DevCon School

Технологии будущего

DevCon School
Технологии будущего

Знакомство с Ethereum Virtual Machine

Сергей Лоншаков
Blockchain разработчик, Airalab

Microsoft

Занимаюсь исследованиями/созданием:

- Bitcoin/Altcoin/криптовалютных проектов с 2011.
- Smart contract/Ethereum проектов с 2014.
- DAO (децентрализованных автономных организаций) с 2015.
- Проектов в области децентрализованного интернета вещей с использованием технологии Blockchain с осени 2015 года.

Цели

Децентрализованный компьютер Ethereum

Разберемся в абстрактном представлении Ethereum Virtual Machine

Анатомия умного контракта

Изучим внутреннее содержание умного контракта с точки зрения EVM

Инструменты и примеры DAO

Узнаем об основных клиентах сети Ethereum и примерах популярных сценариев применения умных контрактов

Децентрализованный компьютер Ethereum

#msdevcon

DevCon School
Технологии будущего

Определение Ethereum Virtual Machine

Абстрактно: часть протокола, которая фактически обрабатывает внутреннее состояние хранилища и выполняет вычисления называется Ethereum Virtual Machine (сокр. EVM)

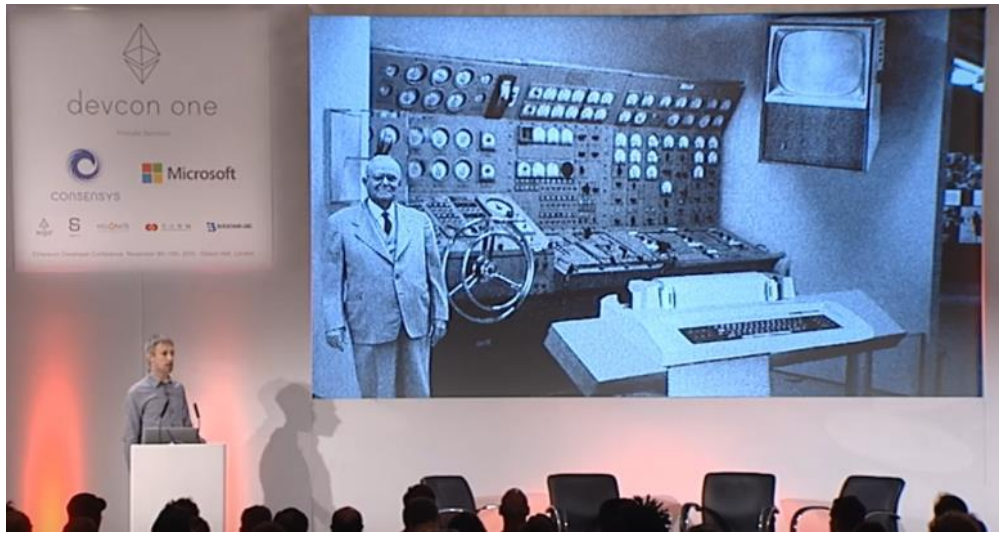
В СМИ: EVM можно рассматривать как децентрализованный компьютер, содержащий миллионы объектов, называемые "аккаунты", которые имеют возможность поддерживать / изменять внутреннюю базу данных, выполнять код и общаться друг с другом.

Среди разработчиков: Разработчики могут создавать особый вид приложений - DApp, работающие на децентрализованном компьютере (EVM) с помощью дружественных языков программирования смоделированных на основе существующих языков, таких как JavaScript и Python ..


