“Market that can operate freely is like a wheel that can turn freely: it needs an axle and well-oiled bearings. How to provide that axle and keep those bearings well oiled is what market design is about.”

— Alvin E. Roth, Who Gets What — and Why: The New Economics of Matchmaking and Market Design

Overview of the blockspace market

Blockspace is the commodity that powers the heartbeats of all cryptocurrency networks.

In the blockspace market, miners are the producers, mining pools are the auctioneers, and users are the bidders. The influences of the blockspace market are so pervasive that they touch almost every facet of the cryptocurrency ecosystem.

After a user initiates a transaction, it is propagated peer-to-peer in each node’s mempool. Each transaction has a fee attached to it. The fee signals the desire to purchase blockspace, which allows the transaction to be processed and included in a block.

Every moment there are numerous proposed blocks existing in this “Schrödinger’s state” between unconfirmed and confirmed, competing to find the first hash output that satisfies the difficulty target. Each block has a probability of becoming the next block. By contributing billions of computations per second, the miners collapse the probability wave and materialize the ledger history.

Since the size of a block is capped, there is a limited number of transactions that can go through at a given time, thereby giving blockspace an implicit time-value

. A transaction that stays unconfirmed for too long may be subject to market volatility, or get frontrun by arbitrage bots. The fee users pay to purchase blockspace, reflects their willingness to bid for its spacetime. The blockspace market connects the miners and users together.

On the surface, the blockspace market looks complex and chaotic because it lacks central coordination. It relies on detailed rules, procedures and the confluence of supply and demand to make self-adjustments. How do we know if the current market design is optimized for success?

Nobel Laureate Alvin E. Roth is considered a pioneer in the field of market design. In his seminal book “Who Gets What - and Why” he states that in order to function properly the markets need to do at least three things:

1. Market depth:

a large enough number of potential buyers and sellers to interact. In the case of the blockspace market, the suppliers are incentivized by the block reward to provide hashpower. On the other hand, demand for blockspace increases as more people use the network for transactions.

1. Safety:

market participants must feel safe to reveal or act on confidential information they may hold. Due to the transparent nature of on-chain transactions, users submitting sealed bids may not always get the outcome that they intended. Furthermore, transactions require a high degree of settlement assurance. That is, there should be sufficient hashpower to make re-orgs expensive.

1. Lack of congestion:

transactions should go through or get cancelled in a timely manner. When a market doesn’t deal effectively with congestions that volume brings, participants may not be able to get their transaction included in a block without too much delay. As witnessed from the recent popularity of Ethereum Dapps, gas price also skyrocketed as a result of congestions.

In both Bitcoin and Ethereum's history, how to optimize the design of the blockspace market structure often sparks many heated debates. In the following sections, we illustrate the structure of the Ethereum blockspace market from the perspectives of the supply (miner) and the demand (users)

. We examine if the current blockspace market design provides depth, ease congestion, or participation is safe and simple. Next, we discuss the popular proposals to optimize the market structure, as well as how the blockspace market will likely evolve in the future.

The supply side: the structure of Ethereum mining

The ultimate purpose of the entire mining industry is serving as a decentralized transparent clearinghouse for a single commodity: the blockspace.

The task is by no means trivial. In a distributed system that operates globally 24/7 without an authoritative coordinator, miners need to provide strong settlement assurance on the blockspace auctioned anonymously, by contributing a significant amount of capital on hardware and energy to produce an astronomical number of computations to secure the network.

Despite popular concerns of hashpower concentration, the mining industry is not a single-minded organism. Fluctuations in the blockspace market affect each component with different degrees of impact; and each individual miner is heavily affected by factors like location, machine type, temperature, maintenance, and mining strategies.

Bitcoin and Ethereum mining have distinctly different market structures. Bitcoin and a number of PoW coins have almost fully migrated to the ASIC era. Ethereum on the other hand, despite being the second largest in market cap, has barely any ASIC presence. While every once a while rumors of new ASIC manufacturers would emerge, it is estimated that around 80-90% of the current Ethereum hashpower is dominated by GPUs.

Structurally, how does a blockspace supplier market consisting primarily of GPUs differ from a market mainly of ASICs?

