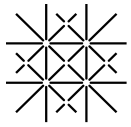


University of Basel

Center for Innovative Finance

Smart Contracts and Decentralized Finance

Gas and Fees

Prof. Dr. Fabian Schär
University of Basel

Release Ver.: (Local Release)
Version Hash: 34e09b088b6ea52cabd4443f56991b3f9d4fdc35
Version Date: 2022-09-16 16:04:03 +0200

The Halting Problem and its Implications

230 A. M. TURING [Nov. 12,

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π, e, etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.

Although the class of computable numbers is so great, and in many ways similar to the class of real numbers, it is nevertheless enumerable. In § 8 I examine certain arguments which would seem to prove the contrary. By the correct application of one of these arguments, conclusions are reached which are superficially similar to those of Gödel†. These results

† Gödel, "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I", *Monatshefte Math. Phys.*, 38 (1931), 173–198.

In 1936, Alan Turing has shown that a (turing) machine cannot tell if a script will halt or run forever, before execution.

↗ Online PDF

$\Rightarrow$ Infinite loops or resource intensive scripts are a potential attack vector that must be addressed.

Bitcoin and Ethereum Deal With This Problem in Different Ways

- Bitcoin Script is a deliberately limited scripting language.
- Ethereum has a Turing complete instruction set. It charges a small fee (gas) for each computation step.

Ethereum Gas Fees: The Basics

Each EVM operation consumes a defined amount of gas. The user cannot change these amounts. Some examples:[1]

Addition

→ 3 gas units

Multiplication

→ 5 gas units

Store 256 bits

→ 20k gas units

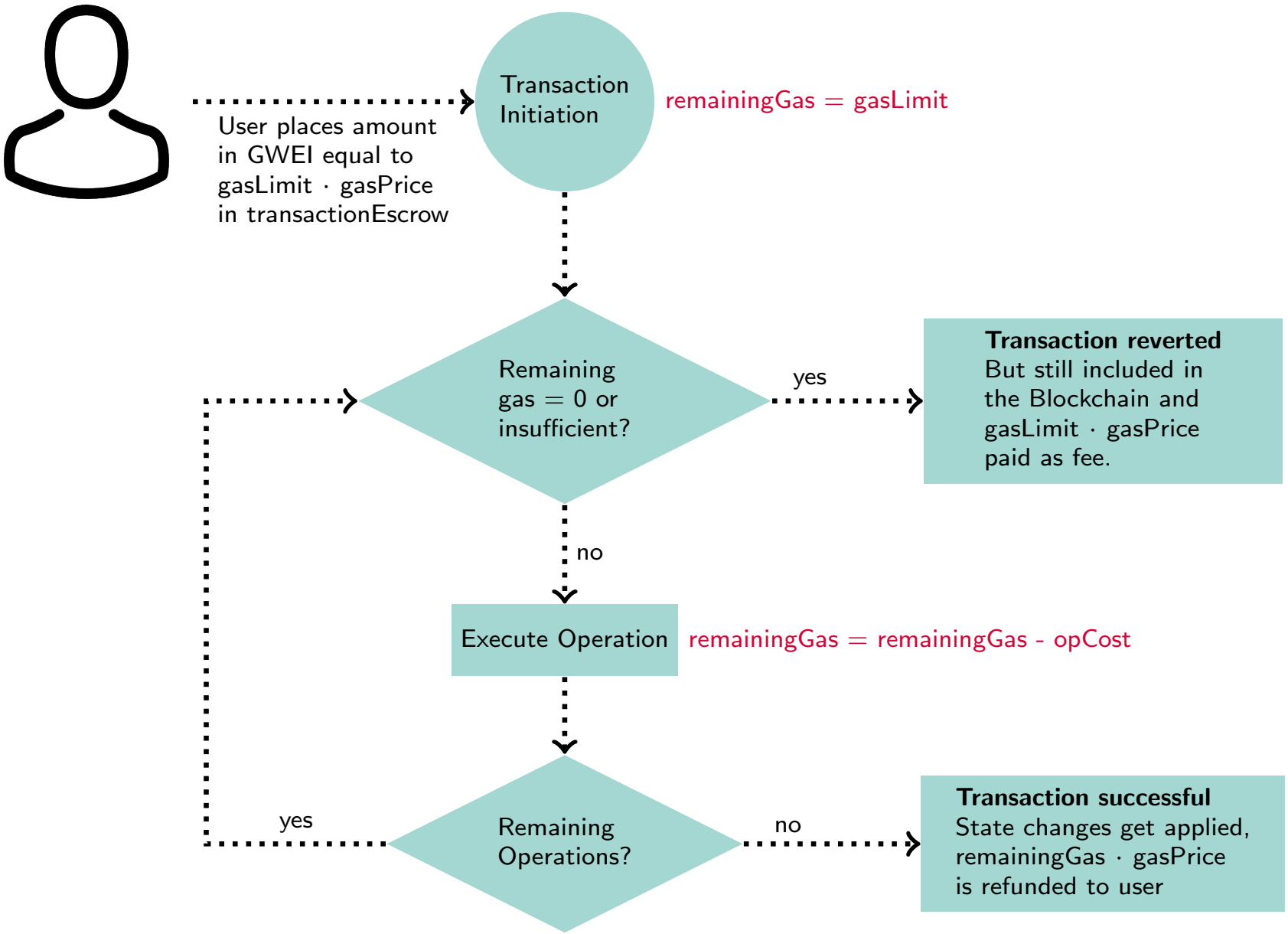
For each transaction the user specifies a **gas limit**, i.e., the maximum amount of gas that can be consumed by it. Examples:

- $21k$ gas units are required to send ETH.
- Gas consumption of contract execution varies.

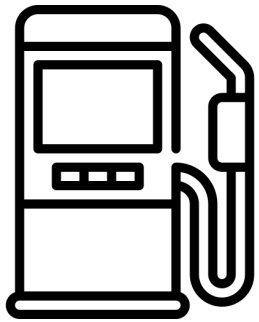
The user also sets the **gas price** for each transaction, i.e., the price in μETH or gwei the user offers to pay per unit of gas.

[1] Full list

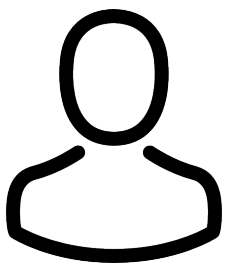
Understanding the Ethereum Fee Process

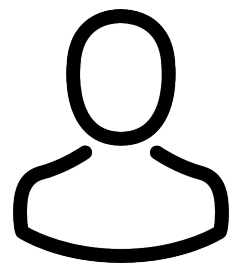


A Gas Consumption Example



gasLimit: 100
remainingGas: 100979262
gasPrice: x





100 · x GWEI

62 · x GWEI

Start

+100

ADD

-3

MUL

-5

SHA3BASE

-30

End

EVM Operations

Ethereum Gas Fees: EIP-1559

On August 5, 2021, the Ethereum gas mechanism was updated with EIP-1559[2] as part of the London hard fork.[3]

Issues addressed by the proposal:

- Mismatch between volatility of transaction fee levels and social cost of transactions.
- Needless delays for users.
- Inefficiencies of first price auctions.
- Instability of blockchains with no block reward.

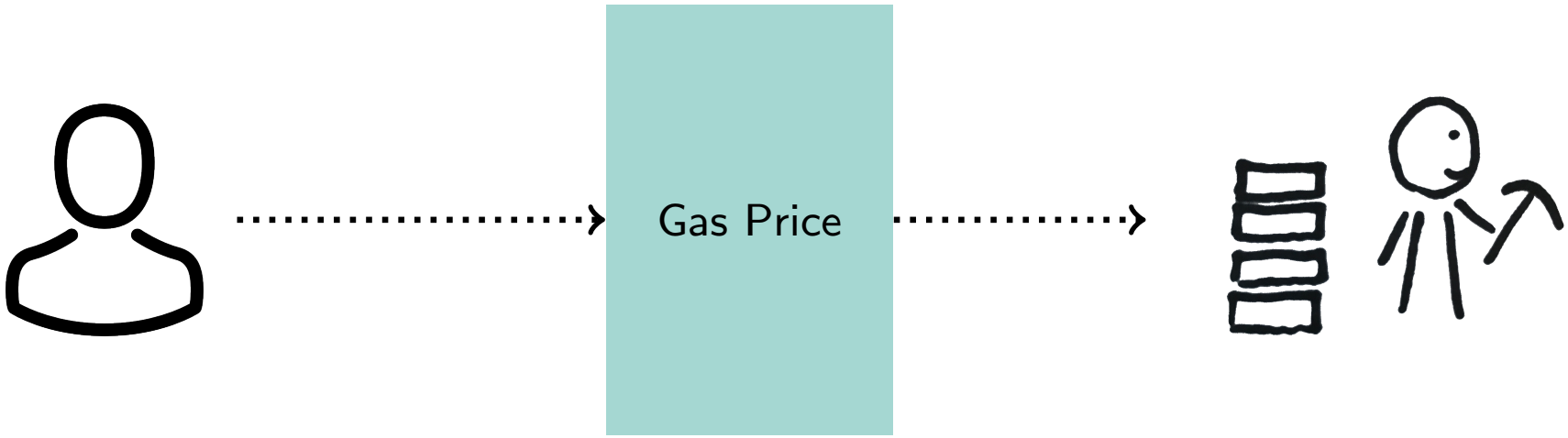
Key changes:

- Dynamic base fee calculated and burned by the network.
- Variable block size.

