Introduction to the gas markets

Ethereum is in the business of selling blockspace. This is a commodity that allows users to settle their transactions or interact with smart contracts. The amount of blockspace, however, is limited. To guide which transactions are and which are not included in a block, the gas market was created.

All computations executed on the EVM consume real-world computational power. To compare the costs of these different operations, also known as opcodes, these costs are represented relative to one another using units of gas. For example, adding two numbers costs 3 units of gas; multiplying two numbers costs 5 units of gas.

When submitting a transaction, users specify the price per unit of gas they are willing to pay. Users who bid a higher gas price are more likely to be included in the next block than lower bidders. This is referred to as the priority gas auction, first formalized in Flashboys 2.0.

EIP-1559 changed this fee market. Users now pay a fee consisting of a base fee, which is burned, and a tip, that goes to the block builder.

The maximum block size doubled to 30 million gas units, however, the target block size is half of that. If there are few users willing to pay the base fee and the block size is below the target, the base fee decreases. Similarly, if the block size is above the target, the base fee increases.

Figure 1: Decomposition of the gas fee after EIP-1559

EIP-1559 made gas prices more predictable, yet they still fluctuate heavily over time. For many applications it may be necessary to not be exposed to this price volatility.

Figure 2: Volatility of the gas price over the last 90 days.

Introducing, blockspace derivatives, financial contracts that allow users to hedge their exposure to fluctuations in gas prices.

In this article we will investigate the design space of such on-chain blockspace derivatives.

First the exact scenario for blockspace derivatives is formalized. Second, common use cases are shown and we look at a current and past solution. Then, the risks of structuring these types of financial contracts are explored. Finally, we investigate the possible design options and elaborate on why some may be more useful than others.

Scenario sketch

Let's try to make this scenario a bit more formal. Assume Alice knows at block N

that she wants to include a transaction, consuming m

units of gas, within the blocks N + k

up to N + k + z

, with $k \geq 1$

and $z \geq 0$

.

Alice does not want to be exposed to risks concerning inclusion on-chain and therefore decides to hedge her risk by entering into an agreement with Bob, transferring this risk in exchange for paying a fixed price: a financial derivative.

If Alice wants her transaction to be included in the range of block N + k

to N + k + z

, she and Bob must come to an agreement on the price and details of the derivative before block N + k

.

Figure 3: Sketch representing the blockchain partitioned in a buying range and execution range.

Applications

There are many applications for blockspace derivatives, here some common use cases are given that already exist and could grow in the future.

Rollups

Rollups sell Layer 2 blockspace to their users before knowing the marginal Layer 1 gas costs that these transactions will impose.

This means that rollups are exposed to the gas price of Layer 1 in the short-term. Thereby, they effectively become sellers of blockspace derivatives, a type of vertical integration that may not be wanted. During a talk at ETHconomics, Ed Felten from Arbitrum, mentioned that they are looking for solutions to this problem.

Well-designed blockspace derivatives are a part of the solution to this problem. Rollups are also some of the largest buyers of Layer 1 blockspace and therefore there exists a sizeable market for blockspace derivatives.

For a deeper dive into rollup economics, read this post by Barnabé.

Figure 4: Timeline of users buying L2 blockspace and settlement of these transactions on L1.

Aggregators and other dApps

Some dApps like CoWswap give their users the guarantee that their transaction will be executed regardless of changes in the gas prices. They are thus also sellers of short-term blockspace futures.

"Once accepted the order is expected to be executed even if gas prices change"CoW Documentation

By a similar argument, they may also want to use blockspace derivatives.

Wallets

Usually, wallets provide users with an estimated gas price. EIP-1559 has made this easier, however, it does not offer a guarantee. Wallets could provide the service that they sell blockspace derivatives to the users, thereby guaranteeing a fixed transaction cost for their users and creating a cash flow for wallets. Wallets could compete on how well they offer this service and how well they trade off time until inclusion and transaction costs.

