



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

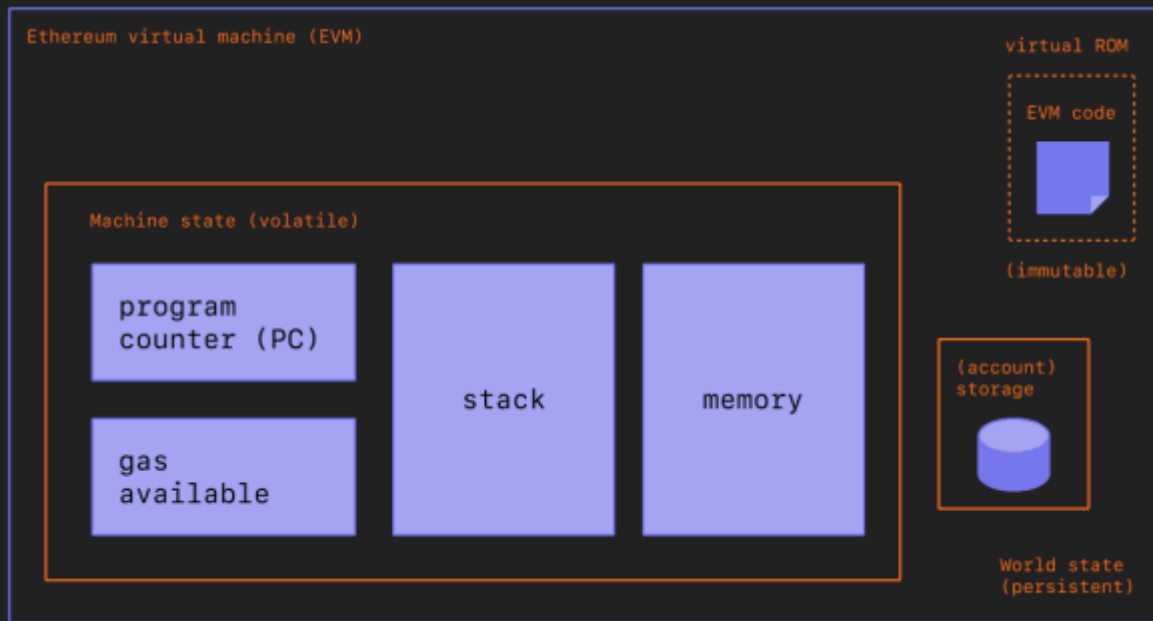
- Ethereum Virtual Machine
- Транзакция
- Контракт



tinyurl.com/4we2sf35

Ethereum Virtual Machine (EVM)

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



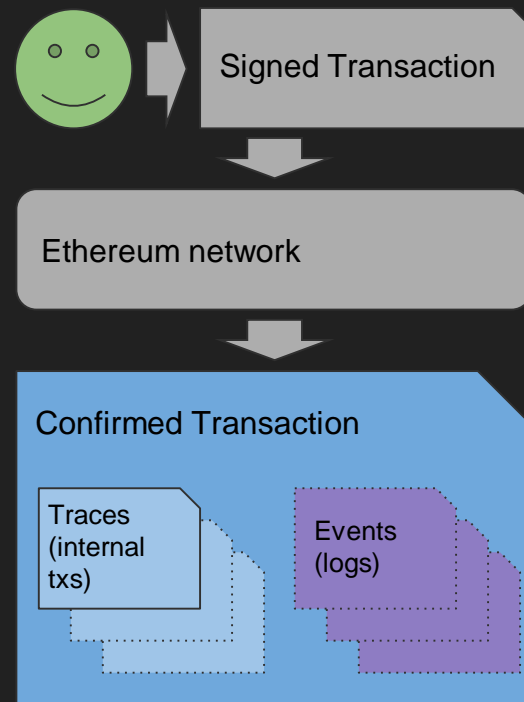
Что такое транзакция (transaction, tx)

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)










Самая большая транзакция в ноябре 2022



etherscan.io/tx/0x67fbcfe377c93800e673f168ca71fe4b20f25e6ed6ecc64f5ecd941d6cdf967b

tinyurl.com/2p9d5yew

Самая большая транзакция в феврале 2022

Overview		State	Comments
Transaction Hash:	0x67fbcfe377c93800e673f168ca71fe4b20f25e6ed6ecc64f5ecd941d6cdf967b 		
Status:	 Success		
Block:	 15933553 199262 Block Confirmations		
Timestamp:	 27 days 20 hrs ago (Nov-09-2022 04:06:59 PM +UTC)  Confirmed within 5 secs		
Sponsored:			
From:	0xf977814e90da44bfa03b6295a0616a897441acec (Binance 8) 		
To:	0x28c6c06298d514db089934071355e5743bf21d60 (Binance 14) 		
Value:	800,000 Ether (\$960,160,000.00)		
Transaction Fee:	0.001750259605206 Ether (\$2.14)		
Gas Price:	0.000000083345695486 Ether (83.345695486 Gwei)		
Ether Price:	\$1,104.17 / ETH		

