ethereum

Everton Fraga

Software Engineer

Mist Team

ev@ethereum.org

# Blockchain

*"Blockchains são bancos de dados* ***distribuídos****,*
*que mantém uma* ***lista crescente de registros****,*
*os blocos, e é* ***à prova de alterações****."*

Wikipedia

# Blockchain

*distribuído*

*lista crescente de registros*

*à prova de alterações*

# Consenso

- Quem garante o saldo da sua conta?
- Quem inventou o fim de semana?
- “Quando as partes concordam, vira verdade.”
- Algoritmo de consenso

# Ethereum - Como surgiu

Jeffrey Wilcke

Geth

Vitalik Buterin

Dr. Gavin Wood

Eth, Parity

# Ethereum Foundation

- 2014, via financiamento coletivo
- Open Source Software
- ~100 projetos online
- 40 pessoas, distribuídas no mundo
- 2 brasileiros :)

Ethereum Foundation

# Ethereum Foundation

*Research, Development and Education on decentralized technologies.*

Ethereum Foundation

Ethereum developers applaud audience at Devcon

# ethereum

# Ecossistema

- Blockchain (Eth, Geth, Parity)
- Whisper
- Swarm

# Blockchain

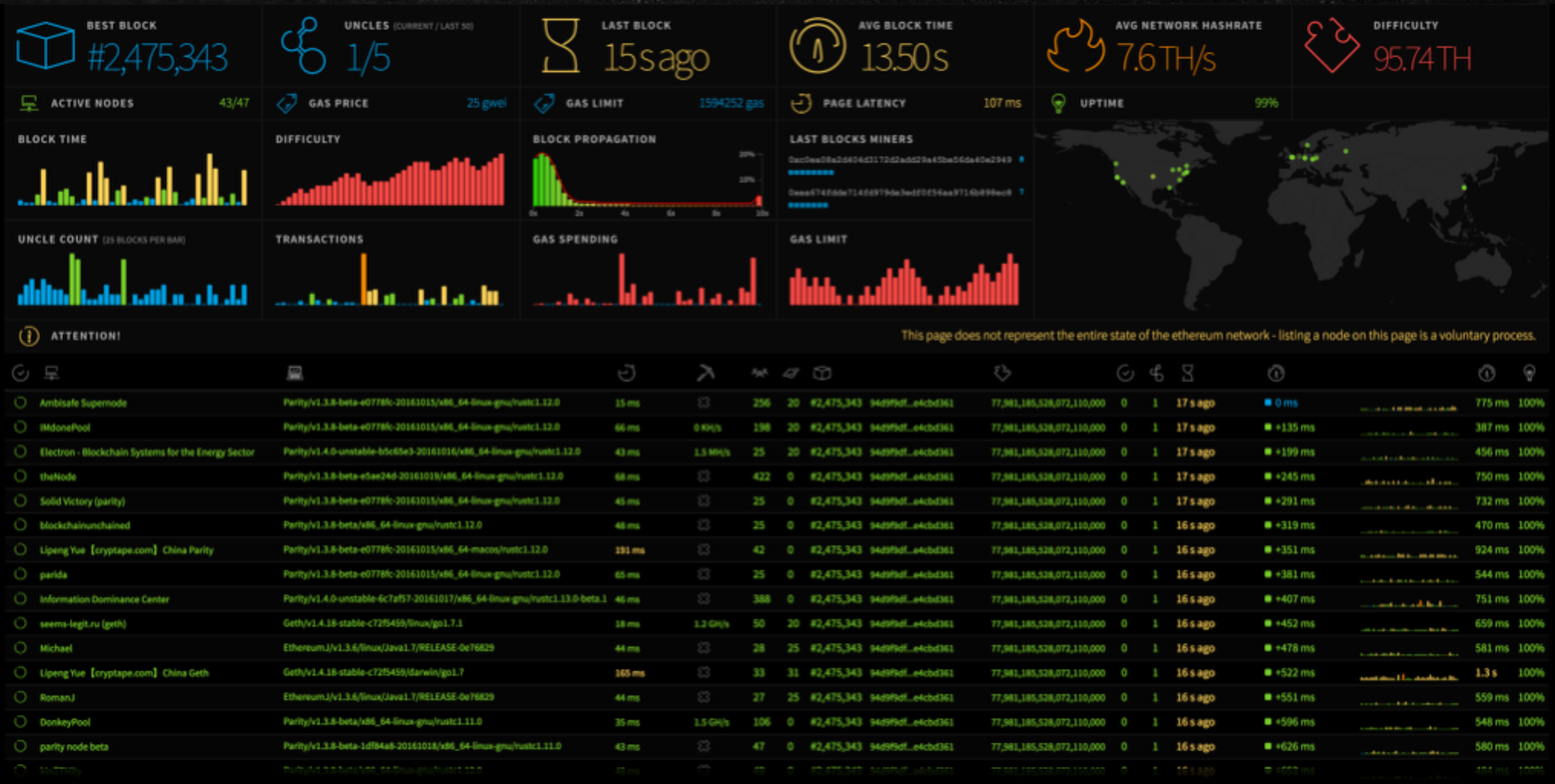
*Quem mantém a rede viva? E por quê?*

# Proof of Work

- Incentivo financeiro sobre poder computacional
- Mining power
- Funciona bem, mas pode melhorar

