

# ethereum

## And decentralized applications

LECTURER: ZVEZDIN BESARABOV

# Smart Contract Development with Solidity - януари 2018

▶ 25 януари 2018 ⌚ 9 седмици 🎓 6 кредита

ЛЕКТОР

Към лекторската администрация за курса

ВИЖ ПЪЛНА ИНФОРМАЦИЯ ЗА КУРСА

## ЗА КУРСА

- |    |  |    |  |
|----|--|----|--|
| 1  | RESOURCES  | 2  | COURSE OVERVIEW  |
| 3  | BLOCKCHAIN FUNCTIONALITY SUMMARY                                 | 4  | INTRODUCTION TO ETHEREUM AND SMART CONTRACTS. SET-UP FOR DEVELOPMENT |
| 5  | BASICS OF CONTRACTS: VARIABLES, FUNCTIONS AND CONTROL STRUCTURES | 6  | SOLIDITY DATA TYPES  |
| 7  | INHERITANCE AND MULTIPLE CONTRACTS                               | 8  | WORKING WITH CONTRACTS FROM APPLICATIONS: WEB3 API                   |
| 9  | OPTIMIZING CONTRACTS   | 10 | SECURITY IN CONTRACTS AND UNIT TESTING                               |
| 11 | WORKING ON THE PRACTICAL PROJECTS                                | 12 | FINAL PROJECT - LIVE DEFENSE   |

# Predicting digital asset market based on blockchain activity data

Zvezdin Besarabov

National School of Mathematics and Natural Sciences  
Sofia, Bulgaria  
me@zvezd.in

Todor Kolev

Comrade Cooperative  
Sofia, Bulgaria  
todor@comradecoop.com

## ABSTRACT

In our paper we explore how modern Deep Learning techniques can be applied to predict future facts about the Ethereum blockchain. Specifically, we are interested if blockchain's public raw data, such as the transaction count and the account balance distribution, can be used to predict other measures like the number of new accounts created and the market price per ETH token.

During a series of experiments, we achieved 330% lower error scores with blockchain data than an LSTM approach with trade volume data. By utilizing blockchain account distribution histograms, stacked dataset modeling, and a Convolutional architecture we reduced the error further by 35%.

Moreover, we have developed a reusable framework providing data gathering, processing, and storing functionality for performing Deep Learning experiments over blockchain data. Our future plans are towards automating neural network architecture and meta-parameter optimization tasks through training controller Machine Learning models on these tasks. Since the Ethereum network

not disclose the details needed to reproduce their results. Two more recent projects on Github also explore Bitcoin predictions [2] [19], however, both of them focus primarily on historical price data and did not reveal their data processing algorithms and neural architectures.

## 1.1 Project Goals

Our goal is to explore how modern Deep Learning techniques can be applied in estimating future facts about cryptoassets. More specifically we are interested in whether we can utilize the abundant blockchain data to improve our estimates.

We aim to create a flexible and open cryptocurrency prediction framework. The framework allows the collection of blockchain and financial data, and provides a way for a quick implementation of data processing and feature extraction algorithms. The extracted features (or properties) are compiled into a dataset using different modeling strategies. Custom neural architectures are built, trained, evaluated and compared on the output dataset. The prediction

# Plan for today

1. Introduction to Ethereum
2. Ethereum decentralized applications
  - Functionality, interface, key moments, pros/cons
3. Practical part
  - Hello world, Voting, ERC20 token
4. Dangers of decentralized applications
5. Historical events in Ethereum
  - Forks, DAO / Parity hack
6. Useful websites

