Анализ транзакций и контрактов

Сергей Недашковский
Blockchain Data Scientist

Зачем анализировать данные цепочки

- Понять какие транзакции совершаете и с какими адресами взаимодействуете
- Проверить достоверность информации о проекте, кто владеет и участвует в проекте
- Оценить риски блокировок и заморозки средств в контрактах
- Определить стадию развития блокчейна

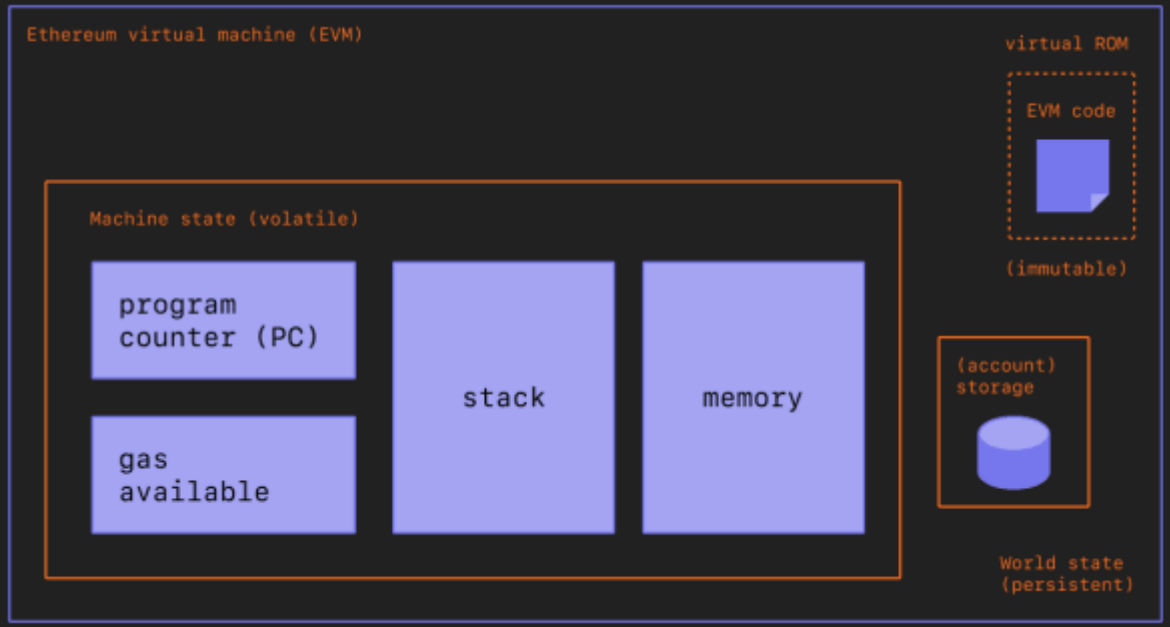
Базовые понятия

- Ethereum Virtual Machine
- Транзакция
- Контракт

tinyurl.com/4we2sf35

Ethereum Virtual Machine (EVM)

Единый глобальный 256-битный компьютер, в котором исполняются транзакции и хранится состояние сети



ethereum.org/en/developers/docs/evm

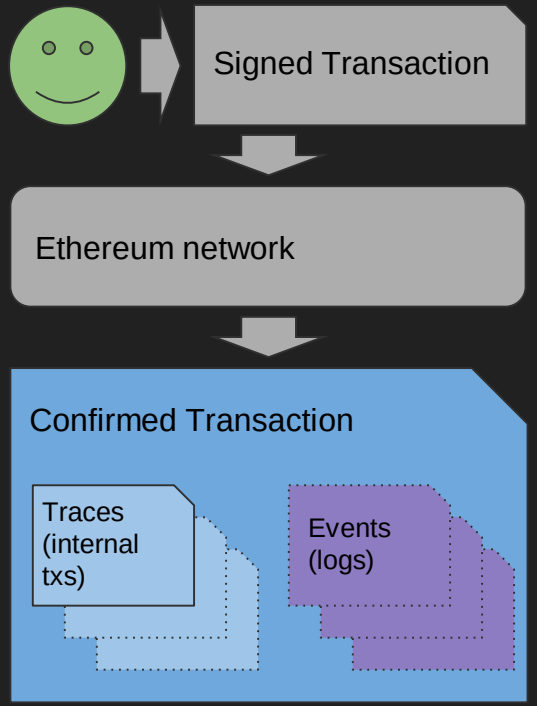
Что такое транзакция (transaction, tx)

Криптографически подписанная аккаунтом инструкция для атомарного изменения состояния сети.

Транзакции могут быть исполнены или отклонены.

Транзакция состоит из одного или более шага (trace), двух типов:

- вызов функций (call)
- создание контракта (create)



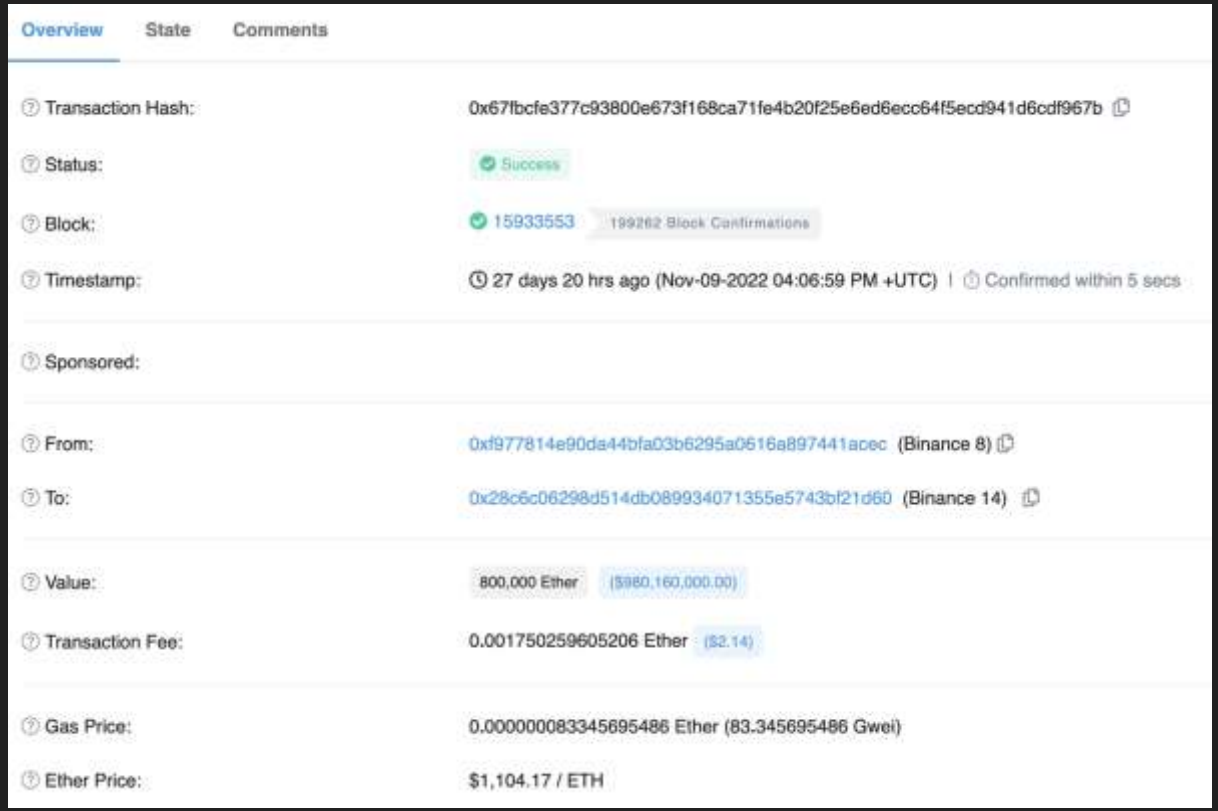
ethereum.org/en/developers/docs/transactions

Самая большая транзакция в ноябре 2022

etherscan.io/tx/0x67fbcfe377c93800e673f168ca71fe4b20f25e6ed6ecc64f5ecd941d6cdf967b

tinyurl.com/2p9d5yew

Самая большая транзакция в феврале 2022



Контракт. Создание

Программа, исполняемая в виртуальной машине блокчейна (ex. EVM)

