



Москва переходит на блокчейн. Обзор реализованных проектов

Кирилл Поляков,
Руководитель блокчейн проектов, ДИТ Москвы



Проблематика

Задачи бизнеса -

1. Протестировать новую технологию
2. Применить блокчейн в услугах и сервисах города, имеющих недоверие со стороны жителей для решения выявленных проблем

Разработчики разрабатывают блокчейн

Задача юристов - запустить проекты в рамках правового поля и обеспечить связанность с внутренними регламентами

АКТИВНЫЙ гражданин

Проект «Активный гражданин» — площадка для проведения открытых референдумов в электронной форме, созданная по инициативе Правительства Москвы в 2014 году.

- Количество активных пользователей 2 млн. человек
- Объем вопросов - проведено более 3 214 голосований
- Принято 91,6 млн. мнений граждан
- Проект отмечен наградой Smart Cities Awards-2015



АГ: Правовая модель

Как мы блокчейн проект АГ вводим в правовое поле:

- Не храним перс. данные
- Не осуществляем начисление баллов
- Исследование применимости и первый пилот осуществлялся в результате НИОКР

Хранение данных пользователей:

- Связка персональных данных и УИП пользователя на закрытом сервере в защищенном контуре ЦОД ДИТ
- Хранение в блокчейн только УИП

Баллы АГ: Валюта или нет?

Валюта!

1. За голосование по городским вопросам житель получает в среднем 20 баллов
2. На полученные баллы он может купить вознаграждение
(например за 1200 баллов пополнить
Тройку на 175 рублей)

А вот и нет!

1. Нельзя использовать как платежное средство.
2. Нельзя передать 3-м лицам.
3. Нет механизма вывода в расчетную единицу РФ (Рубли)

Ярмарки выходного дня

—услуга, позволяющая фермерам получить бесплатное место на ярмарке выходного дня. Для участия фермер подаёт заполненную заявку через портал mos.ru

