

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

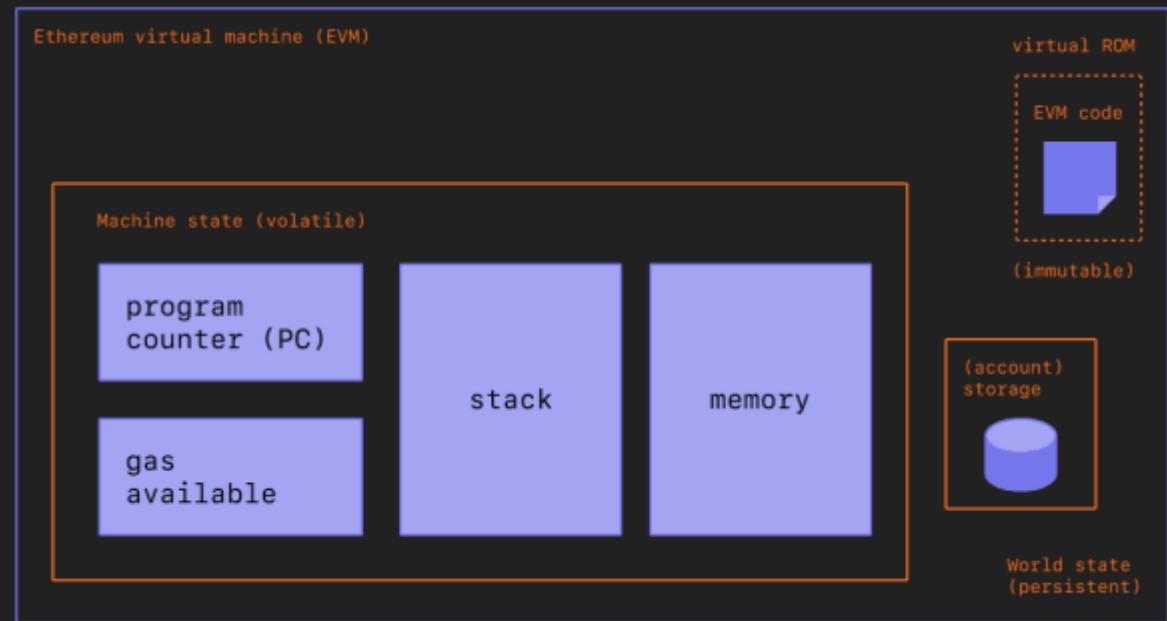
- Ethereum Virtual Machine
- Транзакция
- Контракт



tinyurl.com/4we2sf35

Ethereum Virtual Machine (EVM)

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



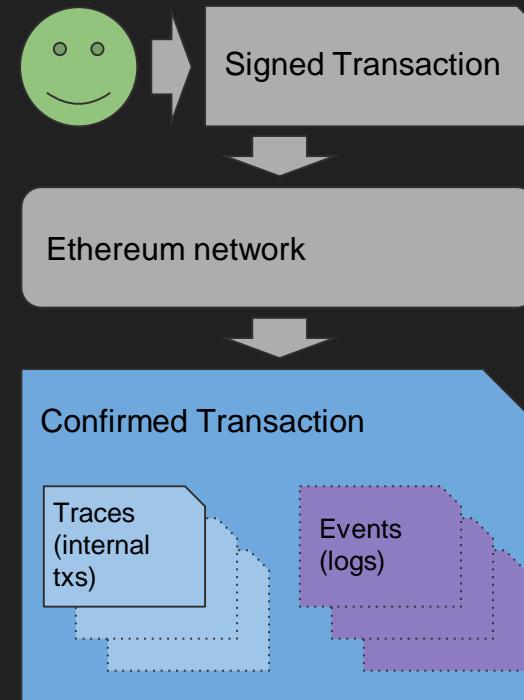
Что такое транзакция (transaction, tx)