Proof of Work

# Blockchain



BEST BLOCK #2,475,343

UNCLES (CURRENT / LAST 50) 1/5

LAST BLOCK 15s ago

AVG BLOCK TIME 13.50s

AVG NETWORK HASHRATE 7.6 TH/s

DIFFICULTY 95.74 TH

ACTIVE NODES 43/47

GAS PRICE 25 gwei

GAS LIMIT 1594252 gas

PAGE LATENCY 107 ms

UPTIME 99%

LAST BLOCKS MINERS

0xc0ea08a2d404d3172d2add29a45be56da40e2949 8

0xea674fdde714fd979de3edf0f56aa9716b898ec8 7

ATTENTION! This page does not represent the entire state of the ethereum network - listing a node on this page is a voluntary process.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ○ | Ambisafe Supernode | Parity/v1.3.8-beta-e0778fc-20161015/x86_64-linux-gnu/rustc1.12.0 | 15 ms | ☒ | 256 | 20 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 17 s ago | ■ 0 ms | 775 ms | 100% |
| ○ | IMdonePool | Parity/v1.3.8-beta-e0778fc-20161015/x86_64-linux-gnu/rustc1.12.0 | 66 ms | 0 KH/s | 198 | 20 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 17 s ago | ■ +135 ms | 387 ms | 100% |
| ○ | Electron - Blockchain Systems for the Energy Sector | Parity/v1.4.0-unstable-b5c65e3-20161016/x86_64-linux-gnu/rustc1.12.0 | 43 ms | 1.5 MH/s | 25 | 20 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 17 s ago | ■ +199 ms | 456 ms | 100% |
| ○ | theNode | Parity/v1.3.8-beta-e5ae24d-20161019/x86_64-linux-gnu/rustc1.12.0 | 68 ms | ☒ | 422 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 17 s ago | ■ +245 ms | 750 ms | 100% |
| ○ | Solid Victory (parity) | Parity/v1.3.8-beta-e0778fc-20161015/x86_64-linux-gnu/rustc1.12.0 | 45 ms | ☒ | 25 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 17 s ago | ■ +291 ms | 732 ms | 100% |
| ○ | blockchainunchained | Parity/v1.3.8-beta/x86_64-linux-gnu/rustc1.12.0 | 48 ms | ☒ | 25 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +319 ms | 470 ms | 100% |
| ○ | Lipeng Yue 【cryptape.com】 China Parity | Parity/v1.3.8-beta-e0778fc-20161015/x86_64-macos/rustc1.12.0 | 191 ms | ☒ | 42 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +351 ms | 924 ms | 100% |
| ○ | parida | Parity/v1.3.8-beta-e0778fc-20161015/x86_64-linux-gnu/rustc1.12.0 | 65 ms | ☒ | 25 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +381 ms | 544 ms | 100% |
| ○ | Information Dominance Center | Parity/v1.4.0-unstable-6c7af57-20161017/x86_64-linux-gnu/rustc1.13.0-beta.1 | 46 ms | ☒ | 388 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +407 ms | 751 ms | 100% |
| ○ | seems-legit.ru (geth) | Geth/v1.4.18-stable-c72f5459/linux/go1.7.1 | 18 ms | 1.2 GH/s | 50 | 20 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +452 ms | 659 ms | 100% |
| ○ | Michael | EthereumJ/v1.3.6/linux/Java1.7/RELEASE-0e76829 | 44 ms | ☒ | 28 | 25 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +478 ms | 581 ms | 100% |
| ○ | Lipeng Yue 【cryptape.com】 China Geth | Geth/v1.4.18-stable-c72f5459/darwin/go1.7 | 165 ms | ☒ | 33 | 31 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +522 ms | 1.3 s | 100% |
| ○ | RomanJ | EthereumJ/v1.3.6/linux/Java1.7/RELEASE-0e76829 | 44 ms | ☒ | 27 | 25 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +551 ms | 559 ms | 100% |
| ○ | DonkeyPool | Parity/v1.3.8-beta/x86_64-linux-gnu/rustc1.11.0 | 35 ms | 1.5 GH/s | 106 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +596 ms | 548 ms | 100% |
| ○ | parity node beta | Parity/v1.3.8-beta-1df84a8-20161018/x86_64-linux-gnu/rustc1.11.0 | 43 ms | ☒ | 47 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +626 ms | 580 ms | 100% |
| ○ | [illegible] | Parity/v1.3.8-beta/x86_64-linux-gnu/rustc1.12.0 | 48 ms | ☒ | 49 | 0 | #2,475,343 | 94d9f9df...e4cbd361 | 77,981,185,528,072,110,000 | 0 | 1 | 16 s ago | ■ +653 ms | 484 ms | 100% |

Ethereum Network Stats

# Proof of Stake

- Protege valor e valida transações
- Desincentivo para fugir do consenso
- Naturalmente mais seguro

Proof of Stake

# Proof of Authority

- Caso especial, blockchains privadas

- “Eu sou o Porto de Santos”, ou
  “Eu sou o governo de Dubai”

Proof of Authority

# Blockchain

- Softwares atuais:
  - Geth, Eth, Parity, EthereumJ, Pyethereum.
- Usuário comum - sincronizar a rede antes de usar
- Ethereum Light Client

# Smart contracts

- Core do Ethereum
- Código que manipula o estado da rede
- Solidity - Linguagem touring complete
- Gas: combustível para os contratos executarem na rede

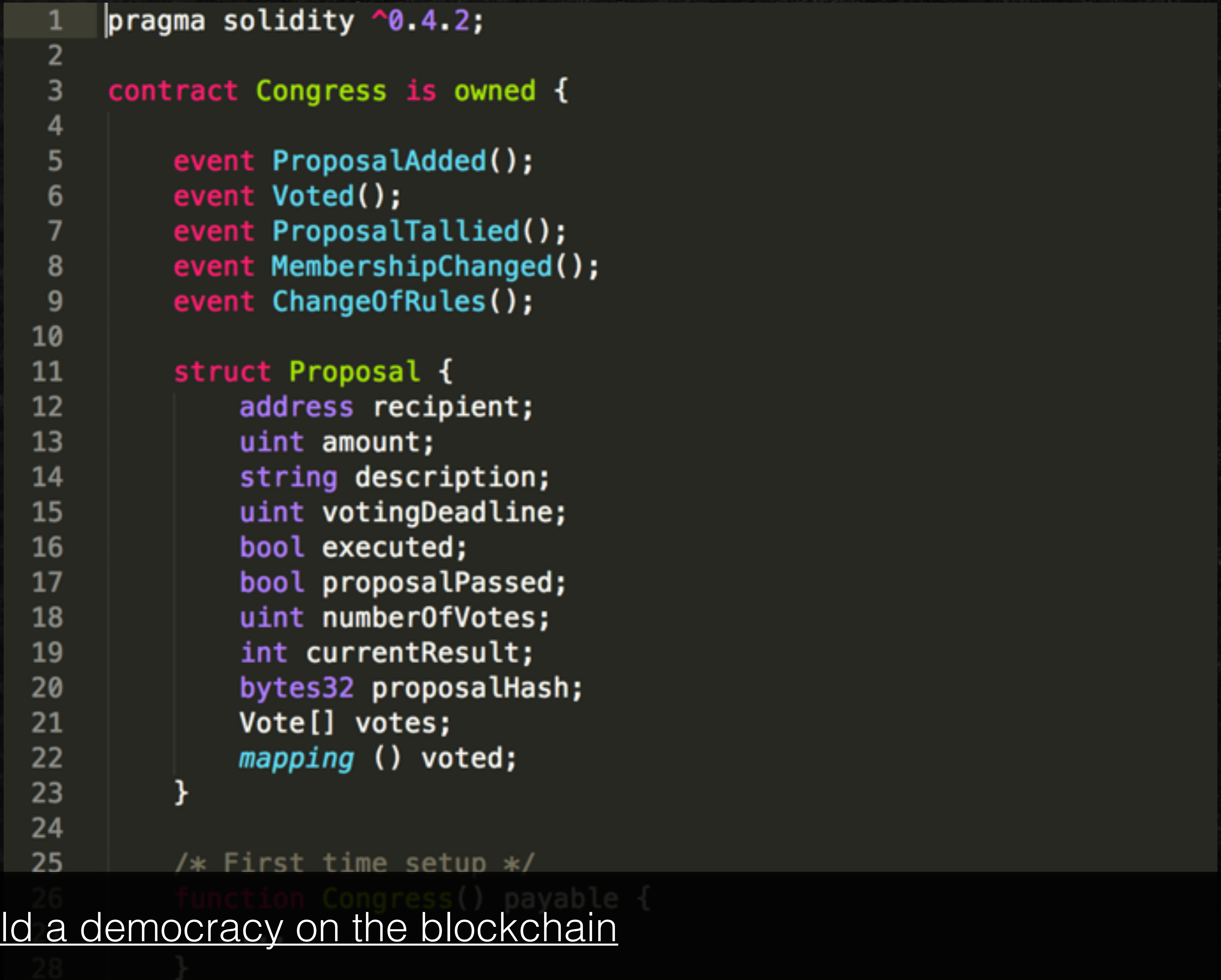
Introduction to Smart Contracts with Solidity