Every story of GPU mining begins with NVIDIA and AMD. They either directly sell discrete graphics cards or wholesale GPU chips and memory to lower stream graphics card manufacturers. These in turn manufacturers remove functions that have nothing to do with mining, and thus are referred to as "mining cards". There are many white-label custom mining card brands.

There are significantly more OEMs than the ASICs market. As a result, the hashpower composition of Ethereum is much more diverse than a typical ASICs network. This also makes it challenging for distributors to monopolize the channels. There are more options for miners, as they don't have to wait for ASIC manufacturers such as Bitmain, Whatsminer to sort out supply chain constraints. This means that the initial supply is usually not as bottlenecked as ASICs that use advanced backend processes. In addition, GPU miners are not tied to any specific networks. Miners engaging in speculative mining almost exclusively use GPU miners. Moreover, retail GPU cards are valuable in other areas of computing such as gaming, datacenter, and AI jobs. Overall, GPU miners have higher option value in their hardware.

Structure determines properties. The hardware composition determines the industry's capex and energy consumption. The two factors are pivotal in calculating mining expense, which has a rippling effect on the rest of the mining ecosystem: from manufacturing, distribution, hosting facilities, fluctuation of gas cost, preference for EIPs, to the defining characteristics of its mining cycles.

In The Alchemy of Hashpower, we introduced the four archetypal phases of the mining cycle according to the relative rates of change between Bitcoin price and network hashrate:

Due to the inherent illiquidity of hardware, network hashpower tends to lag price changes. The "hardware reaction time" is determined by various exogenous factors such as manufacturers' supply chain constraints, foundry wafer backlog, facility capacity, and even shipping logistics.

These delays are especially significant this year as the market sails full throttle into a raging bull trend. Miners and investors rush to place orders for new machines. The manufacturers on the other hand, are just beginning to recover from the supply chain halt during COVID, and the global integrated circuits shortage is forcing all semiconductor businesses - mining, automobile, consumer electronics, to wait in a long queue for wafer allocation.

In addition, NVIDIA recently announced that they will artificially nerf the performance of Ethash on the newest cards to discourage miners from buying up all the GPU inventory. This means that unless coin price or fee continue to rise astronomically from here, by the time the backlog of machines finally come online, the "inventory flush" and "shakeout" phase can be potentially very painful.

In Ethereum, mining revenue primarily comes from three sources:

1. coinbase reward (2 ETH per block + uncle rewards)
2. transaction fees, and
3. miner extractable value (more on this later).

Transaction fees as a percentage of total block reward are much higher in Ethereum than in Bitcoin. This means miners pay attention to not just coin price but also gas trends. Even if price stays flat, increase of transaction fees will be sufficient to incentivize miners to increase hashpower-under-management.

(Data source: Coinmetrics)

In addition, as discussed in the earlier sections, due to the option value of GPUs and flexibility in distribution, it is easier to scale up or down hashpower compared to an ASIC network. As a result, the cycles in Ethereum mining tend to be shorter:

A shorter cycle means competition ramps up faster when mining revenue is high, and hardware option value means it is easier for hashpower to unwind when revenue is low. Unit profitability (block reward per Megahash/s) can fluctuate wildly, making it challenging to predict earnings as a result:

(Data source: CoinMetrics)

A noticeable increase in coin price and fees attract more miners to participate. However, unlike most commodity markets, more producers doesn't mean an increase in the supply of blockspace. The supply of blockspace is determined by block size and the average block time. This means that the increase in hashpower does not drive down network transaction fees but increases the security budget of the network

. As more miners enter the competition, it becomes more expensive to re-org historical blocks, and therefore improves the network's settlement assurance.

The demand side: the time-value of blockspace

Since the block size is limited, participation in a permissionless manner requires competition over the system's resources. For anyone initiating on-chain transactions, the fee paradigm is a defining core user experience.

As the most popular platform for storing and executing smart contracts, Ethereum experienced a meteoric rise in utility. DeFi "money legos" have enabled products and services to interlock permissionlessly, and greatly fuel innovation in new financial schemes.

Ethereum users today participate in the blockspace market via a repeated first-price auction. It is a simple auction where users submit a bid for their transaction to be included in the next block, which is paid to the miner in the form of a transaction fee. Users can choose their bid via their transaction's "gas price", denominated in gwei/gas (1gwei = 1e-9 ETH). Empirical observations of mining pools' transaction selection methodologies shows that over 75% of them follow a default strategy without prioritization. That is, simply including transactions with descending order in fees without prioritizing any specific addresses.