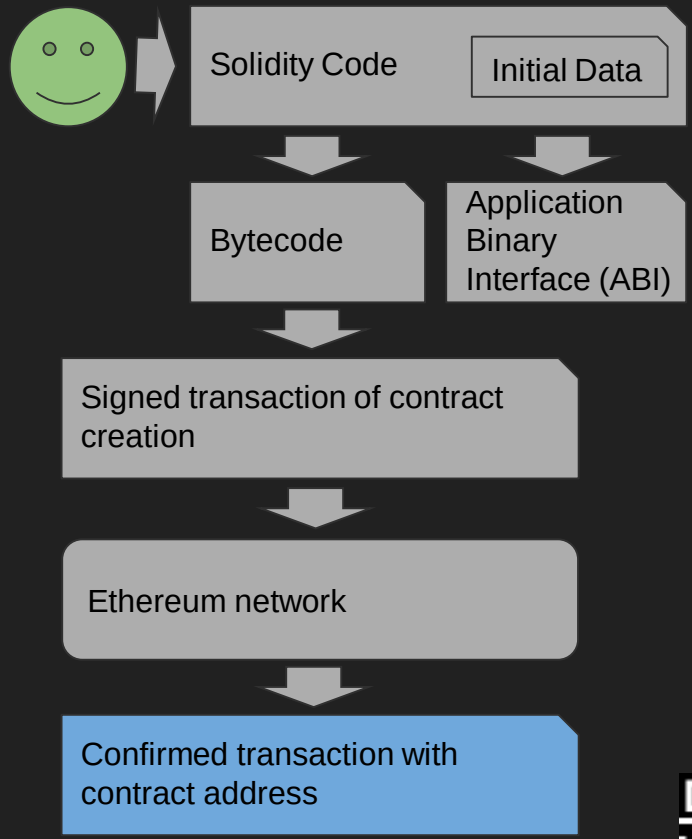
Контракт может быть создан:

- Отправкой транзакции с байт-кодом контракта
- Вызовом функции контракта-фабрики

Initial Data - набор начальных параметров контракта

Bytecode - код исполняемый в виртуальной машине

ABI - инструкции по взаимодействию с контрактом



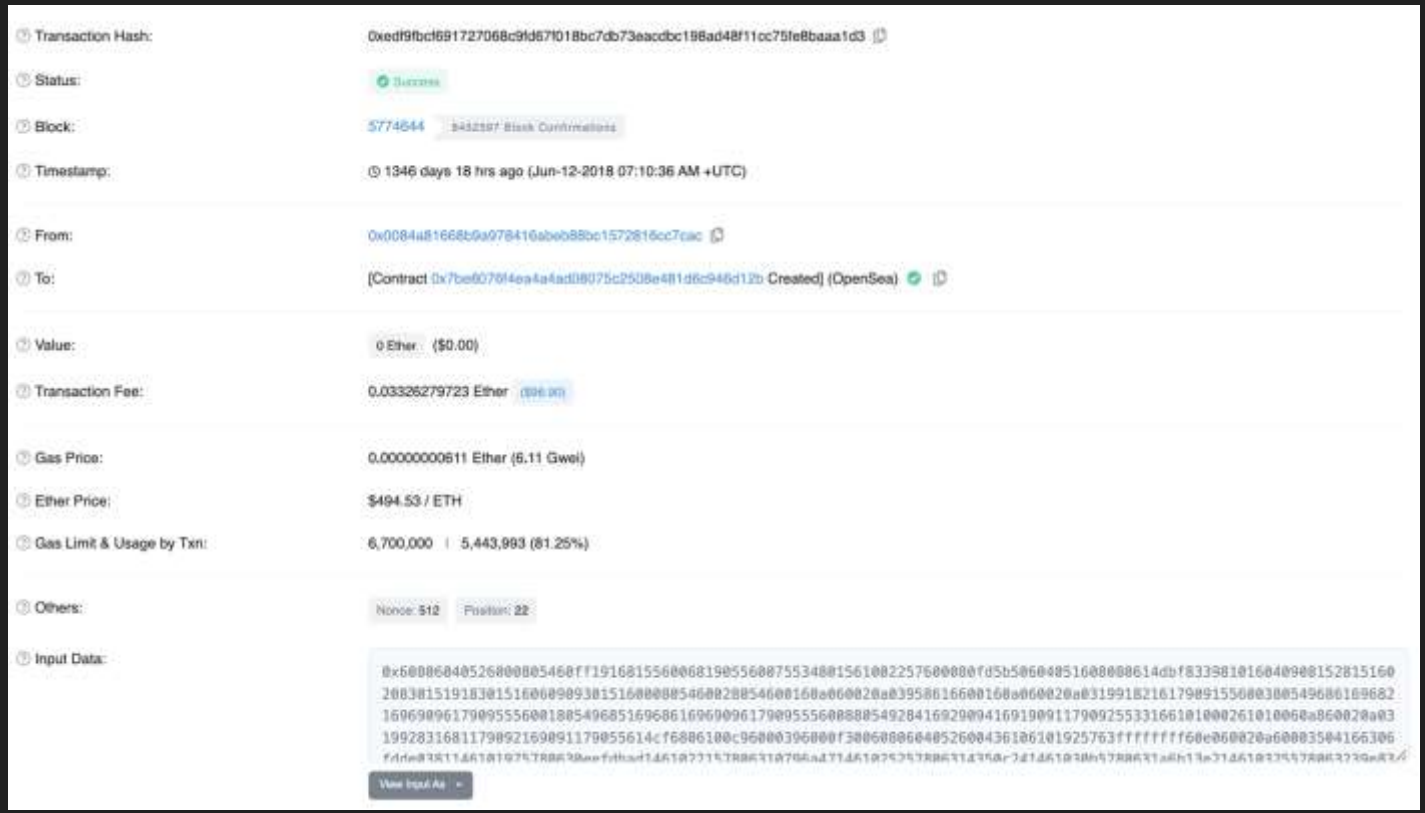
ethereum.org/en/developers/docs/smart-contracts/anatomy

Контракт. Создание OpenSea

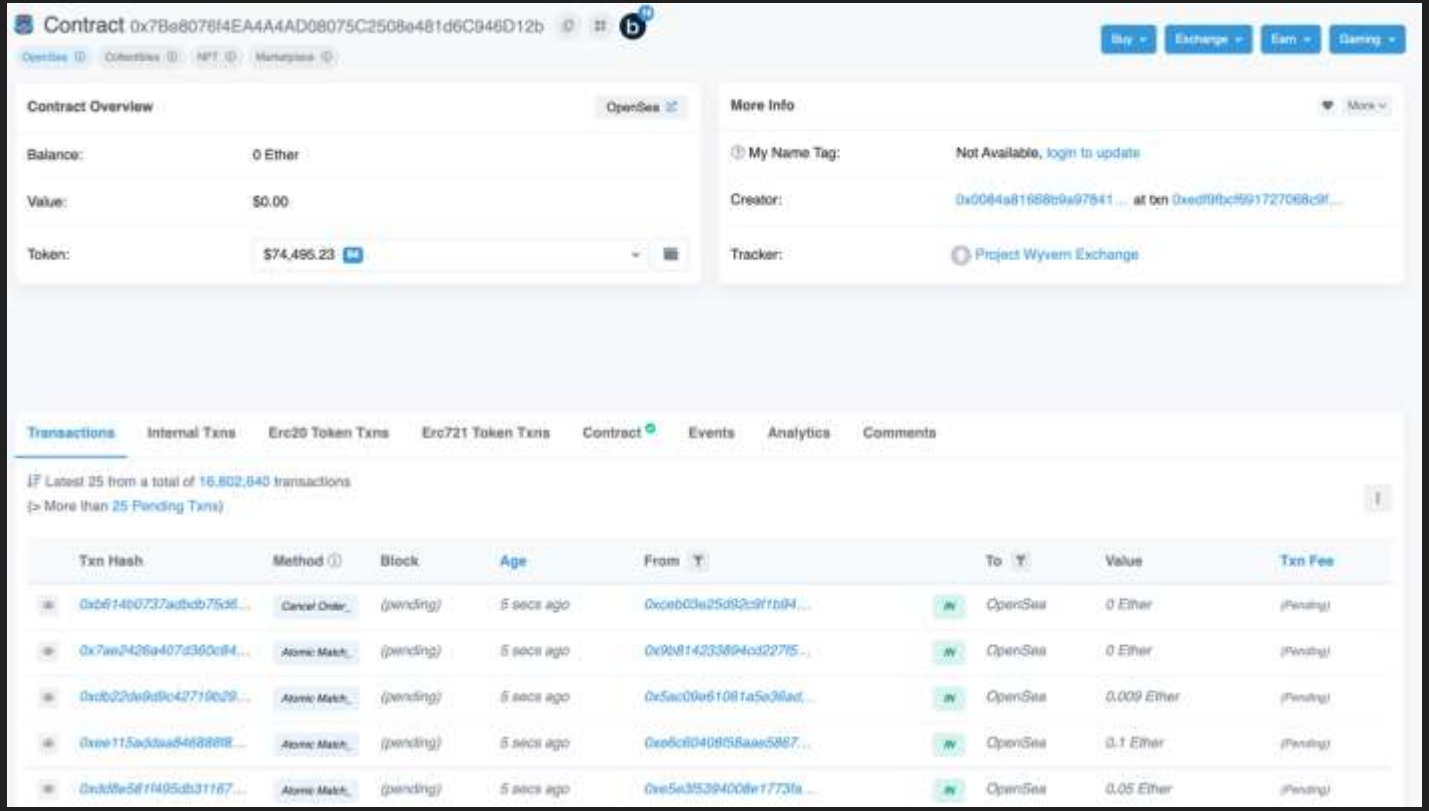
etherscan.io/tx/0xedf9fbcf691727068c9fd67f018bc7db73eacdbc198ad48f11cc75fe8baaa1d3

