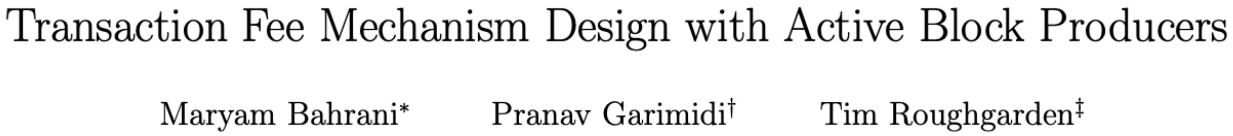
Lots of competing proposals out there for how to deal with MEV: OFAs and other competitive markets, encrypted mempools, MPC, TEEs, etc. But do we truly need any of these? Yes! And, with @bahrani_maryam and @PGarimidi, we have the math to prove it:👇
1/12



Transaction Fee Mechanism Design with Active Block Producers

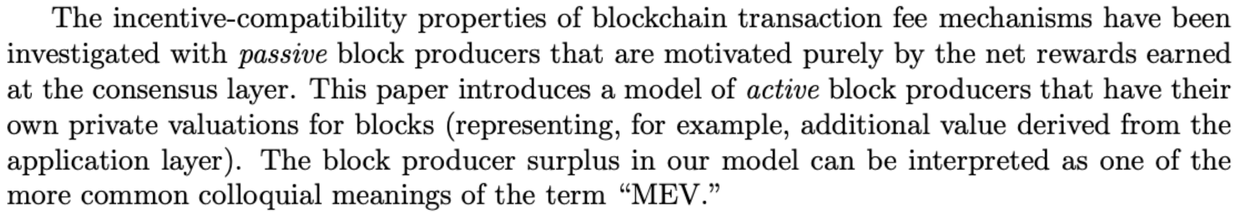
Maryam Bahrani[*] Pranav Garimidi[†] Tim Roughgarden[‡]

Background: a transaction fee mechanism (TFM) is the part of a blockchain protocol responsible for figuring out which transactions should be included and who should pay what. Example: EIP-1559.
2/12

One minimal thing you'd really like from a TFM is good UX, meaning that bidding is easy for users (one of the original motivations for EIP-1559). This idea is encoded by a mathematical property called "DSIC."
3/12

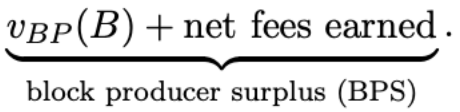
A second is a form of credibility called "BPIC," meaning that a validator responsible for supplying the TFM's inputs should be properly incentivized to behave as intended.
4/12

DSIC+BPIC have been studied in a pre-MEV world (e.g., with EIP-1559 achieving both, as long as its base fee is not crazy low for the current demand).
5/12



The incentive-compatibility properties of blockchain transaction fee mechanisms have been investigated with *passive* block producers that are motivated purely by the net rewards earned at the consensus layer. This paper introduces a model of *active* block producers that have their own private valuations for blocks (representing, for example, additional value derived from the application layer). The block producer surplus in our model can be interpreted as one of the more common colloquial meanings of the term "MEV."

We model a post-MEV world via block producers with private valuations for blocks (e.g., due to application-layer value that they can extract), above and beyond whatever fees they might earn at the consensus layer:
6/12

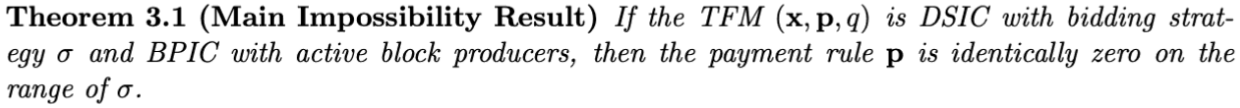


$$\underbrace{v_{BP}(B) + \text{net fees earned}}_{\text{block producer surplus (BPS)}}.$$

And boy does MEV change things; for example, EIP-1559 is no longer incentive-compatible for both users and block producers (even with a correctly set base fee)!
7/12

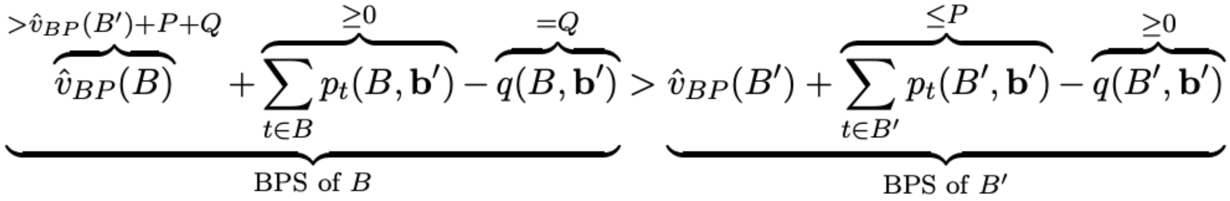
Intuitively, the issue is that, when there's MEV, a user can't know whether to underbid to take advantage of a block producer that might be willing to subsidize the difference.
8/12

Our main result shows that the problem is fundamental, rather than a flaw in the EIP-1559 design: with MEV, *no* non-trivial or approximately welfare-maximizing TFM can be both DSIC and BPIC!
9/12



