Starknet

Executive Summary

The following report goes over Transaction Fees on Starknet and its profitability. It covers both the Revenue Side (gas fees acquired) and the cost side (transaction fee payments for DA and Proof submission on Ethereum by Starknet) excluding proof generation costs as that data is not publicly available.

Starknet employs an unorthodox approach to transaction fees. As of version 0.13.1, it uses both ETH and STRK as its currencies for paying transaction fees for interacting with and deploying on the network. The network operates with a block time of 6 minutes or until the block limit of 40,000,000 Cairo Steps is reached, and has a gas limit of 5 million for L2 to L1 messages. Starknet has also announced Volition, which introduces flexible data storage options expected to be implemented after EIP-4844.

This allows users to post data either to Ethereum or off-chain alternatives such as Celestia or EigenDA, potentially reducing fees further.

In Starknet's old fee model, fees were denominated in ETH (wei), and the prover generated proofs for execution traces up to a maximum length. The new model involves a portion of the fees paid in STRK being converted to ETH by the receiving sequencer to cover Ethereum L1 gas costs. Users specify the maximum amount and price for each resource. Future updates will introduce charges for L2 gas, as currently, only proof verification in L1 gas is charged. For transactions prior to v3, fees were denominated in WEI, whereas transactions from v3 onwards are denominated in STRK.

Despite things mentioned above, profits have slowed down, with Starknet experiencing unprofitable weeks after implementing EIP-4844. Total profit: 18,000.00 ETH.

Impact on our design: A majority of transaction pricing model Implementing a similar dual currency model could offer our users flexibility in transaction fee payments. Implementing a similar Volition mechanism can reduce costs and increase scalability. Providing flexible data storage options can give users the ability to choose the most cost-effective and efficient data storage method. This needs to be researched further.

Introduction

Starknet is a Layer 2 Zero knowledge rollup built on Ethereum launched in October 2021. As of version 0.13.1 It uses both ETH and STRK as its currency for paying transaction fees for interacting with and deploying on the network. Block time is 6 minutes (or until it achieves block limit) block limit is 40,000,000.00 Cairo Steps, Gas limit for L2 to L1 messages is 5 million gas. Maximum transaction size is 4 million Cairo steps (more details on Cairo steps in the following paragraphs). It uses a centralized sequencer (decentralization is planned in the future) and proofs were submitted from 3 different addresses to the Starkware Verifier so far. It implemented EIP-4844 on March 20th 2024.

Ten billion Starknet tokens were created by StarkWare in May 2022 and minted on-chain on November 30, 2022. On February 20, 2024 $STRK launched on the exchanges.

Goals & Methodology

The main goal of the report is to analyse Starknet data before and after TGE:

- Average cost of verification
- Number of transactions over time
- Data Availability cost (ETH)
- Average time between submissions for both Data Availability and ZK Proofs
- Fee (movement, adj fee)
- Total revenue
- Economics specifics

This research is performed by obtaining data using Dune Analytics for Ethereum Data, Token Terminal for Starknet fee data and performing statistical analysis. The Economy and other specifics are acquired by reading official documentation, blogs, and other materials on Starknet network.

Results & Discussion

Economics Specifics

Starknet's token STRK allocation is as follows:

- 20.04% for early contributors (team members and early contributors)
- 18.17% for investors
- 10.76% for StarkWare operations
- 12.93% for grants (research, development, deployment, and maintenance)
- 9.00% for community provisions
- 9.00% for community rebates (onboarding costs, available in 2024)
- 10.00% for the Starknet Foundation's strategic reserves
- 8.10% for the Starknet Foundation's treasury
- 2.00% for donations (universities, NGOs)

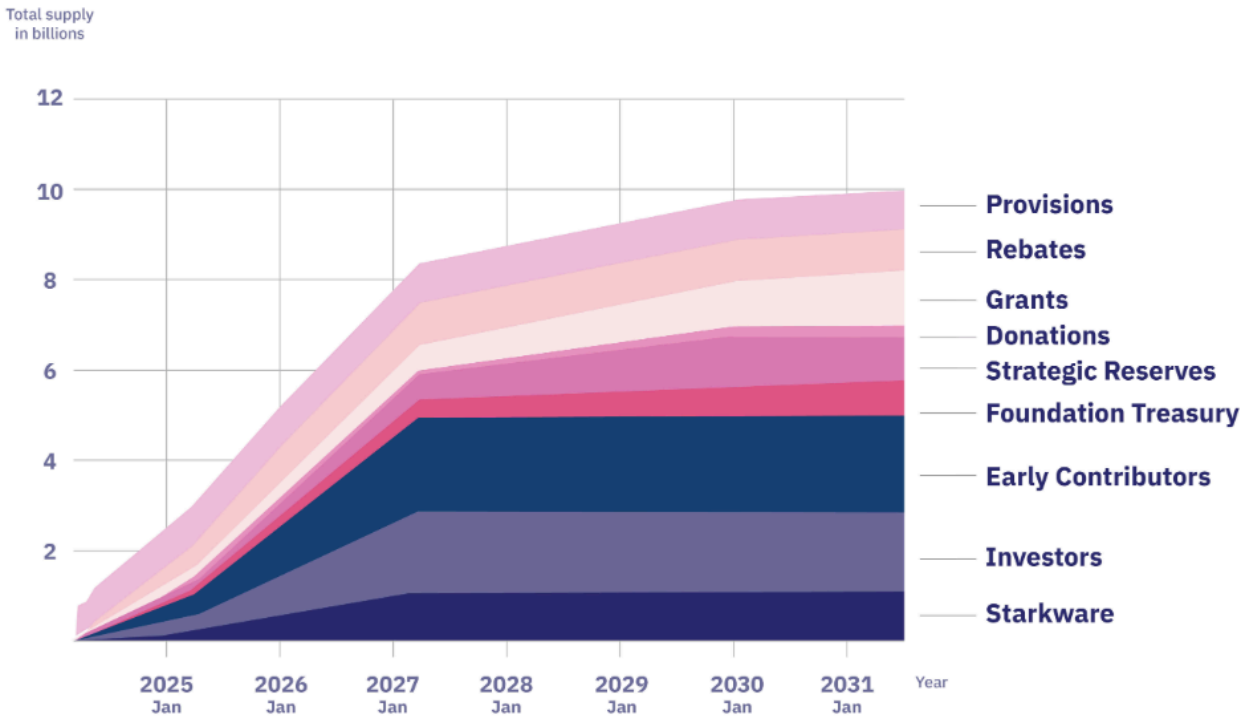
Utility:

Main utilities of STRK are as follows:

- Transaction Fees - transactions can be paid for using STRK as well as ETH
- Governance - voting, either directly or via delegation is required for changes to the protocol
- Staking - Still not implemented, to quote : "Certain services that are critical to the liveness and security of Starknet may require the staking of Starknet tokens."

Lock-Up Schedule

Up to 0.64% (64 million tokens) will be unlocked monthly from April 15, 2024, to March 15, 2025, totaling 7.68% (768 million tokens). Up to 1.27% (127 million tokens) will be unlocked monthly from April 15, 2025, to March 15, 2027, totaling 30.48% (3.048 billion tokens)



We can see a somewhat fast unlock schedule in that ~8.5 billion STRK of 10 billion STRK will be unlocked by 2027 while the rest will be unlocked by end of 2031. There is also possibility of minting new tokens once the Starknet decentralizes further.

Circulating Supply

The circulating supply is planned to increase over time through staking rewards and other mechanisms, but no new tokens will be issued for block rewards while StarkWare operates the sequencer.

Transaction Pricing Mechanism Specifics

Current Transaction Fee Model (v0.13.1.1)

In the current transaction fee model transactions can be paid for using STRK as well as ETH. A portion of the fees paid in STRK are converted to ETH by the receiving sequencer, in order to cover Ethereum L1 gas costs.

Starknet distinguishes between blocks whose state diffs are sent to L1 as calldata and blocks whose state diffs are sent to L1 as blobs. Naturally cost of computation is the same but the data availability costs differ. Currently L1 DA MODE is set to: BLOB. Source.

Users specify the max amount and max price for each resource. Currently the only resource is L1 gas. In future they will introduce L2 gas as currently they are only charging for proof verification in L1 gas. That means computational complexity, on-chain data, L2 → L1 messages, L2 calldata

For transactions prior to v3, the fee is denominated in WEI. For transactions v3 and later, the fee is denominated in STRK.

Blob transactions

$$
\begin{aligned}
F = gas\_price \cdot \Bigg(& \max_k v_k w_k \\
& + message\_calldata\_cost \cdot 3t \\
& + (message\_calldata\_cost + l1\_log\_data\_cost) \cdot \sum_{i=1}^{t} q_i \\
& + (l1\_storage\_write\_cost + log\_message\_to\_l1\_cost) \cdot t \\
& + l2\_payload\_costs \Bigg) \\
& + data\_gas\_price \cdot felt\_size\_in\_bytes \cdot (2(n-1) + 2(m-1) + \ell + 2D)
\end{aligned}
$$

Parameters:

v - vector that represents resource usage, where each of its entries v_k represents different resource types like Cairo Steps, Pedersen hashes, etc.

w - CairoResourceFee weights vector

l - number of contracts whose class was changed (only for contract deploying and applying the replace_call syscall)

n - number of unique contracts updated, fee token is always updated but it does not incur any so (n-1) is included in the formula.

m - number of values updated , the same above condition applies (m-1)

D is 1 if the transaction is of type Declare.

L2 → L1:

- message_calldata_cost = 1124 gas per 32 byte word
- l1_log_data_cost = 256 gas
- l1_storage_write_cost is the cost of writing to new slot = 20,000 gas

felt_size_in_bytes = number of bytes required to encode a single STARK field element

l2_payload_costs =

Resource	**Gas cost**
Event key	0.256 gas/felt
Event data	0.128 gas/felt
Calldata	0.128 gas/felt
CASM bytecode	1 gas/felt
Sierra bytecode	1 gas/felt
ABI	0.032 gas/character

Transactions with calldata:

$$
\begin{aligned}
F = gas\_price \cdot \Bigg(& \max_k v_k w_k \\
& + da\_calldata\_cost \cdot \left(2(n-1) + 2(m-1) + \ell + 2D + 3t + \sum_{i=1}^{t} q_i \right) \\
& - contract\_update\_discount \cdot (n-1) - 240 \\
& + message\_calldata\_cost \cdot 3t \\
& + (message\_calldata\_cost + l1\_log\_data\_cost) \cdot \sum_{i=1}^{t} q_i \\
& + (l1\_storage\_write\_cost + log\_message\_to\_l1\_cost) \cdot t \\
& + l2\_payload\_costs \Big)
\end{aligned}
$$

Parameters:

v,w,n,m,t,l,D parameters are unchanged

message_calldata_cost, l1_log_data_cost, log_message_to_l1_cost, l1_storage_write_cost, l2_payload_costs parameters are unchanged

da_calldata_cost 551 gas per 32-byte word. It is comprised of:

- 512 gas per 32-byte word for calldata.
- ~100 gas for onchain hashing that happens for every sent word.
- a 10% discount, because the sequencer does not incur additional costs for repeated updates to the same storage slot within a single block.