tinyurl.com/2p9dh6y9

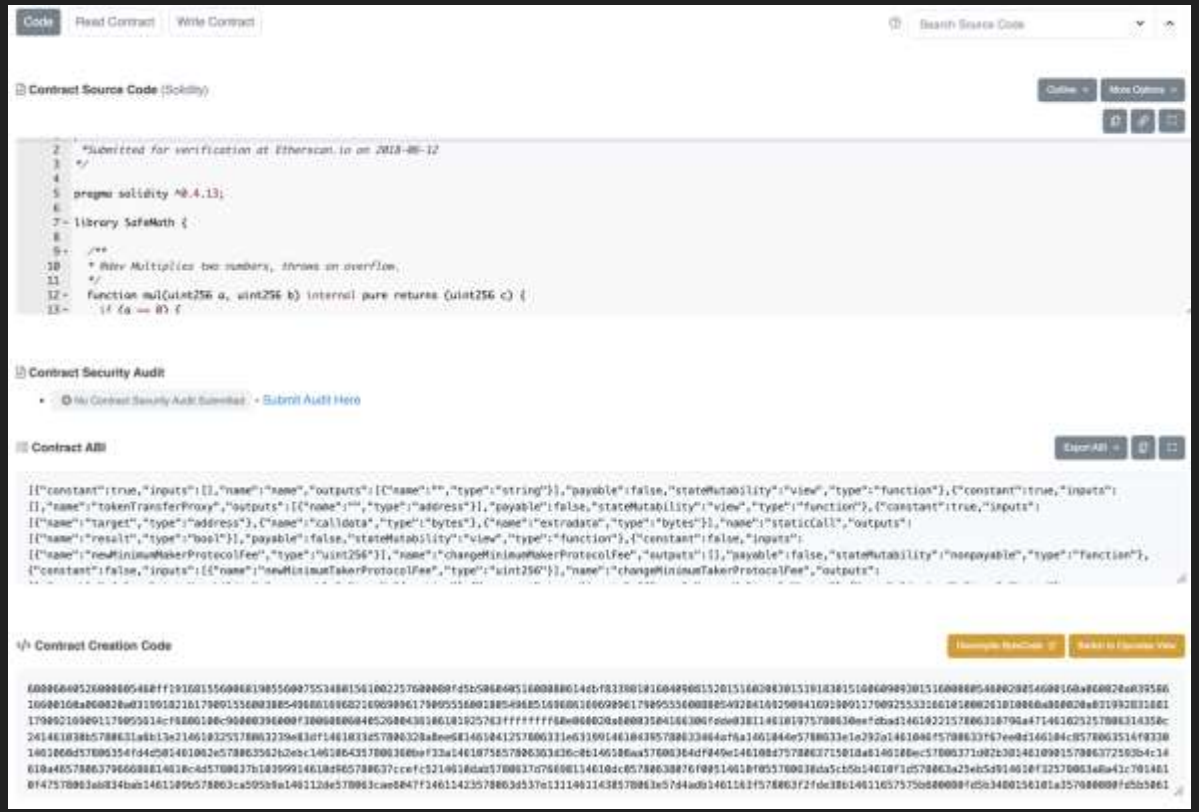
Контракт. Создание OpenSea



Контракт. Создание OpenSea



Контракт. Создание OpenSea



Контракт

Данные (data)

- Переменные заданные при создании контракта: прочитать в Solidity коде
- Публичные переменные: получить значение из ноды по API
- Внутренние переменные: рассчитать

Функции (functions)

- Публичные (public): можно вызвать
- Внутренние: могут быть вызваны только другими функциями контракта

События (events, logs)

Подписаться на события по из ноды API

public	**internal**
public variables	other variables
public functions	other function
all events	

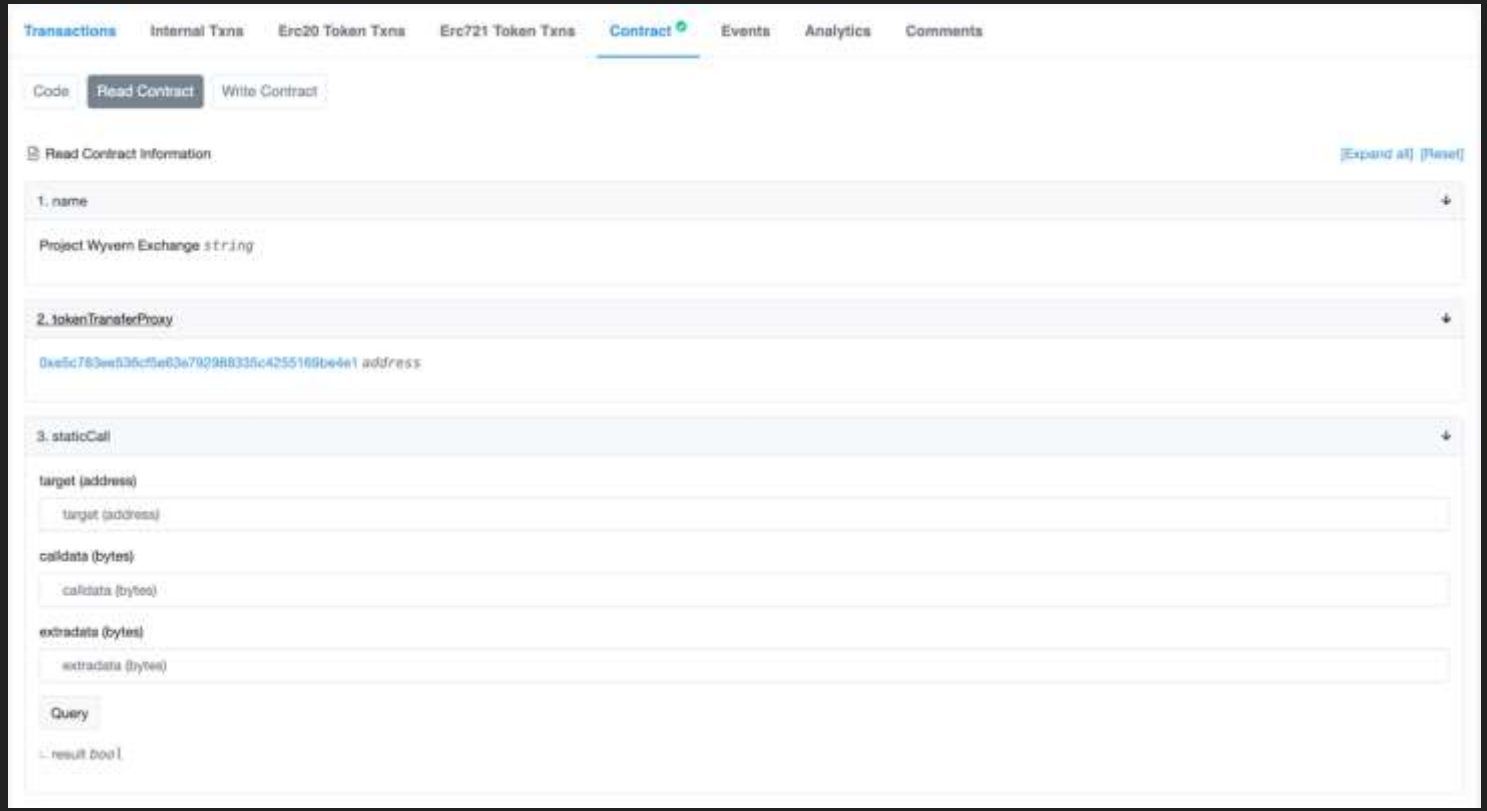
ethereum.org/en/developers/docs/smart-contracts/anatomy

