BIS

BIS Bulletin

No 58

Miners as intermediaries: extractable value and market manipulation in crypto and DeFi

Raphael Auer, Jon Frost and Jose Maria Vidal Pastor

16 June 2022

BIS Bulletins are written by staff members of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS. The authors are grateful to Mike Alonso, Sirio Aramonte, Carlos Cantú, Stijn Claessens, Giulio Cornelli, Sebastian Doerr, Leonardo Gambacorta, Wenqian Huang, Ross Leckow, Andreas Schrimpf and Christian Upper for comments, and to Agostino Capponi, Arthur Gervais, Kaihua Qin and Liyi Zhou for providing data and input. The authors thank Louisa Wagner for administrative support, Ann Neale for graphics support and Martin Hood for editorial review.

The editor of the BIS Bulletin series is Hyun Song Shin.

This publication is available on the BIS website (www.bis.org).

ISSN: 2708-0420 (online)
ISBN: 978-92-9259-579-1 (online)

Raphael Auer
raphael.auer@bis.org

Jon Frost
jon.frost@bis.org

Jose Maria Vidal Pastor
JoseMaria.VidalPastor@bis.org

Miners as intermediaries: extractable value and market manipulation in crypto and DeFi

Key takeaways

- *Cryptocurrencies such as Ethereum and decentralised finance (DeFi) protocols built on them rely on validators or "miners" as intermediaries to verify transactions and update the ledger.*
- *Since these intermediaries can choose which transactions they add to the ledger and in which order, they can engage in activities that would be illegal in traditional markets such as front-running and sandwich trades. The resulting profit is termed "miner extractable value" (MEV).*
- *MEV is an intrinsic shortcoming of pseudo-anonymous blockchains. Addressing this form of market manipulation may call for new regulatory approaches to this new class of intermediaries.*

Far from being "trustless", cryptocurrencies and decentralised finance (DeFi) rely on intermediaries who must be incentivised to maintain the ledger of transactions. Yet each of the validators or "miners" updating the blockchain can determine which transactions are executed and when, thus affecting market prices and opening the door to front-running and other forms of market manipulation.

These intrinsic shortcomings of permissionless blockchain technology are well known in the field of computer science and the cryptocurrency industry (see Daian et al (2020)). In fact, a new term has been coined for the profits that miners can make via their ability to choose which transactions to include and in which order: "miner extractable value" (MEV).[1] This is defined as the profit that miners can take from other investors by manipulating the choice and sequencing of transactions added to the blockchain.

This bulletin explains MEV and why it arises, documents the amounts involved, and draws regulatory implications for cryptocurrencies, DeFi and other blockchain-based applications.

What is MEV and why does it arise?

In traditional financial markets, user transactions are sequenced by a trusted and regulated intermediary in the order in which they are received. In a blockchain, by contrast, the updating of a block is competitive and random. For example, in a cryptocurrency based on proof-of-work such as Bitcoin, all miners use their computing power to quickly solve a puzzle that will allow only one of them to add the next block (see Auer (2019)). The probability that a given miner will add the next block is equal to that miner's share in the total computing power expended. This process can be considered "decentralised" and equitable in the sense that there are many different miners, and no single miner can censor a specific transaction forever. This is because, if the fee that a transaction pays is high enough, some other miner will eventually include

[1] Sometimes, this is also referred to as "maximum extractable value" as measures often gauge the maximal theoretical value that can be extracted from transaction ordering in permissionless settings – ie networks where any entrant can serve as a miner. It can also be termed "blockchain extractable value."