# The centralization problem

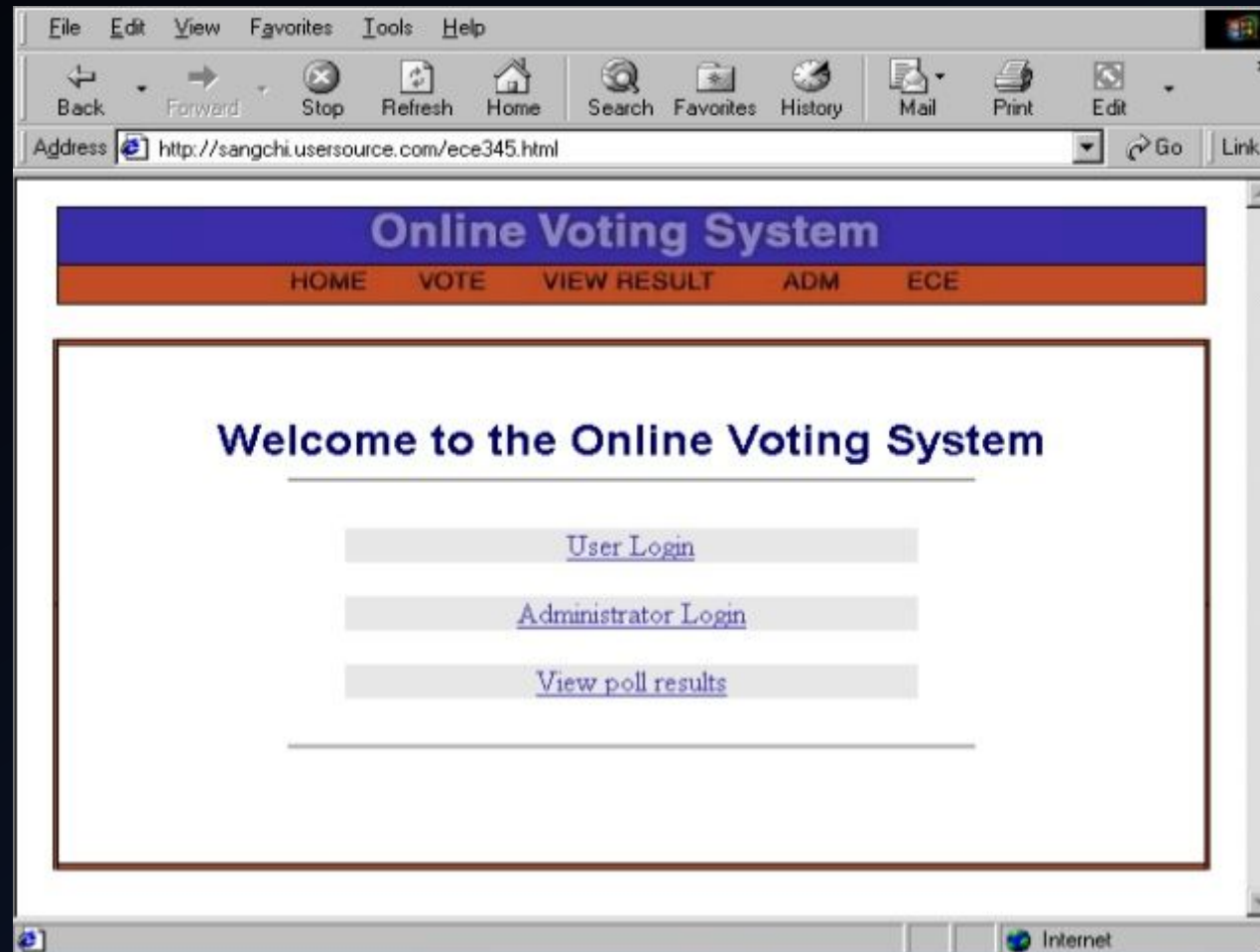


# Cryptocurrencies - lack of intermediary





# Centralized applications









ethereum

HOMESTEAD RELEASE

BLOCKCHAIN APP PLATFORM



# Ethereum

#	COIN	PRICE	24H	MKT CAP	LIQUIDITY	DEVELOPER	COMMUNITY	TOTAL	LAST 7 DAYS
1	 Bitcoin BTC	\$7,302.92	0.5%	\$125,966,102,842	\$4,703,050,094	98% ⓘ	88% ⓘ	91%	
2	 Ethereum ETH	\$286.43	-1.2%	\$29,152,026,385	\$2,153,484,268	95% ⓘ	71% ⓘ	83%	