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/0x67fbcef377c93800e673f168ca71fe4b20f25e6ed6ecc64f5ecd941d6cdf967b

tinyurl.com/2p9d5yew

Самая большая транзакция в феврале 2022

Overview	State	Comments
Transaction Hash:	0x67fbfce377c93800e673f168ca71fe4b20f25e6ed6ecc64f5ecd941d6cdf967b	Copy
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:	0xd977814e90de44bfa03b6295a0516a897441apec (Binance 8)	Copy
To:	0x28c6c06298d514db089934071355e5743bf21d60 (Binance 14)	Copy
Value:	800,000 Ether	(\$860,160,000.00)
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)

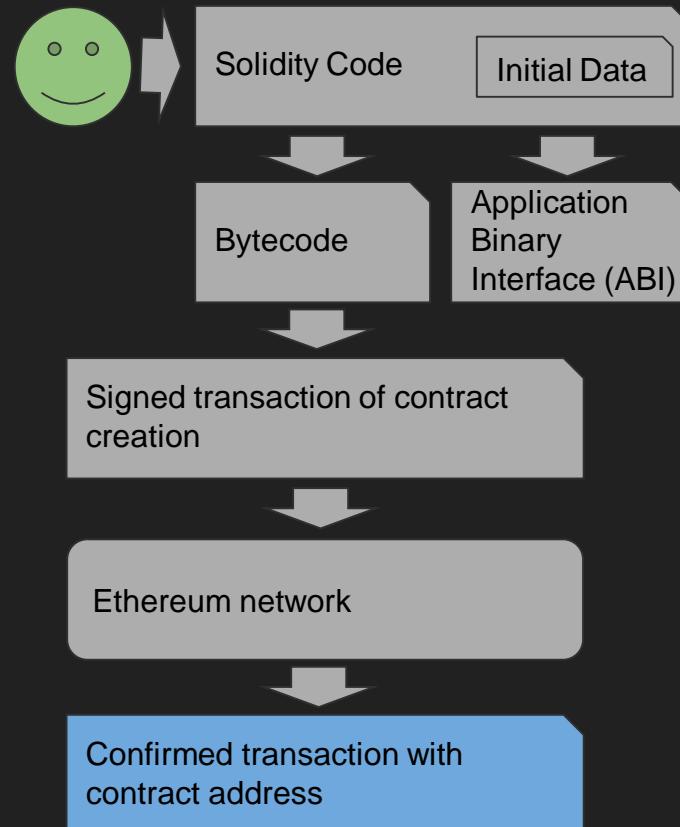
Контракт может быть создан:

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

Контракт. Создание OpenSea

Contract 0x7Be8078f4EA4A4AD08075C2508e481d6C946D12b

Overview Collectives NFT Marketplace

Buy Exchange Swap Gaming

Contract Overview

Balance: 0 Ether

Value: \$0.00

Token: \$74,496.23

More Info

My Name Tag: Not Available, login to update

Creator: 0x0004e81688b9a97541... at bcn 0xed0fbcb591727088c9f...

Tracker: Project Wyvern Exchange

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

16 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
0xb67140737a9db75d8...	Cancel Order	(pending)	5 secs ago	0x0e03a25d92e97fb04...	OpenSea	0 Ether	(Pending)
0x7a7426a407d300c04...	Atomic Match	(pending)	5 secs ago	0x98f14233894c3227f5...	OpenSea	0 Ether	(Pending)
0xb022d9db42719c29...	Atomic Match	(pending)	5 secs ago	0x5ac00e61081a5e3fad...	OpenSea	0.009 Ether	(Pending)
0xne115ad3da54688888...	Atomic Match	(pending)	5 secs ago	0x080f0408f5baa55827...	OpenSea	0.1 Ether	(Pending)
0x1d0e5ef7405cb31167...	Atomic Match	(pending)	5 secs ago	0x0e035394008e17731a...	OpenSea	0.05 Ether	(Pending)

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	



Контракт. Чтение переменных OpenSea



etherscan.io/address/0x7be8076f4ea4a4ad08075c2508e481d6c946d12b

tinyurl.com/bn4t8fy8

Контракт. Чтение переменных OpenSea

The screenshot shows the OpenSea interface for interacting with a smart contract. The top navigation bar includes tabs for Transactions, Internal Txns, Erc20 Token Txns, Erc721 Token Txns, Contract (selected), Events, Analytics, and Comments. Below the navigation is a toolbar with Code, Read Contract (selected), and Write Contract buttons. The main content area is titled 'Read Contract Information' and contains three expandable sections: 1. name, 2. tokenTransferProxy, and 3. staticCall. The 'name' section shows the value 'Project Wyvern Exchange string'. The 'tokenTransferProxy' section shows the value '0x6fc783eeb36cf5e63a79298335c4255169be6e1 address'. The 'staticCall' section has fields for target (address) and calldata (bytes). At the bottom, there is a 'Query' section with a 'Query' button and a 'result bool' field.