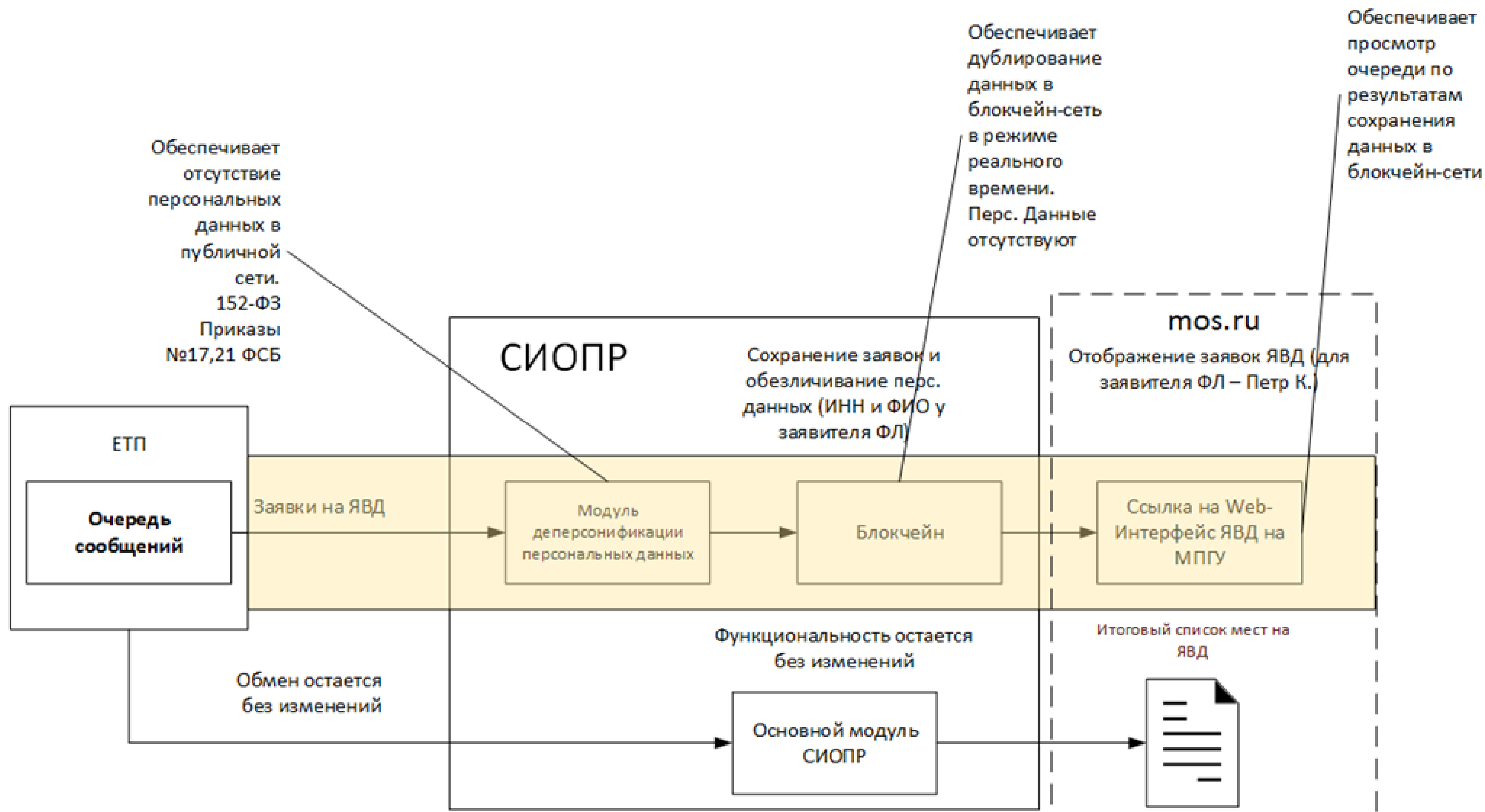
Проблемы сервиса

1. Доверие участников в правильности зафиксированного времени подачи заявки (таймстэмп)
2. Проблема доверия к алгоритму расчета заявок
3. Высокая нагрузка в момент подачи заявок - 60 тыс заявок за заявочную кампанию.

Решение

Внедрён блокчейн дублирующим слоем для фиксации времени подачи заявок, самих заявок и итогового списка мест

Ярмарки: схема технического решения





Развилки по ярмаркам

Через какие развилки решений мы прошли:

1. Хранение персональных данных внутри блокчейна целиком или сокращёнными
2. ГИС или не ГИС

Наши решения:

1. Отсутствие перс. данных. Не нужно сертифицировать систему.
2. Отсутствие ГОСТ криптографии - невозможность получить статус ГИС.

Блокчейн - часть существующей системы.



ГИС “Распределенный реестр”

Плюсы создания:

- Высокое доверие к данным
- Хранение разносортных данных

Преграды создания

- Невозможность хранить персональные данные
- Отсутствие ГОСТ криптографии
- Отсутствие регулирования

Итого: наша позиция - не создавать ГИС на данном этапе правового регулирования и развития блокчейн.



Взаимодействие с внешними узлами

Каждый пользователь может скачать копию блокчейна себе на компьютер и контролировать все что происходит внутри системы.

Нужна ли регистрация пользователя?

Пользователь не хранит персональных данных других граждан. Прав на создание каких-либо объектов нет.

Нужна ли оферта?

Используем опенсорс-программный продукт на основе GNU GPL.

Blockchain

Проект реализован на платформе Ethereum, работающей на базе смарт-контрактов, разработанной в 2015 году. Разработчиком платформы является некоммерческая организация, целью которой является предоставление возможностей платформы для реализации решений разработчиков.

- Приватный блокчейн
- Оболочка платформы Parity
- Решение реализовано на открытом исходном коде
- Язык программирования Solidity
- Алгоритм консенсуса Proof-of-authority



Зачем?



