Short Note on {Monarch, Moloch, Mafia} Extractable Value

we provide a friendly intro to the concept of {Monarch, Moloch, Mafia}EV.

Or, 3EV, or, ΣEV (both are sideway “M”), and represents sum types

for a detailed, formalized description of 3EV, refer to

- https://hackmd.io/@sxysun/this-is-mev/edit
- https://hackmd.io/@sxysun/semantics-lattice/edit
- https://www.youtube.com/watch?v=8qPpiMDz_hw
- https://docs.google.com/presentation/d/1MyGRlZTHzppFYfEF04cCf0DbkokNTs6BZLeLqV99F7A/edit#slide=id.g163c2a140da_0_99

for background in mechanism design and an advanced discussion on MEV, refer to

- https://docs.google.com/presentation/d/1kM7YdFK1nHQjBXU11o9Oge-seorWNWxV6TdW6a_QaSI/edit#slide=id.g14adc9fe041_0_67
- https://docs.google.com/presentation/d/1V_FCxLnF-8O1aBxLbrj3KZWYMigBjnaKTBnQbKGABAU/edit?usp=sharing
- https://docs.google.com/presentation/d/1OYfQoJeqdEcLN8G5b3msluHhhR9QGO9bHKEaGM1A6pI/edit?usp=sharing

Definition

Mafia

Extractable Value arises from the fact that there exists an asymmetric knowledge of one agent to another agent’s private information (e.g., in the case of sandwiching/PFOF market making/generalized frontrunning), basically activities 1&2 that I mentioned in “Response to Arbitrum.” Fundamentally, MafiaEV emerge because some users are unsophisticated and thus fail to communicate their preferences to the coordinator/mechanism, and since other users are sophisticated (and they know some others are unsophisticated), they can play strategically and harm the unsophisticacted users. Another example of MafiaEV is trading using the imbalance of the orderbook (e.g., relying on the latency advantage, seeing more bid than asks, then take the first ask, pushing the orderbook to be more imbalanced), this is MafiaEV because it is a bayesian extraction (you gained the evidence that the other party has some utility).

Moloch

Extractable Value is just the value that has been surrendered to the Moloch (uncoordination). In general, MolochEV maximally equals the Price of Anarchy. For example, absent x-chain bridges/messaging protocols, the x-domain arbs lose value because the searchers will have to price in the risk of executing their bundle, therefore making them only want to make the market more efficient when there’s enough inefficiency (e.g., suppose searcher A has an asset that it wants to use to market make some Solana AMM pool, but the asset is on Ethereum, and since there exists no SUAVE for Solana and Ethereum, the searcher will have to price in the asset transfer risk and thus would charge higher spreads for the user). So in the end user bears the burden of MolochEV. A more direct example is that in using vanilla-FCFS, the searchers are doing an uncoordinated behavior of using latency-auctions to approximate the perfect spec-on-state auction, therefore, this approximation generates additional cost and uncertainty which will be priced into the worse execution that are provided to users.

Monarch

Extractable Value arises from the fact that the coordinator (e.g., sequencer, validator, proposer) has the ultimate power of deciding the ordering/allocation of spec-on-state. So whenever there exists a conflict of preferences, the coordinator will be able to extract value. MonarchEV also maximally equals to Price of Anarchy. This is because the coordinator can maximally extract value equaling to the amount of value that the agents would have got absent the coordinator: if it were to try extract more, the agents will have no reason to even participate in the mechanism. Concretely, think of a x-domain market maker bridge like Hop, the monarch is the bridge operator, whose revenue comes from better market making strategies of x-domain swaps. So Hop can maximally extract value equaling to the delta between “the best execution Hop can offer” and “what ppl would have got if Hop didn’t exist,” which, considering the x-domain volume, should be huge. This is also the bullcase for SUAVE, because in equilibrium, SUAVE validators are the new Monarch and can extract value maximally equaling the delta between “perfect coordination” and “what ppl are getting now absent a x-domain MEV mechanism”

Conclusion

I argue, Moloch + Monarch + Mafia is the total MEV. And you can choose to adjust the percentage of those three kinds of MEV. The most ideal world would be we have 0% Mafia, 0% Moloch, and 100% Monarch where the Monarch profits are decentralized

molochEV can be eliminated, but it turns into monarchEV, which can be then turned into molochEV in the process of decentralizing the monarch

Q&A

- Why redistribution?
    - Monarch needs to emphasize the long-term side (in long term, if Monarch is centralized, people have no incentive to recognize the Monarch and then all is lost), and since monarch usually is here for long term, and their revenue is MEV which is essentially a call option to the future economic acitivity on the domain, their rational action would be to encourage long-

term decentralization and redistribution of MonarchEV (e.g., public goods funding). So a Monarch being Mafia is irrational behavior