Контракт. Чтение переменных OpenSea

etherscan.io/address/0x7be8076f4ea4a4ad08075c2508e481d6c946d12b

tinyurl.com/bn4t8fy8

Контракт. Чтение переменных OpenSea



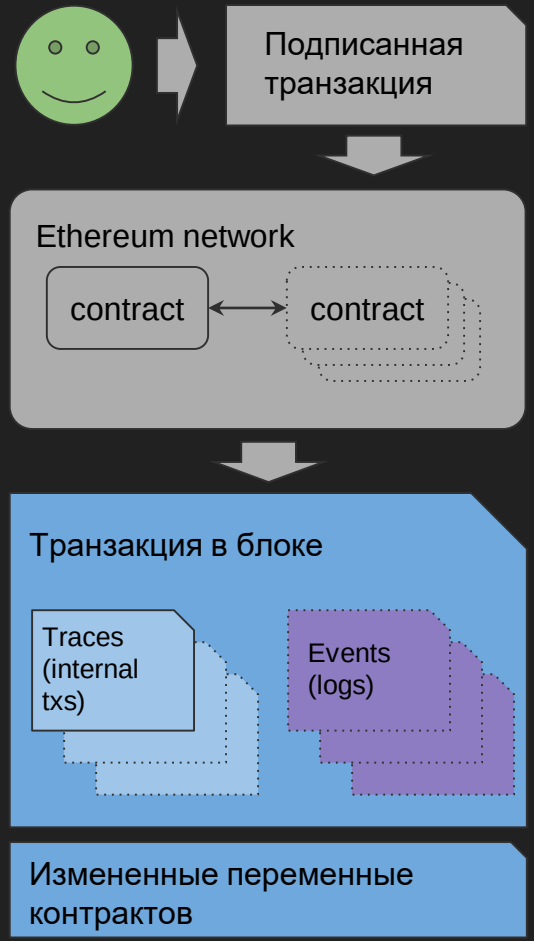
Транзакция контракта

В одной транзакции вызывается одна функция, а исполнено может быть много

Контракт может вызвать другой контракт

Исполнение каждой функции записывается во внутреннюю транзакцию (internal transaction / trace)

Функции могут создавать события (events / logs)



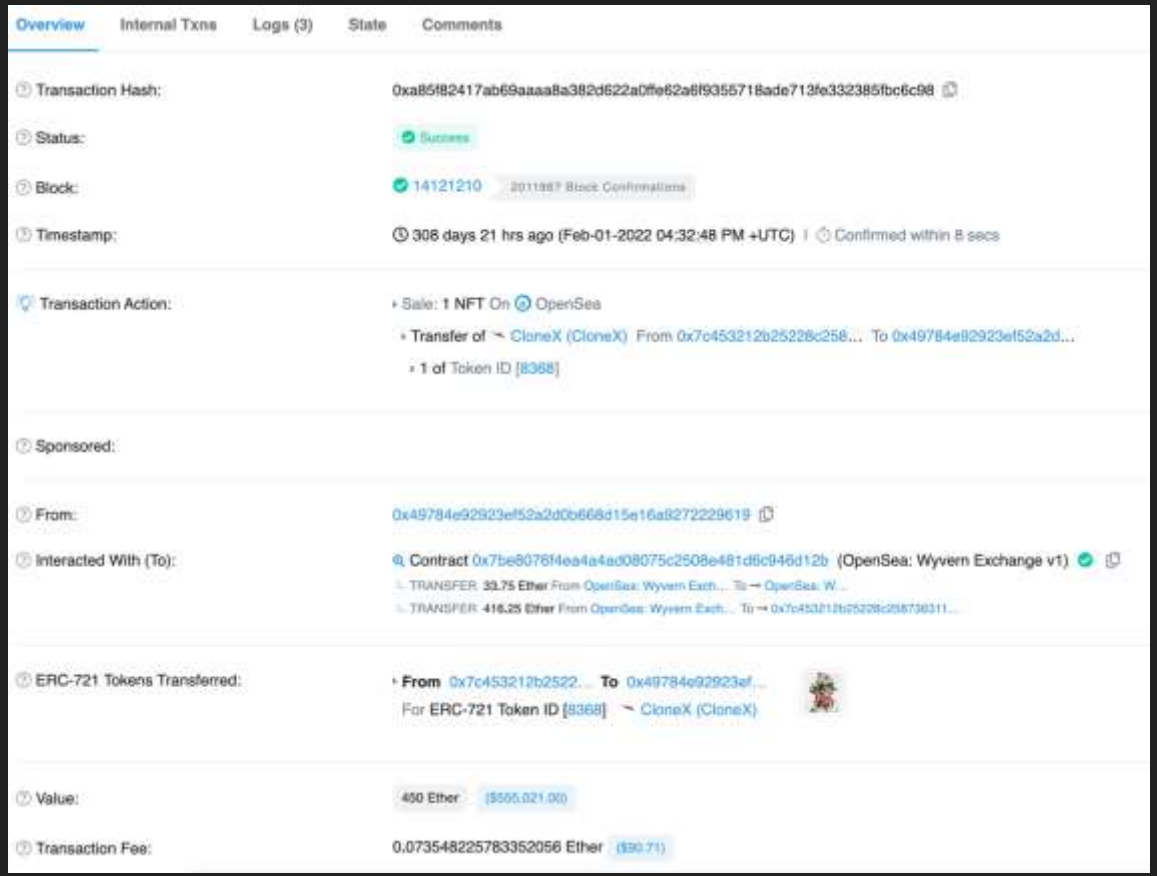
ethereum.org/en/developers/docs/transactions

Транзакция контракта. Закрытие сделки OpenSea

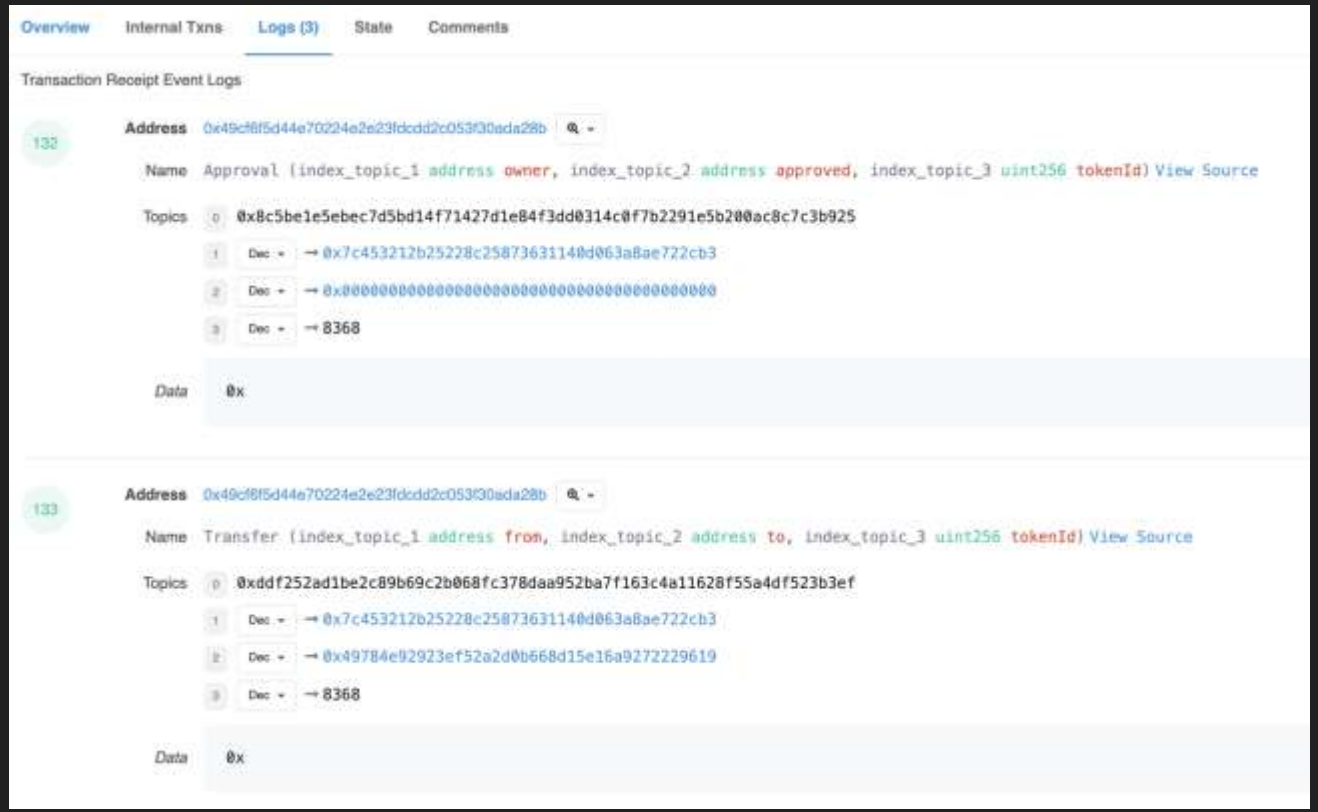
etherscan.io/tx/0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98