\$1,750.00

\$1,500.00

\$1,250.00

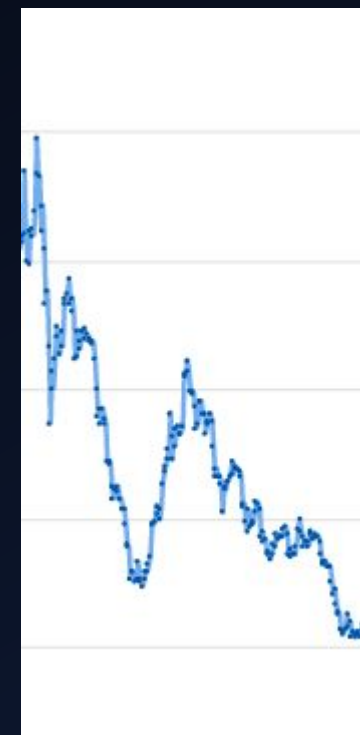
\$1,000.00

\$750.00

\$500.00

\$250.00

\$0.00



# Decentralized applications (contracts)

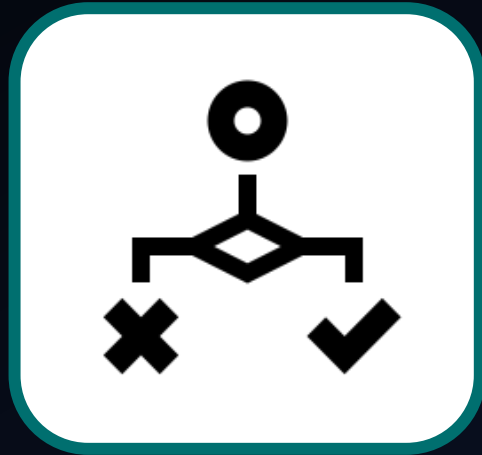
- Code on the blockchain (turing complete)
- Decentralized
- Autonomous
- Immutable
- No censorship, control
- „Contracts“