ethereum

Децентрализованный компьютер, O_o

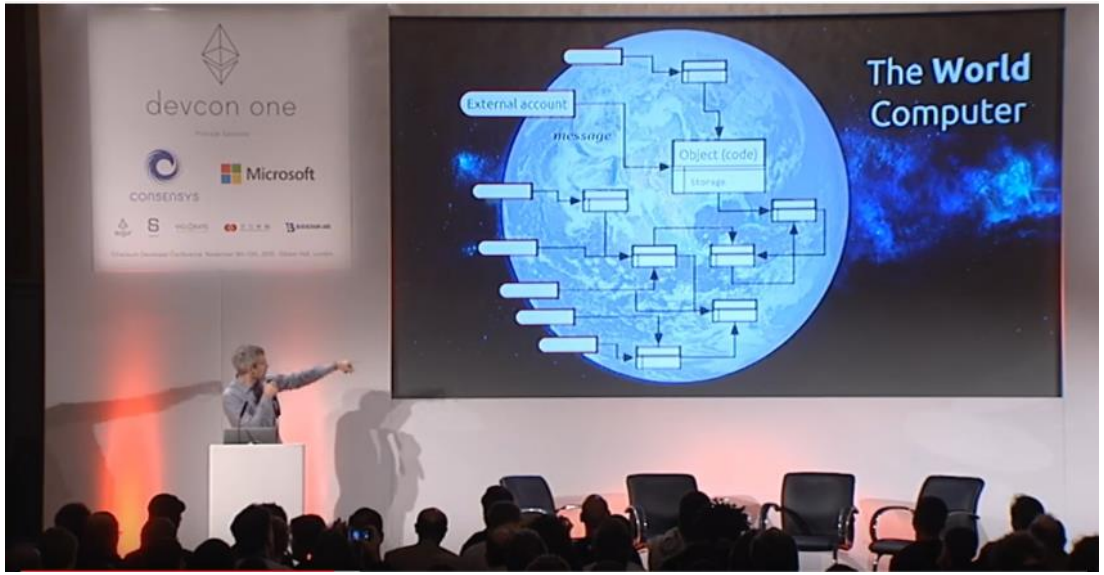
- Код исполняется в 5 - 100 раз медленнее, чем скомпилированный для локального запуска.
- Стоимость использования вычислений, памяти и хранилища примерно на уровне 1950-х годов.
- Информация может быть изменена в первые 60с после получения информации от подключенных узлов.



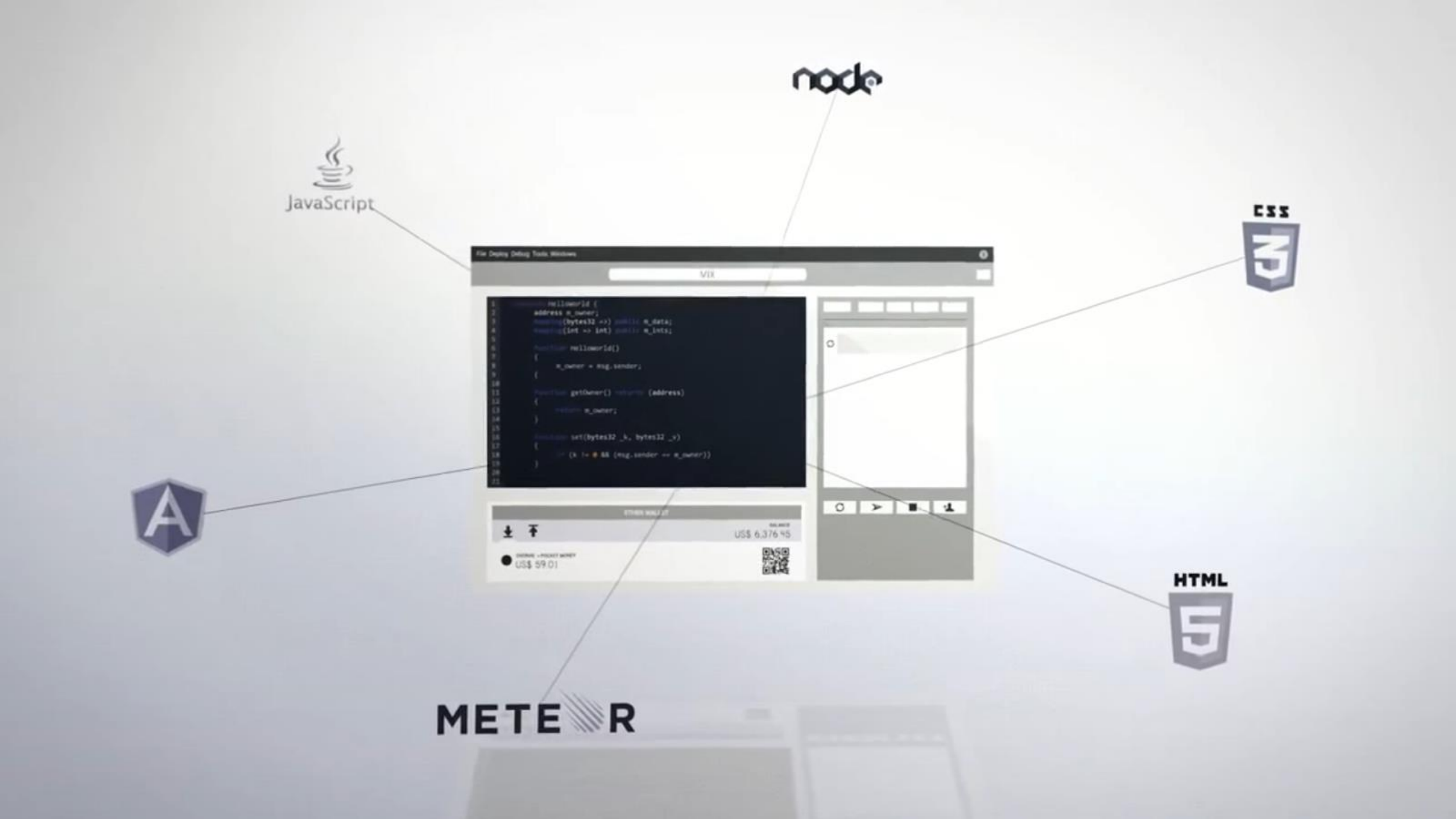
EVM - это не очень хороший компьютер, он медленный и очень очень дорогой.
Dr. Gavin Wood, devcon1, 2015 год

