
Value Extractable by a Monopolistic Coordinator
Sorry but this formulation of MEV is mid
Permissionless Value on the Blockchain
Frontrunning

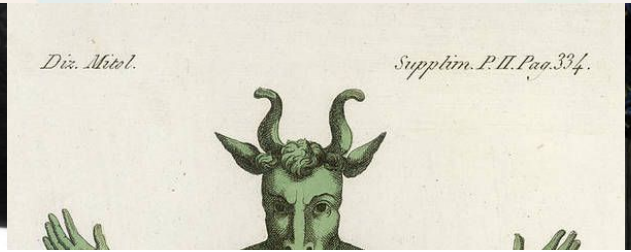

THEY DON'T KNOW THIS IS NOT MEV
YES WE KNOW
WE JUST DON'T CARE, IT'S A GOOD MEME
imgflip.com

So my take is that MEV is a severely unformalized orphaned initialism, abused just like incentive compatibility in mechanism design. In MEV there is no Lipschitz continuity so you can't even analyze to have good bounds, we can mitigate tengentially by dictating this is NOT MEV because

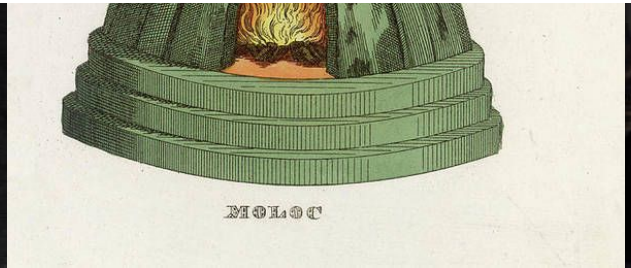
$$
\begin{aligned}
\dot{V}_1 \le & -(\lambda_{\min}(\Sigma) - \varepsilon \| J^{-1} \|) \| \tilde{\omega} \|^2 + \tilde{\omega}^{\mathrm{T}} J^{-1} \tilde{f} \\
& - \tilde{\omega}^{\mathrm{T}} J^{-1} \mathrm{Y} \hat{\dot{f}} + \frac{1}{\kappa}(K - K^*) \rho_1 \tilde{\omega}^{\mathrm{T}} \mathrm{sign}(\tilde{\omega}) \\
& + \frac{1}{\beta} \tilde{f}^{\mathrm{T}} \mathrm{Y}^{\mathrm{T}} ((-\Sigma + \varepsilon \| J^{-1} \|) \mathrm{Y} + I_3) \tilde{f} - \frac{1}{\beta} \tilde{f}^{\mathrm{T}} \mathrm{Y}^{\mathrm{T}} \mathrm{Y} \hat{\dot{f}} \\
& + \frac{1}{\beta} \tilde{f}^{\mathrm{T}} \mathrm{Y}^{\mathrm{T}} \mathrm{Y} \dot{f} + \| J^{-1} \| (\bar{d} \tilde{\omega}^{\mathrm{T}} \mathrm{sign}(\tilde{\omega}) - K \tilde{\omega}^{\mathrm{T}} \mathrm{sign}(\tilde{\omega})) \\
& + \| J^{-1} \| (K^* \tilde{\omega}^{\mathrm{T}} \mathrm{sign}(\tilde{\omega}) - K^* \tilde{\omega}^{\mathrm{T}} \mathrm{sign}(\tilde{\omega})),
\end{aligned}
$$

Al Capone, Evil Deity, Louis XVI

Al Capone, Evil Deity, Louis XVI



This is MEV



Abstraction

Romance of the three MEV

Al Capone the Mafia

Mafia Extractable Value arises when one agent (coalition of agents) gains an asymmetric knowledge of another agent's private information (asymmetric sophistication).

Examples:

- Sandwiching
- Generalized Frontrunning
- Trading on limit-order-book imbalance, gain knowledge of other agent's utility (intent): see more bid than ask, take best ask and make best bid

Evil Deity the Moloch

Moloch Extractable Value is the value that is surrendered to the Moloch, i.e., uncoordination.

Examples:

- Negative externalities caused by inexpressive mechanisms, e.g., shrinked transaction quality trilemma because of spam from random ordering
- OG “High Frequency Trading Arms Race” where arms race cost is transferred into higher spread for users
- Lack of x-domain bundles make searchers price-in the risk, does less arbs, making market less efficient

Louis XVI the Monarch

Monarch Extractable Value arises from the fact that the coordinator (e.g., sequencer, validator) has the ultimate power of deciding the ordering/allocation of spec-on-state (which specification/property does the next state satisfy).