Контракт. Создание

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

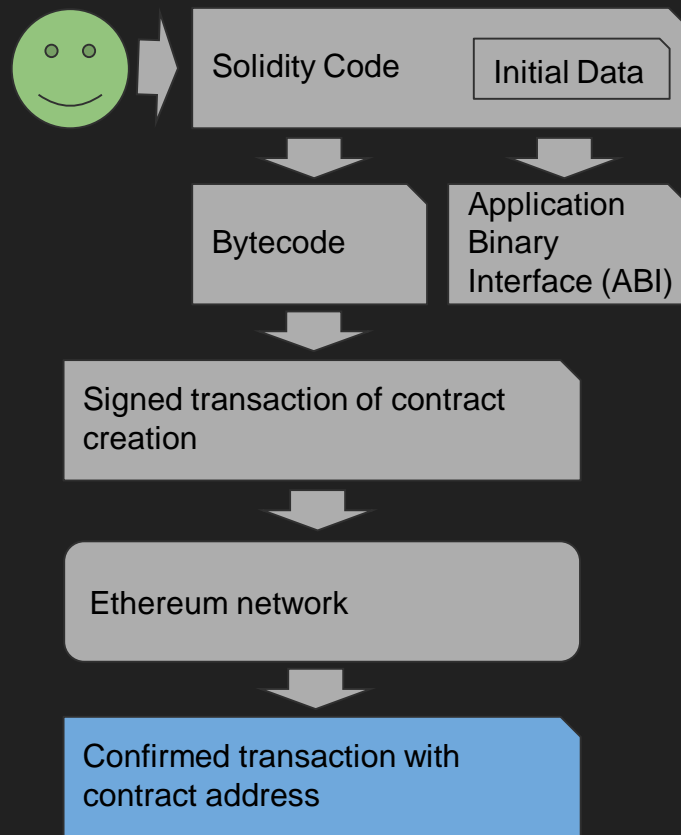
Контракт может быть создан:

- 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



Контракт. Создание OpenSea



etherscan.io/tx/0xedf9fbcf691727068c9fd67f018bc7db73eacdbc198ad48f11cc75fe8baaa1d3

tinyurl.com/2p9dh6y9

Контракт. Создание OpenSea

Transaction Hash:	0xedf9fbcb691727068c9fd67f018bc7db73aeacdbc198ad48f11cc75fe8baaa1d3
Status:	Success
Block:	5774544 3432387 Block Confirmations
Timestamp:	1346 days 18 hrs ago (Jun-12-2018 07:10:36 AM +UTC)
From:	0x0084a81668b59a78416abeb88bc1572816cc7cac
To:	[Contract 0x7be0764e4a4ad08075c2508e481d6c946d12b Created] (OpenSea)
Value:	0 Ether (\$0.00)
Transaction Fee:	0.03326279723 Ether (\$06.00)
Gas Price:	0.00000000611 Ether (6.11 Gwei)
Ether Price:	\$494.53 / ETH
Gas Limit & Usage by Txn:	6,700,000 5,443,993 (81.25%)
Others:	Nonce: 512 Position: 22
Input Data:	<pre> 0x6080604052600005460ff1916815560068190556007553480156108225760000fd5b50604051600008614dbf833981016040900152815160 20038151918301516000909381516000805460028054600160a060020a03958016600160a060020a0319918216179091550003005496006109602 16069096179095556001805496005169606169690961790955560088054928416929094169190911790925533166101000261010060a060020a03 1992831681179092169091179055614cf6806100c9600039600f3060806040052600436106101925763ffffffffff60e060020a060003504166306 fd8ce83811d610107478063060fd8ce83811d61077178063710706ad71d610774780631d630r3d1d61078063780631ad6h19a71d6107747806377060e7d View Input As... </pre>

Контракт. Создание OpenSea

Contract 0x7B8076f4EA4A4AD08075C2508a481d6C846D12b

OpenSea | Coinbase | NFT | Marketplace

Buy | Exchange | Earn | Gaming

Contract Overview

OpenSea

Balance: 0 Ether

Value: \$0.00

Token: \$74,485.23

More Info

My Name Tag: Not Available, login to update

Creator: 0x0084a81688b9a97b41... at txn 0xed9fbc591727068c9f...

Tracker: Project Wyvern Exchange

Transactions | Internal Txns | Erc20 Token Txns | Erc721 Token Txns | Contract | Events | Analytics | Comments

17 Latest 25 from a total of 16,802,840 transactions
(> More than 25 Pending Txns)

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0xb614b0737ad1eb75d6...	Cancel Order	(pending)	5 secs ago	0xcab03a25d92c9f1b04...	OpenSea	0 Ether	(Pending)
0x7ae2426a407d360c84...	Atomic Match	(pending)	5 secs ago	0x9b14333694cd2275...	OpenSea	0 Ether	(Pending)
0xb022d69d9c42719c29...	Atomic Match	(pending)	5 secs ago	0x5ac09e61081a5e36ad...	OpenSea	0.009 Ether	(Pending)
0x9e115a03aa846888e...	Atomic Match	(pending)	5 secs ago	0x6c0d408f56aac5887...	OpenSea	0.1 Ether	(Pending)
0xb08e5f1495db31167...	Atomic Match	(pending)	5 secs ago	0xe5e35394208e1773fa...	OpenSea	0.05 Ether	(Pending)

Контракт. Создание OpenSea

Code

Read Contract

Write Contract

Search Source Code

Contract Source Code (Solidity)

Outline

More Options

```
1 //
2 //Submitted for verification at Etherscan.io on 2018-06-12
3 //
4
5 pragma solidity ^0.4.13;
6
7 library SafeMath {
8
9     /**
10      * @dev Multiplies two numbers, throws on overflow.
11      */
12     function mul(uint256 a, uint256 b) internal pure returns (uint256 c) {
13         if (a == 0) return b;
```