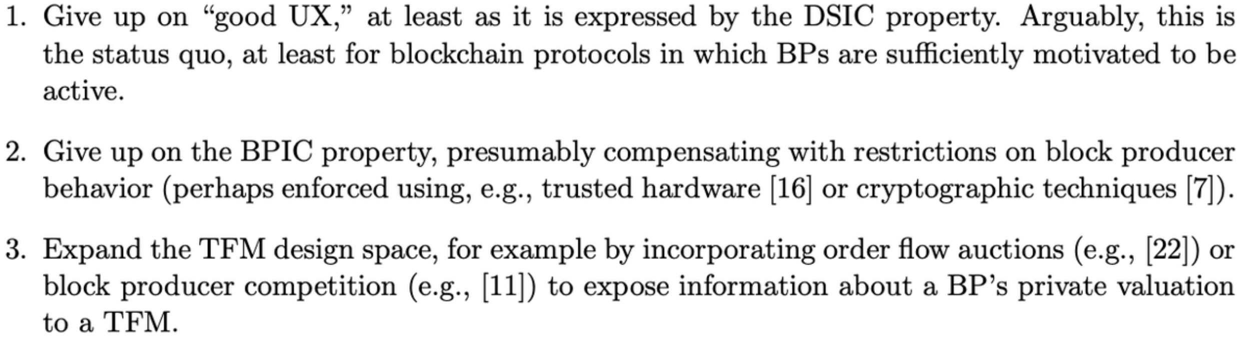
Theorem 3.1 (Main Impossibility Result) *If the TFM* $(\mathbf{x}, \mathbf{p}, q)$ *is DSIC with bidding strategy* σ *and BPIC with active block producers, then the payment rule* $\mathbf{p}$ *is identically zero on the range of* σ*.*

The proof isn't short enough to summarize here, but this inequality captures part of it:
10/12



$$\underbrace{\overbrace{\hat{v}_{BP}(B)}^{>\hat{v}_{BP}(B')+P+Q} + \overbrace{\sum_{t\in B} p_t(B,\mathbf{b}')}^{\geq 0} - \overbrace{q(B,\mathbf{b}')}^{=Q}}_{\text{BPS of } B} > \underbrace{\hat{v}_{BP}(B') + \overbrace{\sum_{t\in B'} p_t(B',\mathbf{b}')}^{\leq P} - \overbrace{q(B',\mathbf{b}')}^{\geq 0}}_{\text{BPS of } B'}$$

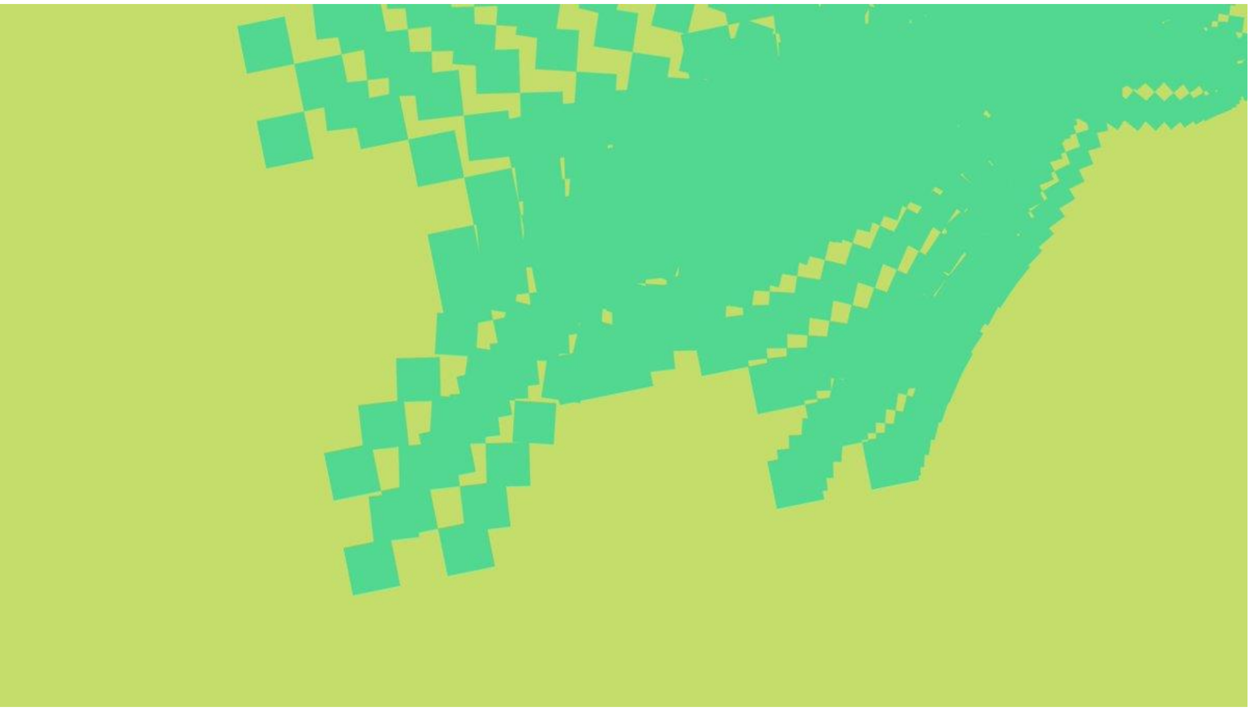
The role of an impossibility result like this is not to discourage but to illuminate, highlighting the most promising paths forward. From it, we learn that our options are (i) constrained; and (ii) already
being actively explored by the community:
11/12



1. Give up on "good UX," at least as it is expressed by the DSIC property. Arguably, this is the status quo, at least for blockchain protocols in which BPs are sufficiently motivated to be active.
2. Give up on the BPIC property, presumably compensating with restrictions on block producer behavior (perhaps enforced using, e.g., trusted hardware [16] or cryptographic techniques [7]).
3. Expand the TFM design space, for example by incorporating order flow auctions (e.g., [22]) or block producer competition (e.g., [11]) to expose information about a BP's private valuation to a TFM.

Here's the paper, comments and questions are of course welcome!
https://arxiv.org/pdf/2307.01686.pdf
12/12

PS -- and here's a summary blog post:



[New paper alert: “Transaction Fee Mechanism Design with Active Block Producers”]