240 gas discount for updating sender balance

contract_update_discount is 312 gas

Whenever a transaction updates some value in the storage of some contract, the following data is sent to L1:

- two 32-byte words per contract
- two 32-byte words for every updated storage value

- storage update fee:

$$\underbrace{gas\_price\left(da\_calldata\_cost \cdot 2(n-1) - contract\_update\_discount \cdot (n-1)\right)}_{\text{contract addresses + new nonce and number of storage updates}} + \underbrace{gas\_price \cdot \left(da\_calldata\_cost \cdot 2(m-1) - 240\right)}_{\text{storage updates}}$$

n - number contracts updated (-1 because fee token contract is always updated each transaction)

m- number of values updated (-1 because sequencer balance is always uodated)

contract discount is 312 gas for every updated contract

240 is the gas discount for updating the senders balace

Currently Starkware is working on this: *"If different transactions within the same block update the same storage cell, there is no need to charge for both transactions, because only the last value reaches L1. In the future, Starknet might include a* ***refund mechanism for such cases****."*

What is priced in general:

- Computational complexity: The marginal cost of verifying the transaction on L1, measured in L1 gas
- Data: The cost of posting the state diffs induced by the transaction to L1. It is measured in L1 gas or L1 data gas, depending on whether or not the L2 block in which the transaction was included uses calldata or blobs.
- L2→L1 messages: Messages sent to L1 are eventually sent to the Starknet core contract as L1 calldata by the sequencer; therefore L2 transaction that send L2→L1 messages incur an additional L1 gas cost.
- L2 calldata, events and code: From Starknet 0.13.1 onwards, there is a per-byte (or per felt) price for L2 payloads.

Example for the transaction gas pricing:

If a transaction uses 10,000 Cairo steps and 500 Pedersen hashes. At most 40,000 such transactions can fit into the hypothetical trace (20,000,000/500). Therefore, its

gas price correlates with **1/40,000** of the cost of submitting proof on L1.

Volition

With Volition Starknet introduces Flexible Data Storage options. This is expected to be introduced some time after EIP-4844 implementation. Users will have an option to post data either to Ethereum or off-chain alternatives such as Celestia or EigenDA. This is expected to bring fees down even further.

Data Availability & Proofs

Periodically, Starknet sends a validity proof to Layer 1 (see Data Analysis portion) . This proof attests to the computations of all the blocks processed since the last proof was sent. Along with the validity proof, Starknet sends the state difference. This state difference details the changes from the empty state to the current state, as a result of executing transactions in all these blocks. The state difference is transmitted to Layer 1. As Starknet continues to produce more blocks on Layer 2, the process repeats. At some point, a new validity proof, along with a new set of transactions for data availability and the new state difference, is sent to Layer 1.

The proof is sent to L1 when any of the Cairo steps, Pedersen hashes etc. slots is filled.

Old Transaction Fee Model (Before **Jan 10, 24**)

Fees are denominated in ETH (wei) . Starknet’s prover generates proofs for execution traces, up to some maximal length L.

Users specify the maximum fee that they are willing to pay for a transaction.

Gas was more expensive per step in this version.

For each transaction, the sequencer calculates a vector CairoResourceUsage holding:

- Number of cairo steps
- Number of aplications (pedersen hashes etc)

The sequencer crosses this information with the CairoResourceFeeWeights vector. For each resource type , CairoResourceFeeWeights has an entry that specifies the relative gas cost of that component in the proof. Formula:

$$\max_k [\text{CairoResourceUsage}_k \cdot \text{CairoResourceFeeWeights}_k]$$

Storage Update Fee

Storage update fee for a transaction updating n unique contracts and m unique keys is:

$$\text{gas\_price} \cdot c_w \cdot \underbrace{(2n + 2m)}_{\text{number of words}}$$

Parameters:

c_w = calldata cost per word

L2→L1 message fee:

$$\text{gas\_price} \cdot c_w \cdot (3 + \text{payload\_size})$$

Deploying contracts fee:

$$gas\_price \cdot 3cw$$

Fee formula is then:

$$F = \text{gas\_price} \cdot \left(\max_k v_k w_k + c_w \left(2(n+m) + 3t + \sum_{i=1}^{t} q_i + 3\ell \right) \right)$$

Parameter:

W is the weights vector

c_w = calldata cost per word

l = contract deployments

t = messages with payload sizes q1....qt

n = unique contract updates

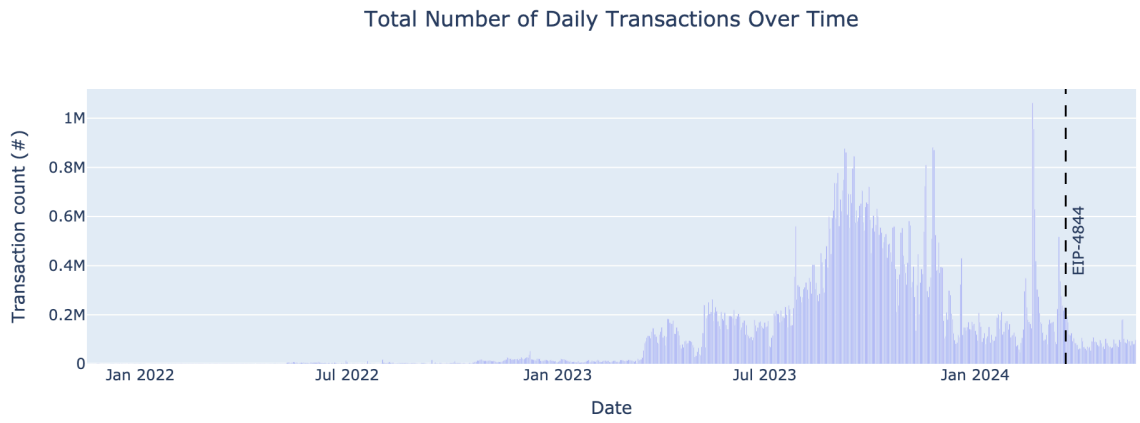
Gas Per Step New vs Old

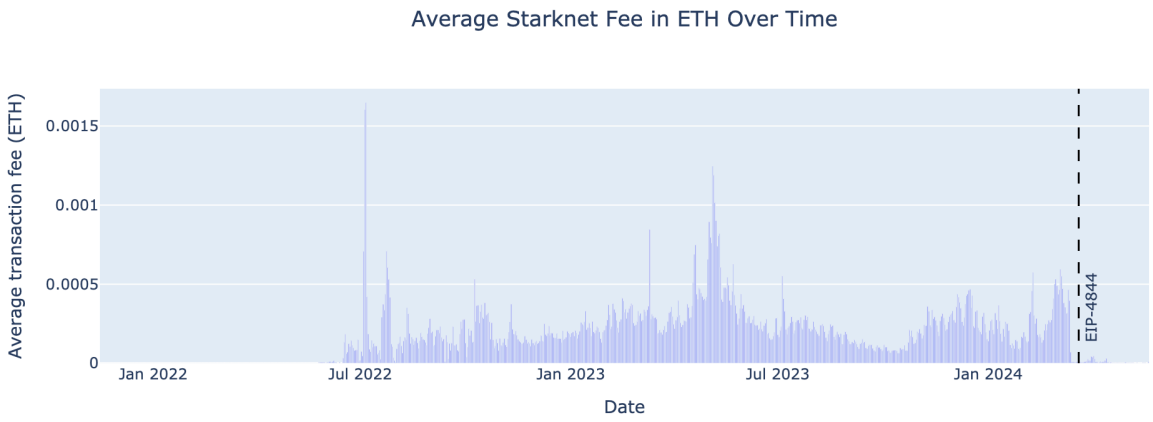
Step	Gas cost (New)	Gas Cost (Old)
Cairo step	0.0025 gas/step	0.01 gas/step
Pedersen	0.08 gas/application	0.32 gas/application
Poseidon	0.08 gas/application	0.32 gas/application
Range check	0.04 gas/application	0.16 gas/application
ECDSA	5.12 gas/application	20.48 gas/application
Keccak	5.12 gas/application	20.48 gas/application
Bitwise	0.16 gas/application	0.64 gas/application
EC_OP	2.56 gas/application	10.24 gas/application

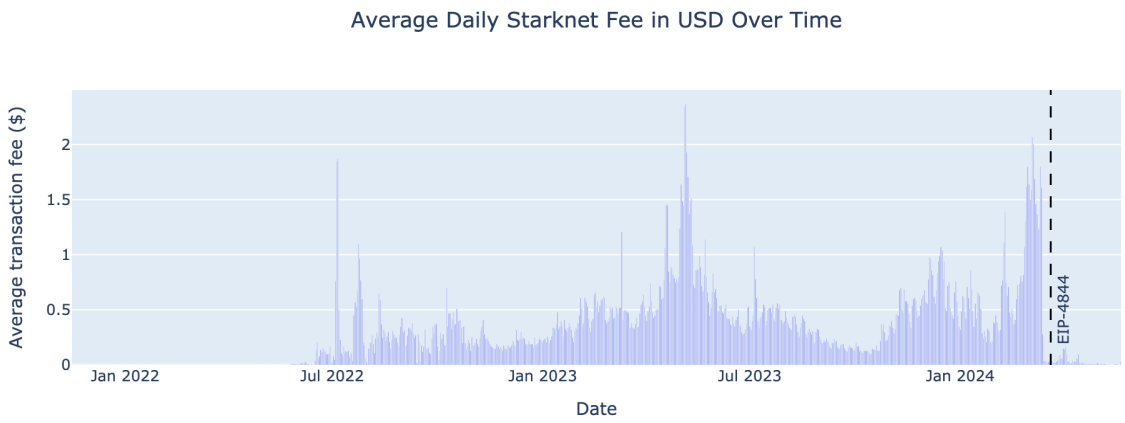
We can see that gas costs per step are lower in the new model.