Contract Security Audit

No Contract Security Audit Submitted

Submit Audit Here

Contract ABI

Export ABI

```
[{"constant":true,"inputs":[],"name":"name","outputs":[{"name":"","type":"string"}],"payable":false,"stateMutability":"view","type":"function"},{"constant":true,"inputs":[],"name":"tokenTransferProxy","outputs":[{"name":"","type":"address"}],"payable":false,"stateMutability":"view","type":"function"},{"constant":true,"inputs":[],"name":"target","type":"address"},{"name":"calldata","type":"bytes"},{"name":"extradata","type":"bytes"},{"name":"staticCall","outputs":[{"name":"result","type":"bool"}],"payable":false,"stateMutability":"view","type":"function"},{"constant":false,"inputs":[],"name":"newMinimumMakerProtocolFee","type":"uint256"},{"name":"changeMinimumMakerProtocolFee","outputs":[{"name":"","type":"function"},{"constant":false,"inputs":[{"name":"newMinimumMakerProtocolFee","type":"uint256"}],"name":"changeMinimumMakerProtocolFee","outputs":[]}]
```

Contract Creation Code

Example Raw Code

Switch to Example View

```
60060604052000805400ff19160155600401905560075534001561002257000000f45b50040051600080146b783300181604050015201516030030151818301510060900301516000805400020054600160400002004039500
16000160400200319018216179001556003805400018000216009006179005556003805400015600016000900617900555600380540016020004169190012700925531661018002610100060400020031902031601
179002109001179055014c79000100c900039600073000000004052000430186181025763ffffffffff6000020040003504166300f0e03811461819757000300c0ad146102215700031879047171461023257000314350c
24146103805700031a0b13e214610325700032390830f1461033457000320a00004146104125700031a631091461043957000330440f6a146104465700033e1e292014610405700033767ee0d146104c057000351678330
1401060d57000354f4c5001461062e57000356262ec14610643570003600ef732a1461075657000363c36c81461080a57000364d7949e14610847570003725018a1461086ec57000371002c301461090157000372502b4c14
610a0570003796608014610c4d5700037b18799914610d905700037ccef5214610da05700037d76000134610d4c05700038076f09514610f055700038da5c05014610f71c5700038a25eb5014610f7325700038a041c701461
0f475700038a034b0146110005700038a05050a14611005700038a06047f346112425700038a03653314611314014385700038a0365704401461141f57000372f2dc380146116575700080000f45b3400156101a357000000f45b5001
```

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	



Контракт. Чтение переменных OpenSea



etherscan.io/address/0x7be8076f4ea4a4ad08075c2508e481d6c946d12b

tinyurl.com/bn4t8fy8

Контракт. Чтение переменных OpenSea

[Transactions](#) [Internal Txns](#) [Erc20 Token Txns](#) [Erc721 Token Txns](#) [Contract](#) [Events](#) [Analytics](#) [Comments](#)

[Code](#) [Read Contract](#) [Write Contract](#)

Read Contract Information

[\[Expand all\]](#) [\[Reset\]](#)

1. name

Project Wvern Exchange string

2. tokenTransferProxy

0xe5dc783ee535cf5e83e792988335c4255189b44e1 address

3. staticCall

target (address)

target (address)

calldata (bytes)

calldata (bytes)

extradata (bytes)

extradata (bytes)

Query

result bool

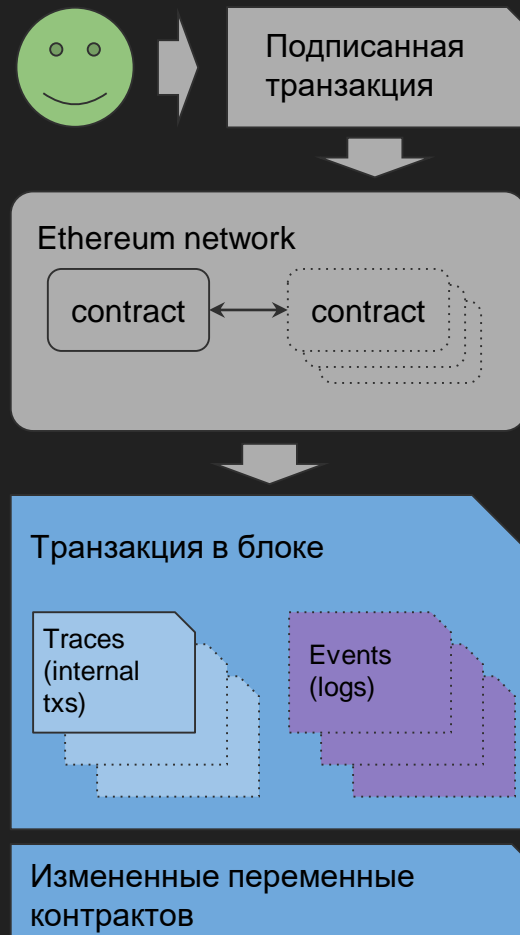
Транзакция контракта

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)



Транзакция контракта. Заккрытие сделки OpenSea



etherscan.io/tx/0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98

tinyurl.com/2p8sshhs

Транзакция контракта. Заккрытие сделки OpenSea

[Overview](#) [Internal Txns](#) [Logs \(3\)](#) [State](#) [Comments](#)

Transaction Hash: [0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98](#)

Status: Success

Block: 14121210 2011987 Block Confirmations

Timestamp: 308 days 21 hrs ago (Feb-01-2022 04:32:48 PM +UTC) Confirmed within 8 secs

Transaction Action:

- Sale: 1 NFT On [OpenSea](#)
- Transfer of [CloneX \(CloneX\)](#) From [0x7c453212b25228c258...](#) To [0x49784e92923ef52a2d...](#)
- 1 of Token ID [\[8368\]](#)

Sponsored:

From: [0x49784e92923ef52a2d0b668d15e16a8272229619](#)

Interacted With (To):

- Contract [0x7be807614ea4e4ad08075c2508e481d6c946d12b](#) (OpenSea: Wyvern Exchange v1)
- TRANSFER: 33.75 Ether From OpenSea: Wyvern Exch... To → OpenSea: W...
- TRANSFER: 416.25 Ether From OpenSea: Wyvern Exch... To → 0x7c453212b25228c258736311...