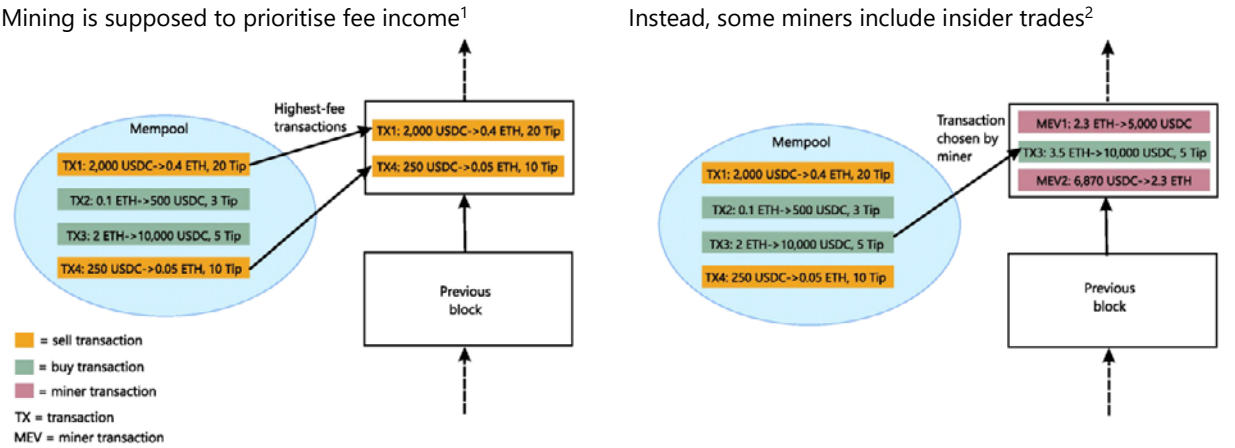
it in the block. Similar arguments hold for a proof-of-stake-based network, into which the Ethereum network aims to transition.[2]

Still, when a miner can add a new block, they are free to assemble this block in any way they want. This lets them extract value from other users. Beside collected legitimate transaction fees (eg the "gas" fees in Ethereum), they can assemble their block from all pending transactions – the memory pool or "mempool" – in such a way as to maximise MEV. The latter are profits that are made by manipulating market prices via a specific ordering – or even censoring – of pending transactions.[3] Because the ledger is publicly observable, these forms of market manipulation can be seen, even if the underlying identity of the miners or other parties in question is unknown.

Graph 1 illustrates a hypothetical example of a sandwich trade by a miner with transactions in the stablecoin USD Coin (USDC) and Ethereum's cryptocurrency Ether (ETH). Several different users put in buy and sell transactions in the mempool, and the miner can select which orders to include in this block. In theory, miners should select and order transactions based on fees only (left-hand panel). As each Ethereum transaction needs computing power and resources to be executed, a fee is paid to the miners to execute the transaction, paid in small units of ETH (gigawei or "gwei", each equal to 0.000000001 ETH). Total fees are the sum of a base fee (which is destroyed or "burned") plus a priority fee ("Tip", decided by the user when sending the transaction to the mempool).

Fee-based mining allows for value extraction

Graph 1



[1] The mempool contains various signed but pending transactions, which are ordered and added to the next block according to the amount of Tip, whether or not it is a buy or a sell order, assuming a constant base gas fee.[2] Miners add their own transactions to the block to profit from a different ordering of pending transactions based on the size and direction of the largest-volume transaction, therefore altering its market price and benefiting from a trading advantage.

Source: Authors' elaboration.

A miner should build the next block by ordering the transactions based on the Tip – that is, the transactions (Tx) with a higher Tip should be given priority. Thus, the first transaction to enter the new block should be Tx 1, which involves selling 0.4 ETH and includes a Tip of 20 gwei (in addition to the base gas fees). Subsequently, Tx 4 is the next one to enter the block, as it has the second highest combined fee.

[2] In these networks, miners have to "stake" a set quantity of coins, which they stand to lose if it is determined that they have falsified the ledger.

[3] There is only a certain probability that a single miner will actually get the privilege to add the next block to the blockchain and collect these fees and MEV. If instead a different miner adds the next block, the mempool changes and the game starts anew. From the perspective of a single miner, MEV is probabilistic: it sometimes generates an extra profit.

However, miners can extract value by ordering the transactions within the next block in the way that is most profitable to them. In this case, transactions are not ordered based on fees, but based on the profit opportunities they generate for the miner (Graph 1, right-hand panel). In this example, a large transaction can move prices. Therefore, by introducing its own transaction prior to the large transaction, the miner can earn a profit in addition to the regular fees. Not only does this profit come at the expense of other market participants, but the miner's transactions also delay other legitimate transactions.[4] It thus forms an "invisible tax" on regular market participants.