Децентрализованный компьютер, Yep

- Это действительно единый мировой компьютер для всей планеты и навсегда.
- Не может быть остановлен и не зависит от государств и корпораций в работе.
- EVM - вездесущий, доступный повсюду, где есть интернет.



Можно найти на Youtube по запросу: DEVCON1: Ethereum for Dummies - Dr. Gavin Wood


node
JavaScript
CSS
HTML
METEOR

Ethereum Virtual Machine и Тьюринг полнота

- Формально EVM может выполнить любое вычисление, которое возможно выполнить, включая бесконечные циклы.
- Поддержка Тьюринг полных языков программирования Solidity (from Javascript), Serpent (from Python), LLL (from Lisp)

Ethereum Virtual Machine и умные контракты

Есть два типа аккаунтов в Ethereum:

Аккаунт пользователя (Externally owned account сокр. EOAs): учетная запись контролируемая закрытым ключом, и если у вас есть закрытый ключ, связанный с EOA у вас есть возможность отправлять эфиры и сообщения от EOA.

Контракт: учетная запись, которая имеет свой собственный код, и управляемая с помощью кода.

Анатомия умного контракта: bytecode

- Контракты живут в Ethereum Blockchain в бинарном формате (EVM bytecode).
- Контракты, как правило, создаются на языке высокого уровня (Solidity), компилируются в машинно-независимый код низкого уровня (bytecode) из исходного кода.
- Bytecode загружается в Ethereum Blockchain с помощью отправки транзакции специального вида “Создание контракта” в сеть обычным клиентом сети.

Анатомия умного контракта: abi

- Abi - Application Binary Interface – Бинарный интерфейс приложения.
- Abi контракта не хранится в Blockchain.
- Abi контракта генерируется при компиляции контракта и может быть передано в готовой форме пользователю или “зашито” в коде DApp.