Time-fixed transactions

There are also plenty of other, more traditional, use cases for these kind of derivatives. Some businesses that accept ETH as payment method for example, may need to liquidate their positions each month and do not want to be exposed to fluctuations in gas price, therefore they may want to enter into a swap contract, a derivative contract in which two parties exchange cash flows from two different financial instruments, for example base fees and a fixed notional amount.

Figure 5: Timeline of a real-world business settling their position at the end of each month.

Cross-domain MEV

When MEV searchers can guarantee that they control blockspace in certain blocks ahead of time, they can exercise cross-domain MEV opportunities. This presents an interesting use case as the payoff of the seller and the buyer of such a blockspace derivative is not zero-sum, because the existence of this contract makes the blockspace more valuable.

Cross-domain MEV is an underresearched field and its effect and magnitude still needs to be established. Cosmos has also worked on a form of blockspace futures enabling cross-domain MEV.

Current and past solutions

GasToken

GasToken was an ERC-20 token functioning as a derivative on the gas price (This is before EIP-1559). A user would store data on the blockchain, thereby paying gas fees. The user could then later use the refund mechanism to delete the data from the blockchain and claim back around 50% of the gas fees, thereby effectively using Ethereum as a bank. This mechanism worked, even though a user would not be paid back for all of the gas units they consumed. GasToken is now outdated as the refund mechanism was removed from the protocol after the London hardfork.

Biconomy

Biconomy is a service that offers their partners fixed price transaction subscriptions. This is similar to a permissioned swap contract on gas prices. A user pays a fixed price to Biconomy in exchange for Biconomy consuming a pre-specified amount of gas on the user's behalf. Biconomy then hedges their exposure to the gas price by entering into an agreement with an intermediary. For more details on this subject, have a look at this post. Currently, Biconomy only functions in a permissioned form. Furthermore, the gas price risk is difficult to hedge since the base fee is burned.

Pitch Lake

Pitch Lake implements base fee derivatives on a time-weighted average basis, meaning that the payoff of the option is determined by the average base fee in a pre-specified time interval. The advantage of this is that the average base fee is more costly to manipulate (although a manipulator does not have to manipulate a large part of the base fees to make a profit). The disadvantage is that as the time interval increases, the hedge the option provides, decreases. In their paper the interval is set to a month. The variance in base fee between months is not as substantial as the variance within a month, meaning this hedge only helps large buyers of blockspace who buy uniformly in a month.

Risks

Insider trading

Let's say you have insider knowledge about the launch date of the next big NFT project. This increases demand for blockspace, meaning gas prices will spike during these mints. In this case, it would be beneficial for you to buy a lot of blockspace derivatives for said date.

It is very difficult to avoid this risk for sellers of these derivatives, yet it could lead to high losses. Having traders with insider information trade in the market could cause traders with less information to exit the market, eventually leading to a market for lemons.

If the time to maturity is short, it is less likely for many users to demand blockspace while the seller of a blockspace derivative did not know about this demand beforehand. For example, it is unlikely that a big NFT drop will happen in the next five blocks and that derivative sellers do not know about it. For shorter time to maturity, the risk of insider trading becomes smaller.

Block manipulation

Another risk is that the base fee is manipulable. As stated before, if a block is larger than the target block size, the base fee increases. It decreases if the block size is smaller than the target. A block builder has full control over how large to make the block, hence if it is profitable, builders will manipulate the size of the block and increase or decrease the base fee in the next block.

Whilst the block builder is the only one who can censor and supply an empty or smaller than target block, any user could manipulate the base fee by artificially increasing demand by simply sending very many transactions.

Overcoming this problem is related to the dynamics of the EIP-1559 fee market.

Finality risk

Let's assume there exists a well-functioning market for blockspace derivatives. Even if a contract is executed as promised, there still remain finality problems.

Uncle Risk

What if a user exercises the blockspace derivative and their transaction is included in a block that is uncled? The seller of the derivative has satisfied the requirement of including the user's transaction, however, the user is not satisfied since their transaction is not in the canonical chain.