П. Польза

1

Повысить доверие жителей к городской услуге
Возможность проверить неизменность. Следить за голосованием онлайн.

2

Пилотный проект. Сбор мнений профессионального сообщества
на GitHub и других ресурсах

3

Это первое в мире высоконагруженное голосование в государственном секторе

4

Перспективы внедрения в другие государственные услуги
- Запись на ярмарки выходного дня
- Проект Росреестра и ЕГРН

Р. Результаты

всего голосований в блокчейне - 2045

нагрузка - 860 тыс. голосов в сутки

среднесуточная нагрузка 1,3 голоса в секунду

максимальный % от предельной пропускной способности - 12,34%

64 копии кода на GitHub

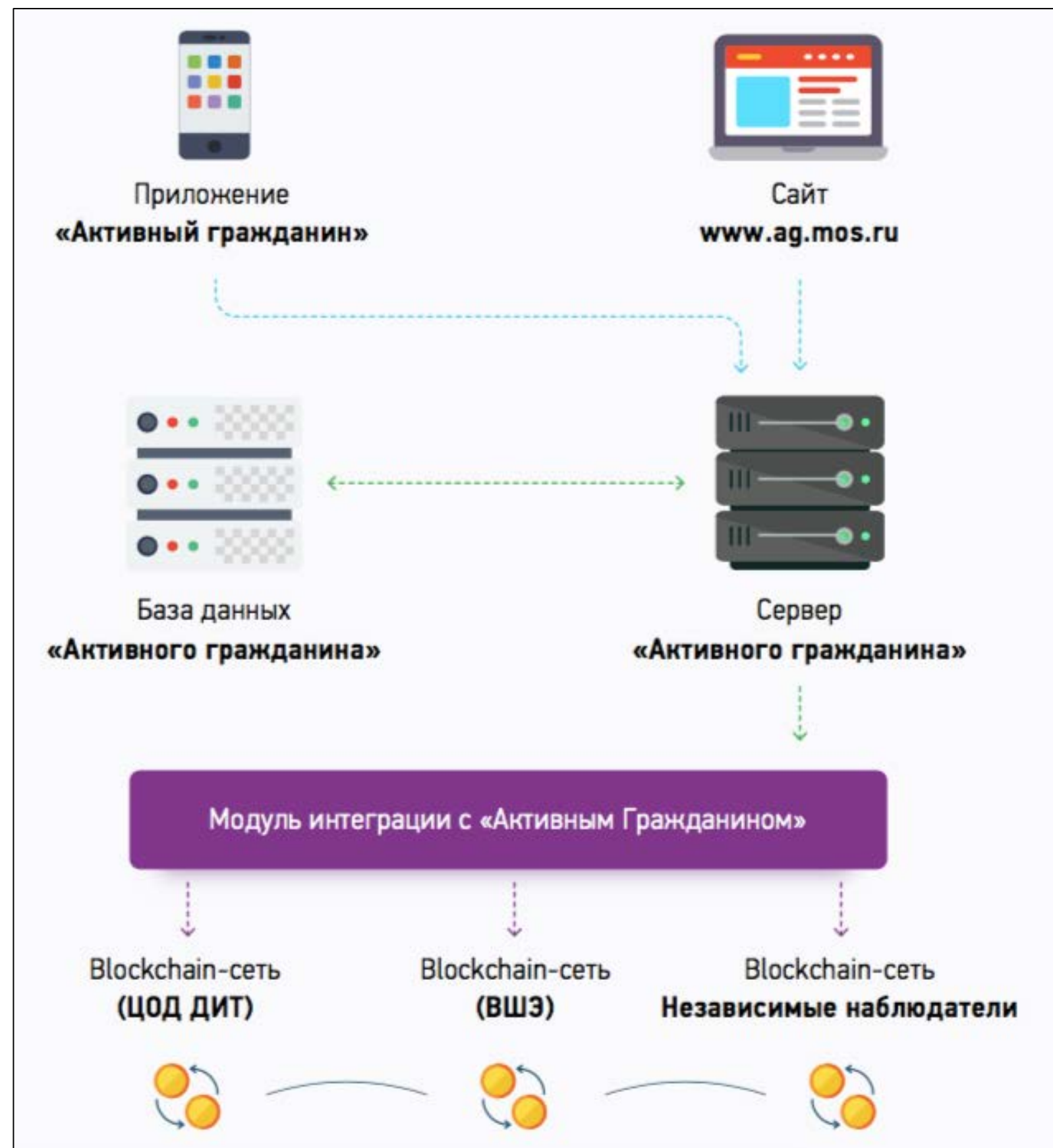
развернуто под независимых наблюдателей - 145