[2] More details on EIP 1559

[3] More details on the London hard fork

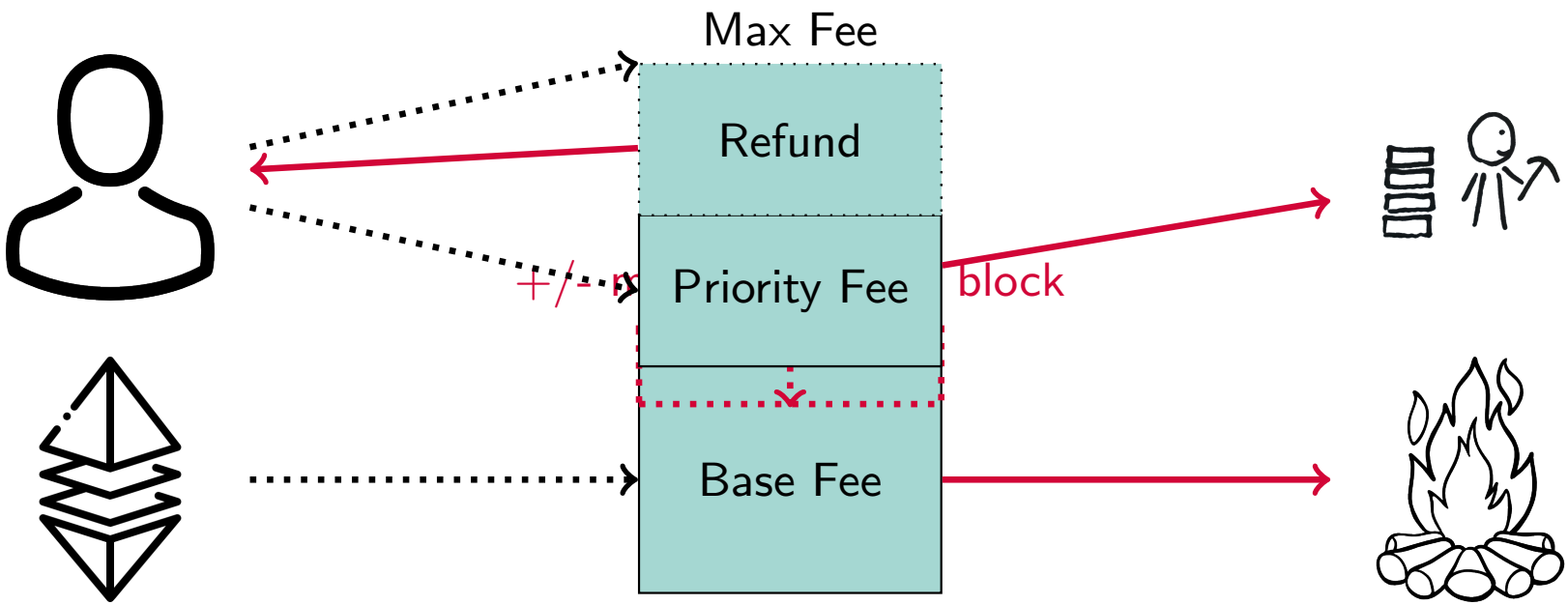
Ethereum Gas Fees: Gas Price Before EIP-1559



First-price auction

- User specifies gas price, he is willing to pay for the transaction.
- Miners are incentivized to include transactions with higher gas prices first.
- All transaction fees ($\texttt{gasPrice} \cdot \texttt{gasUsed}$) go to miner of the block.