Abilities



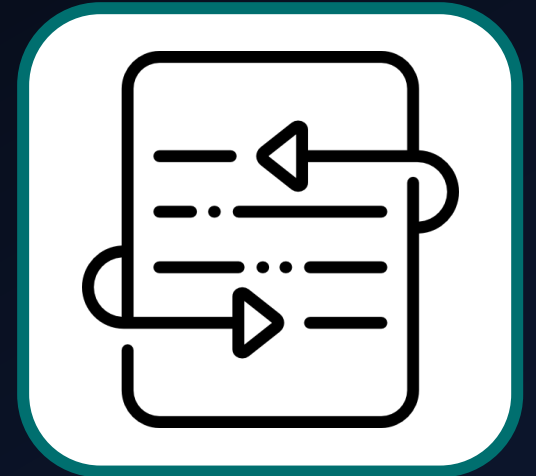
Data  
storage



Logic



ETH  
Balance



Multicontract  
interaction

## Method of execution



Execution is done on an **outside call**



Execution is a **transaction**



```

1 pragma solidity ^0.4.0;
2 contract Ballot {
3
4     struct Voter {
5         uint weight;
6         bool voted;
7         uint8 vote;
8         address delegate;
9     }
10    struct Proposal {
11        uint voteCount;
12    }
13
14    address chairperson;
15    mapping(address => Voter) voters;
16    Proposal[] proposals;
17
18    /// Create a new ballot with $( _numProposals ) different proposals.
19    function Ballot(uint8 _numProposals) public {
20        chairperson = msg.sender;
21        voters[chairperson].weight = 1;
22        proposals.length = _numProposals;
23    }
24
25    /// Give $(toVoter) the right to vote on this ballot.
26    /// May only be called by $(chairperson).
27    function giveRightToVote(address toVoter) public {
28        if (msg.sender != chairperson || voters[toVoter].voted) return;
29        voters[toVoter].weight = 1;
30    }
31
32    /// Delegate your vote to the voter $(to).
33    function delegate(address to) public {
34        Voter storage sender = voters[msg.sender]; // assigns reference
35        if (sender.voted) return;
36        while (voters[to].delegate != address(0) && voters[to].delegate != msg.sender)
37            to = voters[to].delegate;
38        if (to == msg.sender) return;
39        sender.voted = true;
40        sender.delegate = to;
41        Voter storage delegateTo = voters[to];
42        if (delegateTo.voted)
43            proposals[delegateTo.vote].voteCount += sender.weight;
44        else
45            delegateTo.weight += sender.weight;
46    }
47
48    /// Give a single vote to proposal $(toProposal).
49    function vote(uint8 toProposal) public {
50        Voter storage sender = voters[msg.sender];
51        if (sender.voted || toProposal >= proposals.length) return;
52        sender.voted = true;
53        sender.vote = toProposal;
54        proposals[toProposal].voteCount += sender.weight;
55    }
56
57    function winningProposal() public constant returns (uint8 _winningProposal) {
58        uint256 winningVoteCount = 0;
59        for (uint8 prop = 0; prop < proposals.length; prop++)
60            if (proposals[prop].voteCount > winningVoteCount) {
61                winningVoteCount = proposals[prop].voteCount;
62                _winningProposal = prop;
63            }
64    }
65 }

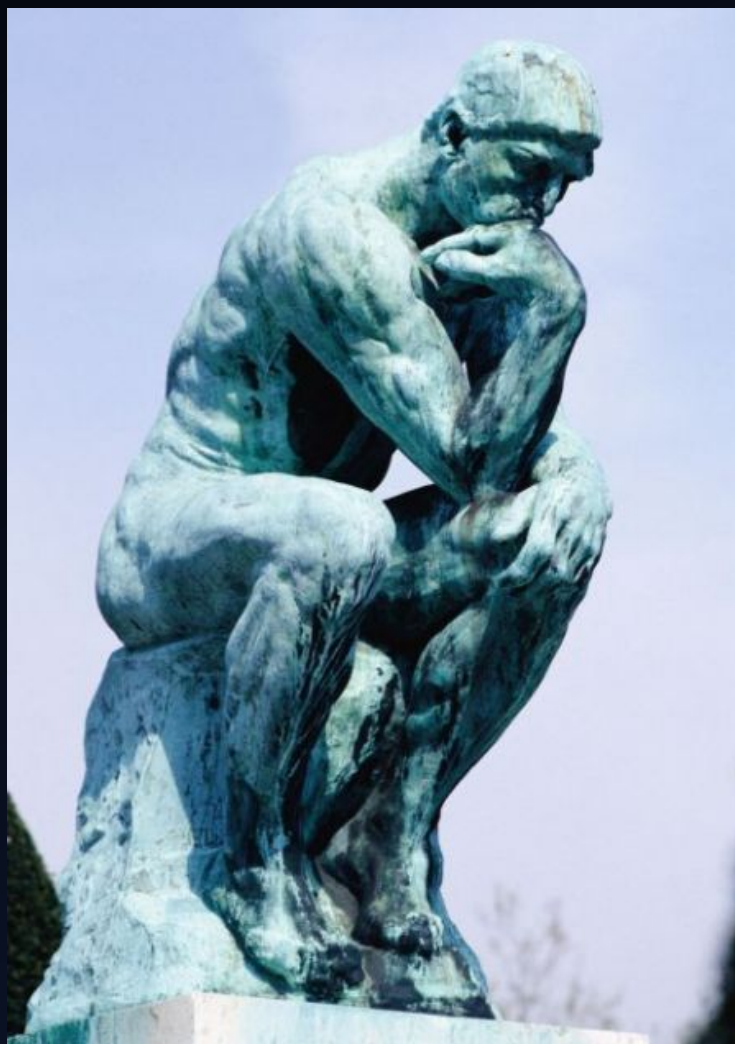
```

# Publicity

- Transactions, balances, activity
- Contract logic
- Data
- Accessibility
- Prone to attacks



Do you really need a crypto contract?





Practical part

## In short: pros

- Blockchain guarantee
  - 100% uptime
  - No censorship
  - Autonomy
  - Infinite life
- Accessibility
- Easy to develop \*
- Easy to use \*\*
- Like a law





## In short: cons

- Gas expenses
- Gas limit
- Publicity
- Blockchain limitations
  - No internet access



# Smart contract applications

- Voting
- Freedom of speech
- Social networks
- Crowdfunding
- ICOs



# WeTonomy

- Framework for cooperation and creation of cooperatives
- Based on consensus between members
- Rewards hard work



# Aeternity

- Better Ethereum
  - Better EVM + 2 languages
- Raised a lot from crowdfunding
- Strong bulgarian participation
- Created an incubator



# ICOs in a nutshell

- Crowdfunding of projects
- Public token sale





# Hotel Booking & Vacation Rental Marketplace With 0% Commissions

Blockchain Powered Marketplace & Technology, Where Hoteliers And Property Owners Can Rent Their Property Globally, Collect Money And Manage Bookings Without Paying Any Commissions To Middlemen

[Watch Video](#)

[One-Pager](#)

[WhitePaper](#)

## Token Sale Ends In:

28

days

1

hours

55

minutes

48

seconds

E-mail

[Buy LOC](#)



# MUST BUY ICO



Useless Ethereum Token

[About](#) [Contributing](#) [Token details](#) [FAQ](#) [Twitter](#) [GitHub](#)

## The world's first 100% honest Ethereum ICO.

---

You're going to give some random person on the internet money, and they're going to take it and go buy stuff with it. Probably electronics, to be honest. Maybe even a big-screen television.