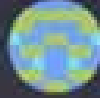

Как?



Архитектура

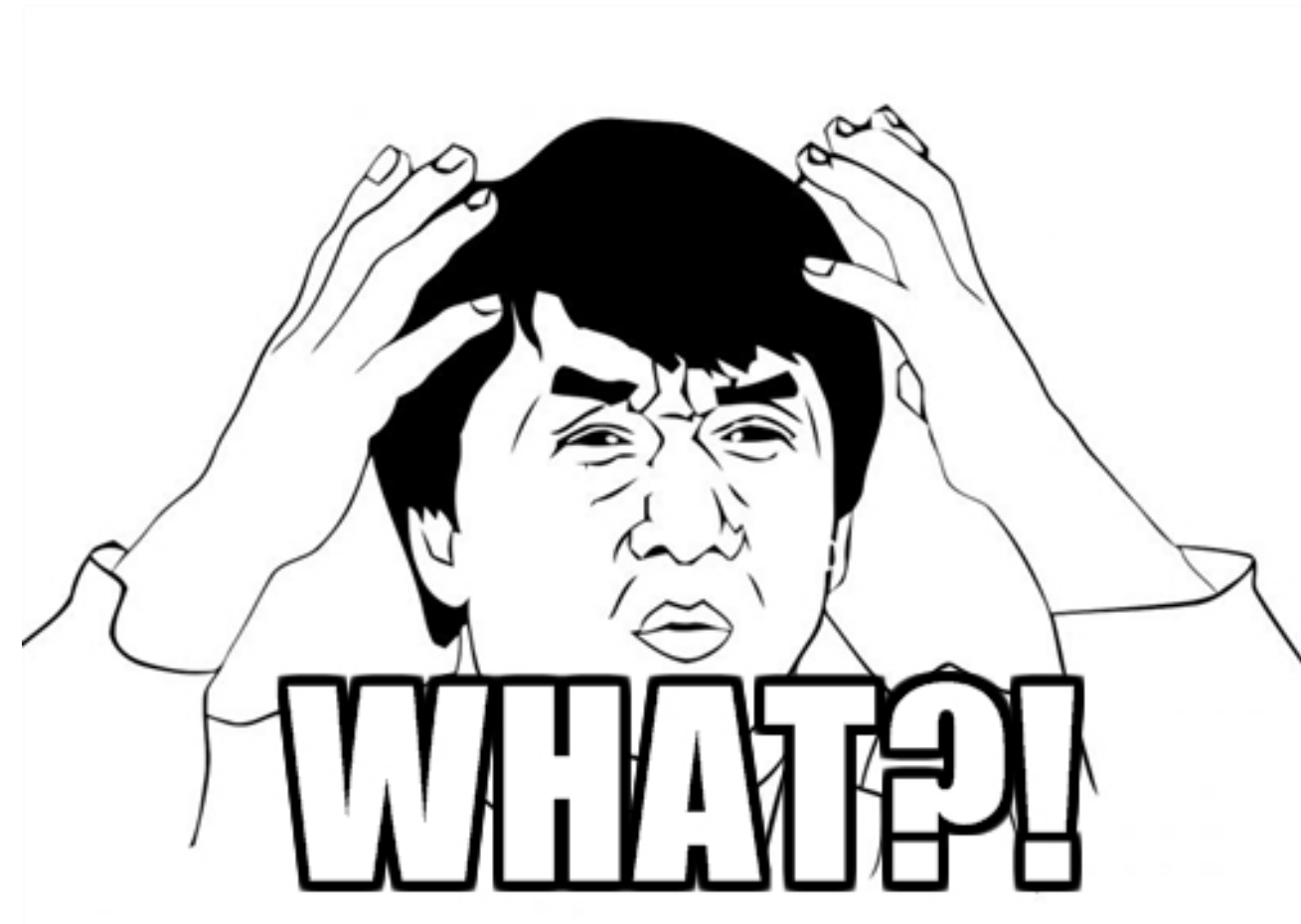
- Приватный блокчейн Ethereum
- Оболочка платформы - Parity
- Открытый исходный код
- Язык программирования - Solidity
- Алгоритм консенсуса Proof-of-authority