tinyurl.com/2p8sshrs

Транзакция контракта. Закрытие сделки OpenSea



Транзакция контракта. Закрытие сделки OpenSea

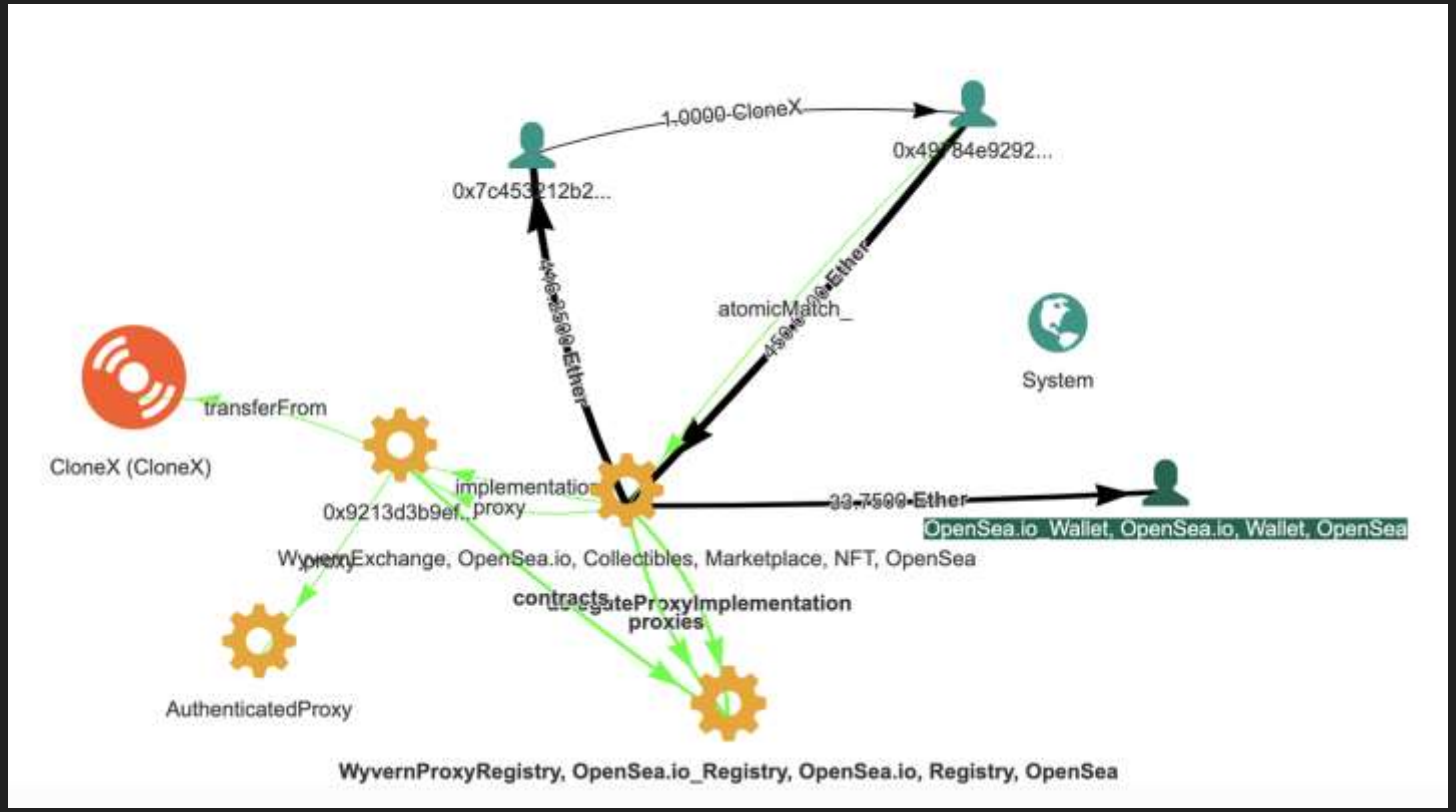


Транзакция контракта. Закрытие сделки OpenSea

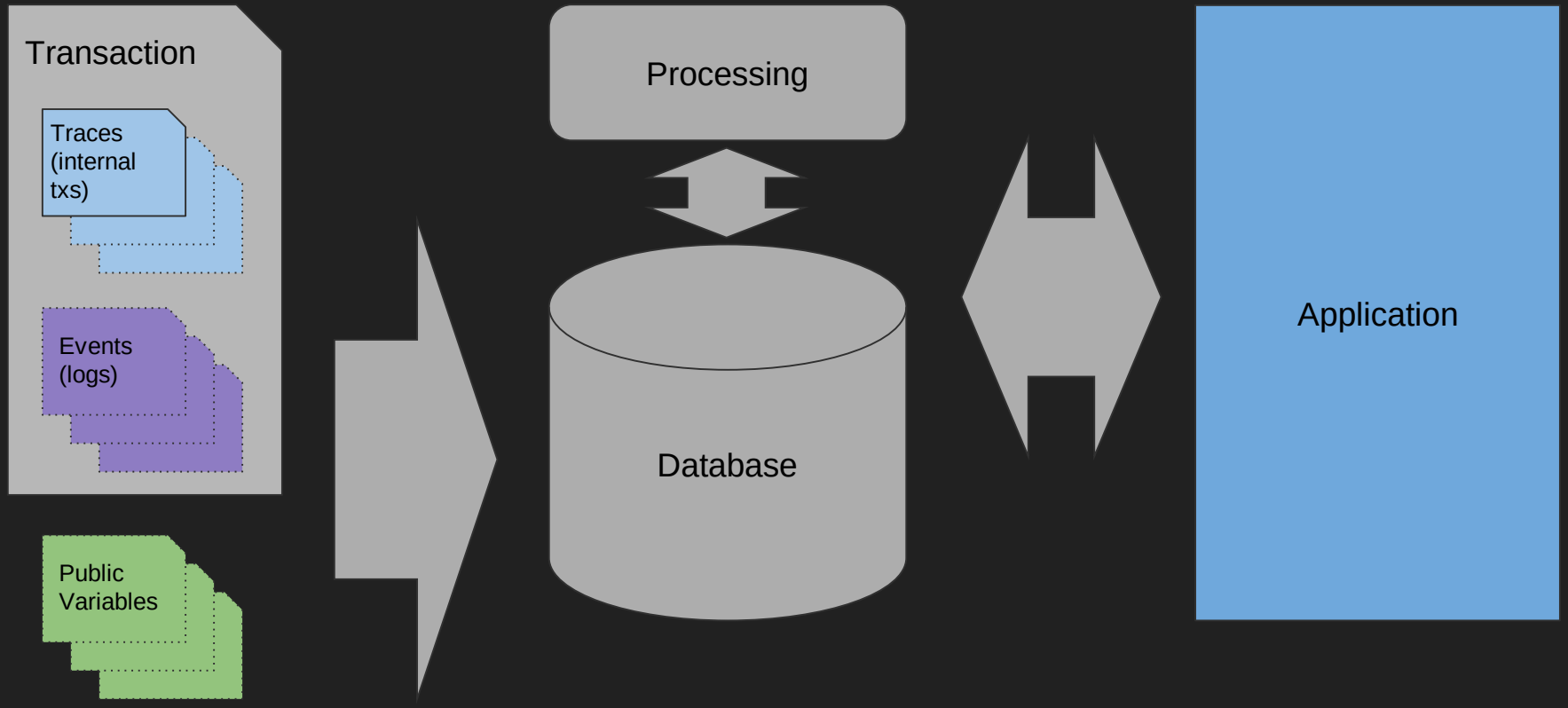
bloxy.info/tx/0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98

tinyurl.com/4fs6vt4z

Транзакция контракта. Закрытие сделки OpenSea



Как работают аналитические системы



Блокчейн эксплореры

Etherscan.io

- проверка стоимости газа
- оценка времени подтверждения транзакции
- просмотр кода контрактов и ABI
- чтение публичных переменных контрактов
- вызов функций контрактов

Bloxy.info

- активность адресов во времени
- граф транзакции и граф активности
- аналитика по методам контрактов