Анатомия умного контракта: gas

- Gas - это метрика для мирового компьютера Ethereum (EVM).
- Чем больше вычислений и использования хранилища, тем больше требуется газа.
- Gas не равно Fee. Fee = Amount of gas * gasPrice

Анатомия умного контракта: gas

- Каждая операция в EVM требует определенное количество газа.
- В любой момент времени известен gasLimit в сети.
- Если транзакция не помещается в gasLimit (Out of Gas), она не будет выполнена, но fee будет снято с отправителя.
- Майнер, нашедший блок может изменить gasLimit +/- 0.0976 % для следующего блока.

```
contract = eth.compile.solidity(source).test
{ code: '605280600c6000396000f3006000357c010000000000000000000000000000000000000000000000000090048063
         c6888fa114602e57005b6037600436041565b8060005260206000f35b60006007820290506004d565b91905056',
         info: {
                  language: 'Solidity',
                  languageVersion: '0',
                  compilerVersion: '0.9.13',
                  abiDefinition: [{
                           constant: false,
                           inputs: [{
                                    name: 'a',
                                    type: 'uint256'
                                    } ],
                           name: 'multiply',
                                    outputs: [{
                                    name: 'd',
                                    type: 'uint256'
                                    } ],
                           type: 'function' } ],
                           userDoc: {
                                    methods: {
                                             }
                           },
                           developerDoc: {
                                    methods: {
                                             }
                           },
                  source: 'contract test { function multiply(uint a) returns(uint d) { return a * 7; } }'
                  }
         }
```

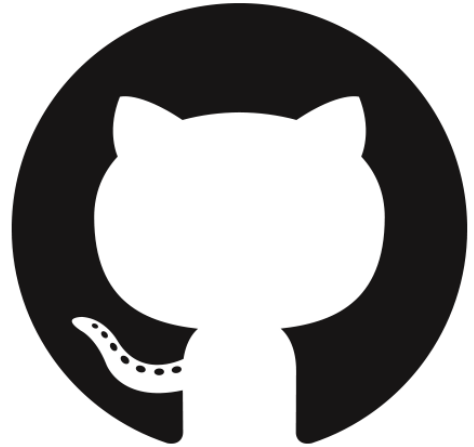
Инструменты для работы с Ethereum Blockchain

#msdevcon

DevCon School
Технологии будущего

Geth

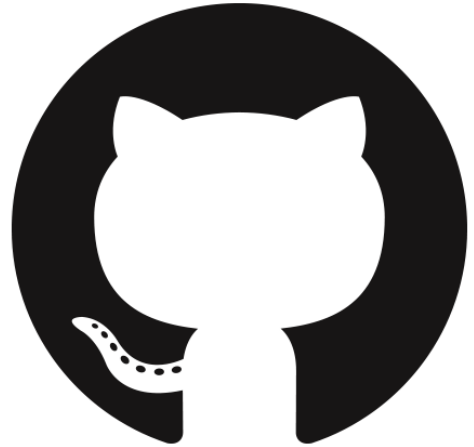
- Geth это интерфейс командной строки для запуска полного узла Ethereum Blockchain.
- Реализован на языке Go.
- Является основным результатом работы Frontier Release.
- Выпущено 106 релизов начиная с 8 февраля 2014 года.



/ethereum/go-ethereum

Geth: interfaces & API

- Javascript Console.
- web3 JavaScript Dapp API
- JSON RPC API
- JSON-RPC server.
- Command line options.



/ethereum/go-ethereum

```
contract = eth.compile.solidity(source).test
{ code: '605280600c6000396000f3006000357c010000000000000000000000000000000000000000000000000090048063
         c6888fa114602e57005b6037600436041565b8060005260206000f35b60006007820290506004d565b91905056',
         info: {
                  language: 'Solidity',
                  languageVersion: '0',
                  compilerVersion: '0.9.13',
                  abiDefinition: [{
                           constant: false,
                           inputs: [{
                                    name: 'a',
                                    type: 'uint256'
                                    } ],
                           name: 'multiply',
                                    outputs: [{
                                    name: 'd',
                                    type: 'uint256'
                                    } ],
                           type: 'function' } ],
                           userDoc: {
                                    methods: {
                                             }
                           },
                           developerDoc: {
                                    methods: {
                                             }
                           },
                  source: 'contract test { function multiply(uint a) returns(uint d) { return a * 7; } }'
                  }
         }
```