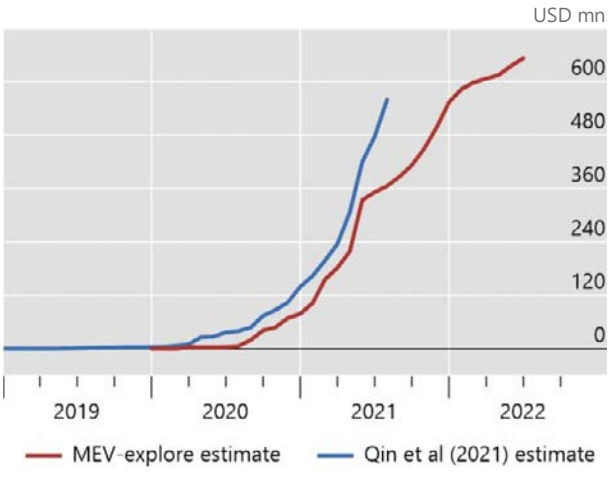
MEV can hence resemble illegal front-running by brokers in traditional markets: if a miner observes a large pending transaction in the mempool that will substantially move market prices, it can add a corresponding buy or sell transaction just before this large transaction, thereby profiting from the price change (at the expense of other market participants). Miners can also engage in "back-running" or placing a transaction in a block directly after a user transaction or market-moving event. This could entail buying new tokens just after they are listed, eg in automated strategies from multiple addresses, to manipulate prices. Finally, miners can engage in "sandwich trading", where they execute trades both before and after a user, thus making profits without having to take on any longer-term position in the underlying assets.

Market manipulation is not a theoretical notion

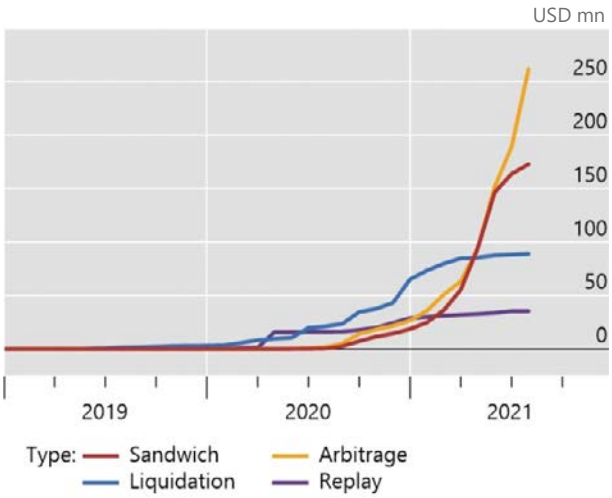
Since 2020, total MEV has amounted to an estimated USD 550–650million on just the Ethereum network, according to two recent estimates (Graph 2, left-hand panel). In addition to sandwich attacks, MEV results from liquidation attacks (ie forcing liquidations), replay attacks (cloning and front-running a victim's trade) and decentralised exchange arbitrage (right-hand panel; online appendix). Notably, these estimates are based on just the largest protocols and are hence likely to be understated. Thus, the amount of MEV captured in the data is only one portion of the total profits that miners can extract from other users.

Measures of miner extractable value are accumulating over time — Graph 2

Cumulative miner extractable value on Ethereum[1]



Cumulative extractable value by attack type[2]



[1] The MEV-explore estimate includes arbitrage and liquidation attacks from nine Ethereum protocols (Aave, Balancer, Bancor, Compound, Cream, Curve, Uniswap V2, Uniswap v3 and 0x). It is calculated as successful MEV transactions + successful MEV transactions gas fees + failed MEV transactions gas fees. It reflects extracted MEV, but not all theoretical total extractable value. The Qin et al (2021) estimate includes sandwich, liquidation, arbitrage and replay attacks in 1inch, Aave, Bancor, Compound, Curve, dYdX, Sushiswap, Swerve, UniswapV1, UniswapV2 and UniswapV3. Both refer only to the Ethereum blockchain. [2] Based on Qin et al (2021).

Sources: Qin et al (2021); MEV-Explore v1; authors' calculations.