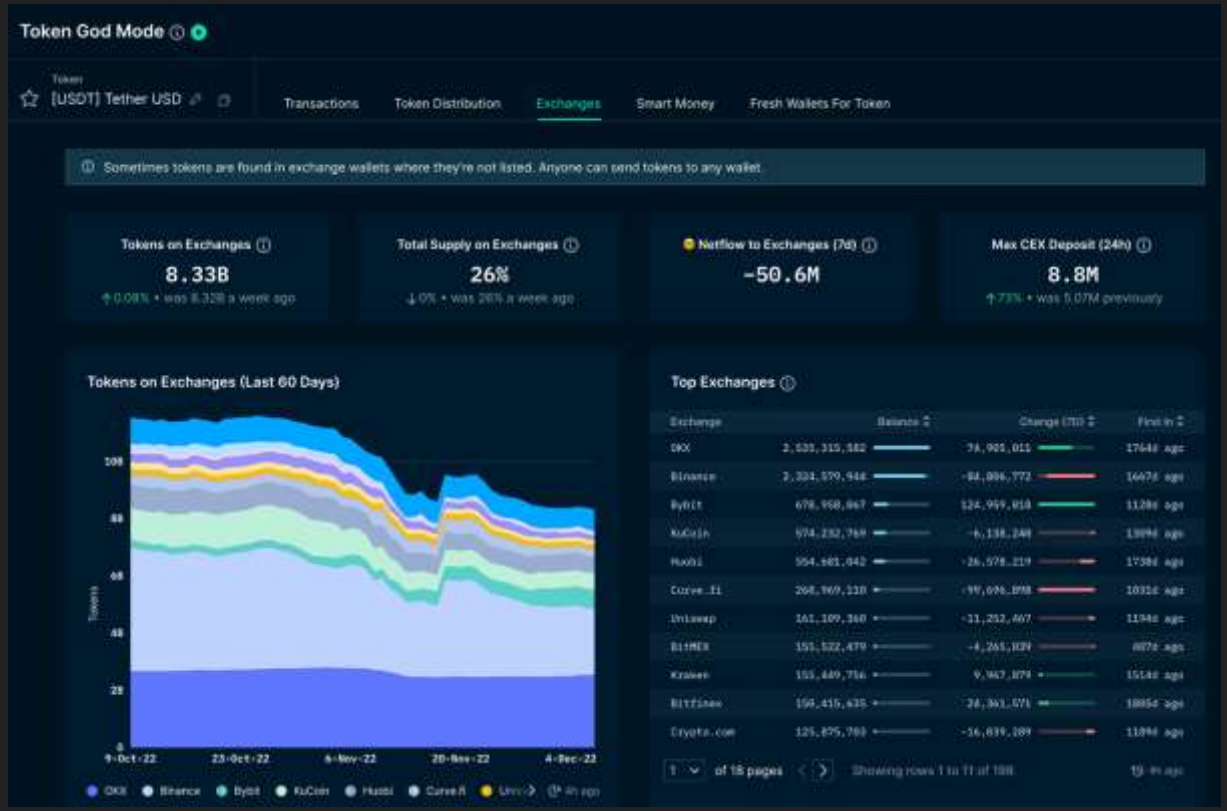
Аналитические сервисы. Что предоставляют?

- Web App: Data Studio, API constructor, Research
- API
- Integration: Google Sheets, TradingView
- Alerts: Telegram, WhatsApp, mail

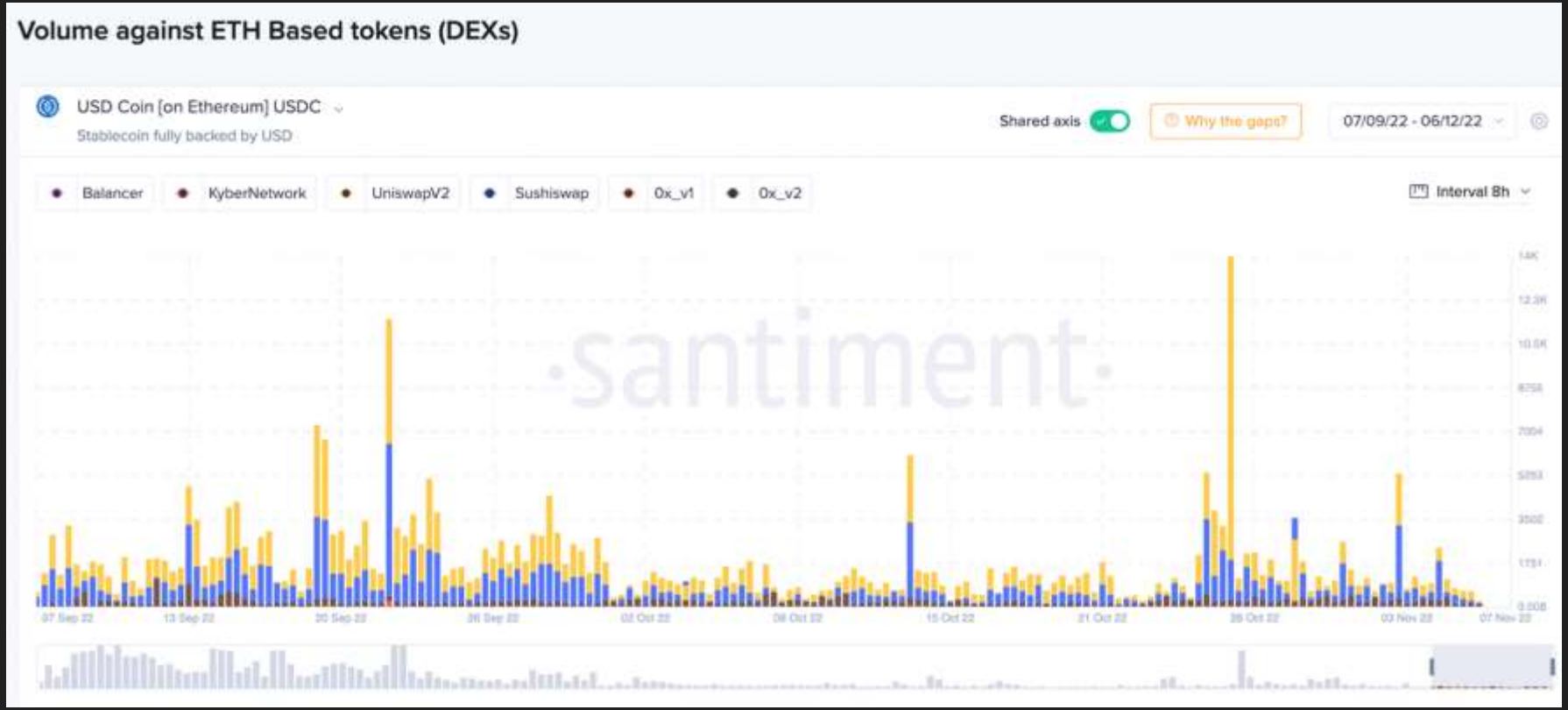
Аналитические сервисы. Nansen.ai

- Проект вырос из Blockchain ETL и ориентирован на анализ транзакций через разметку адресов и транзакций
- Лучшая разметка Ethereum адресов среди публичных сервисов
- Отличная разметка CEX, DEX, DeFi
- Один из лучших аналитических сервисов по NFT