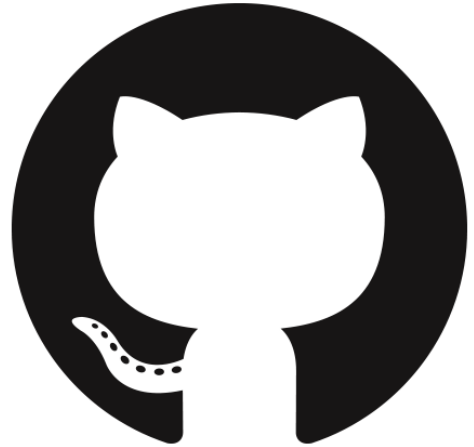
Отправляем контракт в сеть

```
(1) primaryAddress = eth.accounts[0];

(2) MyContract = eth.contract(abi);

(3) contact = MyContract.new(arg1, arg2, ...,{from: primaryAddress, data: evmCode});
```

```
(4) MyContract.new([arg1, arg2, ...,]{from: primaryAccount, data: evmCode},
    function(err, contract) { if (!err && contract.address) console.log(contract.address); });
```

Parity

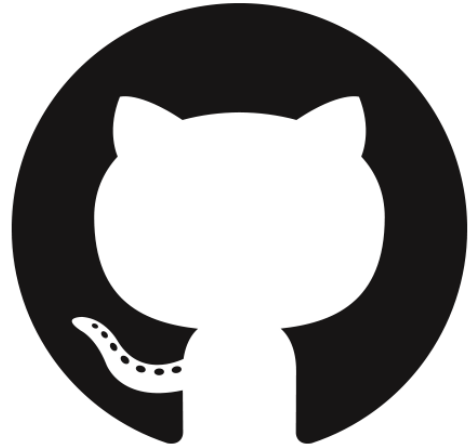
- Parity это интерфейс командной строки для запуска полного узла Ethereum Blockchain.
- Реализован на языке Rust.
- Является разработкой команды Ethcore, Гевина Вуда.
- Выпущено 35 релизов начиная с 8 февраля 2016 года.



/ethcore/parity

Parity: interfaces & API

- Parity имеет режим совместимости с geth.
  Parity --geth
- JSON RPC API
- parity JavaScript Dapp API (+web3)
- web3 JavaScript Dapp API



/ethereum/go-ethereum

Ethereumj

- ethereumj - Java implementation of the Ethereum protocol.
- The Java library that can be embedded in any Java project
- Является разработкой команды Hack.ether.camp.
- Выпущено 25 релизов начиная с 15 сентября 2014 года.

/ethereum/ethereumj

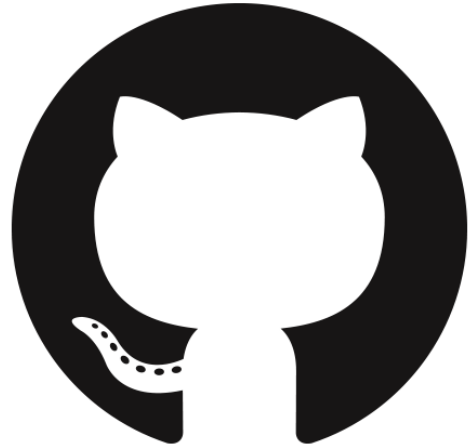
Ethereum Wallet & Mist

- Использует geth как протокол общения с сетью Ethereum.
- The Mist - это браузер для запуска DApp, работающих с web3 JavaScript Dapp API
- Ранние релизы.
- Платформа написания: Meteor + Electron.

/ethereum/mist

MetaMask

- Плагин для браузера Google Chrome, позволяющий запускать DApp без полной ноды на клиенте.
- Общается с полной нодой через JSON RPC API.
- Ранние релизы.
- Написан на Javascript