HOW TO BUILD A

# DEMOCRACY

ON THE BLOCKCHAIN

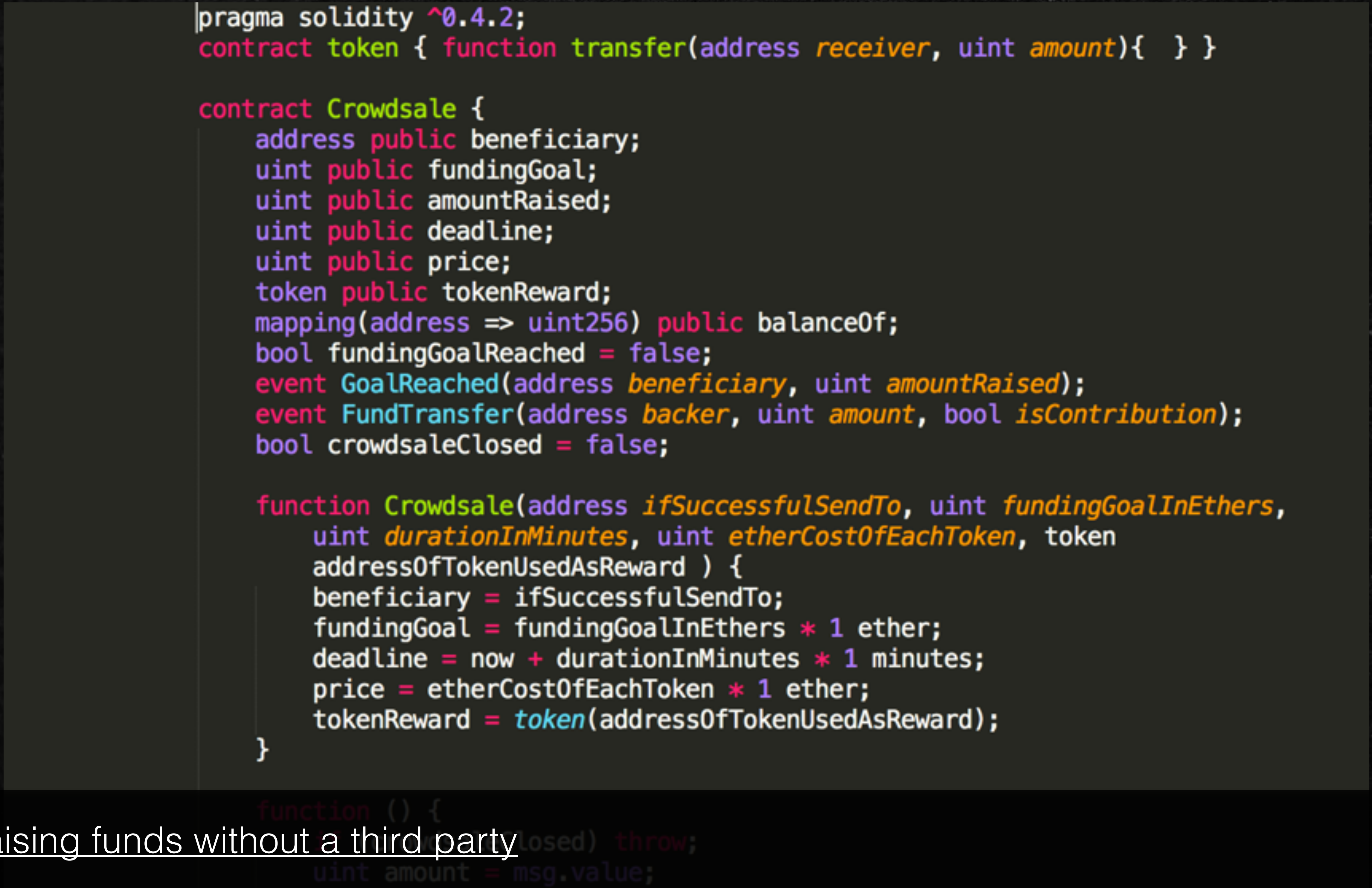
# Criando uma democracia



```
pragma solidity ^0.4.2;

contract Congress is owned {

    event ProposalAdded();
    event Voted();
    event ProposalTallied();
    event MembershipChanged();
    event ChangeOfRules();

    struct Proposal {
        address recipient;
        uint amount;
        string description;
        uint votingDeadline;
        bool executed;
        bool proposalPassed;
        uint numberOfVotes;
        int currentResult;
        bytes32 proposalHash;
        Vote[] votes;
        mapping () voted;
    }

    /* First time setup */
    function Congress() payable {
```