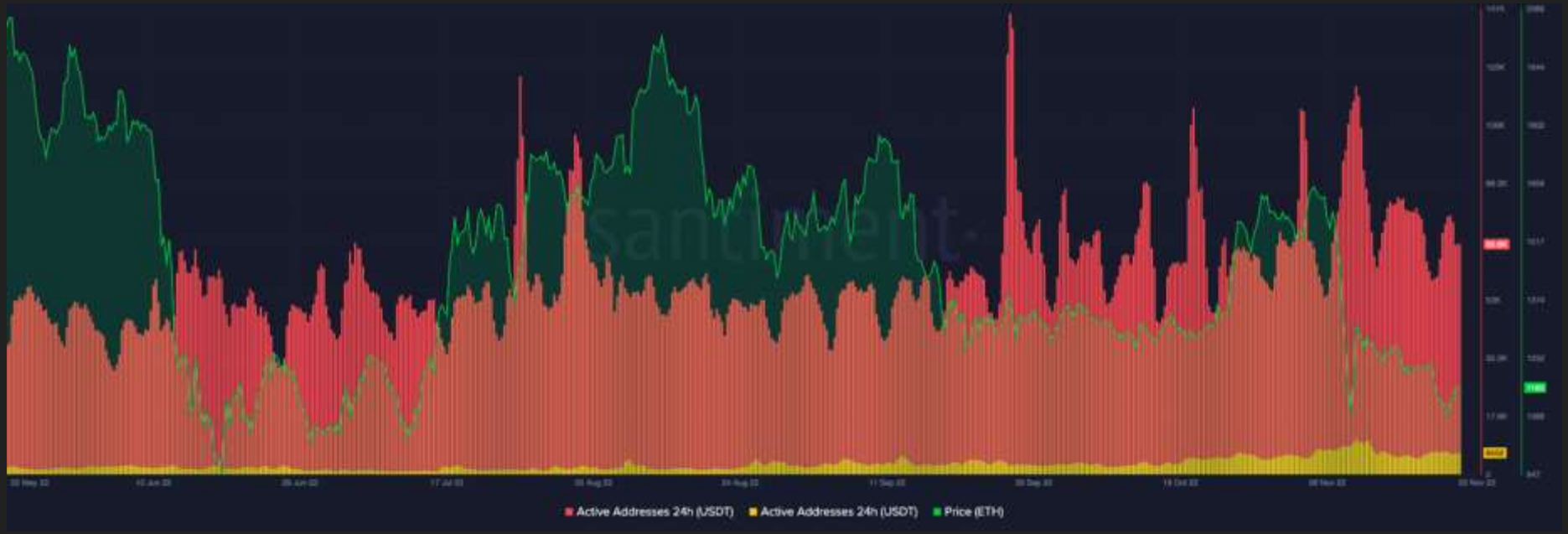
Аналитические сервисы. Nansen.ai



Аналитические сервисы. Santiment.net

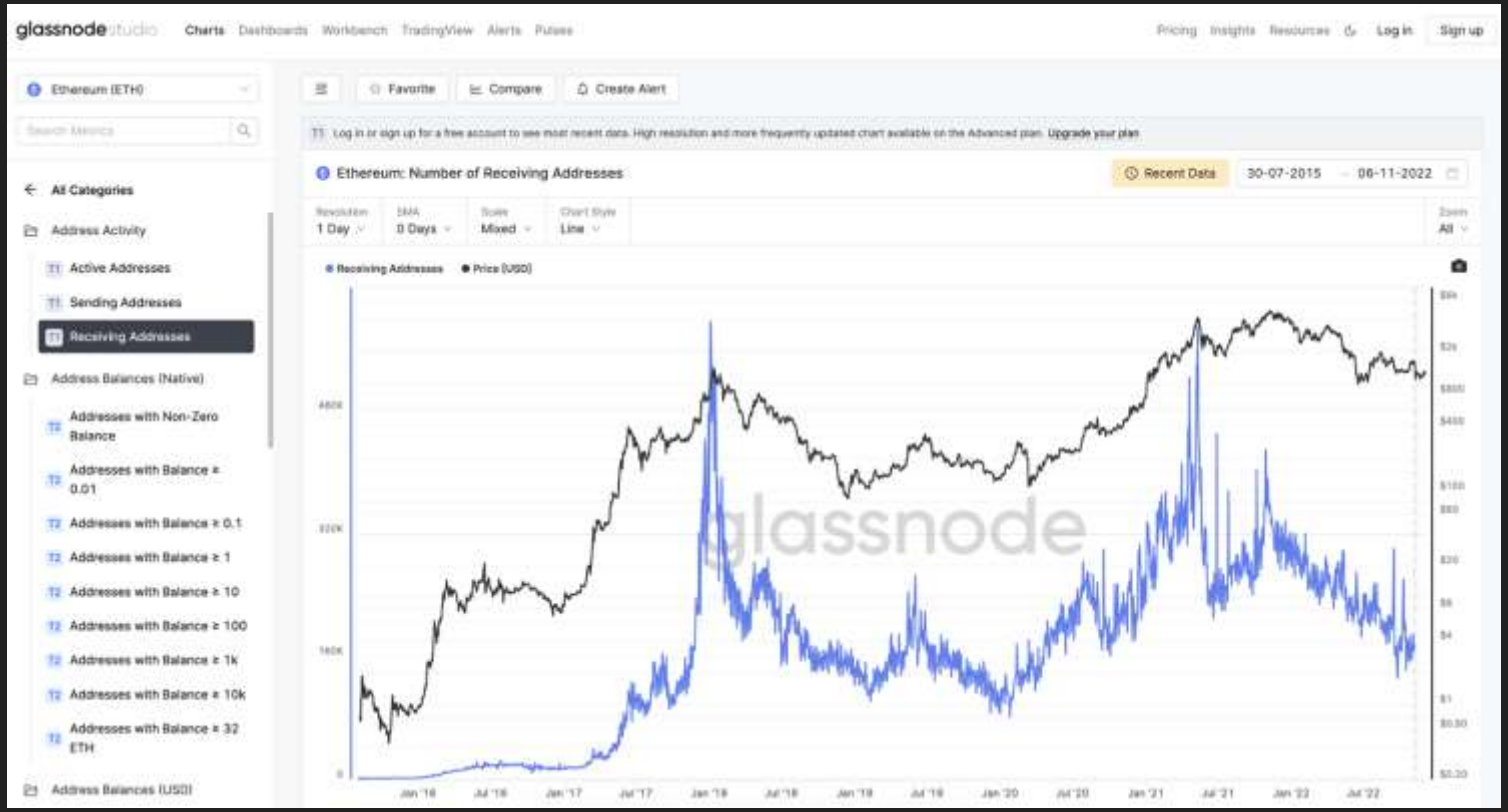


Аналитические сервисы. Santiment.net



USDT, active addresses compared on a shared axis. Red — USDT on Ethereum, yellow — USDT on Arbitrum

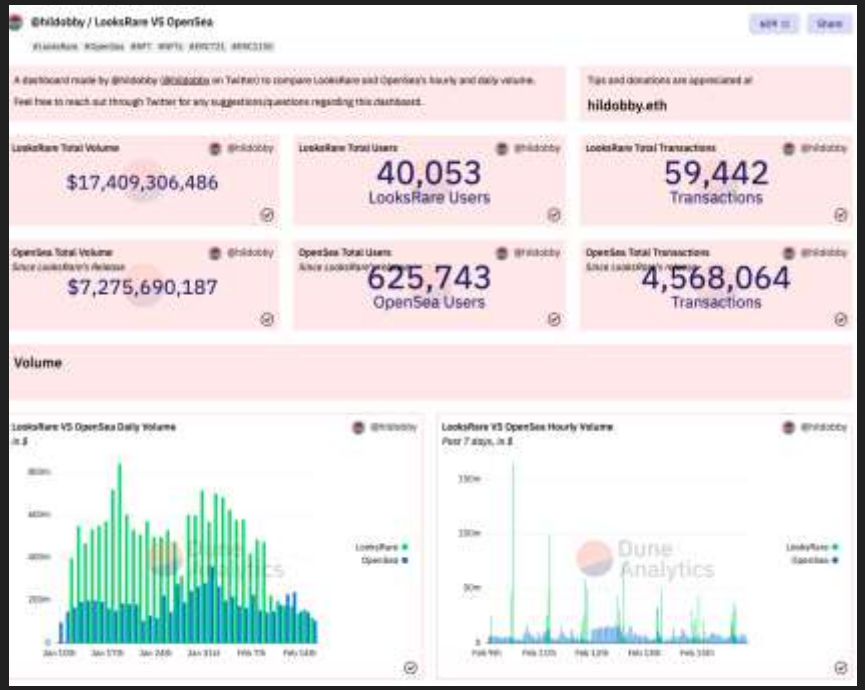
Аналитические сервисы. Glassnode.com



Аналитические дашборды

Dune Analytics dune.xyz

- Парсинг событий
- Множество дашбордов по NFT, DeFi, DEX и др.
- Можно создать и опубликовать свой дашборд, в том числе по активности вашего проекта



Поставщики данных

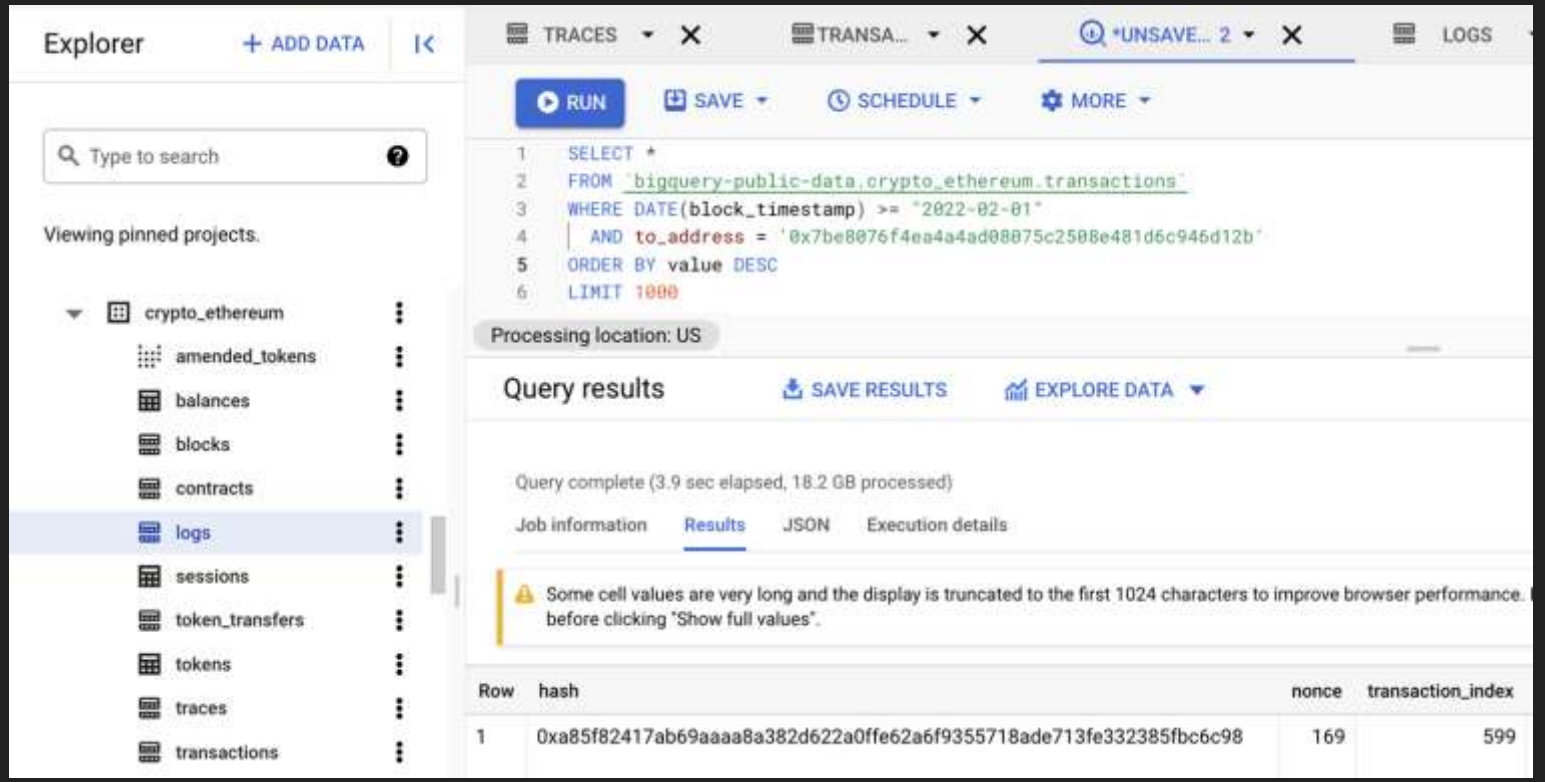
Blockchain ETL. BigQuery public datasets github.com/blockchain-etl/public-datasets