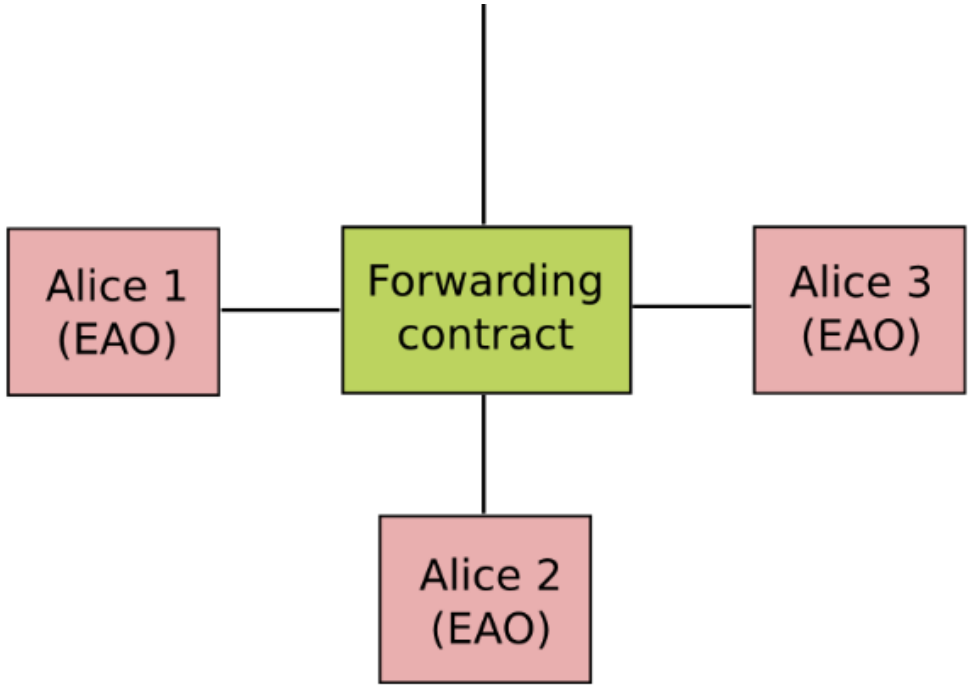


/MetaMask/metamask-plugin

Примеры DAO

Умный кошелёк, multisig

1. Полная свобода в проектировании кошелька .
2. Автономность^2 = автономная ценность на счету автономного кода.
3. Банк?



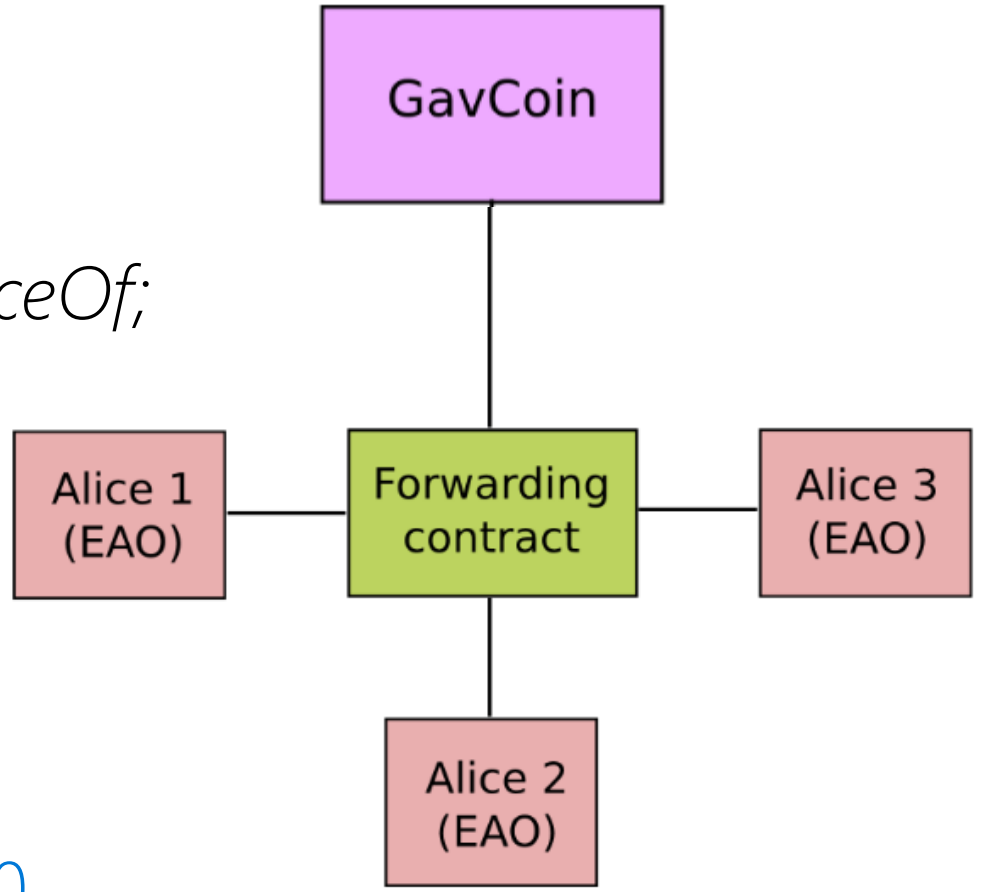
Токены

contract MyToken {

/ This creates an array with all balances */*

mapping (address => uint256) public balanceOf;