Seriously, don't buy these tokens.

---



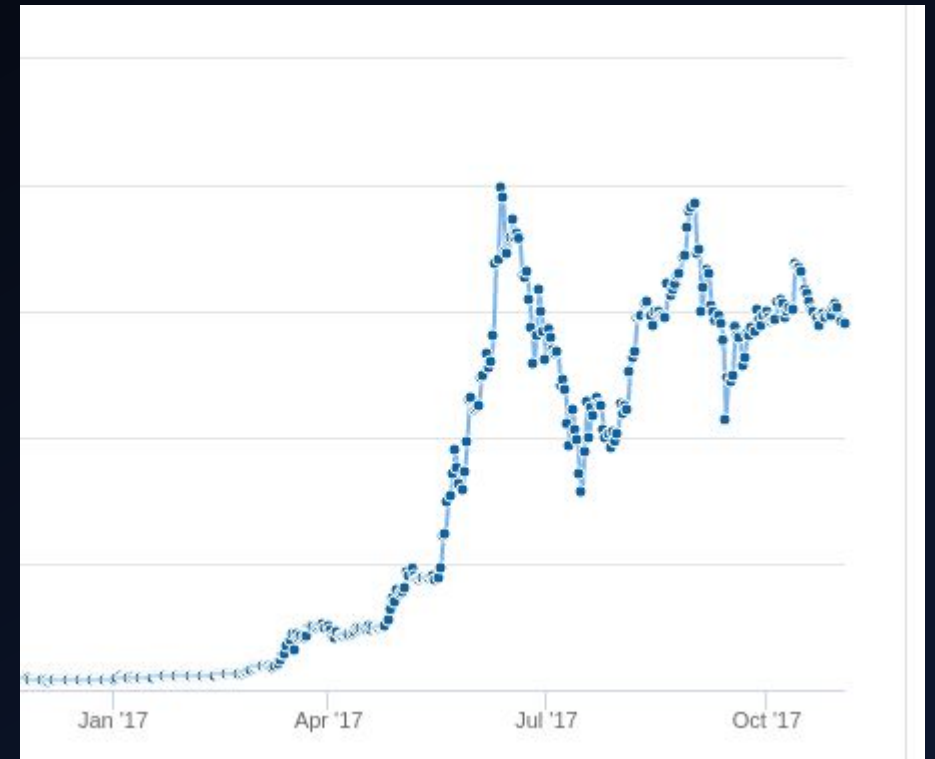
Reddit



Hacker News

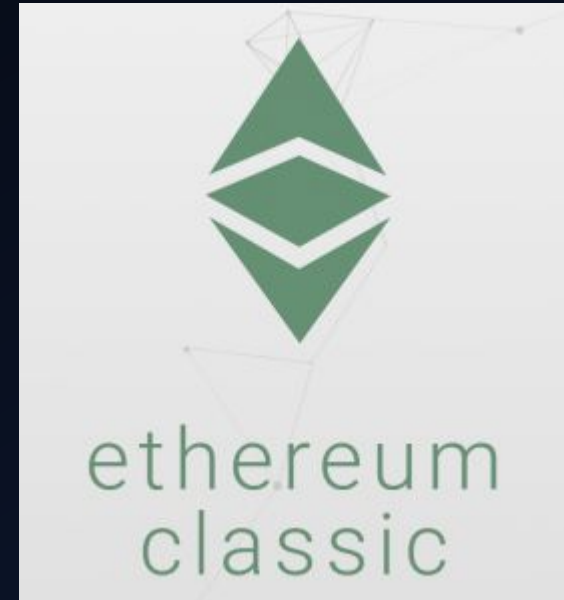
# Artificial ETH Price increase

- Speculative investment
- Boom of ICOs
- Bad for contracts
  - The main objective of Ethereum