ERC-721 Tokens Transferred:

- From [0x7c453212b2522...](#) To [0x49784e92923ef...](#)
- For ERC-721 Token ID [\[8368\]](#) [CloneX \(CloneX\)](#)

Value: 450 Ether (\$505,021.00)

Transaction Fee: 0.073548225783352056 Ether (\$90.71)

Транзакция контракта. Заккрытие сделки OpenSea

[Overview](#) [Internal Txns](#) [Logs \(3\)](#) [State](#) [Comments](#)

Transaction Receipt Event Logs

132

Address [0x49cf8f5d44e70224e2e23fdccd2c053f30ada28b](#) [Q](#) [-](#)

Name Approval (index_topic_1 [address](#) [owner](#), index_topic_2 [address](#) [approved](#), index_topic_3 [uint256](#) [tokenId](#)) [View Source](#)

Topics [0](#) [0x8c5be1e5ebec7d5bd14f71427d1e84f3dd0314c0f7b2291e5b200ac8c7c3b925](#)

[1](#) [Dec](#) [-](#) [→ 0x7c453212b25228c25873631140d063a8ae722cb3](#)

[2](#) [Dec](#) [-](#) [→ 0x00](#)

[3](#) [Dec](#) [-](#) [→ 8368](#)

Data [0x](#)

133

Address [0x49cf8f5d44e70224e2e23fdccd2c053f30ada28b](#) [Q](#) [-](#)

Name Transfer (index_topic_1 [address](#) [from](#), index_topic_2 [address](#) [to](#), index_topic_3 [uint256](#) [tokenId](#)) [View Source](#)

Topics [0](#) [0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef](#)

[1](#) [Dec](#) [-](#) [→ 0x7c453212b25228c25873631140d063a8ae722cb3](#)

[2](#) [Dec](#) [-](#) [→ 0x49784e92923ef52a2d0b668d15e16a927229619](#)

[3](#) [Dec](#) [-](#) [→ 8368](#)

Data [0x](#)

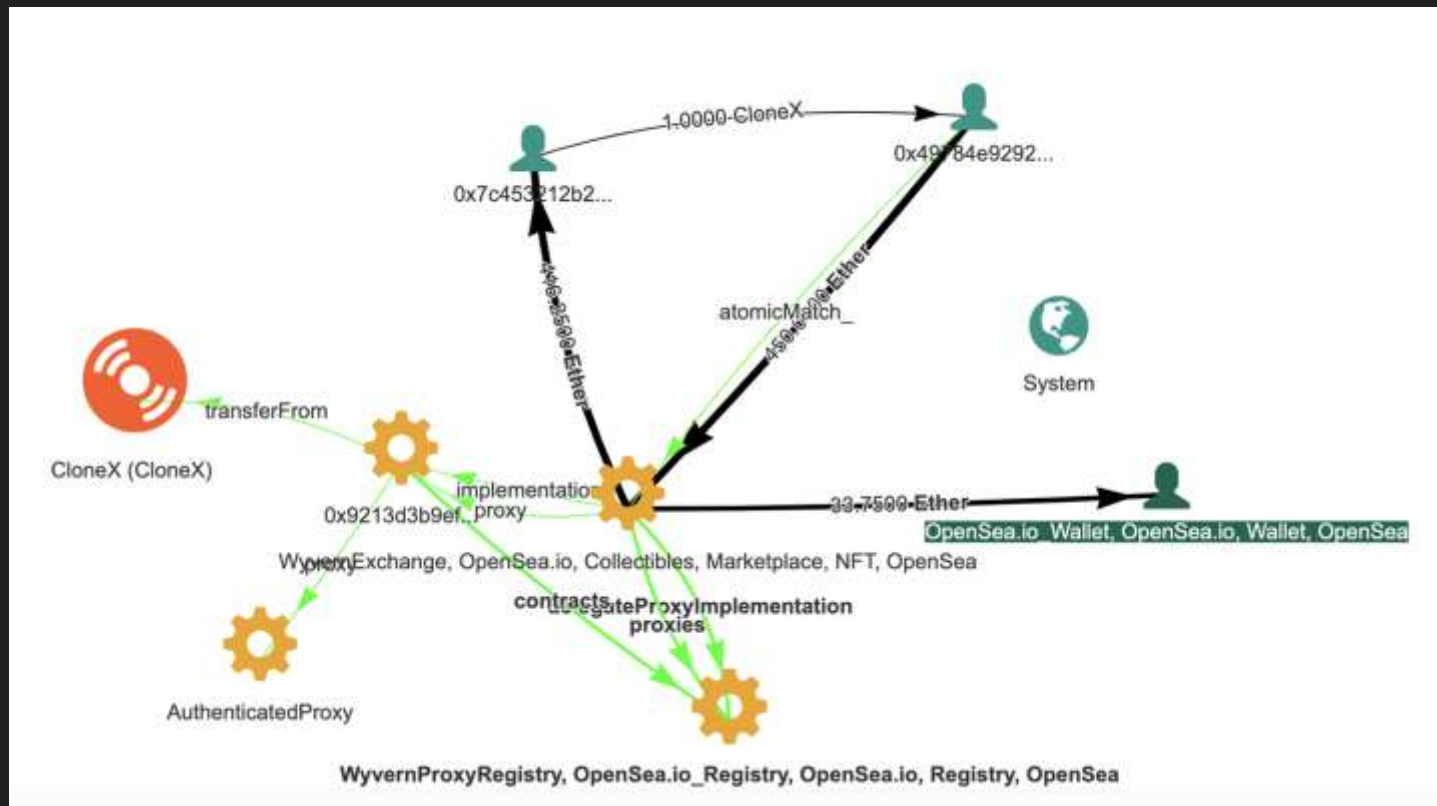
Транзакция контракта. Заккрытие сделки OpenSea