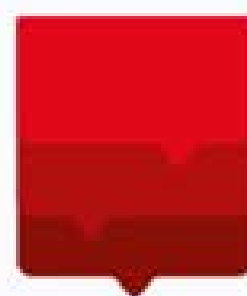
 <p>КАТАЛОГ ОПРОСОВ 0xFDb76D8aAF371bF5C7122f6f1104458440454FBB1</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3236 0xf8a020D5A8337D8885A6cb1f6c63007b586799122</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3236 ВОПРОС 1 0x801a7bcA411953Fc807Faa8AFe5cc5d3D8b6b8E1</p> <p>← 0.000 ETH</p>
 <p>ГОЛОСОВАНИЕ 3237 0x118837bED60e842D9F74bE7c821E74C76dA5098B</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3237 ВОПРОС 1 0x7C041C33dDe100C736271D2682A90997Aeb6E392</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3240 0x7b5720Fcb1c35E072F1a8e2bf20AC159b73aF159</p> <p>← 0.000 ETH</p>
 <p>ГОЛОСОВАНИЕ 3240 ВОПРОС 1 0x59578954A96C1023733485915b83d81a8E24538D</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3241 0x319Fa17a03EeD57936aC600D0dA5F6f535c3E10</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3241 ВОПРОС 1 0x689415A7c158D8d1f8Ff69c2Aca4c63586C88Def</p> <p>← 0.000 ETH</p>
 <p>ГОЛОСОВАНИЕ 3242 0x4C38951A39357315E02a6E23b4330aDcC94df36d</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3242 ВОПРОС 1 0xDA0EB854864d33980860039a119E615897e22A96</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3243 0xCcB025598d1BcE13c3CC885606d81eA5616c2d4f</p> <p>← 0.000 ETH</p>
 <p>ГОЛОСОВАНИЕ 3243 ВОПРОС 1 0x538e50d8aaa800161494c93Ad70F83CFd144c169</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3244 0x60C6f90b522CC29b3D835274269bc45De7793d09</p> <p>← 0.000 ETH</p>	 <p>ГОЛОСОВАНИЕ 3244 ВОПРОС 1 0xc5Ee1A5ADD511402e1fCEe36727D26F69188CC7B</p> <p>← 0.000 ETH</p>

Наши любимые вопросы

1. Это криптовалюта?
2. Если я скачаю себе ноду, я буду майнить? Могу намайнить себе баллов?
3. Мои персональные данные теперь хранятся у майнеров?
4. А какой закон регулирует криптовалюты и блокчейн?



Всегда на связи!



ДИТ



www.twitter.com/emoskva



www.dit.mos.ru



www.facebook.com/SmartMoscow



Telegram
t.me/kirznau