Whether or not the contract has been honoured in this case, is a difficult decision to make as a block builder cannot avoid the uncle risk.

Re-org

If the value of blockspace derivatives becomes large enough, it may become profitable for a malicious actor to re-org the chain and thereby manipulate payoffs for the contracts. This means that even blocks that are a certain amount of blocks deep into the canonical chain do not guarantee that a contract is executed correctly.

Re-org attacks become more difficult as the length of the chain after the target block becomes longer. For contracts with a short time to maturity, re-org attacks could be a realistic risk.

Figure 4: Visualisation of a re-org. Block n+2 is thrown out for block n+1.

These finality risks are very difficult to overcome and therefore it is incredibly important to clearly stipulate what the exact agreement of the blockspace derivative is.

Choosing the underlying

In traditional commodity futures market there is a big distinction between derivatives that demand physical delivery or cash settlement.

With blockspace, this distinction becomes even more important, as guaranteeing blockspace is more difficult than with some other commodities.

Up until this point we have used the word blockspace derivative without distinguishing between blockspace and gas fees. Now we do make this distinction but whether blockspace is physically delivered or cash settled in the form of gas fees does not matter for the payoff of the option.

Blockspace

Selling a derivative guaranteeing inclusion in a certain block means that you need to control which transactions are allowed in that block. Since only the block builder can control this, it means that you need to be the block builder or control the block builder.

This is virtually impossible as it means that you need to control all the hash power or stake in a network, thereby breaking all decentralization. In the case of long-term derivatives you even need to control any builders that may want to enter the system, thereby creating a permissioned system.

Since this is so far out of line of the Ethereum ethos, trustless blockspace derivatives are not possible in the current protocol.

In-protocol blockspace derivatives

Arthur Breitman has argued for a different form of on-chain blockspace derivatives that involve changing the protocol.

A portion of blockspace in future blocks would be auctioned off at an earlier date, thereby fixing the gas price paid by the

user. This would allow regular users to land their transactions on-chain without worrying about the gas price.

This change would come with a few challenges and complicate the protocol further.

Transactions cannot be submitted in advance since they may very well not be valid in the future state of the chain. If the risk of non-valid transactions is accepted, this would waste more blockspace and the transactions would leak information thus allowing more MEV to be extracted, even if the transactions would be encrypted.

The derivatives could also be a claim to a certain amount of blockspace in the future. In this case the derivatives would be resellable as any transaction could be inserted.

As the time to maturity for a future goes to zero, the value approaches the value of the underlying. In the case of blockspace derivatives, it means that the value will converge to the gas price.

Blockspace derivatives essentially function the same as gas fee derivatives. The opportunity costs of exercising a blockspace derivative are the gas fees in that block. If a holder of a blockspace derivative finds that gas prices are too high, they are better off selling the derivative than exercising it.

This makes a blockspace derivative in reality a gas price future, which can be accomplished without partitioning the blockspace and complicating the protocol.

In-protocol derivatives under PBS

Proposer builder separation divides the role of a block builder into a builder and a proposer. Although this mechanism is not currently part of the Ethereum protocol, Flashbots' MEV-boost achieves a similar result out-of-protocol.

Builders will be sophisticated algorithms that maximize MEV. Under thecurrent PBS setting, proposers will simply choose the block that offers them the highest tip. Builders will thus be more centralized entities whilst proposers will be highly decentralized validators. This scenario is a very plausible endgame for Ethereum.

To preserve some decentralization under block builders, they must do more than only be the most efficient MEV extractor, as this could lead to one single winner for the majority or even all blocks.

A builder feature could be offering blockspace derivatives. Since these entities will be fairly centralized, they can offer blockspace derivatives for inclusion within some time interval in the future such that the probability that they propose zero blocks is below a certain level.