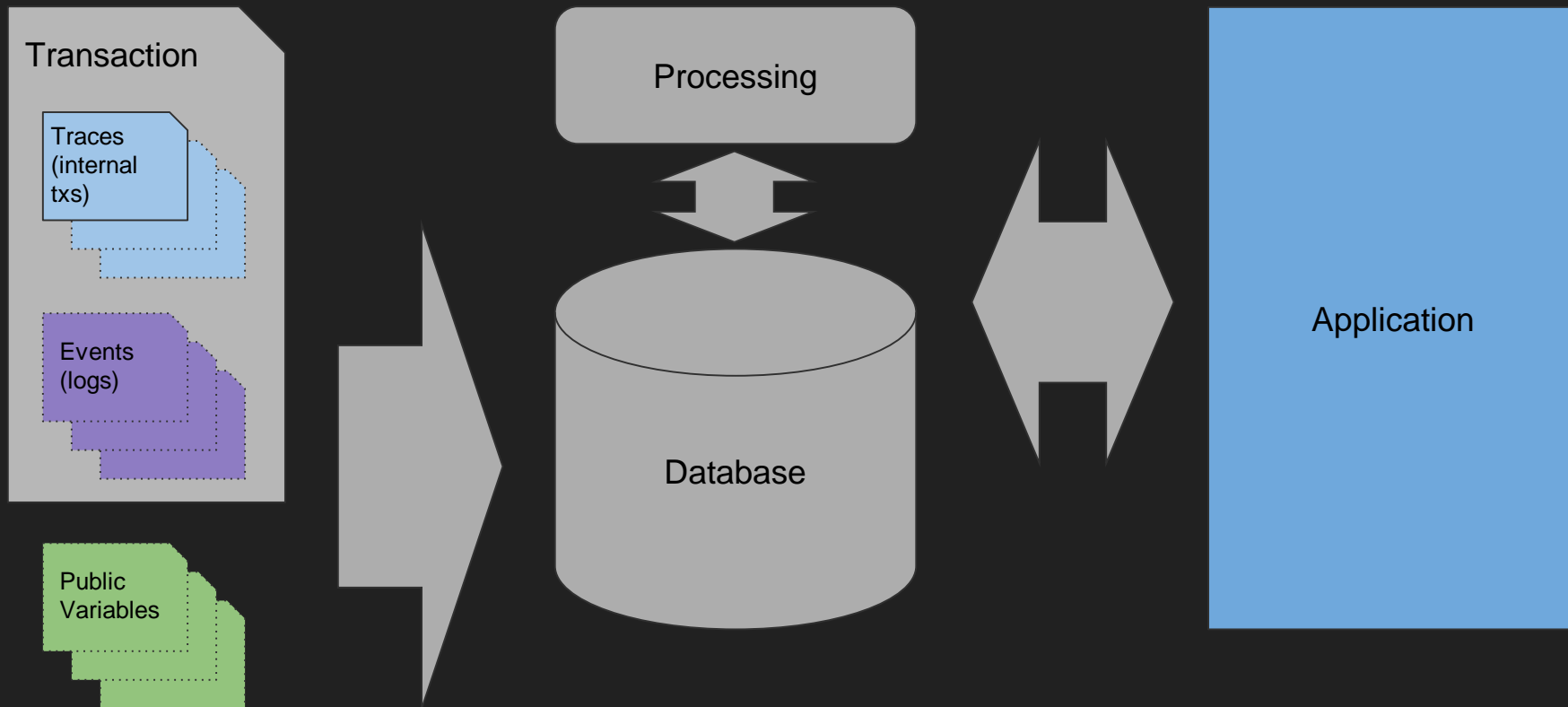
bloxy.info/tx/0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98

tinyurl.com/4fs6vt4z

Транзакция контракта. Заккрытие сделки OpenSea



Как работают аналитические системы



Блокчейн эксплореры

[Etherscan.io](https://etherscan.io)

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

[Bloxy.info](https://bloxy.info)