Examples:

- Validators accrue value because they have the power of determining block content
- X-domain market maker bridge extracting value by market making swaps
- Colocation fees that accrue to exchanges/latency service providers, who has power of deciding the outcome

{Mafia, Moloch, Monarch}

Suppose M is the Monarch in our universe/game E, and W is the social welfare function.

- MolochEV = W(M*) - W(M), where M* is the best possible mechanism for E to allocate spec-on-state
- MonarchEV = W(M) - W(-M), where -M is the game E without M as coordinator
- MonarchEV + MolochEV = W(M*) - W(-M), is innate to the game E and does not depend on M, so it is a constant (fixing E)
- MafiaEV depends on the sophistication details/power of agents in M (how much ex-post knowledge, or “last look,” you can have over other agents)

The three values have distinct sources, and those sources of value are non-overlapping.

Thus, we call them 3EV, {Mafia, Moloch, Monarch} Extractable Value, sum type, perfection.

Future is in our hands

MafiaEV + MolochEV + MonarchEV = 100% MEV

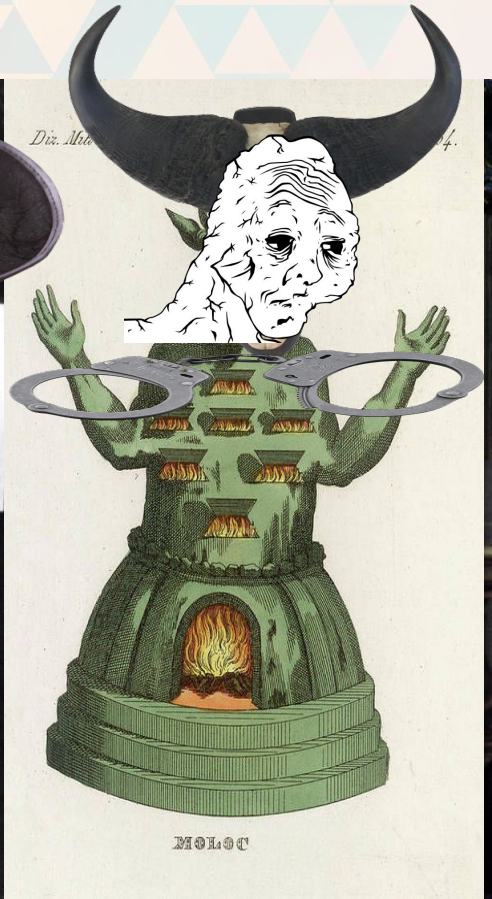
MonarchEV + MolochEV = a constant depending only on E, but percentage depends on M. Nice link with Price of Anarchy meme (can give bound version).

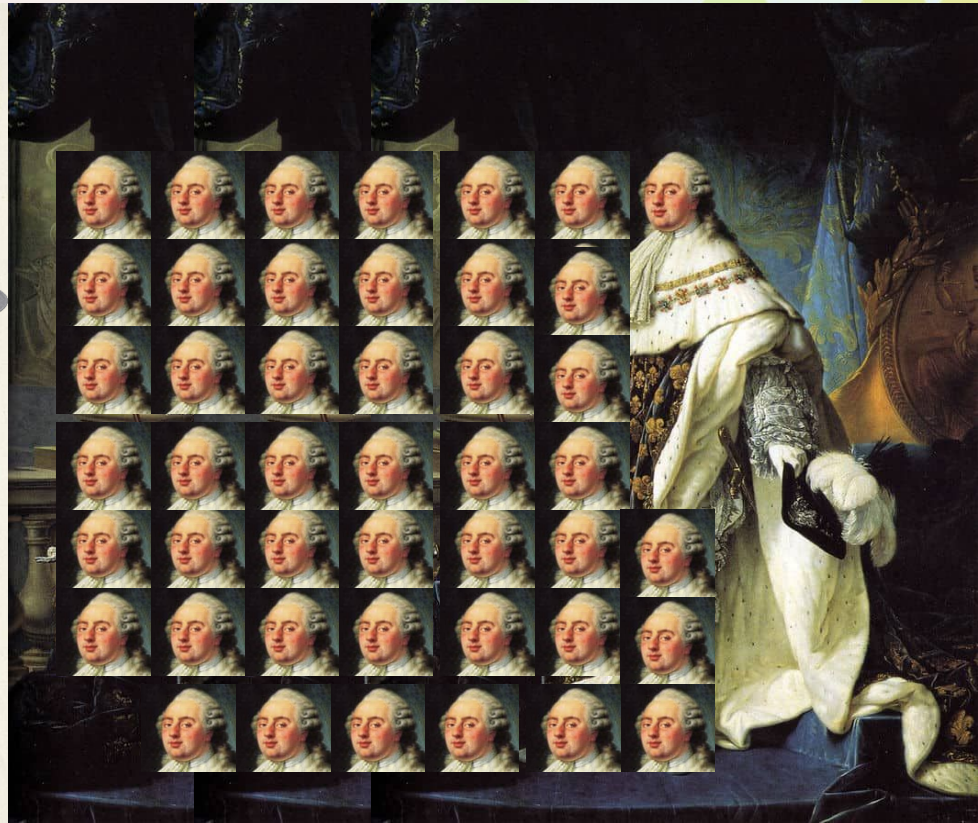
MafiaEV = a constant depending on M.