(Source: Ethereum Gas Price Statistics)

The market structure is simple: users want to minimize the fees paid to miners to enjoy a smooth experience, whereas miners want to maximize their revenue since they are for-profit entities.

It is an undisputed fact that the fees paid by users will always obey the laws of supply and demand: blockspace per second is the scarce asset, and as a result users that want immediate inclusion of their transactions will always pay more than users willing to wait for the next block, as evidently seen by the shape of the pending transaction queue below.

The pending transaction queue. [source]

Blockspace is the closest thing in crypto to "digital real estate". Blockspace has the inherent value of being "a real estate" where economic activities occur.

For miners, blockspace in the future has lower time value due to uncertainties in price, network difficulty, and fees. For users, blockspace in the future has lower time value because of the uncertainty in the profitability and the utility of their transaction.

Congestion and fees

The time value of blockspace directly translates to the amount of fees users pay. In this fee paradigm, estimating the "correct" gas price is a hard problem as evidently seen by the volatility of gas prices in the span of a single block.

Median gas prices fluctuate from 100 to 400 Gwei in the span of a week[source]

Recall Roth's three requirements for successful market design: depth, safety, and overcome congestions. It is clear that in times of congestions, the gas price often spikes too much for general users. Where exactly is the bottleneck?

This unpredictability stems from the fact that users cannot coordinate on the correct fee for being included in the next 1, 5 or 10 blocks. Most users today bid in a "one shot" fashion: They broadcast a transaction once and wait for it to be included. Constant factor improvements can be made by allowing users to express their fee preference over a range of blocks, e.g.

using fee escalation algorithms.

The initial version of a novel technology is always crude. Over the years, different working versions emerge to address the problem of congestion. The market design of blockspace involves balancing the interests of many factions in the ecosystem. At the current juncture, three possible paths have been discussed:

1. Short-term: increase block size. Temporary patch and may compromise security.
2. Medium-term: change auction mechanism. Requires community consensus.
3. Long-term: scalability solutions. Rollups and ETH 2.0.

One may be tempted to increase the size of a block, so that it can fit more transactions (i.e. increase the supply, assuming constant demand). This change would only be a painkiller that temporarily alleviates the pain from high fees, since fresh demand would quickly fill up blocks, bringing fees up again. In addition, block size increases make the blockchain node software more resource intensive, so they should be avoided to preserve the decentralization of the system.

Another approach would be to restructure the bidding process. The fee mechanism in all blockchains today implements a "generalized first price auction". EIP-1559 is a proposal which changes the mechanism to a fixed-price sale when the system is not congested1, allowing users to easily choose the "optimal" bid for their inclusion preferences (contrary to the status quo). Variants of EIP-1559 have been deployed in Near, Celo and Filecoin. It is also scheduled for activation in Ethereum in July 2021, which will be the biggest fee market mechanism change to ever happen in a public blockchain.

EIP-1559 is also one of the most controversial topics in Ethereum to-date. Withover 60% of the mining pools signaling opposition to the proposal, EIP-1559 has turned into a "trade war" between the users and the producers of blockspace. Although the exact impact to miners' fee income is difficult to quantify yet, the mining community generally believes that gas price needs to increase significantly to make up for the difference. A'jian(阿剑), a vocal critic of the proposal in the Chinese Ethereum community, believes that the EIP-1559 "would lose miners' loyalty."

Kevin Pan, the founder of Poolin, thinks that it won't actually impact mining revenue very much, but "it is extremely insulting."

However, not all miners feel the same way. The founders of F2Pool, who are active users of DeFi products themselves, are in favor of the proposal. Even Jihan Wu, the notorious instigator of Bitcoin's block size civil war, voiced support for the change in fee mechanism. Ultimately, in a structureless open ecosystem with roots over different parts of the world, human coordination remains one of the biggest challenges.

Longer term, the proper solution is to allow the supply side to scale horizontally, without meaningfully affecting the trust requirements of the layer 1 system. After all, users want low fees, and low fees are not an economic mechanism design question but a fundamental blockchain scalability question. It is worth noting that scalability also allows more demand to enter the system, which would counterbalance the decrease in the average fee per transaction. The main approach here is the so-called layer 2 solutions, such as Optimistic and ZK Rollups.