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

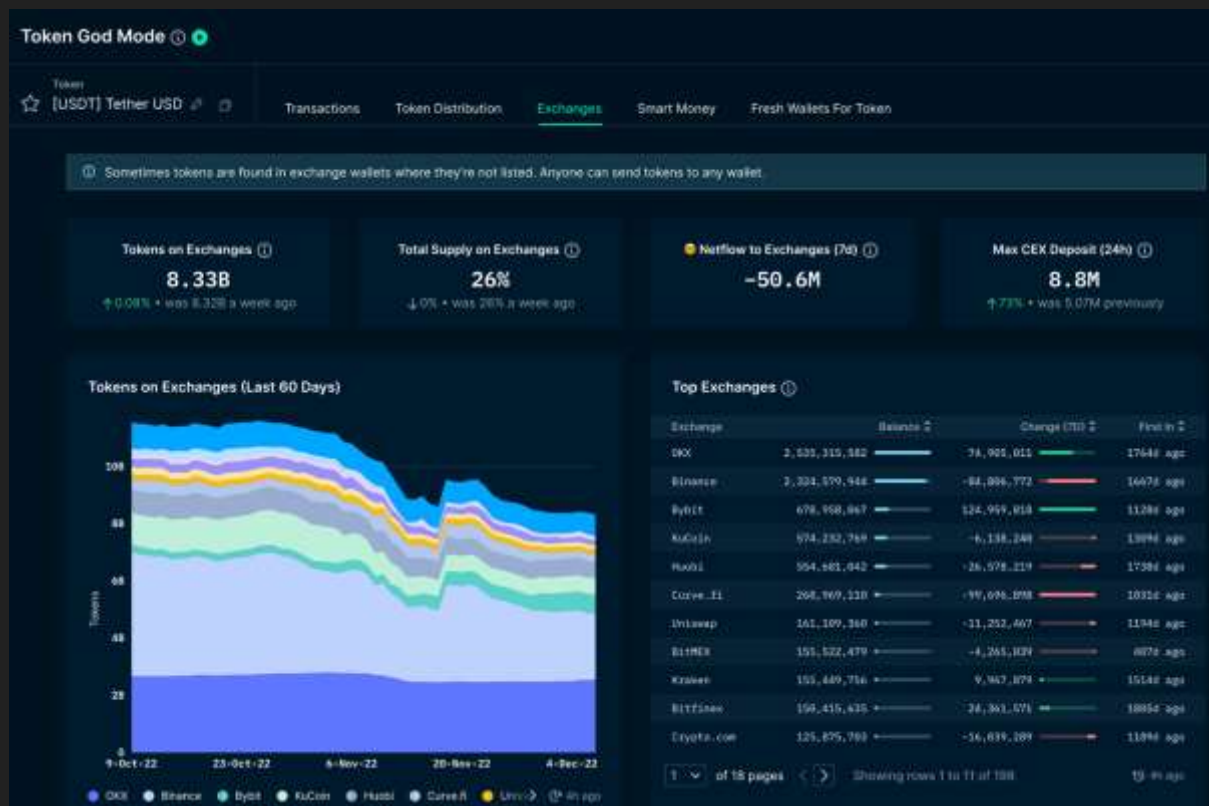
Аналитические сервисы. Что предоставляют?

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

Аналитические сервисы. [Nansen.ai](https://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](https://nansen.ai)



Аналитические сервисы. [Santiment.net](https://santiment.net)

Volume against ETH Based tokens (DEXs)

USD Coin [on Ethereum] USDC
Stablecoin fully backed by USD

Shared axis ☒

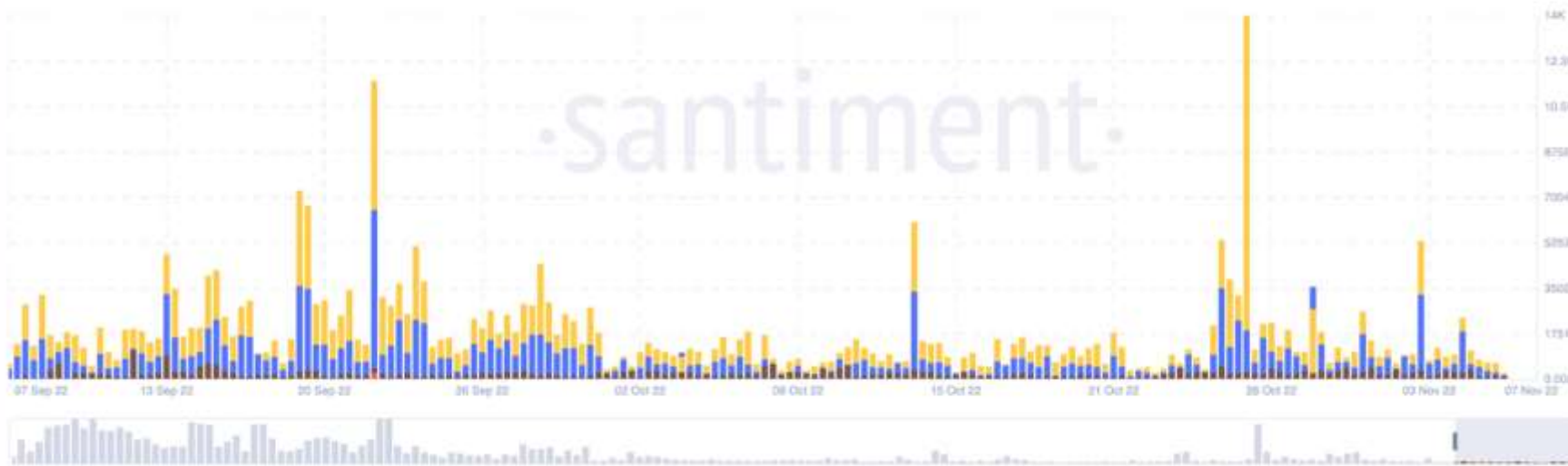
[Why the gaps?](#)