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 Wyvern Exchange string

2. tokenTransferProxy

0x6fc783eeb36cf5e63a79298335c4255169be6e1 address

3. staticCall

target (address)

target (address)

calldata (bytes)

calldata (bytes)

extradata (bytes)

extradata (bytes)

Query

result bool

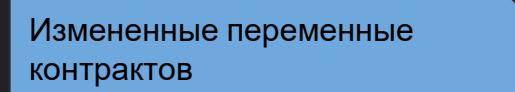
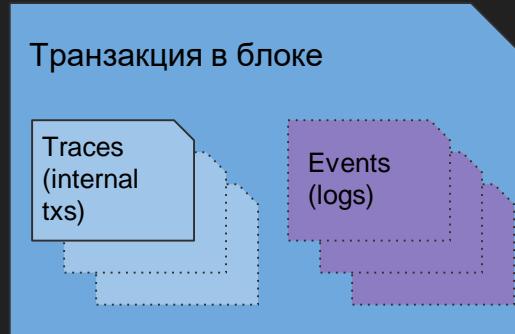
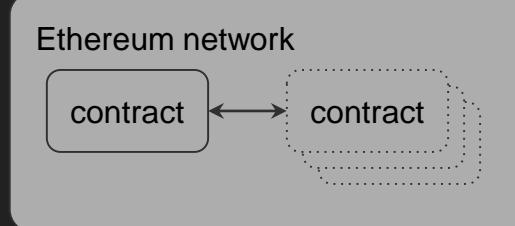
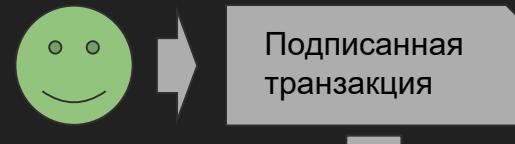
Транзакция контракта

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)



ethereum.org/en/developers/docs/transactions



Транзакция контракта. Закрытие сделки OpenSea



etherscan.io/tx/0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98

tinyurl.com/2p8sshhs

Транзакция контракта. Закрытие сделки OpenSea

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

Transaction Hash: 0xa85f82417ab69aaaa8a382d622a0fe62a8f935571Bade713fe332385fb6c98 ⓘ

Status: Success

Block: 14121210 | 2011987 Block Confirmations

Timestamp: 306 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 0x49784e82923ef52a2d...
↳ 1 of Token ID [8368]

Sponsored:

From: 0x49784e82923ef52a2d0b668d15e16a8272228619 ⓘ

Interacted With (To):
↳ Contract 0x7be8076f4ea4a4ad08075c2508e481d8c94d12b (OpenSea: Wyvern Exchange v1) ⓘ
↳ TRANSFER 33.75 Ether From OpenSea: Wyvern Exch... To → OpenSea: Wyvern Exch...
↳ TRANSFER 416.25 Ether From OpenSea: Wyvern Exch... To → 0x7c453212b25228c258738311...

ERC-721 Tokens Transferred:
From 0x7c453212b2522... To 0x49784e82923ef...
For ERC-721 Token ID [8368] ↳ [CloneX \(CloneX\)](#) 

Value: 450 Ether (\$665,021.00)

Transaction Fee: 0.073548225783352056 Ether (\$90.71)