Ethereum Gas Fees: Gas Price After EIP-1559



Ethereum Gas Fees: Gas Price After EIP-1559

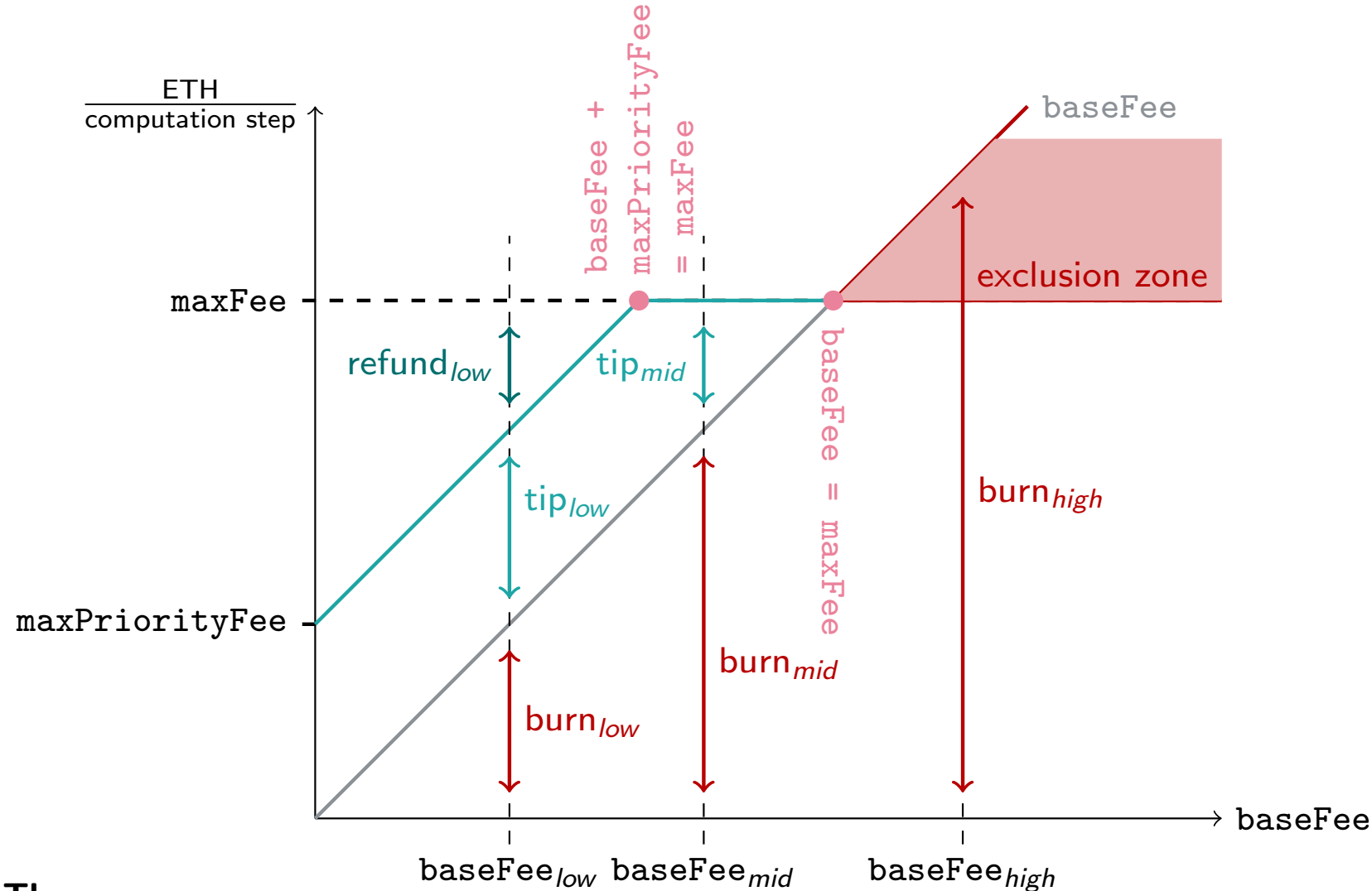
Base fee is calculated by the network depending on demand for block space. It can in- or decrease by max 12.5% from one block to the next. It gets burned by the network, taking ETH out of circulation.

Priority fee (tip) is set by the user to give the miner an incentive to include the transaction in the block. Miner receives the priority fee of all included transactions.

Max fee is set by the user and corresponds to the maximum willingness to pay for one unit of gas. Transaction remains pending if $\texttt{baseFee} > \texttt{maxFee}$.

Refund: $max\,(0,\ \texttt{maxFee} - (\texttt{baseFee} + \texttt{maxPriorityFee}))$ is refunded to the user after transaction execution.