07/09/22 - 06/12/22

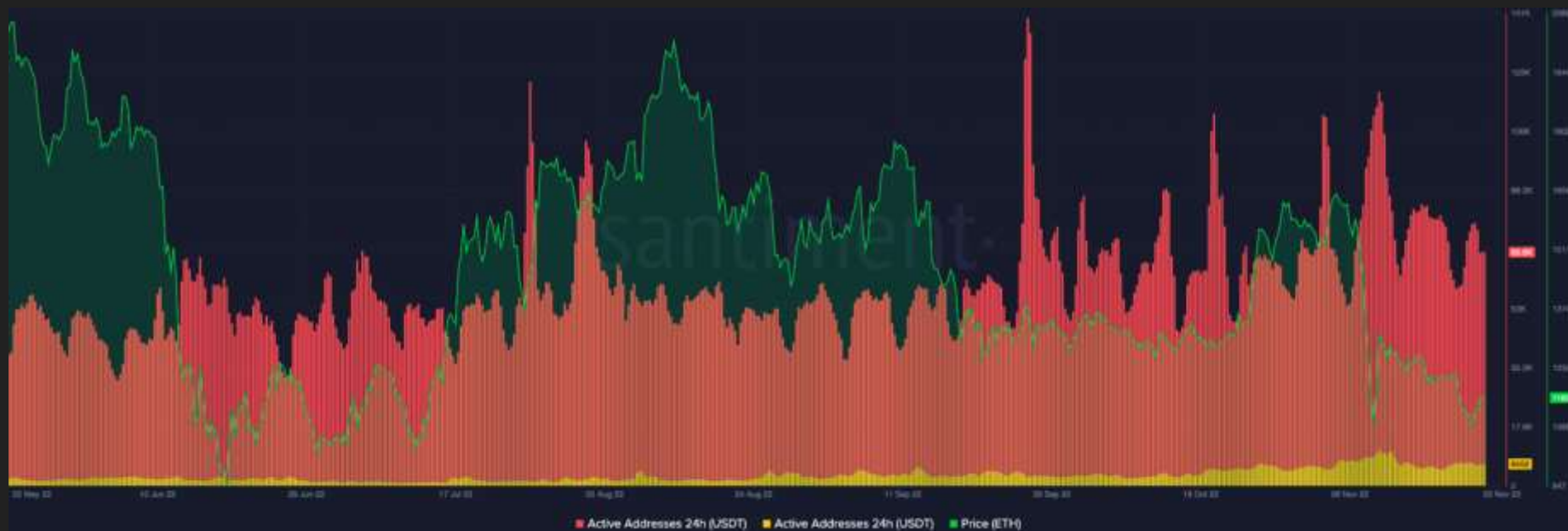


Balancer KyberNetwork UniswapV2 Sushiswap 0x_v1 0x_v2

Interval 8h

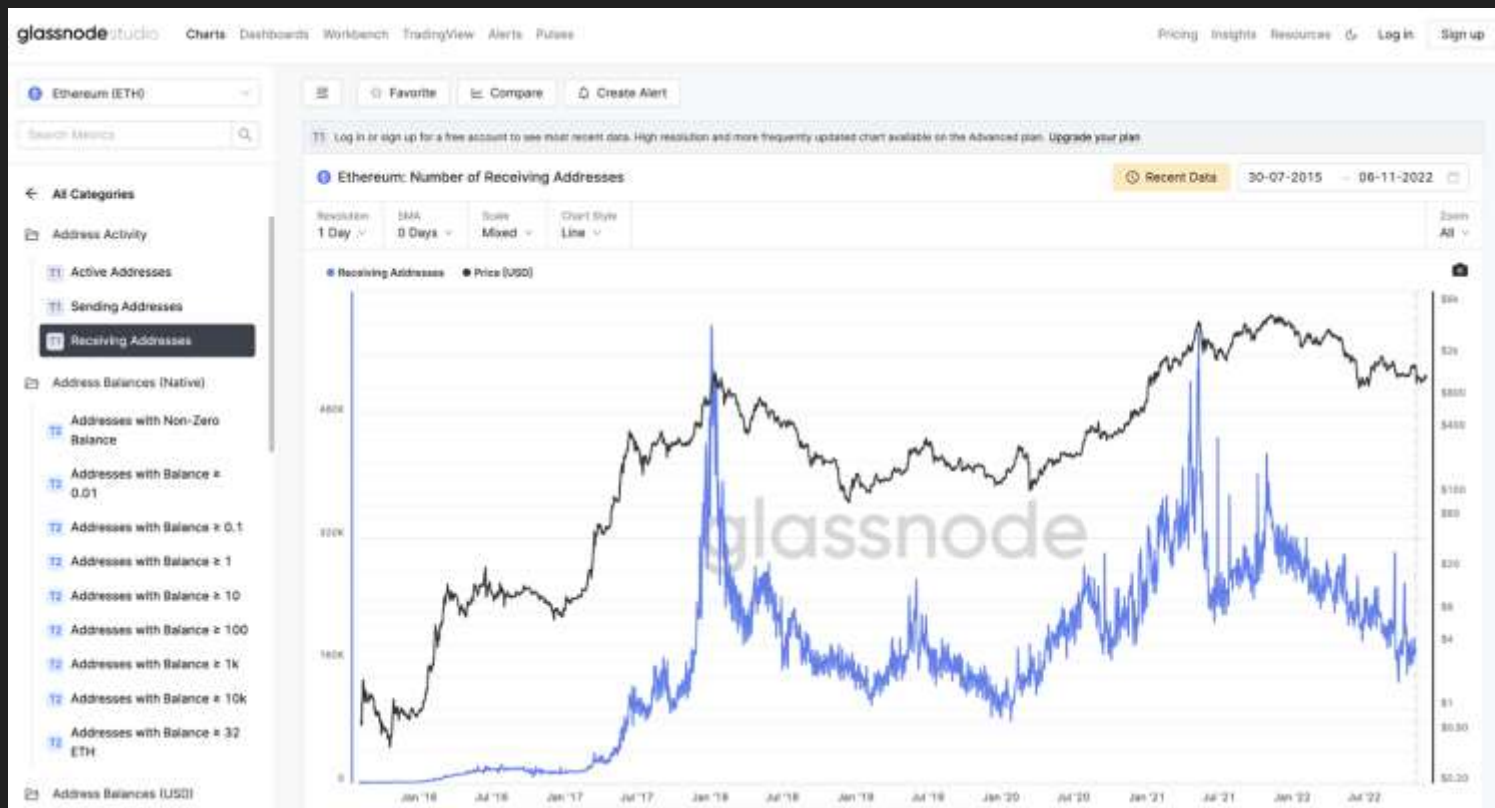


Аналитические сервисы. [Santiment.net](https://santiment.net)



