age	From		To	Value	[TxFee]
0x14052023a3cd84...	3176904	1 min ago	0x539041744529da...	OUT	0x5fd4e6e442288a8...	0 Ether	0.000022381
❗ 0x7f1a56a1559c8da...	3176860	11 mins ago	0x539041744529da...	OUT	0xe7f88821dc5b06e...	1 Ether	0.00105225
0x7cdf07f2c00cb81...	3176807	21 mins ago	0x539041744529da...	OUT	Contract Creation	0 Ether	0.000093193
❗ 0xed973db2b5a379...	3176768	28 mins ago	0x539041744529da...	OUT	0x5fd4e6e442288a8...	0.1 Ether	0.00004209
0xc6249c5a0a9839f...	3176761	30 mins ago	0x539041744529da...	OUT	Contract Creation	0 Ether	0.000188386
❗ 0x133d48575bd3f1d...	3164685	1 day 16 hrs ago	0x539041744529da...	OUT	0xb895caad610c9c...	0.1 Ether	0.000021045
0x213ba80f3d76044...	3164621	1 day 17 hrs ago	0x539041744529da...	SELF	0x539041744529da...	0.1 Ether	0.000021
0xcc749cc8e0c5108...	3164567	1 day 17 hrs ago	0x539041744529da...	OUT	Contract Creation	0 Ether	0.000093193
0x596f959b8e52e55...	3164541	1 day 17 hrs ago	0x539041744529da...	OUT	Contract Creation	0 Ether	0.000093193
0x6897618a51a2f90...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021
0x59275dd194024b...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021
0x69405a14ed69c3f...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021
0x6956b2d3bf691d0...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021
0xe6496f79f3e0f583...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021
0x2266bcf6671a411...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021
0x04a20eda792145...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021
0xc87261c6324b16...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021
0xa50555ed10ee79...	3164314	1 day 18 hrs ago	0x81b7e08f65bdf56...	IN	0x539041744529da...	1 Ether	0.000021

https://ropsten.etherscan.io/address/0x539041744529da70b4eea99487e1784a91ed94a0

66


ROPSTEN Etherscan
The Ethereum Block Explorer
ROPSTEN (Revival) TESTNET
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKEN
CHART
MISC
Home / Contract Accounts / Address
More Options
Transactions
Code
Events
[Download CSV Export]
Got It

Contract Address 0x5fd4E6E442288A867b632507c354BCb9cB16A4Fa

Contract Overview	
Balance:	0 Ether
Transactions:	3 txns

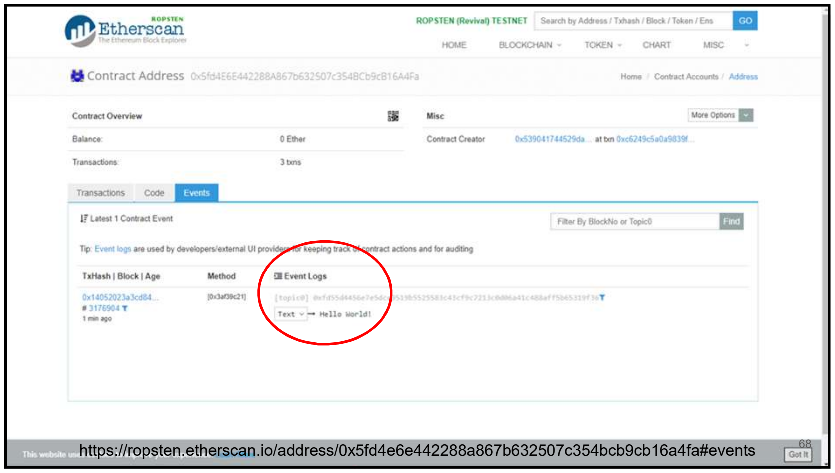
Misc	
Contract Creator	0x539041744529da... at txn 0xc6249c5a0a9839f...

Latest 3 txns

TxHash	Block	Age	From		To	Value	[TxFee]
0x14052023a3cd84...	3176904	1 min ago	0x539041744529da...	IN	0x5fd4e6e442288a8...	0 Ether	0.000022381
❗ 0xed973db2b5a379...	3176768	27 mins ago	0x539041744529da...	IN	0x5fd4e6e442288a8...	0.1 Ether	0.00004209
0xc6249c5a0a9839f...	3176761	29 mins ago	0x539041744529da...	IN	Contract Creation	0 Ether	0.000188386

https://ropsten.etherscan.io/address/0x5fd4e6e442288a867b632507c354bcb9cb16a4fa#events

67


ROPSTEN Etherscan
The Ethereum Block Explorer
ROPSTEN (Revival) TESTNET
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKEN
CHART
MISC
Home / Contract Accounts / Address
More Options
Transactions
Code
Events
Filter By BlockNo or Topic0
Find
Got It

Contract Address 0x5fd4E6E442288A867b632507c354BCb9cB16A4Fa

Contract Overview	
Balance:	0 Ether
Transactions:	3 txns

Misc	
Contract Creator	0x539041744529da... at txn 0xc6249c5a0a9839f...