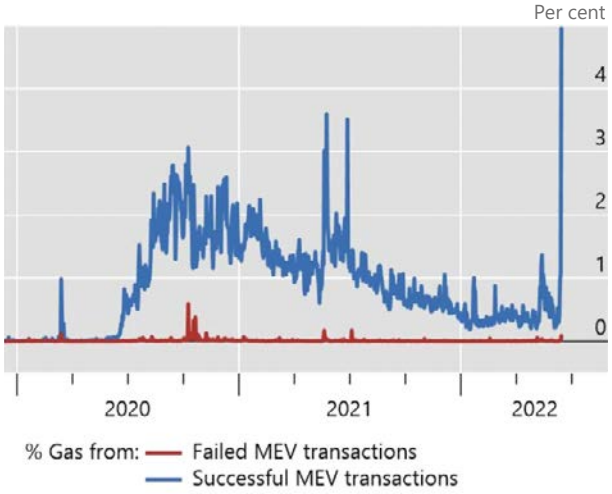
[4] Note that, in practice, attackers may also be other actors who pay miners to execute MEV transactions on their behalf.

In fact, MEV is so pervasive that, at times, one out of 30 transactions is added by miners for this purpose (Graph 3, left-hand panel). This share was even higher in early June 2022, due to a number of particularly large MEV transactions during the recent market stress. These extra transactions added by miners also work to limit the capacity of the entire Ethereum blockchain.[5]

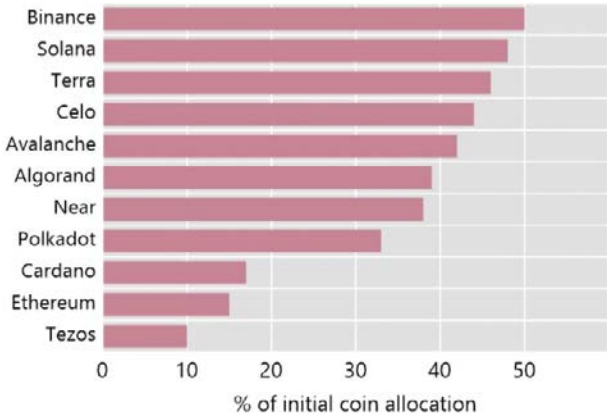
Nor are these the only form of rents to insiders in blockchain-based systems. For instance, new blockchains tend to give large coin allocations to developer teams and venture capital investors (right-hand panel). For applications that promise to cut out middlemen, the rents to (new types of) insiders are conspicuously large.

MEV is only one of many forms of rent in blockchain systems — Graph 3

Total block gas used by MEV transactions in Ethereum



Coins are often allocated to insiders[1]



[1] All listed coins are on Layer 1 blockchains.

Sources: MEV-Explore v1; Messari report (2021, 2022); authors' calculations.

Implications for blockchain-based finance

Regulatory bodies around the world need to establish whether value extraction by miners constitutes illegal activity. In most jurisdictions, activities such as front-running are considered illegal (see eg Scopino (2015)). In traditional markets, regulated intermediaries must process trades in the best interest of the client, in line with best execution rules. By contrast, in a blockchain-based system, miners – even though they may themselves be trading in the same markets – are under no obligation to order them in the sequence received. In an adversarial, pseudo-anonymous system, the attacks and the addresses of the attackers can be publicly observed on the ledger, but the identities of the attackers may not be known.

There are several open questions on whether current regulation on insider trading is directly transferable to MEV. In most jurisdictions, the legal status of these actions is ambiguous. To provide clarity, legal research would have to assess whether the activities permitted by the Ethereum protocol and other DeFi ecosystems should actually be prohibited. In contrast to traditional markets, anyone who participates in such an ecosystem essentially accepts the rules encoded in its protocol. It is therefore unclear whether a participant could object if someone exploits those rules to their advantage.

On the other hand, it might be claimed that market regulations such as injunctions on insider trading will apply whether or not the potentially unlawful action is authorised under the blockchain's rules. Importantly, the miners do not have an information advantage when it comes to the mempool (which is

[5] MEV also occurs in other blockchains that offer programmability.

public). Their ability to extract value arises from their control over the composition of the block they are adding to the blockchain. Whether this may constitute illegal insider trading has yet to be established. While developers and miners may claim decentralisation to shield themselves from legal liability, it has been argued that regulators should not uncritically accept these claims (Walch (2019)). Even so, because the identity of miners is unknown, it may be difficult to enforce any regulatory interventions.