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

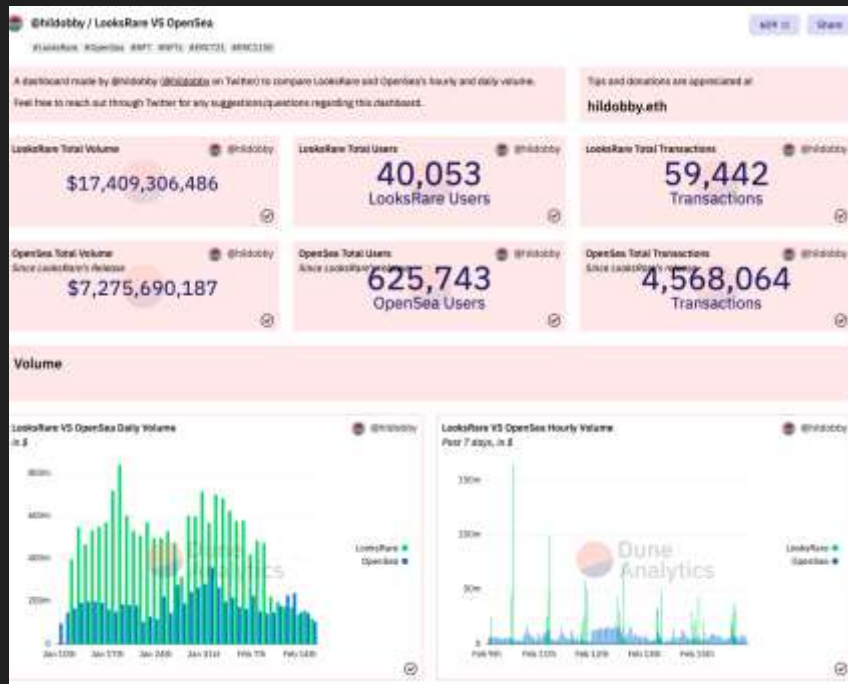
Аналитические сервисы. [Glassnode.com](https://glassnode.com)



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](https://bitquery.io)

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

Blockchain ETL. BigQuery public datasets

The screenshot displays the Google Cloud BigQuery Explorer interface. On the left, the 'Explorer' pane shows a search bar and a list of pinned projects. The 'crypto_ethereum' project is expanded, revealing datasets like 'amended_tokens', 'balances', 'blocks', 'contracts', 'logs' (highlighted), 'sessions', 'token_transfers', 'tokens', 'traces', and 'transactions'.

The main editor area shows a SQL query:

```
1 SELECT *
2 FROM `bigquery-public-data.crypto_ethereum.transactions`
3 WHERE DATE(block_timestamp) >= "2022-02-01"
4     AND to_address = '0x7be8076f4ea4a4ad08075c2508e481d6c946d12b'
5 ORDER BY value DESC
6 LIMIT 1000
```

Below the query, it indicates 'Processing location: US'. The 'Query results' section shows the query is complete (3.9 sec elapsed, 18.2 GB processed). A warning message states: 'Some cell values are very long and the display is truncated to the first 1024 characters to improve browser performance. before clicking "Show full values".'

The results table has the following structure:

Row	hash	nonce	transaction_index
1	0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98	169	599

Bitquery.io

The screenshot displays the Bitquery.io web interface, which is a GraphQL query builder. The top navigation bar includes the Bitquery logo, a 'New Query' button, and a tab for the current query titled 'Buy / sell price spr...'. Below the navigation bar, there are tabs for 'Queries' and 'Builder', with the 'Builder' tab being active. A 'Prettify' button and the URL 'https://graphql.bitquery.io' are also visible.

The left sidebar contains a list of query templates, each with a star icon: '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', and 'Eth2.0 Contract Balance'. The 'Buy / sell price spread' template is selected, and its icon (a link, document, and edit symbols) is shown below the text.

The main workspace is divided into two panels. The left panel shows the raw GraphQL query being constructed, with line numbers 1 through 12. The right panel shows the JSON response of the query, with line numbers 1 through 12. A play button icon is located between the two panels.

GraphQL Query:

```
1 {  
2   ethereum(network: ethereum) {  
3     dexTrades(  
4       date: {is: "2020-11-01"}  
5       exchangeName: {is: "Uniswap"},  
6       baseCurrency: {is: "0xdac17f958d2ee523a2206206994  
7       quoteCurrency: {is: "0xc02aaa39b223fe8d0a0e5c4f27  
8  
9  
10      baseCurrency {  
11        symbol  
12        address
```

JSON Response:

```
1 {  
2   "ethereum.dexTrades": [  
3     {  
4       "baseCurrency": {  
5         "symbol": "USDT",  
6         "address":  
7         "0xdac17f958d2ee523a2206206994597c13d831ec7"  
8       },  
9       "baseAmount": 7699794.407088,  
10      "quoteCurrency": {  
11        "symbol": "WETH",  
12        "address":  
13        "0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2"  
14      },  
15      "quoteAmount": 19829.199117309974,  
16      "trades": 3949,  
17      "quotePrice": 0.0025752894257873066,  
18      "side": "SELL"  
19    },  
20  ]  
21 }
```

At the bottom of the interface, there is a status bar showing 'response' and 'Display' buttons, followed by 'ethereum.dexTrades' and 'Using JSON'.

Вопросы

Сергей Недашковский



[@SergeNedashkovsky](https://www.telegram.me/SergeNedashkovsky)



[@Snedashkovsky](https://github.com/Snedashkovsky)