- Сырые данные транзакций, трейсов, событий и блоков
- Обработанные данные по основным протоколам
- Требуется знать SQL и иметь аккаунт в Google Cloud

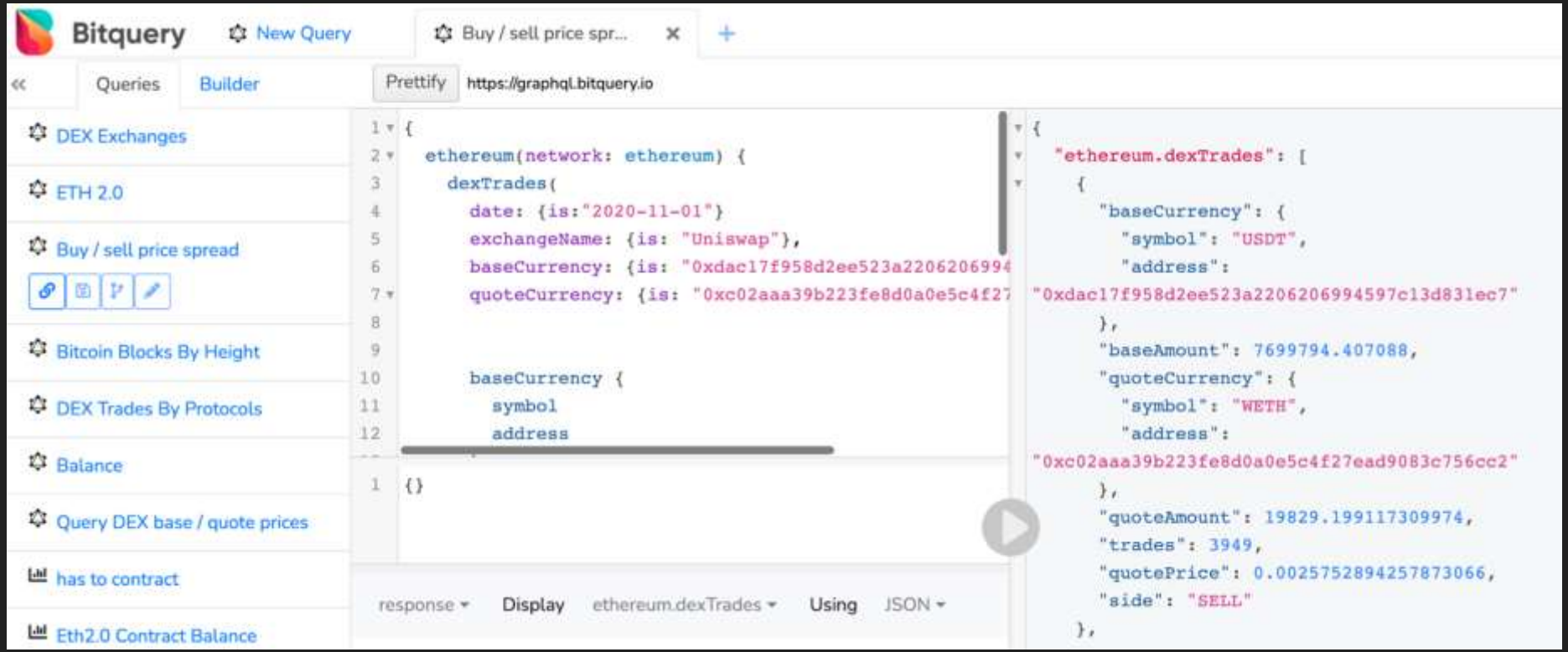
Bitquery.io

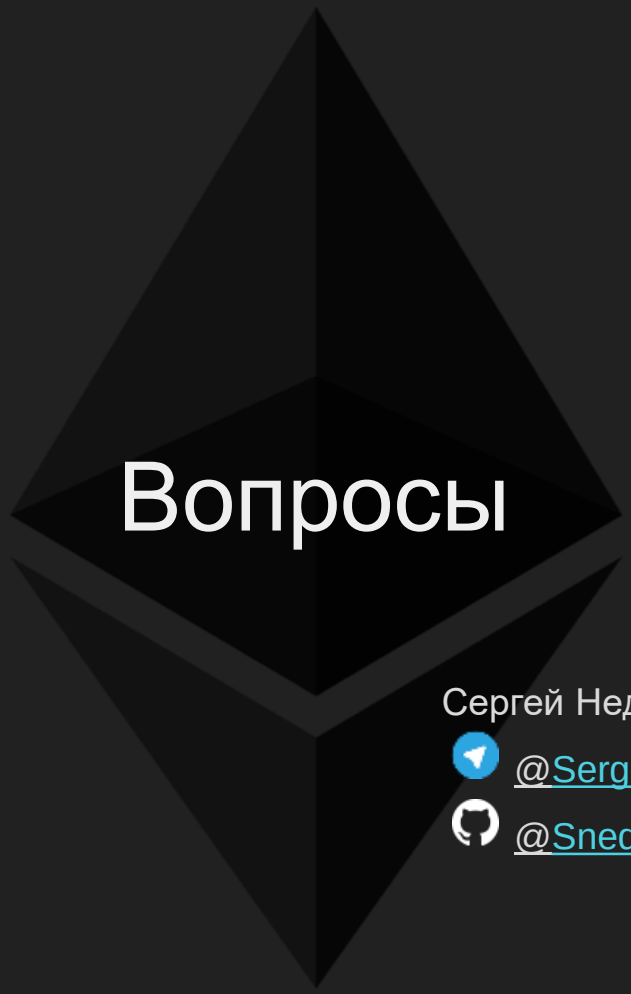
- Большой перечень данных по GraphQL и Rest API
- Отличные данные по DEX и DeFi

Blockchain ETL. BigQuery public datasets



Bitquery.io


Bitquery
New Query
Buy / sell price spr...
Queries
Builder
Prettify
https://graphql.bitquery.io
DEX Exchanges
ETH 2.0
Buy / sell price spread
Bitcoin Blocks By Height
DEX Trades By Protocols
Balance
Query DEX base / quote prices
has to contract
Eth2.0 Contract Balance
{
ethereum(network: ethereum) {
dexTrades(
date: {is:"2020-11-01"}
exchangeName: {is: "Uniswap"},
baseCurrency: {is: "0xdac17f958d2ee523a2206206994
quoteCurrency: {is: "0xc02aaa39b223fe8d0a0e5c4f27
baseCurrency {
symbol
address
{}
response
Display
ethereum.dexTrades
Using
JSON
{
"ethereum.dexTrades": [
{
"baseCurrency": {
"symbol": "USDT",
"address":
"0xdac17f958d2ee523a2206206994597c13d831ec7"
},
"baseAmount": 7699794.407088,
"quoteCurrency": {
"symbol": "WETH",
"address":
"0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2"
},
"quoteAmount": 19829.199117309974,
"trades": 3949,
"quotePrice": 0.0025752894257873066,
"side": "SELL"
},



Вопросы

Сергей Недашковский

@SergeNedashkovsky

@Snedashkovsky