Транзакция контракта. Закрытие сделки OpenSea

Overview	Internal Txns	Logs (3)	State	Comments
Transaction Receipt Event Logs:				
133				
	Address	0x49cf8f5d44e70224e2e23fdcdd2c053f30ada28b		
	Name	Approval (index_topic_1 address owner, index_topic_2 address approved, index_topic_3 uint256 tokenId)	View	Source
	Topics	0x8c5be1e5ebec7d5bd14f7147d1e84f3dd0314c0f7b2291e5b280ac8c7c3b925		
	1	Dec ↴ → 0x7c453212b25228c25873631140d063a8ae722cb3		
	2	Dec ↴ → 0x00		
	3	Dec ↴ → 8368		
	Data	0x		
133				
	Address	0x49cf8f5d44e70224e2e23fdcdd2c053f30ada28b		
	Name	Transfer (index_topic_1 address from, index_topic_2 address to, index_topic_3 uint256 tokenId)	View	Source
	Topics	0xddf252ad1be289b69c2b068fc378daa952ba7f163c48a11628f55a4df523b3ef		
	1	Dec ↴ → 0x7c453212b25228c25873631140d063a8ae722cb3		
	2	Dec ↴ → 0x49784e92923ef52a2d0b668d15e16a9272229619		
	3	Dec ↴ → 8368		
	Data	0x		

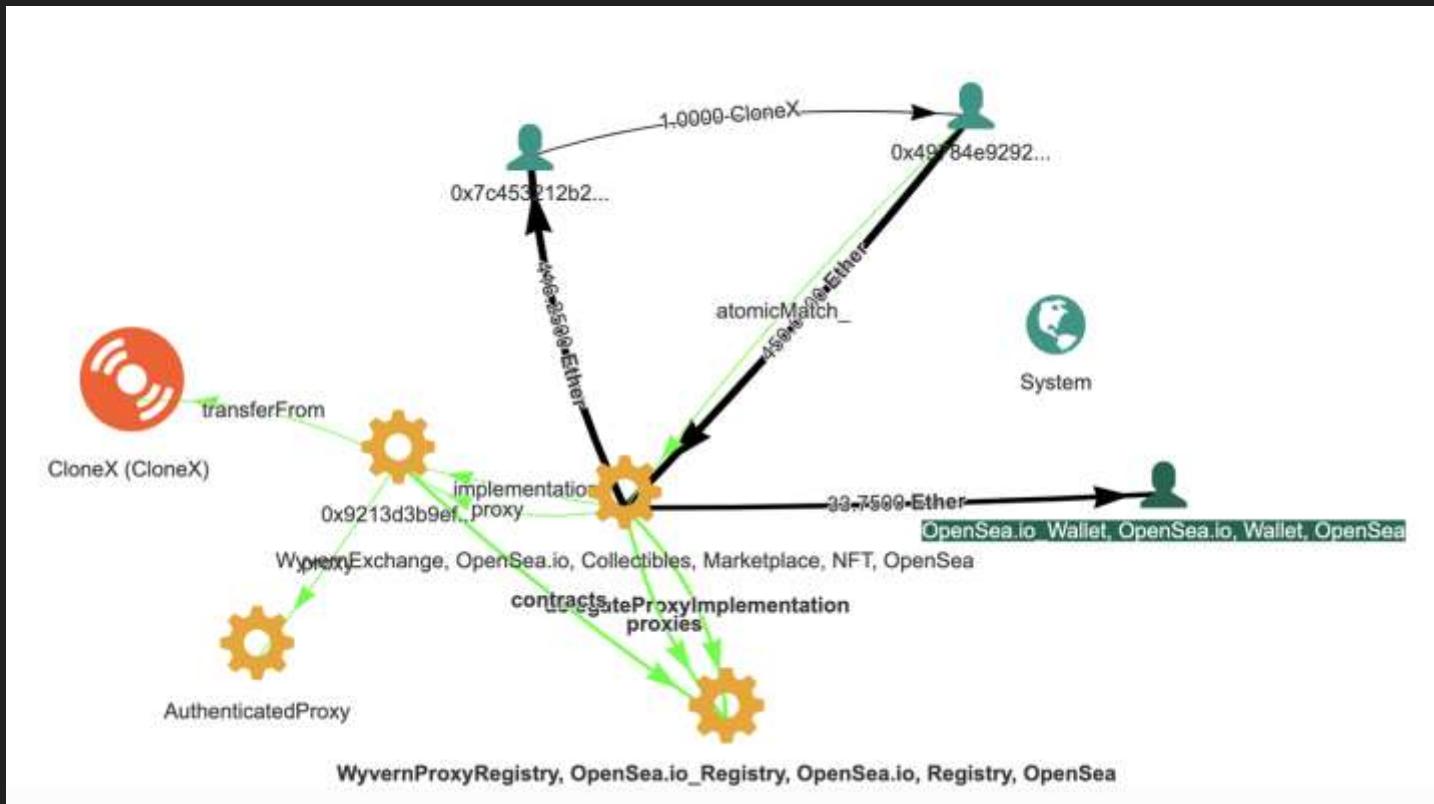
Транзакция контракта. Закрытие сделки OpenSea