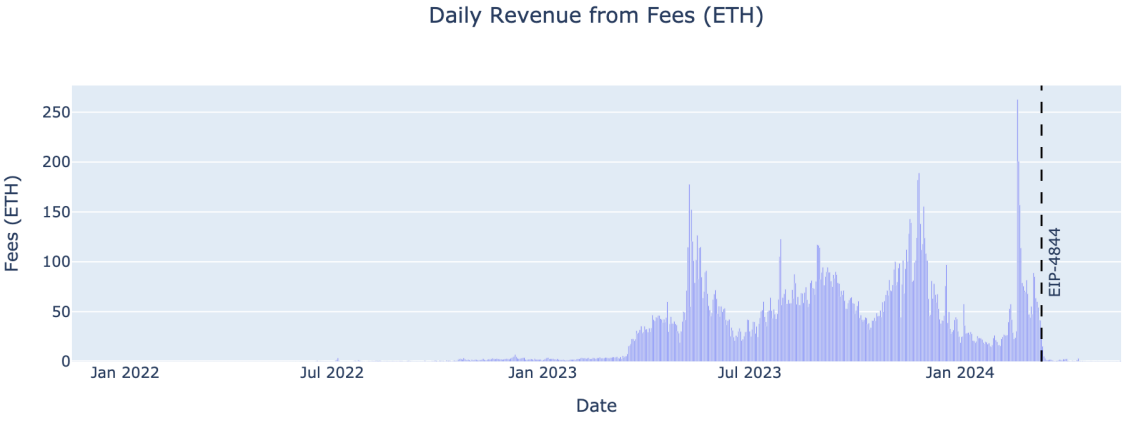
Data analysis

Revenue Side




Average Starknet Fee in ETH Over Time
Average transaction fee (ETH)
0.0015
0.001
0.0005
0
Jan 2022
Jul 2022
Jan 2023
Jul 2023
Jan 2024
Date
EIP-4844

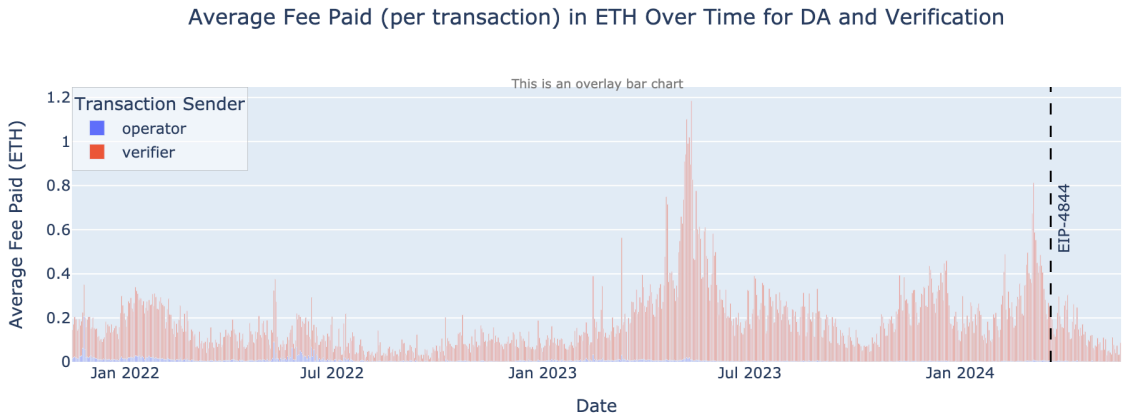

Average Daily Starknet Fee in USD Over Time
Average transaction fee ($)
2
1.5
1
0.5
0
Jan 2022
Jul 2022
Jan 2023
Jul 2023
Jan 2024
Date
EIP-4844


Daily Revenue from Fees (ETH)
Fees (ETH)
250
200
150
100
50
0
Jan 2022
Jul 2022
Jan 2023
Jul 2023
Jan 2024
Date
EIP-4844

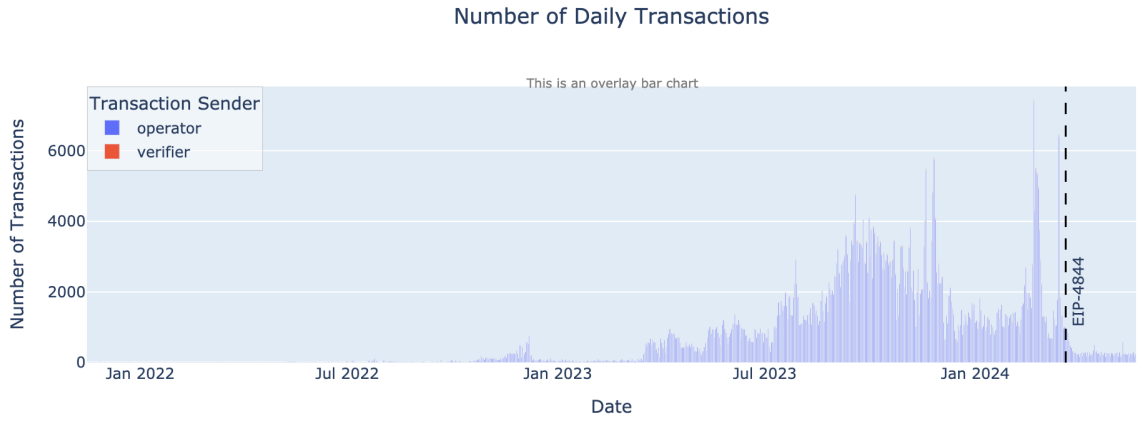
Cost side

In the charts we will separate the fees by the name of the sender:

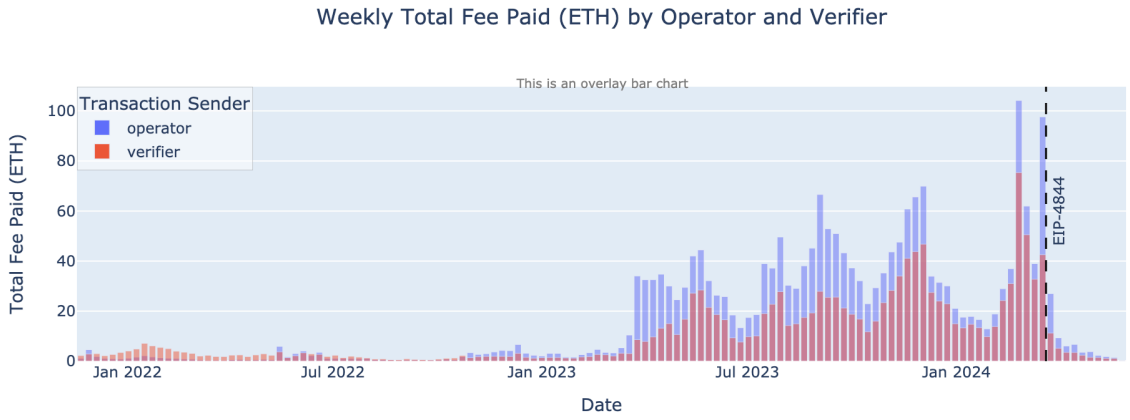
- Verifier - proofs
- Operator - data



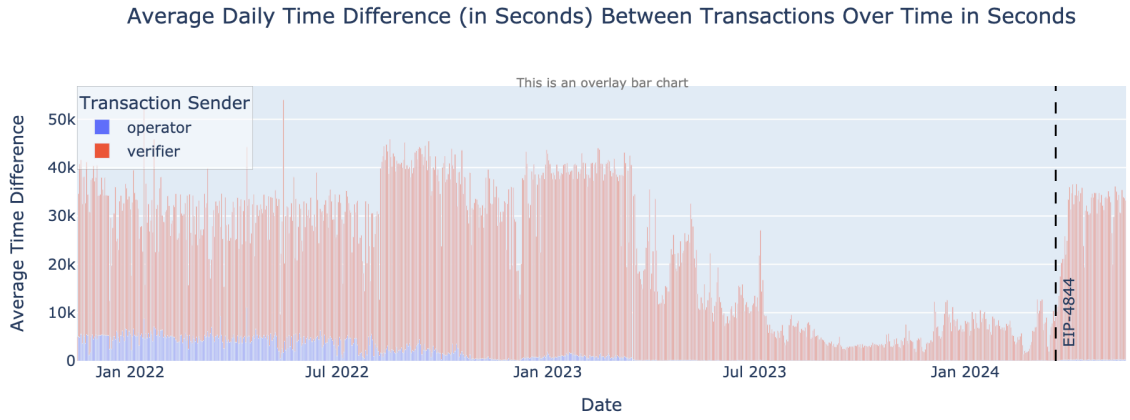
As this is an overlay chart we can see that the average fee for data is smaller in comparison.



We can see that the operator pays less but posts substantially more transactions Daily.