How to build a democracy on the blockchain

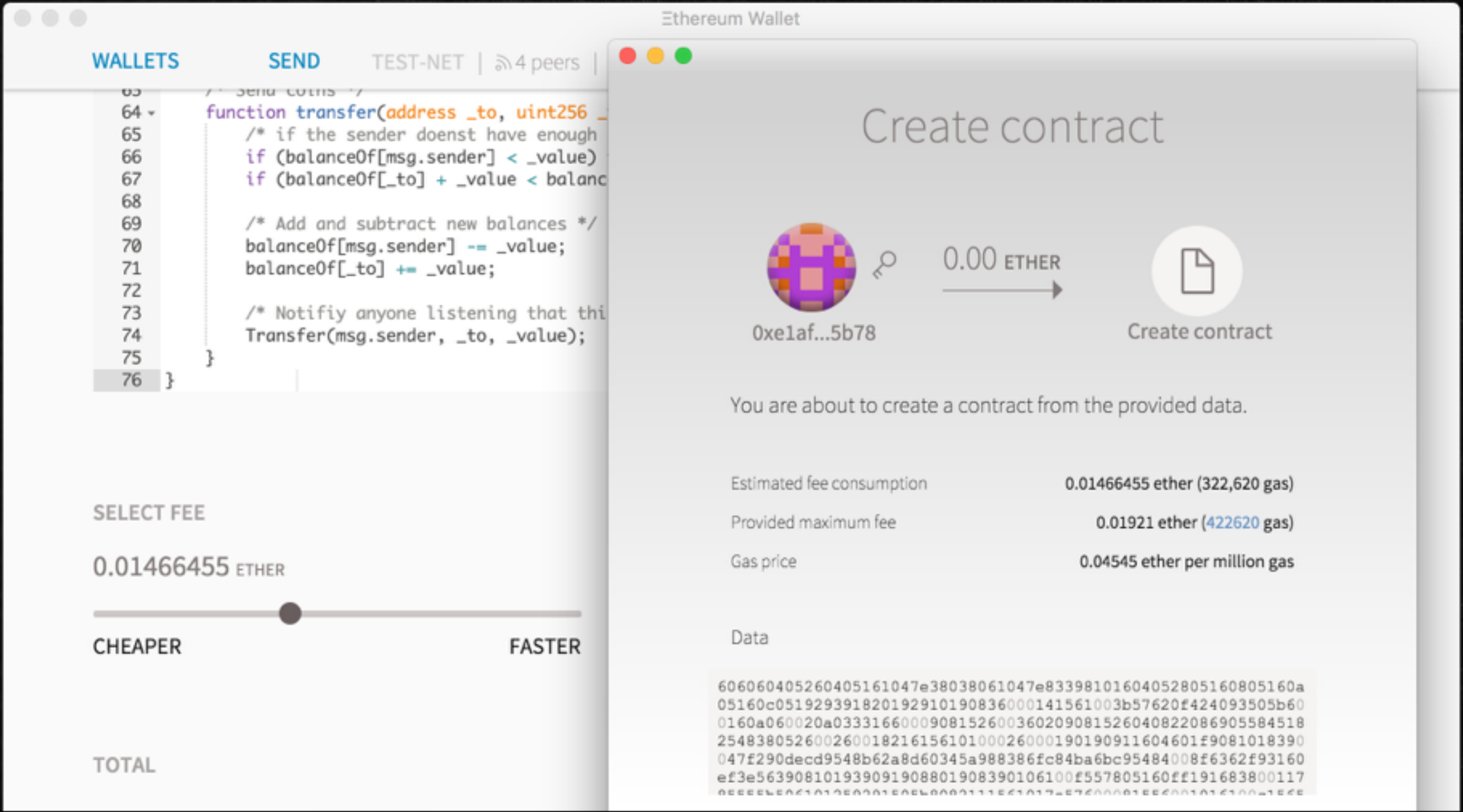
# Crowdfunding sem terceiros



```
pragma solidity ^0.4.2;
contract token { function transfer(address receiver, uint amount){  } }

contract Crowdsale {
    address public beneficiary;
    uint public fundingGoal;
    uint public amountRaised;
    uint public deadline;
    uint public price;
    token public tokenReward;
    mapping(address => uint256) public balanceOf;
    bool fundingGoalReached = false;
    event GoalReached(address beneficiary, uint amountRaised);
    event FundTransfer(address backer, uint amount, bool isContribution);
    bool crowdsaleClosed = false;

    function Crowdsale(address ifSuccessfulSendTo, uint fundingGoalInEthers,
        uint durationInMinutes, uint etherCostOfEachToken, token
        addressOfTokenUsedAsReward ) {
        beneficiary = ifSuccessfulSendTo;
        fundingGoal = fundingGoalInEthers * 1 ether;
        deadline = now + durationInMinutes * 1 minutes;
        price = etherCostOfEachToken * 1 ether;
        tokenReward = token(addressOfTokenUsedAsReward);
    }

    function () {
        if (crowdsaleClosed) throw;
        uint amount = msg.value;
```

[Raising funds without a third party]()

# Ethereum Wallet



```
        /* Send coins */
        function transfer(address _to, uint256 _
            /* if the sender doesnt have enough
            if (balanceOf[msg.sender] < _value)
            if (balanceOf[_to] + _value < balanc

            /* Add and subtract new balances */
            balanceOf[msg.sender] -= _value;
            balanceOf[_to] += _value;

            /* Notifiy anyone listening that thi
            Transfer(msg.sender, _to, _value);
        }
    }
```

SELECT FEE

0.01466455 ETHER

CHEAPER FASTER

TOTAL

0.01466455 ETHER

## Create contract

0xe1af...5b78 → 0.00 ETHER → Create contract

You are about to create a contract from the provided data.

| | |
|---|---|
| Estimated fee consumption | 0.01466455 ether (322,620 gas) |
| Provided maximum fee | 0.01921 ether (422620 gas) |
| Gas price | 0.04545 ether per million gas |

Data

```
60606040526040516104 7e38038061047e83398101604052805160805160a
05160c05192939182019291019083600014156100 3b57620f424093505b60
0160a06000 20a03331660009081526003602090815260408220869055845 18
254838052600260018216156101000260001901909116046 01f9081018390
047f290decd9548b62a8d60345a988386fc84ba6bc95484008f6362f93160
ef3e56390810193909190880190839010610 0f557805160ff191683800117
```