Latest 1 Contract Event

Tip: Event logs are used by developers/external UI providers for keeping track of contract actions and for auditing

TxHash | Block | Age	Method	Event Logs
0x14052023a3cd84... # 3176904 1 min ago	[0x3af39c21]	[topic0] 0xfd55d4456e7e5dc...5519b5525583c43cf9c7213c0d06a41c488aff5b65319f36 Text → Hello World!

https://ropsten.etherscan.io/address/0x5fd4e6e442288a867b632507c354bcb9cb16a4fa#events

68

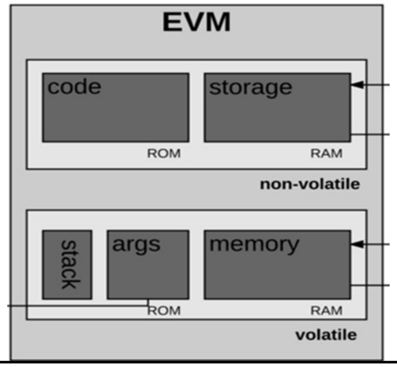
Trabajo Práctico [2]

Extender el práctico 1 de modo que:

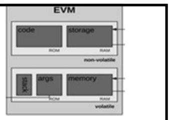
a) se de soporte a diferentes tipos de cuentas;
b) imitar una unidad de procesamiento con operaciones básicas (+costos);
c) permitir la creación de protocolos y tokens derivados;
d) desarrollar un mecanismo que administre el intercambio de tokens entre dos cadenas.
e) Interactuar con el contrato Faucet vía MetaMask.
f) Implementar y desplegar el contrato “Hola Mundo” (testnet)

Ethereum Virtual Machine (*)

- Turing complete VM
- +Limitation by gas (https://ethgasstation.info)
- Stack-based architecture
- Stack size 1024.
- Stack item max. 256-bit



Types of storage

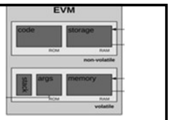


- Volatile**: *Stack***
- Volatile**: Memory**
- No Volatile: **Storage (state fo contract)**

Context information

- Code associated with the contract
- Access to the transaction data field

Stack

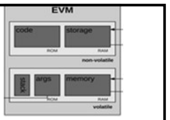


All the operations of the Ethereum Virtual Machine (EVM opcodes), except the STOP, JUMPDEST and INVALID operations, use the stack. Either to read or to write on it. However, operations that only read or store values in the stack, **without making any kind of calculation,** they are:

The stack goes from level 0 to a maximum depth of 1024.

- *POP*: Gets the value of level 0 of the stack
- *PUSH1...PUSH32 (PUSHX)*: Insert X bytes in level 0 of the stack
- *DUP1...DUP16 (DUPX)*: Doubles the value in level X to level O
- *SWAP1...SWAP16 (SWAPX)*: Swap the value at position X with the value at position O

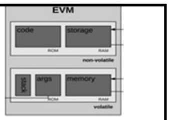
Memory



The operations that interact with memory, whether for writing or reading, are:

- *CALLDATACOPY*: Read the data field of the transaction and load it in memory
- *CODECOPY*: Read the code associated with the contract and load it into memory
- *EXTCODECOPY*: Read the code associated with an external contract and load it in memory
- ***M**LOAD*: Read, from memory, a value
- ***M**STORE*: Saves a value in memory (word size / 32bytes)
- ***M**STORE8*: Saves an 8-bit value (1byte) in memory

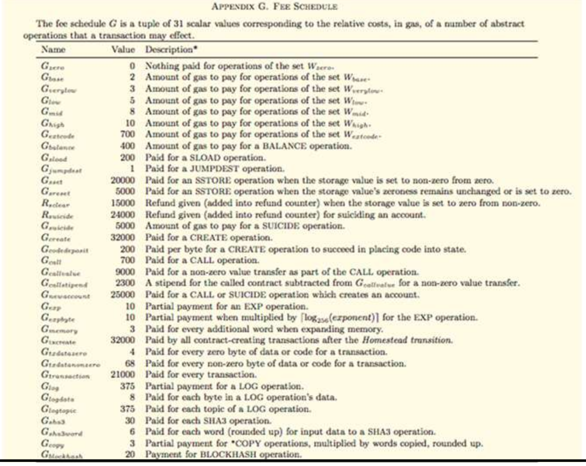
Storage



Unlike the stack or memory, the storage of contract status variables is stored in a persistent space between executions. The operations that are available to operate in this storage are:

- ***S**LOAD*
- ***S**STORE*

Highlight the S and the M of storage and memory, respectively.



Appendix G. Fee Schedule

The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero}.
G_{base}	2	Amount of gas to pay for operations of the set W_{base}.
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low}.
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid}.
G_{high}	10	Amount of gas to pay for operations of the set W_{high}.
$G_{extcode}$	700	Amount of gas to pay for operations of the set $W_{extcode}$.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{sclear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{suicide}$	24000	Refund given (added into refund counter) for suiciding an account.
$G_{suicide}$	5000	Amount of gas to pay for a SUICIDE operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value transfer.
$G_{newaccount}$	25000	Paid for a CALL or SUICIDE operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	10	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
$G_{txcreate}$	32000	Paid by all contract-creating transactions after the *Homestead transition*.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.
G_{log}	375	Partial payment for a LOG operation.
$G_{logdata}$	8	Paid for each byte in a LOG operation's data.
$G_{logtopic}$	375	Paid for each topic of a LOG operation.
G_{sha3}	30	Paid for each SHA3 operation.
$G_{sha3word}$	6	Paid for each word (rounded up) for input data to a SHA3 operation.
G_{copy}	3	Partial payment for *COPY operations, multiplied by words copied, rounded up.
$G_{blockhash}$	20	Payment for BLOCKHASH operation.

Trabajo Práctico [2] 💾

Extender el práctico 1 de modo que:

a) se de soporte a diferentes tipos de cuentas;
b) imitar una unidad de procesamiento con operaciones básicas (+costos);
c) permitir la creación de protocolos y tokens derivados;
d) desarrollar un mecanismo que administre el intercambio de tokens entre dos cadenas.
e) Interactuar con el contrato Faucet vía MetaMask.
f) Implementar y desplegar el contrato “Hola Mundo” (testnet)
g) Contrastar el costo de Gas de las operaciones en Solidity.
h) Elaborar una tabla con secuencias de sentencias semánticamente equivalentes donde se reduzca el costo.