The Dark Forest and the Dark Pools

If we were in the Bitcoin context, then the discussion around the demand side would end here. In Ethereum however, an entire financial system is being built which distorts the rules of the game. Certain "opportunities" may exist on Ethereum for a limited time, in the form of arbitrages waiting to be seized, or limited participation slots in a high-demand sale of an asset (e.g. an ICO). Similarly to how people race to queue up to get limited edition clothing, developers have built software which intelligently races for on-chain opportunities, and even competes with other bots by placing gas price bids.

This concept is called a Priority Gas Auction (PGA) which was first described in Phil Daian et al's seminal paper"Flash Boys 2.0". The "irregular" revenue stream which is generated from PGAs is called Miner Extractable Value or MEV.

Bots participating in PGAs get to have access to a potentially very profitable opportunity, and they are willing to bid at exorbitant gas prices, up to the profit they're going to make.

In Ethereum is a Dark Forest, the authors described one extraction in which around $12k worth of tokens fell into the grasp of the "predators". These predators are arbitrage bots that constantly monitor the activities on the mempool, and try to front run specific types of transactions according to a predetermined algorithm. DEX platforms such as Uniswap are likely infested with arbitrage bots.

As a result, some service providers have started to offer "dark pools" - transactions that bypass the public mempools and therefore are invisible to the public until they land on-chain2. These dark pools do not broadcast to the network, and instead relay the transactions directly to the miners, such that they are not broadcasted to other nodes on the network. These dark pools are not entirely used for profit-maximization purposes. In Escaping the Dark Forest, security researcher samczsun documented how his group rescued 25k ETH from a faulty smart contract using this technique.

Front-running and dark pools are not unique to the cryptocurrency market. They epitome a driving force in finance as old as time: secrecy. Wall Street has long embraced this controversial beast. A market that looks thick on a human timescale, with hundreds of opportunities to trade in the course of a single second, can look comparatively thin to a computer. It is estimated

that after 2015, dark pools account for 15-18% of the trading activities of exchange-listed securities in the U.S.

The “total addressable market” of MEV is exponentially growing, with at least $350m of MEV extracted since the beginning of 2020, one third of which happened during February 2021. Most of the extracted MEV is concentrated in arbitrage actions between popular automated market makers such as Uniswap, Sushiswap, Curve and Balancer, with a smaller slice of the pie being attributed to liquidations on Compound and Aave.

Cumulative Extracted MEV since January 1st 2020 https://explore.flashbots.net

The butterfly effect is staggering: Arbitrage and liquidation opportunities create MEV. MEV gets competed for via PGAs. Fee estimators use PGA-inflated gas prices as a reference, causing users to overpay for their transactions. At its core, the issue stems from the fact that users and bots are in the same pool, independently of whether they go after MEV or not.

Ideally, MEV-transactions should be in a separate transaction pool from non-MEV transactions. This would allow the MEV-extracting bots to compete with each other while all other transactions, say, the transfer of a CryptoPunk, would be in the no-MEV pool, which would enjoy a less volatile gas market.

Unfortunately, such drastic changes to Ethereum would be hard to execute. A simpler way to fix this issue would be to introduce a new API endpoint for miners, where they’d accept bundles of MEV-only transactions. That way, traders would submit their transactions directly to that endpoint, with users continuing to use the rest of the system like today. This is the approach that Flashbots is taking, which is the least disruptive to our knowledge.

How will miners adapt to MEV?

In the past, when fees’ % of total block reward was negligible, a miner’s primary focus was to capture as many shares of the blocksidy as possible. The miner would pick a mining pool that has a sufficiently large amount of hashpower hosted. After years of development, mining pool infractures have more or less been optimized to the same range of performance. A pool that lags behind its peers will be identified easily and quickly filtered out by the competition. Miners don’t really care about which pool they use beyond the basic parameters (luck, payout schedule, and pool fees). Users don’t really care which mining pool picks up their transactions, and the mining pool doesn’t care who the users are as long as the fee is attractive. As MEV grows relative to the block reward, the considerations of miners, mining pools and users start to become more nuanced.