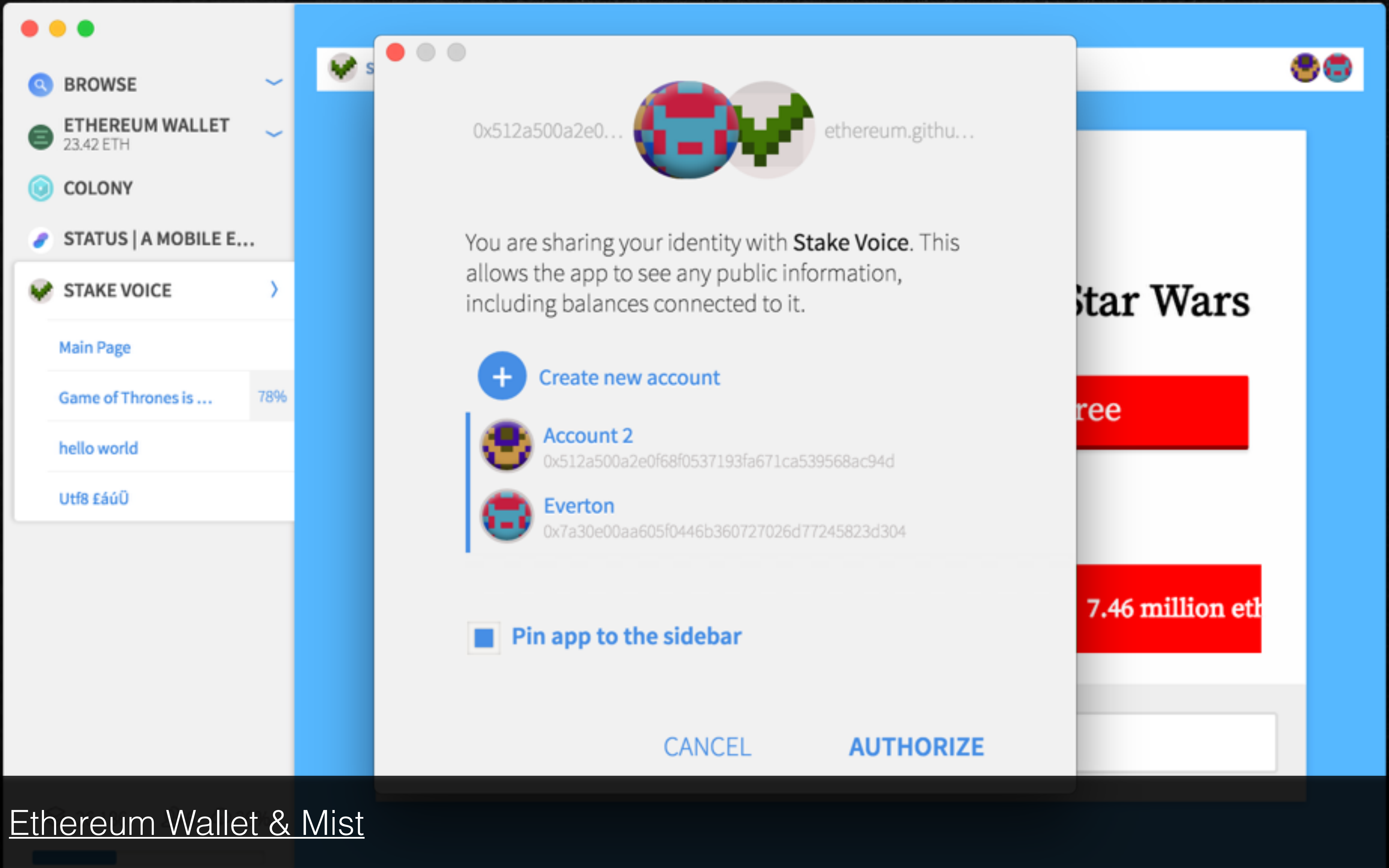
Enter password to confirm the transaction

Ethereum Wallet & Mist

# Dapps

- Sites que interagem com a blockchain
- Contratos com um rosto próprio
- Diversas ferramentas para desenvolvedores disponíveis

# Mist



You are sharing your identity with **Stake Voice**. This allows the app to see any public information, including balances connected to it.

Account 2
0x512a500a2e0f68f0537193fa671ca539568ac94d

Everton
0x7a30e00aa605f0446b360727026d77245823d304

Ethereum Wallet & Mist

# Swarm

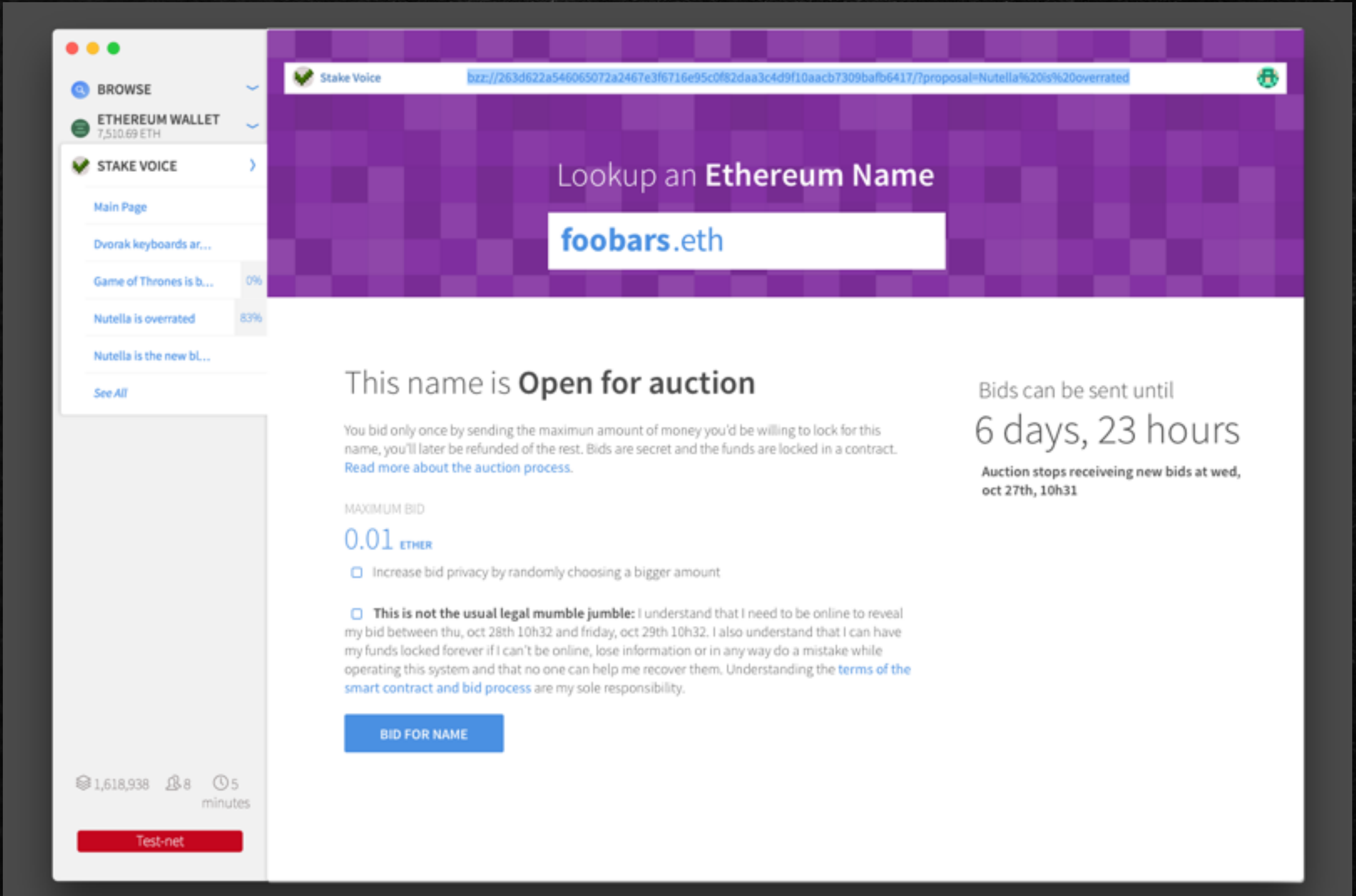
- Armazenamento decentralizado
- Pessoas armazenam dados da rede
- Sistema de incentivo, modelo econômico
- Em fase de integração com o ecossistema

Swarm

# Quebra-cabeças

- Banco de dados decentralizado
- Sites servidos via P2P
- Navegador

# Ethereum Naming System



bzz://263d622a546065072a2467e3f6716e95c0f82daa3c4d9f10aacb7309bafb6417/?proposal=Nutella%20is%20overrated

Lookup an **Ethereum Name**

**foobars**.eth

This name is **Open for auction**

You bid only once by sending the maximun amount of money you'd be willing to lock for this name, you'll later be refunded of the rest. Bids are secret and the funds are locked in a contract. Read more about the auction process.