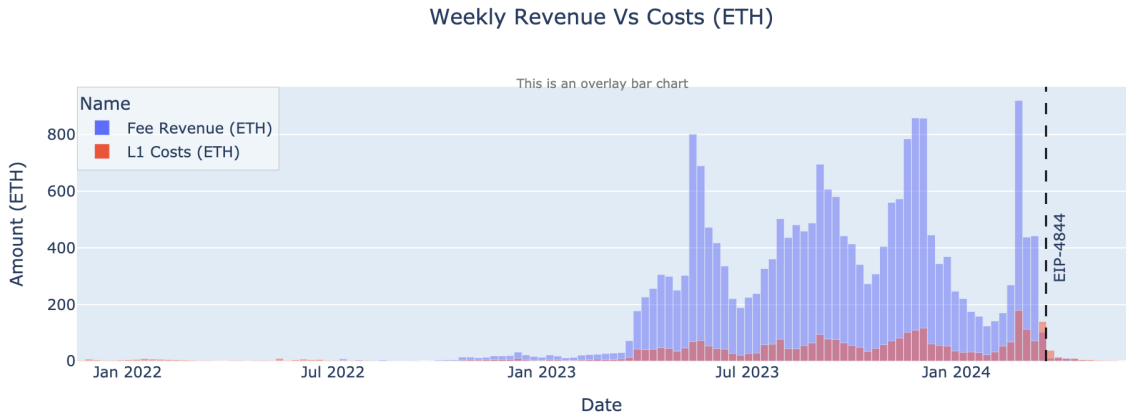


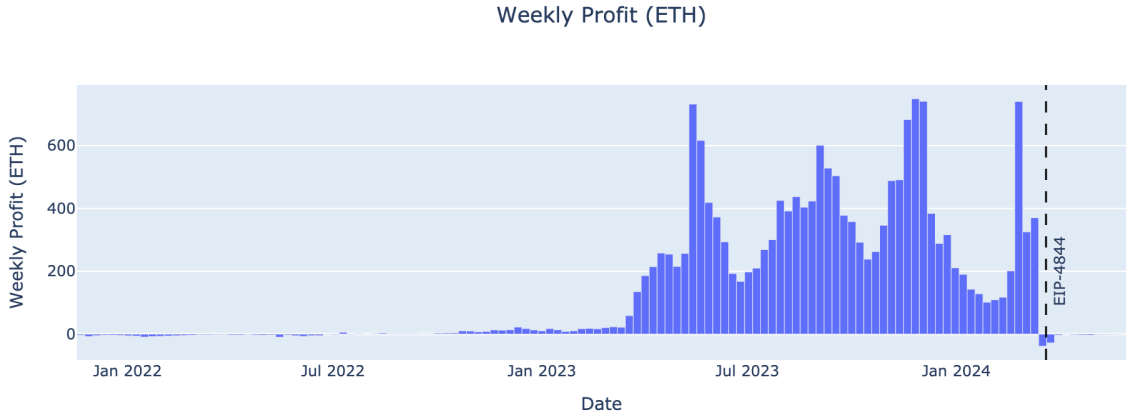
We can see a drop of fees in both proofs and data after EIP-4844 upgrade.

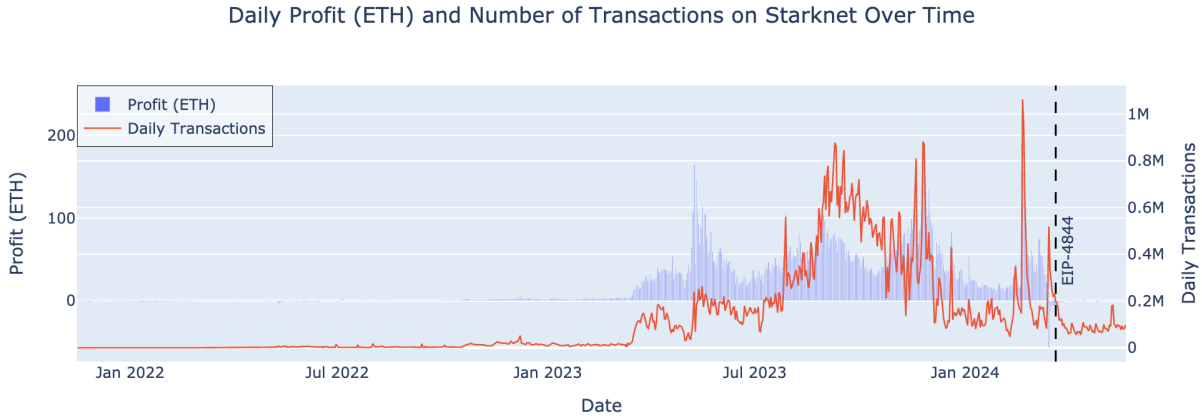


Profitability

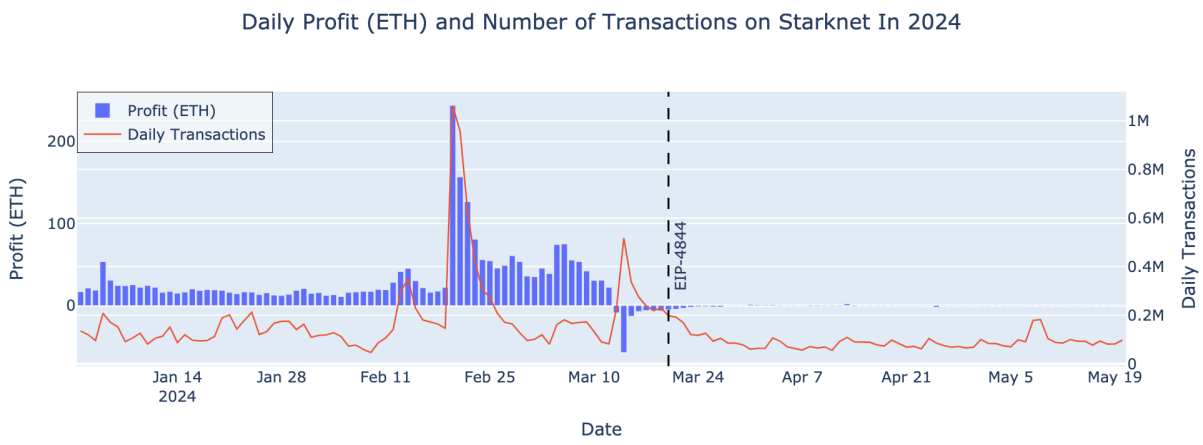
For profitability we have not taken into consideration the proof generation costs as they are not public.