- Where is the negative externality?
    - The negative externalities are exactly Moloch Extractable Value. We also have “Price of MEV” in FRP-19, a full paper quantifying the “negative externality” part, specifically, the MolochEV (PoA where equilibrium is status quo), e.g., one result is that the bound for PoA in latency games is linear with respect to the number of players (searchers).
- You mentioned Price of Anarchy twice, is this the intersection between MolochEV and MonarchEV?
    - Price of Anarchy is not the intersection, I put it there because MolochEV and MonarchEV both maximally equal to the Price of Anarchy (where we define the equilibrium as the worst uncoordination one could get), so MolochEV + MonarchEV = PoA (equilibrium defined as worst possible), and MolochEV = PoA (equilibrium defined as status quo). The three, Monarch, Mafia, Moloch, are disjoint sets (they have no overlap). I didn’t mention it in the short note but the formal model in “this is MEV” captures this clearly, which is also why I this new renaming of MEV can be called 3EV or ΣEV, because the three types constitutes a sum type!
- In the process of eliminating MolochEV, wouldn’t we make MafiaEV (toxic MEV) also increase?
    - Generally, the quantity could increase, but the percentage of MafiaEV will decrease.
    - But I think having quantity increase and not percentage increase is fine.*Because our thesis is that Moloch inflict same burden on user as Mafia*, so in eliminating Moloch by X, and giving that X to Mafia to Monarch, the burden on users will have a net decrease because of the reduced percentage
    - so suppose 100 MEV, “30 Mafia, 35 Monarch, 35 Moloch” By our thesis the total pain on users is 30+35=65. Now, we eliminate 35 Moloch and give 30 to Monarch while giving 5 to Mafia, resulting in “35 Mafia, 65 Monarch, 0 Moloch” By our thesis the total pain on users is 35 < 65. And in reality, MolochEV is so huge such that the resulting reduction in user pain will be large.
- What is NOT MEV?
    - Not all value is MEV, the utterance of MEV has some presuppositions to the value
    - For example, the value that the users would be getting absent the Monarch is not MEV. Concretely, in prisoner dilemma with both betraying generating payoff of (1,1), the (1,1) is not MEV
    - We define Monarch + Moloch to be PoA(worst Eq absent present Monarch, best Eq present best Monarch). So MEV conditions on the present Monarch (if exists a Monarch). This mean by the utterance of MEV we are having a presupposition of the existence of a Monarch.
    - Here our test for non-MEV is having a conservative standard on the context/utterance of MEV by taking a Fregean/Russell standpoint. For elaboration, see “A Philosophcial Foundation for the Salles Test” https://hackmd.io/@sxysun/foundation-test
    - mev implies frontrunning, not the other way around
    - But "physics as coordinator in rugby” doesnt work, because physics isn't an agent, same as fcfs without colocation services, so there exists no coordinator (that is capable of extortion and stealing/zeta), fails presupposition test.
- What if we have multiple Monarchs, or the old Monarch was dethroned and now is fighting the new?
    - extortion between multiple veto players -> what's the core/shapley value
    - inter-temporal coalition factor and monarchs shifting naturally according to which game you are playing

Where we stand

At Flashbots, we try to solve

- MafiaEV using OFA (a mechanism for discovering unsophisticated user’s preferences, and helping them to communicate this preference to the coordinator/mechanism)
- MolochEV using SUAVE (eliminating efficiency and taking value back from the Moloch and give it to the Monarch)
- MonarchEV using redistribution (by decentralizing the Monarch), for more of my ideas on the solution, see:
    - https://hackmd.io/@sxysun/innovation
    - https://www.youtube.com/watch?v=A8YYPeAM6P4
    - https://www.youtube.com/watch?v=JCZDd0iCMsg

Case Study: Vanilla-FCFS v.s. FBA-FCFS

for background, see https://research.arbitrum.io/t/transaction-ordering-policy/127/2?u=sxysun

Essentially, vanilla-FCFS compared with FBA-FCFS:

- Mafia: same if we assume OFA/privacy solutions, vanilla-FCFS is (marginally?) better if those are absent
- Moloch: vanilla-FCFS is guaranteed to create much more MolochEV than FBA-FCFS
- Monarch: vanilla-FCFS is guaranteed to have a much worse solution to MonarchEV

For all “searching for a lower bound of MEV” solutions, as described inhttps://twitter.com/sxysun1/status/1463237051994755072, have neglected the whole MEV space and only focused on MafiaEV. So **in the process of bringing Mafia percentage down, they’ve enlarged the percentage of Moloch and made Monarch more centralized.**And for unsophisticated users, they get the same payoff from Moloch/Mafia, so it doesn’t matter that you make eliminate Mafia better than direct auction, you are just taking the user’s harm from Mafia and give it to Moloch so Moloch can harm users. Plus, here Monarch is more centralized, so the system as a whole is strictly worse than it was before

So as a first step, they should realize that MEV is consisted of three parts, not one. And then, given that they are capable people, they will naturally come up with the same conclusion as us (Flashbots)

Visualizations & Memes

For more memes, see https://www.youtube.com/watch?v=JCZDd0iCMsg