}

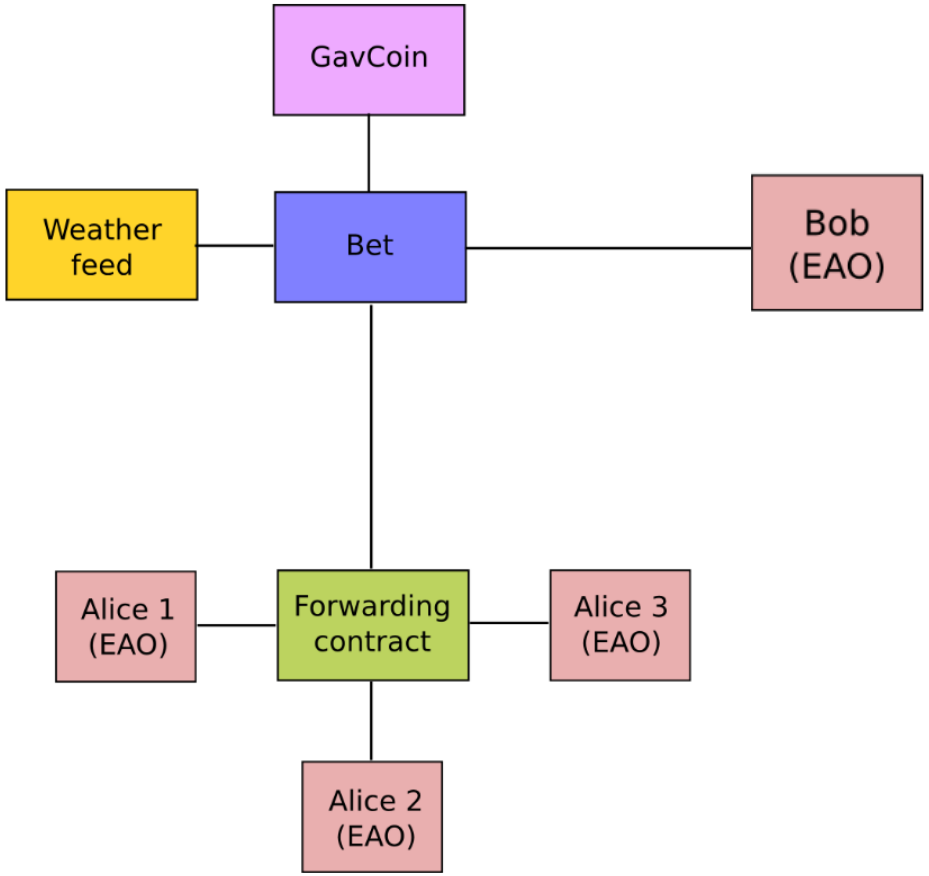


Описание стандарта ERC20:
https://github.com/ethereum/EIPs/issues/20

Управление взаимоотношениями

1. Конгресс / Совет директоров /Демократия
2. Escrow / Аккредитив
3. p2p + Страхование / Кредитование / Финансирование

Управление взаимоотношениями



Alice и Bob заключают пари на 100 GavCoin с триггером на основе данных о температуре в Москве.

Если температура в Москве не будет выше 35 градусов в течении года, то Bob получит 100 GavCoin, иначе их получит Alice.

Первая среда для прямых экономических взаимоотношений человек – робот, робот - робот

Q&A

Знакомство с Ethereum Virtual Machine

Сергей Лоншаков, sergeylonshakov@gmail.com

#msdevcon

DevCon School
Технологии будущего