MAXIMUM BID

0.01 ETHER

□ Increase bid privacy by randomly choosing a bigger amount

□ **This is not the usual legal mumble jumble:** I understand that I need to be online to reveal my bid between thu, oct 28th 10h32 and friday, oct 29th 10h32. I also understand that I can have my funds locked forever if I can't be online, lose information or in any way do a mistake while operating this system and that no one can help me recover them. Understanding the terms of the smart contract and bid process are my sole responsibility.

Bids can be sent until

6 days, 23 hours

**Auction stops receiveing new bids at wed, oct 27th, 10h31**

# Ethereum Naming System

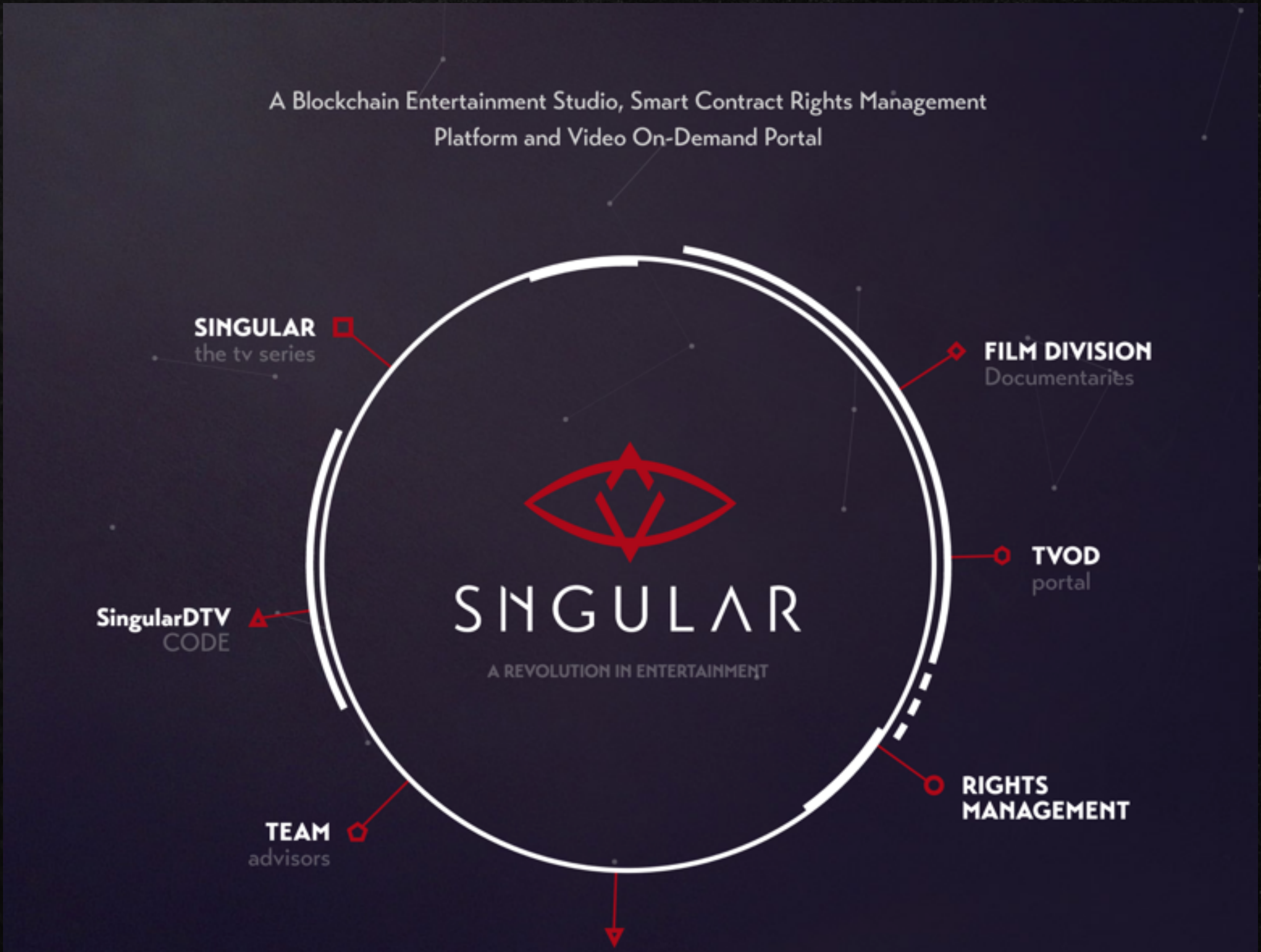
- Smart contract gerencia domínios
- Leilão - com regras apuradas
- Apontar para Swarm, Ethereum addresses, etc.
- 1$^{a}$ fase até o fim do ano

# Devcon

- Encontro anual de entusiastas Ethereum
- 2014 Berlin, 2015 London, 2016 Shanghai
- 700 pessoas