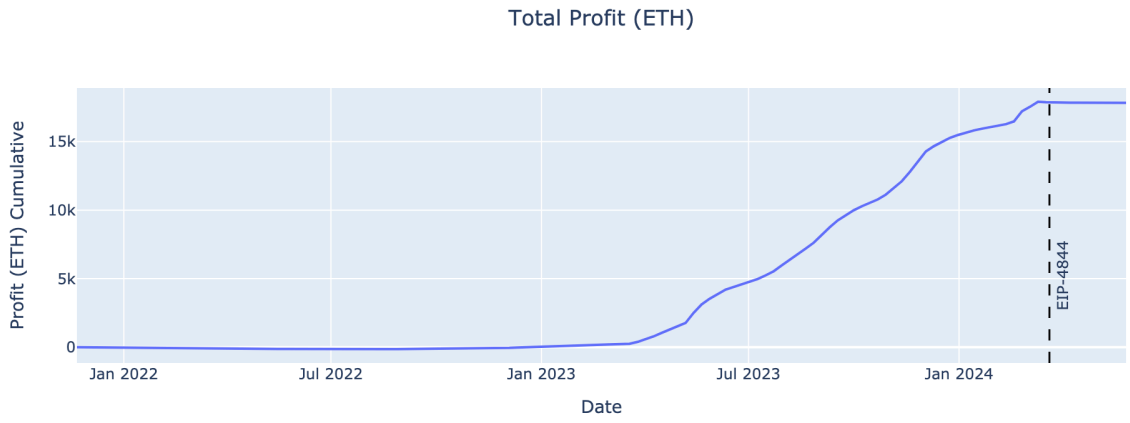




Lets take a look at the 2024 profit data more closely:



We can see the after EIP-4844 upgrade the profits reduced drastically. The cheaper fees did not yield more transaction on Starknet.



We can see a slow down in profitability as a result of EIP-4844 upgrade.

Data Tables

Month	Profit (ETH)
2021-11	-12.2351
2021-12	-18.876
2022-01	-33.1879

2022-02	-19.0465
2022-03	-11.2257
2022-04	-12.8423
2022-05	-23.5297
2022-06	-17.4157
2022-07	4.93387
2022-08	10.8115
2022-09	7.21864
2022-10	28.9231
2022-11	46.9254
2022-12	70.6239
2023-01	54.6786
2023-02	76.1525
2023-03	367.968
2023-04	994.413
2023-05	2183.81
2023-06	1015.76
2023-07	1315.73
2023-08	1961.52
2023-09	1960.26
2023-10	1311.26
2023-11	2730.86
2023-12	1492.21
2024-01	615.849
2024-02	1324.37
2024-03	416.769
2024-04	-9.07754
2024-05	-4.29116

AverageFee Info Before EIP-4844 Implementation (USD)

Statistic	Average transaction fee ($)
mean	0.33638596491228073
std	0.360457250323783
min	0
25%	0.02
50%	0.26
75%	0.48
max	2.37

Average Fee Info After EIP-4844 Implementation (USD)

Statistic	Average transaction fee ($)
mean	0.02774193548387097
std	0.0354095177924079
min	0
25%	0.01
50%	0.01
75%	0.03
max	0.16

Descriptive Statistics for DA and Proofs Before EIP-4844

statistic	metric	operator	verifier
total_transactions	mean	727.6409356725146	6.844262295081967
total_transactions	std	1080.1952230351587	8.40074013411864
total_transactions	min	1	1
total_transactions	25%	14	2
total_transactions	50%	85	2
total_transactions	75%	1097.5	9
total_transactions	max	7367	61
avg_time_diff	mean	1734.5534795681729	21105.8177506438
avg_time_diff	std	2108.750979020295	12792.395226719158
avg_time_diff	min	11.284919234423782	1374.688524590164
avg_time_diff	25%	66.33570923690237	7800.3
avg_time_diff	50%	601.2923076923076	22694
avg_time_diff	75%	3657.7625	31411.5
avg_time_diff	max	11055.833333333334	52295
avg_fee_paid_ETH	mean	0.00783943059423321	0.17972971862828335
avg_fee_paid_ETH	std	0.010870782313389494	0.1441037350750971
avg_fee_paid_ETH	min	0.0008186110495551	0.0131720896214561
avg_fee_paid_ETH	25%	0.0028948920577642	0.08438218229027505
avg_fee_paid_ETH	50%	0.0049471347576707	0.1408491318462852
avg_fee_paid_ETH	75%	0.0089424382388355	0.23226848143706483
avg_fee_paid_ETH	max	0.2075618540881906	1.1739884909939784

Descriptive Statistics for DA and Proofs After EIP-4844

statistic	metric	operator	verifier
total_transactions	mean	298.1639344262295	2.180327868852459
total_transactions	std	142.97857419066548	1.3103205297599447
total_transactions	min	171	1
total_transactions	25%	234	2
total_transactions	50%	266	2
total_transactions	75%	293	2
total_transactions	max	955	8
avg_time_diff	mean	246.18416518196958	30125.329508196723
avg_time_diff	std	63.266501111982144	6426.001519331293
avg_time_diff	min	85.28167539267015	10102.5
avg_time_diff	25%	215.1282051282051	29988
avg_time_diff	50%	248.84641638225256	32964
avg_time_diff	75%	271.85714285714283	34152
avg_time_diff	max	371.6891191709845	36360
avg_fee_paid_ETH	mean	0.0023964024411403735	0.12239644751616711
avg_fee_paid_ETH	std	0.0016939340420129448	0.06872399650321055
avg_fee_paid_ETH	min	0.0005248864042115	0.029230736571974
avg_fee_paid_ETH	25%	0.0011022258492343	0.070215722426883
avg_fee_paid_ETH	50%	0.0018025609600088	0.1112800829545205
avg_fee_paid_ETH	75%	0.0033486731603511	0.1532729352849405
avg_fee_paid_ETH	max	0.0071029090059524	0.2988043843501941