Ethereum Gas Fees: Gas Price After EIP-1559



Three cases:

1. **Refund:** $\texttt{baseFee} + \texttt{maxPriorityFee} < \texttt{maxFee}$
2. **Partial Tip:** $\texttt{baseFee} + \texttt{maxPriorityFee} \geq \texttt{maxFee}$ & $\texttt{baseFee} \leq \texttt{maxFee}$
3. **Pending:** $\texttt{baseFee} > \texttt{maxFee}$

Ethereum Gas Fees: EIP-1559 Base Fee Adjustment

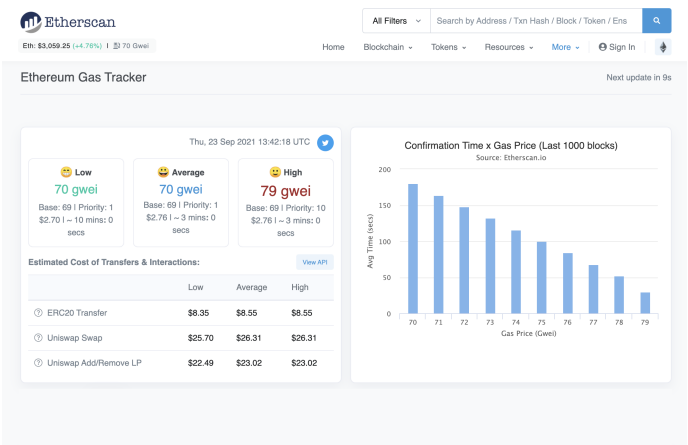
EIP-1559 Base Fee Adjustment Mechanism[4]

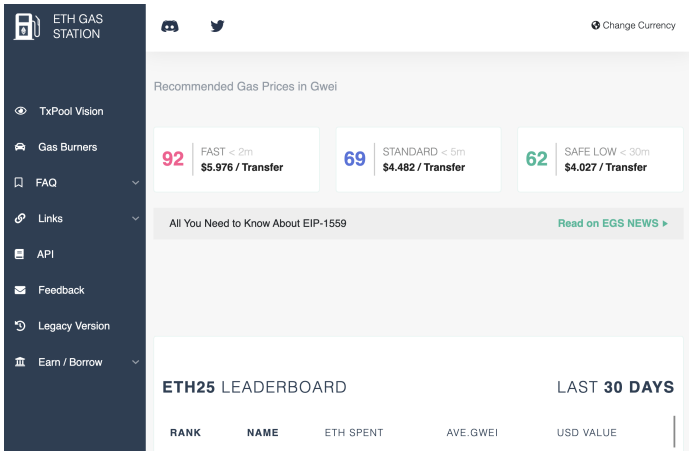
- Target block size: currently 15 million gas (s_{target}).
- Block limit: currently 30 million gas (2x target block size).
- Block size and base fee of previous block (s_{pred}, r_{pred}) determine base fee of current block (r_{cur}).

$$r_{cur} = r_{pred} \cdot \left(1 + \frac{1}{8} \cdot \frac{s_{pred} - s_{target}}{s_{target}}\right)$$

[4] Roughgarden (2020)

Essential Tools: Ethereum Gas Tracker





Etherscan

Eth Gas Station

Exercise 1 - Transactions With EIP-1559

Exercise 1

For the following questions assume a `baseFee` of 0.000000013 GWEI and a threshold `priorityFee` of 1 GWEI:[a]

a. Use your Metamask account to initiate a simple ETH value transaction with a `maxPriorityFee` of 2 GWEI and a `maxFee` of 3 GWEI. How large do you expect the fee to be considering a gasLimit of 21000?

b. Use your Metamask account to initiate a simple ETH value transaction with a `maxPriorityFee` of 0.5 GWEI, a `maxFee` of 1 GWEI and a gasLimit of 21000. What do you expect to happen?

c. Use your Metamask account to initiate a simple ETH value transaction with a `maxPriorityFee` of 2 GWEI, a `maxFee` of 3 GWEI and a gasLimit of 1000000. What do you expect to happen?

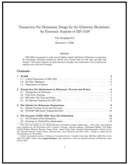
d. Use your Metamask account to initiate a simple ETH value transaction with a `maxPriorityFee` of 2 GWEI, a `maxFee` of 3 GWEI and a gasLimit of 1000. What do you expect to happen?

e. Use your Metamask account to initiate a simple ETH value transaction with a `maxPriorityFee` of 3 GWEI, a `maxFee` of 3 GWEI and a gasLimit of 21000. What do you expect to happen?

---

[a] Please note: The values we use in this exercise have been chosen with Ropsten testnet in mind. The Mainnet `baseFee` is much higher.

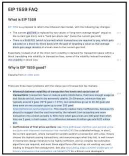
Recommended Reading


Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559*

Tim Roughgarden

December 1, 2020

Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559
Tim Roughgarden, 2020
Online PDF


EIP 1559 FAQ

What is EIP 1559

Why is EIP 1559 good?

EIP-1559 FAQ
Vitalik Buterin, 2021
Online PDF