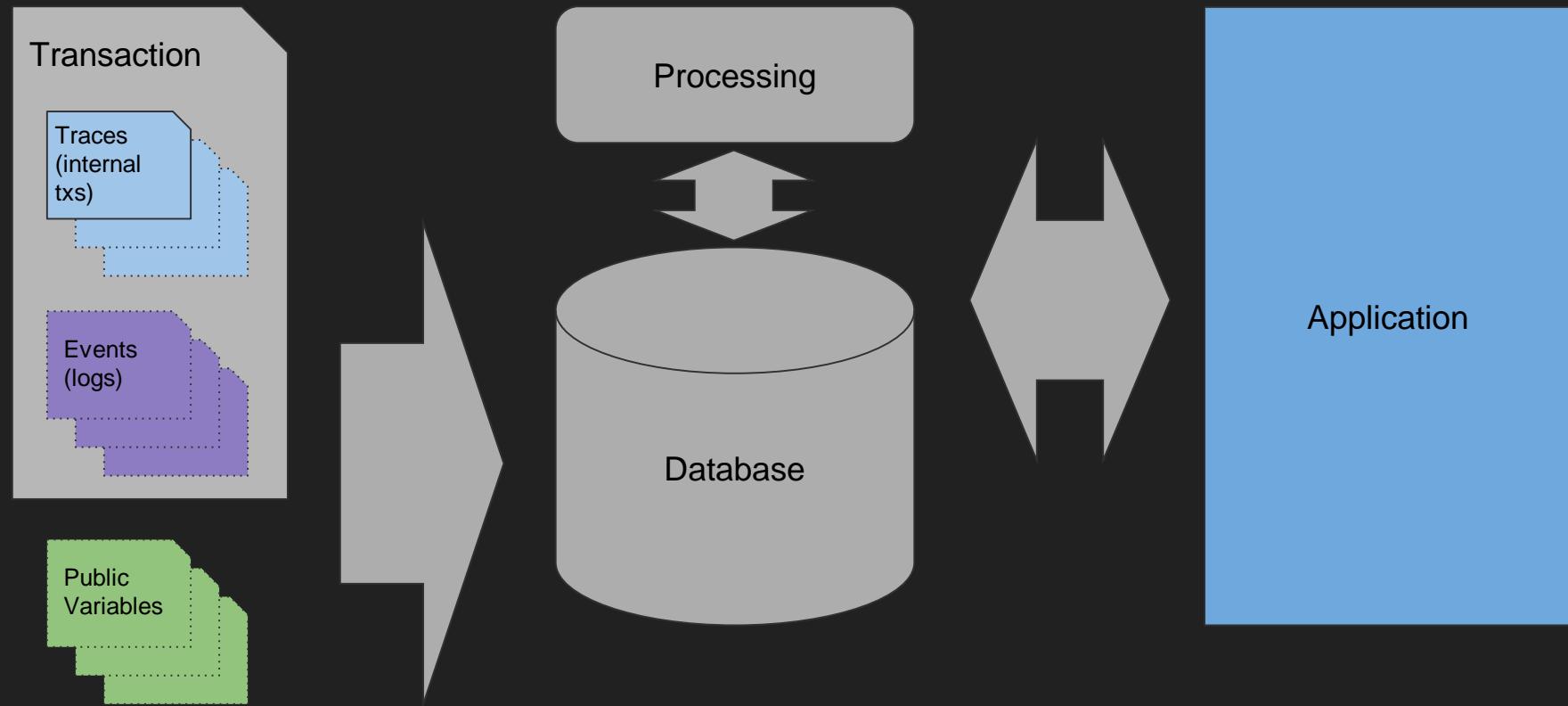
bloxy.info/tx/0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98

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](#)

Token God Mode

Token: [USDT] Tether USD

Transactions, Token Distribution, Exchanges, Smart Money, Fresh Wallets For Token

Sometimes tokens are found in exchange wallets where they're not listed. Anyone can send tokens to any wallet.