# The DAO attack

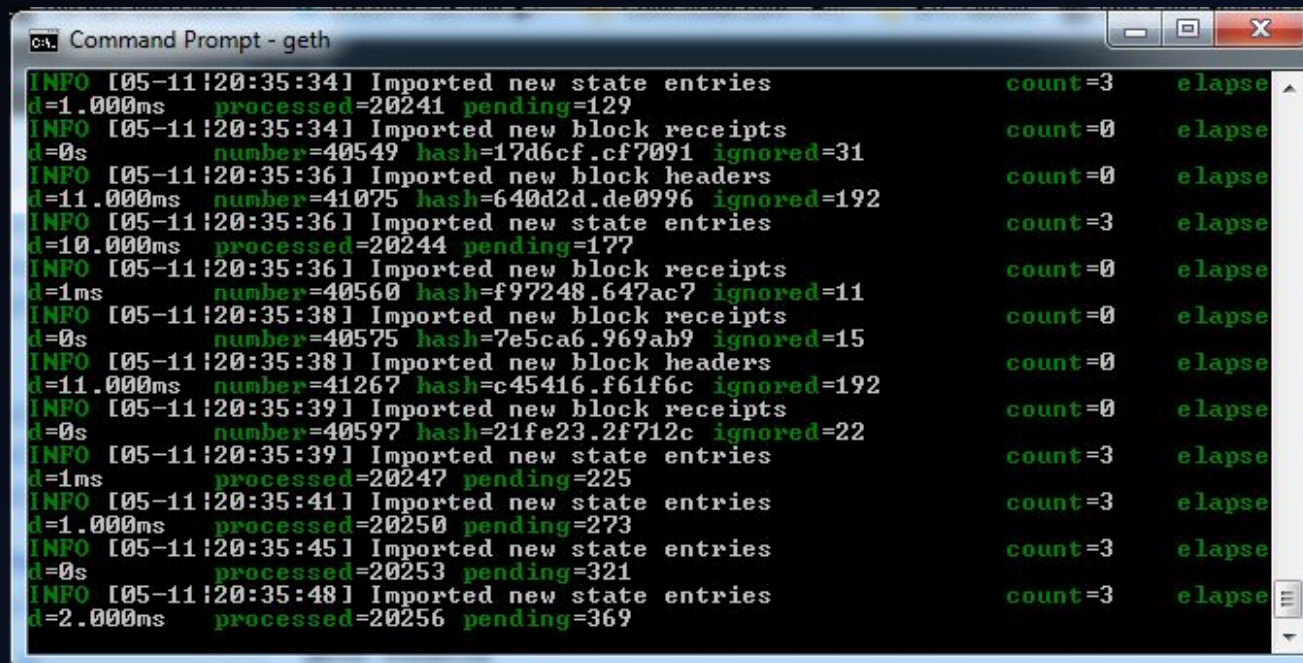
- June 17, 2016
- Vulnerability in the DAO
- Hacker drained \$53M
- Resulted in Hard fork
  - Split into Ethereum and Ethereum classic





# Sep 19, 2016 DOS attack

- Vulnerability in GETH
- Caused a global crash
- During devcon2



```
Command Prompt - geth
INFO [05-11:20:35:34] Imported new state entries          count=3    elapse
d=1.000ms    processed=20241 pending=129
INFO [05-11:20:35:34] Imported new block receipts          count=0    elapse
d=0s        number=40549 hash=17d6cf.cf7091 ignored=31
INFO [05-11:20:35:36] Imported new block headers          count=0    elapse
d=11.000ms   number=41075 hash=640d2d.de0996 ignored=192
INFO [05-11:20:35:36] Imported new state entries          count=3    elapse
d=10.000ms   processed=20244 pending=177
INFO [05-11:20:35:36] Imported new block receipts          count=0    elapse
d=1ms        number=40560 hash=f97248.647ac7 ignored=11
INFO [05-11:20:35:38] Imported new block receipts          count=0    elapse
d=0s        number=40575 hash=7e5ca6.969ab9 ignored=15
INFO [05-11:20:35:38] Imported new block headers          count=0    elapse
d=11.000ms   number=41267 hash=c45416.f61f6c ignored=192
INFO [05-11:20:35:39] Imported new block receipts          count=0    elapse
d=0s        number=40597 hash=21fe23.2f712c ignored=22
INFO [05-11:20:35:39] Imported new state entries          count=3    elapse
d=1ms        processed=20247 pending=225
INFO [05-11:20:35:41] Imported new state entries          count=3    elapse
d=1.000ms   processed=20250 pending=273
INFO [05-11:20:35:45] Imported new state entries          count=3    elapse
d=0s        processed=20253 pending=321
INFO [05-11:20:35:48] Imported new state entries          count=3    elapse
d=2.000ms   processed=20256 pending=369
```