With MEV, the blockspace market mechanism will shift from a pure commodity market to incorporate some elements of a match-making market. When users submit transactions they should be conscious of the mining pool’s ability to execute them in a timely manner.

All else equal, MEV causes gas prices to be higher than they would be if MEV did not exist. This implies that miners are already indirectly extracting a fraction of the total MEV that gets extracted by traders, estimated at ~12% today

. A recent analysis also hinted that the fees earned due to MEV will eventually dominate the fees earned through “regular” revenue streams (if not already!). That said, miners are profit seeking entities and may want to capture more of the MEV. Miners could choose to specialize and run internal trading operations. Using their benevolent powers over transaction ordering, they can choose to insert, re-order and even censor transactions to maximize their trading operation’s profits.

At the limit, it has been theorized that miners will reorganize the blockchain over and over, as they try to extract MEV from past blocks for themselves (colloquially referred to as “time bandit” attacks). While possible, this scenario is not obviously plausible: miners are (for the most part) structurally long ETH, and such an action would directly negatively impact their ETH investment. This train of thought generalizes to the statement that any theoretical miner attack is not going to be executed if it can be detected by users3.

A more optimistic take would be that miners decide to outsource MEV extraction to traders. They could do that either the aforementioned Flashbots approach, where they keep the block reward and outsource just the ordering, or by renting out their hashrate to specialized trading firms.

Independently of the method pursued, we expect that Ethereum mining pools will inevitably start to be more active in the MEV extraction process, as they seek to offer the best yield on their miners’ hashrate. As the race towards MEV extraction heats up, it remains to be seen how the (de)centralization of Ethereum’s mining ecosystem will be affected by this market structure change.

How can the rest of the ecosystem participate in MEV?

Financialization of hashpower is an important underlying trend in the mining space. If blockspace is analogous to real estate, then hashpower is the equity in the property, and a forward contract on hashpower is similar to mortgage. For miners, selling their hashpower through hashpower instruments **is a way for them to lock-in future revenue

. **Similar to renting hashpower on cloud mining platforms, forward contracts let the miner sell a fixed amount of hashpower for a period of time, for an upfront price.

Active DeFi users who are expecting network MEV activities to accumulate can speculate by purchasing these hashpower instruments.

For example, a trader who is expecting network MEV activities to surge in the next 15 days can purchase x amount of hashpower over the next 15 days for an upfront price. During the contract period, the mining rewards plus the MEV revenue captured by the miner will subsequently be forwarded to the trader. If the trader is well positioned, the purchase can potentially earn back the trader's own MEV fees paid to the mining pool. Both liquid hashpower instruments and MEV represent the cutting edge evolution for the mining capital markets. New tools are actively being built to advance in these directions. MEV plus hashpower instruments closes a full loop for the users and the miners.

Conclusion

The Ethereum blockspace market structure is a fascinating topic to study, and for a good reason. In this analysis, we observed key differences between the supply side of the GPU and ASIC hashpower markets. We also identified the key mechanisms which create the demand side dynamics. We then tied the two together under the umbrella of Miner Extractable value.

As Charlie Noyes wrote in MEV and ME: "Any attempt to prevent miners from accessing the revenue stream is liable to incentivize the creation of off-protocol markets."

. MEV is an inevitable result of the growing complexity of Ethereum transaction types. As tools and knowledge base for MEV become more mainstream, more interesting MEV patterns will emerge. These behaviors will profoundly impact how frequent DeFi users plan for their blockspace purchase strategies.

Changing how a commodity is sold on the market changes the way the commodity is produced. MEV creates new avenues for mining revenue, and thus will in turn influence how the mining industry interfaces with the buyers of the blockspace. New patterns will emerge in the Ethereum mining cycles

Notes

1. In times of burst demand, the auction mechanism post-EIP-1559 degrades back to a first price auction. To limit the duration of this phase, EIP-1559 implements an exponentially increasing fee which throttles back the demand to below the supply values, transitioning the mechanism back to the second price auction phase. ↩
2. The transaction can be made public only if the miner decides to publish the transaction themselves.↩
3. We also recommend this recent analysis on how miners could engage in actions which are opposing to users' best interests, as well as this explainer between benign and malicious MEV. ↩