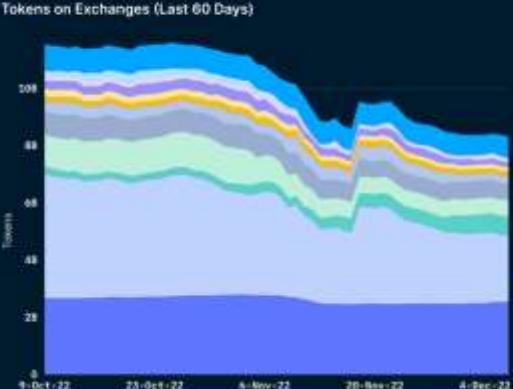
Tokens on Exchanges: 8.33B (↓ 0.08% • was 8.32B a week ago)

Total Supply on Exchanges: 26% (↓ 0% • was 26.5% a week ago)

Netflow to Exchanges (7d): -50.6M (↑ 73% • was 0.07M previously)

Max CEX Deposit (24h): 8.8M

Tokens on Exchanges (Last 60 Days)



Top Exchanges

Exchange	Balance (B)	Change (B)	Last updated
OKX	2,633,315.382	34,905.015	17d ago
Binance	2,304,579.946	-81,895.772	14d ago
Bybit	678,950.967	124,995.813	11d ago
Kucoin	574,232.769	-6,138.246	13d ago
Huobi	554,561.842	-26,578.219	17d ago
Curve.EI	208,169.120	-19,695.010	10d ago
Uniswap	161,109.380	-11,252.467	11d ago
BITMEX	151,532.479	-4,265.109	8d ago
Kraken	155,649.756	9,167.374	15d ago
BITfinex	159,415.435	-24,391.071	10d ago
crypto.com	125,825.760	-16,639.189	11d ago

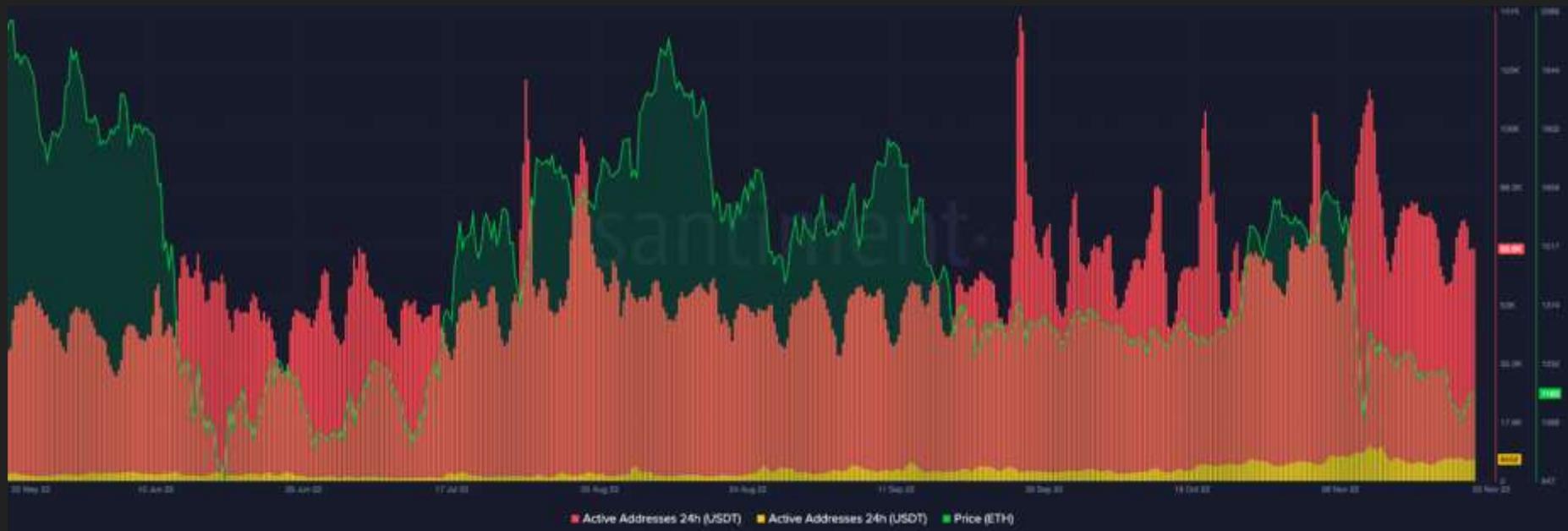
1 of 18 pages < > Showing rows 1 to 11 of 198 19-49 ago