Cross-domain MEV

For cross-domain MEV extraction it is necessary to (partially) control the contents of blocks on multiple domains. Relying on your transactions being included via the normal route

may not suffice. As reasoned above, using the blockspace as underlying is hard to do compared to using total gas or base fees. In a PBS setting this may become easier and thus we may also see more cross-domain MEV extraction.

Base Fee

The Ethereum base fee causes almost all of the variance in the total gas fee. Although it is manipulable, it is more costly to do so than to manipulate the tip. This makes it an excellent candidate to be the underlying of a derivative.

Figure 5: The base fee (blue) and the tip (orange) over the past 30 days.

Market participants and protocol designers do need to be careful not to incentivize manipulating the base fee as this could lead to censored transactions or an attack similar to a DoS attack: all blocks could be filled completely, raising the base fee, until the resouces of the victim are completely drained. This would make the network temporarily unavailable, or very expensive, for regular users.

Total gas fee

Using the total gas fee paid per gas unit means users can fully hedge themselves against any price movements in gas fees.

In theory the tip should be equal to the marginal cost to a block builder of including a transaction in a block. This should thus be constant and maybe slightly decreasing in the very long term as computational power becomes cheaper.

In practice, however, there are some obstacles. Not only is the tip very manipulable, the tip in a block is not equal as for some cases, blockspace is non-fungible. Taking a mean or median does alleviate this problem somewhat, but then you lose the property that you are fully hedged. Furthermore, in the short-term priority gas auctions mean the tip is not always equal to only the marginal cost of including a transaction.

Since the base fee is more predictable in the short-term - it can only deviate by 12.5% from the base fee in the last block, whilst the tip can deviate without bounds - it could be easier to participate in this market and therefore could lead to more liquidity.

These issues makes it more difficult to design derivatives with the total gas fee as the underlying and point towards using the base fee as underlying.

Contract Settlement

After the financial contract has matured, the contract needs to be settled. Assuming we have chosen to use the base fee as the underlying, we need a transfer of funds and we need to determine the realised gas price.

Obtaining the realised base fee can be done in a trustless manner. Hashes of block headers can be saved and when a user wants to verify that a certain base fee is realised, they can check that the hash corresponds with the given base fee.

To settle the contract in cash, the seller of the derivative will need to overcollateralize their position. This means the seller will incur some cost of capital which needs to be paid for by the buyer. In traditional markets an advantage of derivatives is that it allows participants to trade with leverage, meaning their position is undercollateralized. This is not possible yet and researching this is equivalent to researching undercollateralized on-chain lending.

Derivative type

What type of derivative is needed, depends on the situation. However, a distinct advantage that call options offer is that the payoff for the seller is capped by the premium paid. Therefore, the incentive for a seller to manipulate the payoff by proposing empty blocks is limited.

This form of censorship attack can potentially be cheap to pull off as the costs are equal to the opportunity costs of foregoing the tips in that block, usually the tip is smaller than the base fee.

For regular commodities, market participants would be able to transform their payoffs into a put option on the base fee using the put-call parity. However, since the base fee is burned, the base fee cannot be held as underlying and the put-call parity does not hold.

Conclusion

Currently, the only possibility to hedge against transaction costs is off-chain permissioned swap contracts. As Ethereum scales, rollups, dApps and other users need to find a way to also hedge against gas prices moving against them. Creating on-chain, permissionless and incentive-compatible derivatives is the solution to this.

Structuring these derivatives means making difficult decisions on design and risks.

Making the right decisions could lead to a well-functioning market, thereby making Ethereum more accessible.

Making the wrong decisions means that contracts will be exploited and Ethereum will be temporarily unavailable, or prohibitively expensive, for other users until all of the victims resources are drained.

More research into this topic is necessary. These derivatives will eventually be structured but it is important that the risk trade-offs are made well as wrong trade-offs effect all of us.

If you are working on, or interested in blockspace derivatives, please do not hesitate to reach out.

Thanks to Barnabé Monnot for discussion and feedback