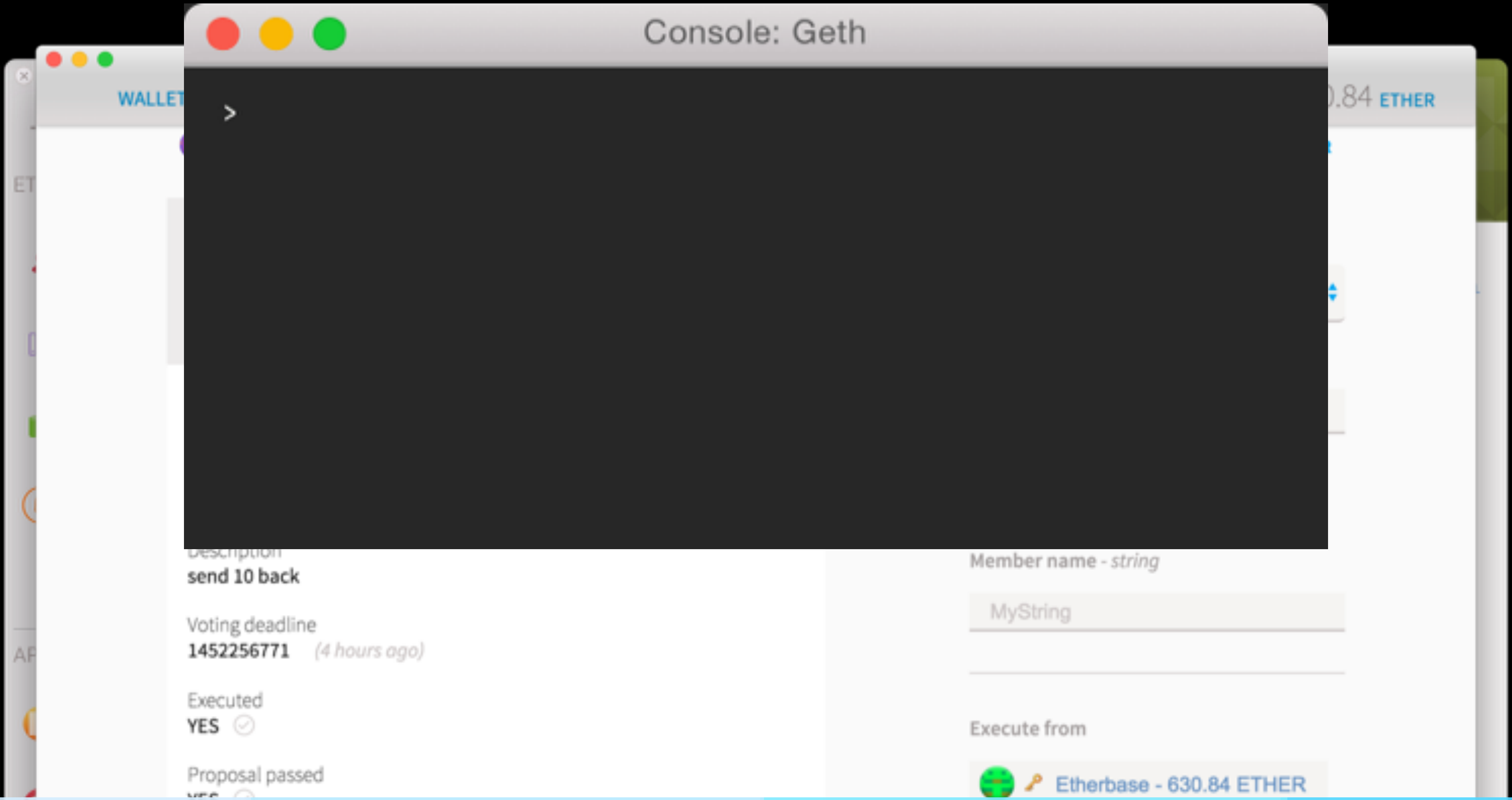
Devcon2 - Shanghai

# Projetos



A Blockchain Entertainment Studio, Smart Contract Rights Management Platform and Video On-Demand Portal

# Ethereum Milestones



```
>
```

Description
send 10 back

Voting deadline
1452256771 (4 hours ago)

Executed
YES

Proposal passed
YES

Number of votes
1

Current result
1

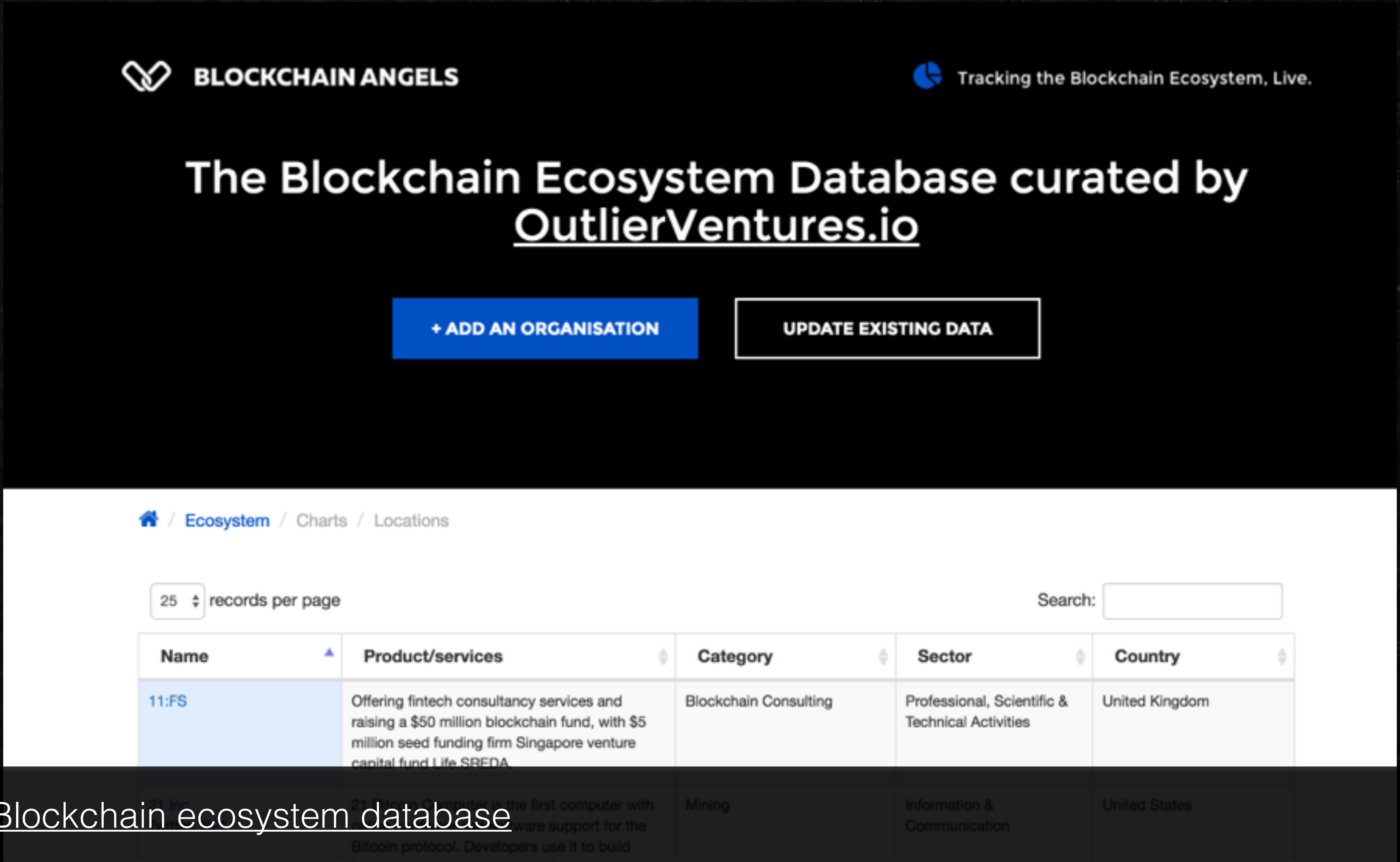
Proposal hash
0xd5cb9dac26ecd3757089d5c84f424baffffa3a2c237ca1501d249f3c

Member name - string
MyString

Execute from
Etherbase - 630.84 ETHER

| Fase 0 | Fase 1 | Fase 2 | Fase 3 |
|---|---|---|---|
| **Frontier** | **Homestead** | **Metropolis** | **Serenity** |
| **Desenvolvedores** | **Early adopters** | **Browser** | **Escalabilidade** |
| **mid-2015** | **early 2016** | **early 2017** | **2017** |

# Ecossistema



Tracking the Blockchain Ecosystem, Live.