# Parity Multi-sig wallet hack

- Jul 19, 2017
- Vulnerability in Parity's Multi-sig wallet
- 150,000 ETH Stolen (~\$30M at the time)
  - Never returned
- Aeternity suffered major loss

```
function() payable {  
  // just being sent some cash?  
  if (msg.value > 0)  
    Deposit(msg.sender, msg.value);  
  else if (msg.data.length > 0)  
    _walletLibrary.delegatecall(msg.data);  
}
```

# Upcoming Casper Update

- Future fork
- PoS consensus
- Sometime 2017?  
2018? 2019?
- GPU Mining obsolete



# Ethereum network statistics

[ethstats.net](https://ethstats.net)




























# State of the Dapps

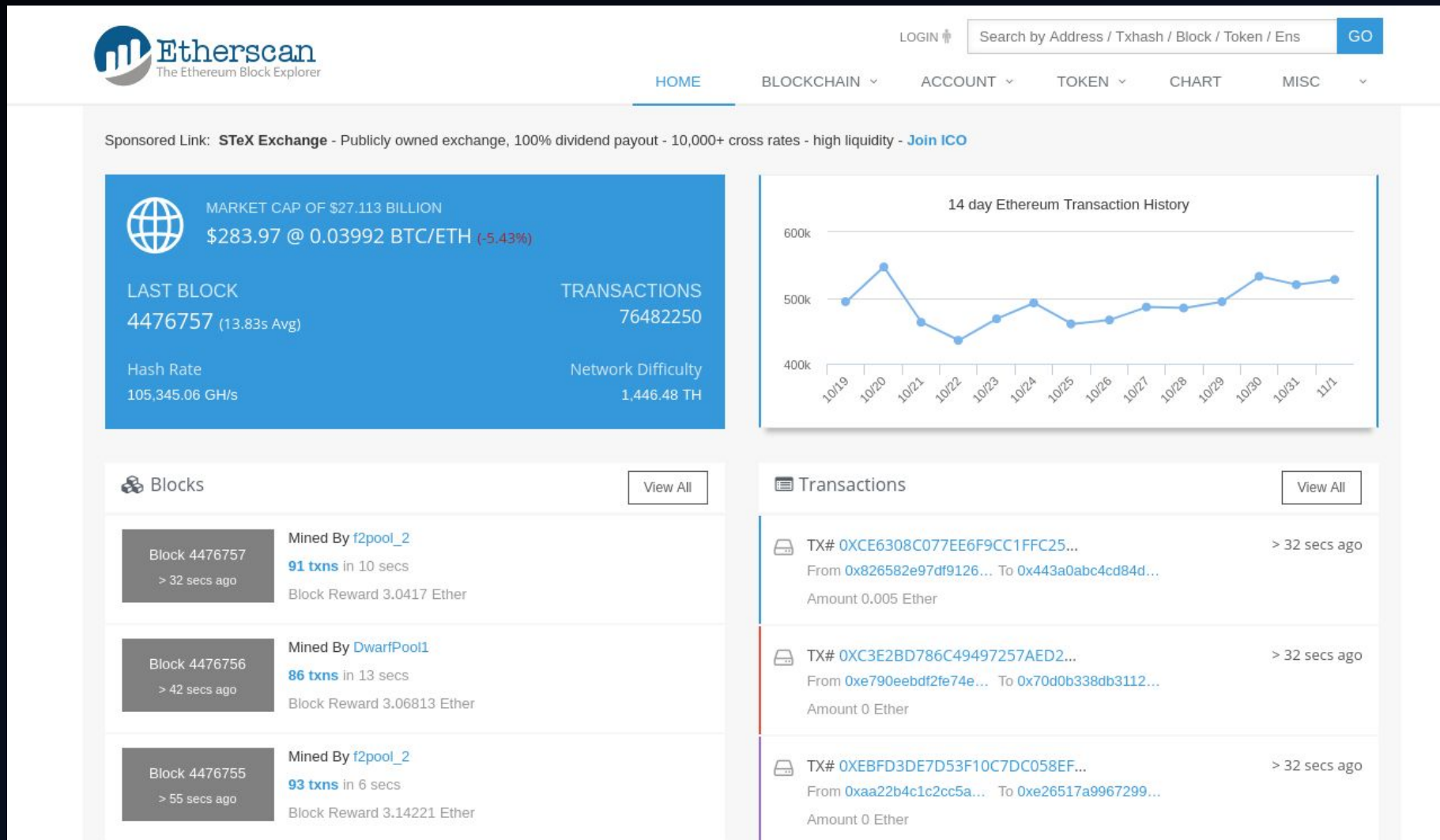
[dapps.ethercasts.com](https://dapps.ethercasts.com)