These considerations on illegality aside, MEV also poses a quintessential problem for the industry itself, as it stands at odds with the idea of decentralisation. A range of new DeFi applications seeks to build financial services on permissionless blockchains (Aramonte et al (2021)). Yet MEV can directly limit the usefulness of these applications.[6] A huge machinery requiring substantial investments is necessary to screen all the MEV possibilities. "Bots" that exploit MEV are now active on different decentralised exchanges. This imposes a fixed cost of mining, encouraging concentration. Solutions such as moving to dark venues, where transactions are only visible to miners, have not so far reduced front-running risk (Capponi et al (2022)). The additional fees and unpredictability for users mean an additional form of insider rents in DeFi markets.

Looking forward, MEV could intensify. Indeed, in general equilibrium, miners may be forced to engage in MEV to survive. Miners who engage in MEV will on average make higher profits and buy more computing power, and they could thus eventually crowd out miners who do not.[7] Thus, a form of rat race develops from the combination of the competitive and decentralised nature of updating and the fact that every miner can assemble their block any way they want. It has been argued that MEV forms an existential risk to the integrity of the Ethereum ledger (Daian et al (2019); Obadia (2020)).

These rents form a fundamental shortcoming of blockchain-based activities. While the decentralised governance of blockchains may be useful in certain settings of low trust (see Auer et al (2021)), it imposes a substantial cost on users and in terms of allocative efficiency. Similar factors lead to a lack of scalability (Boissay et al (2022)). MEV and related issues may be tackled in *permissioned* distributed ledger technology, based on a network of trusted intermediaries whose identities are public. Here, because the identity of any attacker would be known, it could be held accountable under regulation.

[6] The pseudo-anonymity of blockchains also means that credit applications rely to date on overcollateralisation. This makes lending in DeFi systems inefficient and risky, particularly when the underlying collateral is volatile (Aramonte et al (2022)).

[7] This could parallel the competitive race for execution speed seen in high-frequency trading (see Baron et al (2012)).

References

Aramonte, S, W Huang and A Schrimpf (2021): "DeFi risks and the decentralisation illusion", *BIS Quarterly Review*, December, pp 21–36.

Aramonte, S, S Doerr, W Huang and A Schrimpf (2022): "DeFi lending: intermediation without information?", *BIS Bulletin*, no 57, June.

Auer, R, C Monnet and H S Shin (2021): "Permissioned distributed ledgers and the governance of money", *BIS Working Papers*, no 924.

Auer, R (2019): "Beyond the doomsday economics of "proof-of-work" in cryptocurrencies", *BIS Working Papers*, no 765.

Baron, M, J Brogaard and A Kirilenko (2012): "The trading profits of high-frequency traders", *mimeo*.

Boissay F, G Cornelli, S Doerr and J Frost (2022): "Blockchain scalability and the fragmentation of crypto", *BIS Bulletin*, no 56, June.

Capponi, A, R Jie and Y Wang (2022): "The evolution of blockchain: From lit to dark", arXiv:2202.05779.

Daian, P, S Goldfeder, T Kell, Y Q Li, X Y Zhao, I Bentov, L Breidenbach and A Juels (2020): "Flash boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability", 2020 IEEE Symposium on Security and Privacy (SP), vol 1, pp 910–27.

Ethereum (2022): "Gas and fees", https://ethereum.org/en/developers/docs/gas/, accessed 1 March.

Obadia, A (2020): "Flashbots: Frontrunning the MEV crisis", Medium.

Qin, K, L Zhou and A Gervais (2021): "Quantifying blockchain extractable value: How dark is the forest?", arXiv:2101.05511.

Scopino, G (2015): "The (questionable) legality of high-speed pinging and front-running in the futures market", *Connecticut Law Review*, vol 47, no 3, pp 607–97.

Ventoruzzo, M (2014): "Comparing insider trading in the United States and in the European Union: History and recent developments", European Corporate Governance Institute (ECGI) – Law Working Paper, no. 257/2014.

Walch, A (2019) "Deconstructing 'decentralization': Exploring the core claim of crypto systems", in C Brummer (ed), *Cryptoassets: Legal and Monetary Perspectives*, Oxford University Press.