The Blockchain Ecosystem Database curated by OutlierVentures.io

Ecosystem / Charts / Locations

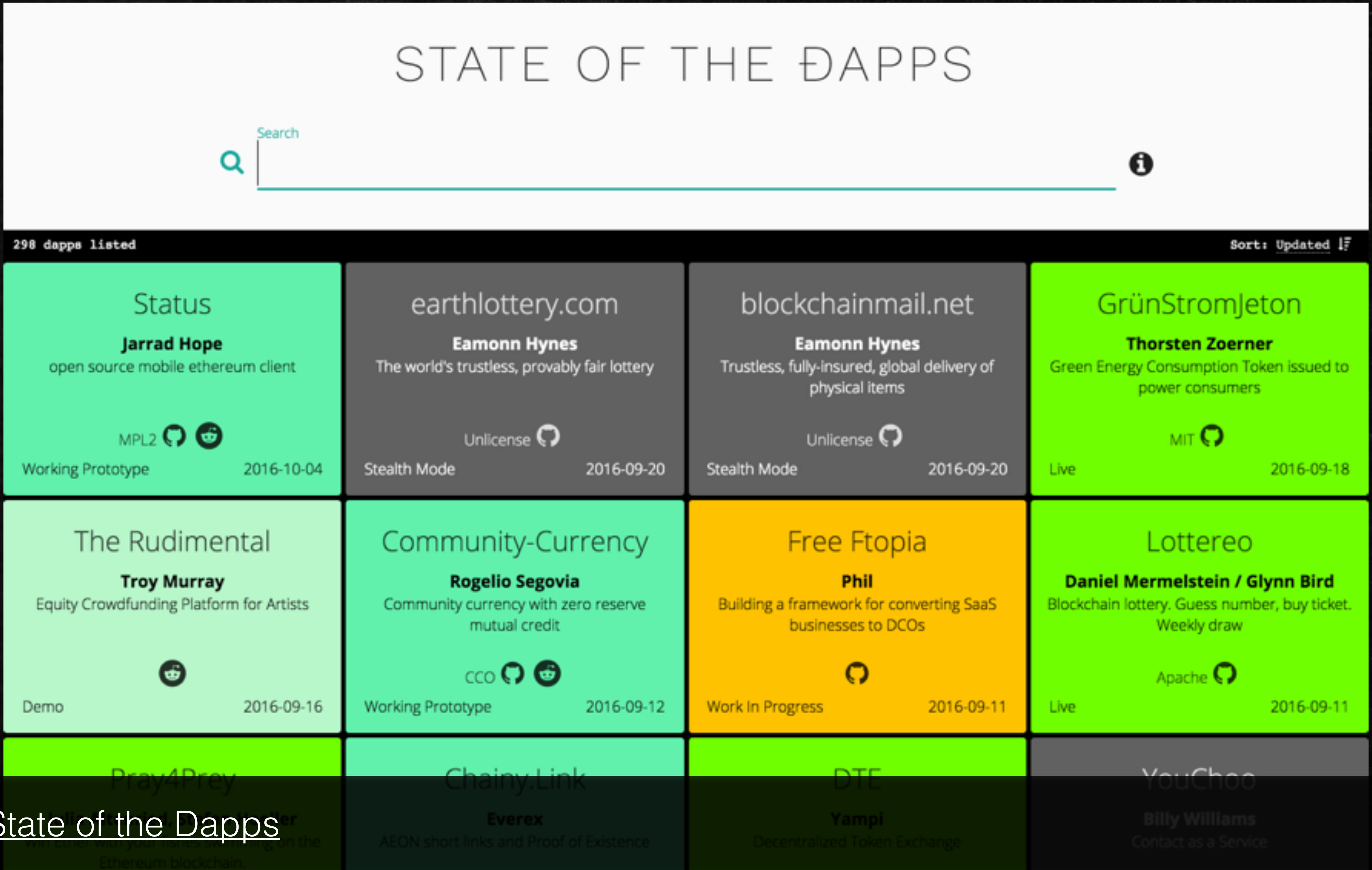
25 records per page

Search:

| Name | Product/services | Category | Sector | Country |
|---|---|---|---|---|
| 11:FS | Offering fintech consultancy services and raising a $50 million blockchain fund, with $5 million seed funding firm Singapore venture capital fund Life.SREDA. | Blockchain Consulting | Professional, Scientific & Technical Activities | United Kingdom |
| 21 Inc | 21 Bitcoin Computer is the first computer with ware support for the Bitcoin protocol. Developers use it to build | Mining | Information & Communication | United States |

Blockchain ecosystem database

# Ecossistema



STATE OF THE ÐAPPS

Search

298 dapps listed

Sort: Updated

**Status**
**Jarrad Hope**
open source mobile ethereum client
MPL2
Working Prototype 2016-10-04

**earthlottery.com**
**Eamonn Hynes**
The world's trustless, provably fair lottery
Unlicense
Stealth Mode 2016-09-20

**blockchainmail.net**
**Eamonn Hynes**
Trustless, fully-insured, global delivery of physical items
Unlicense
Stealth Mode 2016-09-20

**GrünStromJeton**
**Thorsten Zoerner**
Green Energy Consumption Token issued to power consumers
MIT
Live 2016-09-18

**The Rudimental**
**Troy Murray**
Equity Crowdfunding Platform for Artists
Demo 2016-09-16

**Community-Currency**
**Rogelio Segovia**
Community currency with zero reserve mutual credit
CCO
Working Prototype 2016-09-12

**Free Ftopia**
**Phil**
Building a framework for converting SaaS businesses to DCOs
Work In Progress 2016-09-11

**Lottereo**
**Daniel Mermelstein / Glynn Bird**
Blockchain lottery. Guess number, buy ticket. Weekly draw
Apache
Live 2016-09-11

**Pray4Prey**
**Julia Altenried, Stefan Hoeller**
Win ether with your fishes swimming on the Ethereum blockchain.

**Chainy.Link**
**Everex**
AEON short links and Proof of Existence

**DTE**
**Yampi**
Decentralized Token Exchange

**YouChoo**
**Billy Williams**
Contact as a Service

State of the Dapps

# Comunidade Ethereum

- 85.000 pessoas em 400 meetups
- 1.800 projetos públicos no Github
- Ecossistema brasileiro em ascenção

# Comunidade Ethereum

- Last-minute news: http://reddit.com/r/ethereum
- Technical updates: http://github.com/ethereum
- Announcements: twitter.com/ethereumproject

# UN Goals

1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS

UN Sustainable Development Goals

Everton Fraga
ev@ethereum.org

ethereum

Link icon by Hash Basheer from the Noun Project