## STATE OF THE DAPPS

506 dapps listed

<div>WagETH</div> <div>josheth</div> <div>High stakes, high return king of the hill</div> <div></div> <div>Live2017-06-22</div>	<div>NVO</div> <div>Yanni Braggiu</div> <div>Decentralized Exchange</div> <div></div> <div>Work In Progress2017-06-21</div>	<div>FundRequest</div> <div>Karel Striegel</div> <div>Funding contributions to the open source community</div> <div></div> <div>Work In Progress2017-06-21</div>	<div>Ether.Camp</div> <div>Roman Mandeleil</div> <div>Blockchain explorer</div> <div></div> <div>Live2017-06-21</div>
<div>HitFin</div> <div>Patrick Salami</div> <div>OTC Derivatives Settlement</div> <div></div> <div>Demo2017-06-20</div>	<div>Vevue</div> <div>Thomas Olson</div> <div>Bringing Google Street View to life</div> <div></div> <div>Concept2017-06-20</div>	<div>PowerBall</div> <div>Peter Borah</div> <div>"Powerball"-style lottery</div> <div></div> <div>Work In Progress2017-06-20</div>	<div>cyber•Fund</div> <div>Dima Starodubcev</div> <div>Make digital investments comprehensible, accessible, easy and safe</div> <div></div> <div>Concept2017-06-20</div>
<div>Truffle</div> <div>Tim Coulter</div> <div>Development framework for Ethereum</div> <div></div> <div></div>	<div>TrustlessPrivacy</div> <div>sam@trustlessprivacy.com</div> <div>Interoperable electronic health records</div> <div></div> <div></div>	<div>ClimateCoin</div> <div>Dennis Peterson</div> <div>Coins for those who offset carbon</div> <div></div> <div></div>	<div>TimeBank</div> <div>Isaac Ibiapina</div> <div>Store Ether enforceably with a time lock</div> <div></div> <div></div>

# Etherscan.io



# Homework (1/2)

- Create a contract, that:
  - Holds a counter state variable (uint)
  - Has a function that will increment this counter by 1 only if called by the contract owner. If not, it should raise an exception.
  - Has a getter for the counter
  - Has overflow protection (don't hardcode anything related to the type please)



## Homework (2/2)

- Create a DDNS contract (Decentralized Domain Name System), that:
  - Has a method to buy a domain name (string type). The price is 1 ETH. A domain cannot be bought if it is already owned by someone
    - Look up how to send & accept ETH payments using smart contracts (or ask me if you're stuck)
  - Has a method to change/set the IP of a domain to a given value. Can only be called by the domain owner. For testing purposes, you can use regular integers instead of IP addresses.
  - Has a method to get the IP of a given domain.
  - Has a method that allows the contract owner to withdraw money collected in the contract's balance from domain purchases
  - For simplicity, domains cannot expire once they have been purchased.

# Homework (2/2) 2.0

- ...
  - BONUS: If you create and use your own cryptocurrency token for buying domains instead of ETH
  - BONUS: Write JS unit tests using the Truffle framework
- An example template of the DDNS contract can be found here:  
<http://termbin.com/oefb>

# Deadline

- You can email me your solutions (a git repository would be nice) at [git@zvezd.in](mailto:git@zvezd.in) until 23:59:59 at 7.09 (or later for -20% of max points)

## Helpful links

- Solidity documentation (Your bible): <https://solidity.readthedocs.io>
- <https://ethereum.stackexchange.com/> :)

[zvezdin@obecto.com](mailto:zvezdin@obecto.com)