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

Volume against ETH Based tokens (DEXs)



Аналитические сервисы. Santiment.net



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

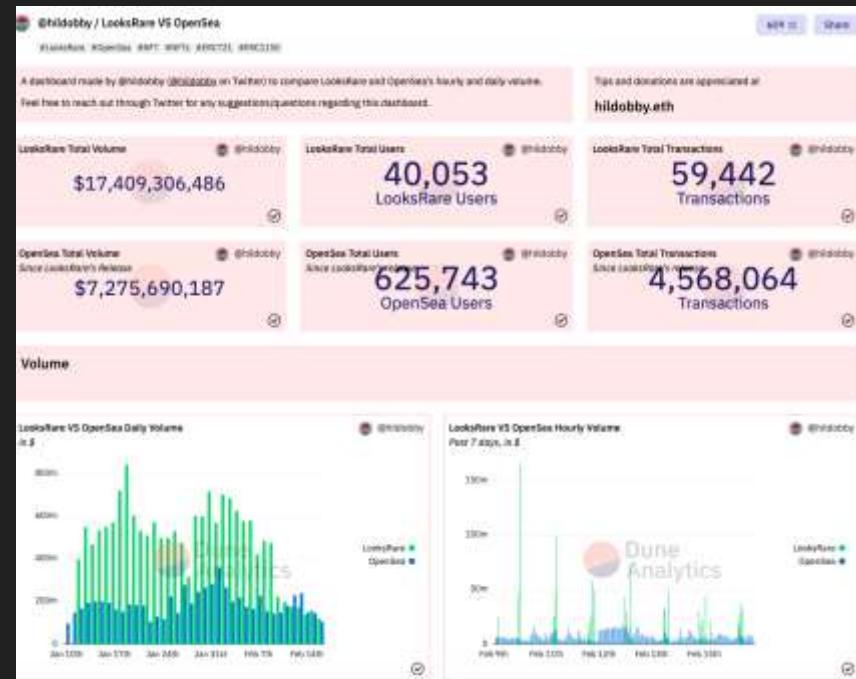
Аналитические сервисы. [Glassnode.com](https://glassnode.com)



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 shows the BigQuery web interface. On the left, the 'Explorer' sidebar is open, displaying a list of datasets and tables under the 'crypto_ethereum' project. The 'logs' table is currently selected and highlighted with a light blue background. The main area shows a query editor with the following SQL code:

```
1 SELECT *
2 FROM `bigquery-public-data.crypto_ethereum.transactions`
3 WHERE DATE(block_timestamp) >= "2022-02-01"
4 AND to_address = '0x7be8076f4ea4a4ad08875c2508e481d6c946d12b'
5 ORDER BY value DESC
6 LIMIT 1000
```

The 'Processing location: US' is specified. Below the code, the 'Query results' section shows a success message: 'Query complete (3.9 sec elapsed, 18.2 GB processed)'. The 'Results' tab is selected, showing the first row of the query results:

Row	hash	nonce	transaction_index
1	0xa85f82417ab69aaaa8a382d622a0ffe62a6f9355718ade713fe332385fbc6c98	169	599

A warning message is displayed: '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".'

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

```
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     baseCurrency {  
10       symbol  
11       address  
12     }  
13   }  
14 }
```

response Display ethereum.dexTrades Using JSON

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

Вопросы

Сергей Недашковский



[@SergeNedashkovsky](https://t.me/SergeNedashkovsky)



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