Since the sources are distinct, we can adjust the percentage of the three variants by transforming one form of MEV into another (by designing a good M)

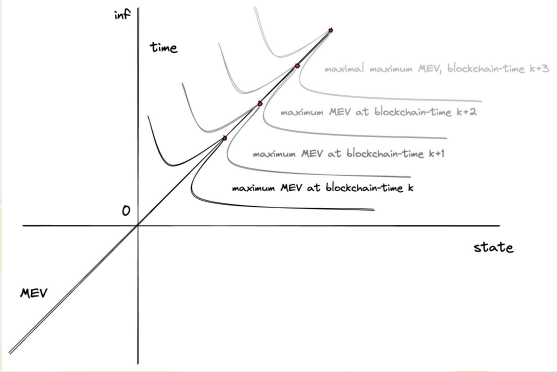
Ideally, we have 0% MafiaEV, 0% MolochEV, 100% distributed MonarchEV

0%, 0%, 100% with distribution





Monarch - Caveats



W(-M) depends on the game E.

Assume M represents a domain/builder/some coalition of agents, we give an inter-domain coalition factor k, where k=1 if M is monopolistic across all domain (including time as a domain, so k is a discounted n-dimensional preference curve), and k=0 if M is powerless.

Forming a larger coalition means higher k, enables more credible extortion, with MonarchEV for M = k*MonarchEV if M and -M forms a grand coalition.

Users can be Monarch if they have a large enough k, similar for validators, searchers, builders, etc,. The inter-domain coalition factor represents your collective bargaining power, which determines how M is setup within E

Monarch - Caveats

However, core of this cooperative game might not exist if we have too many inter-temporal coalitions, i.e., non-monotonicity of coordination/efficiency & incompleteness theorem of MEV.

The specific values of k depends on how we setup the game. We can throne or dethrone different monarchs, ultimately, we want to choose M* that is most incentive aligned with long-term prosperity and is most capable of coordination.

Reason for Monarch abstraction is because outcome is not common knowledge and depends on agents' private information which other agents don't have prior to MEV-time. So it's hard to analyze equilibria (esp. sophistication semantics), thus we reduce guarantee to have bounds on incentive compatibility and individual rationality.

Concretization

Case Studies

On Frequent-batch-auction style first-come-first-serve

Definition 6.2 (Fairness granularity)**.** For granularity g, we consider that timestamps are bucketed into slots of interval g time each (e.g., $[0, g)$, $[g, 2g)$ and so on). Events within a time bucket are assumed to happen at the same time.

Instead of reporting a strict ordering (by receive-order time) of transaction, each individual node report a partial ordering to the leader of the ordering consensus protocol.

>, >=

After aggregating each individual nodes' preferences, the Monarch (leader) gets a weak ordering (by FCFS) with unordered batches in it (caused by condorcet paradoxes and the initial partial ordering). Now the Monarch tries to resolve the order of the unordered batch using auctions

Vanilla-FCFS
v.s.
FBA-FCFS

65%+ of Uniswap volume is from (statistical) arbitrage, and among the other 35% it's a few big market makers.

The burst period on Ethereum (arises from public information reveal) takes around 1.2s, and 75% of the conflict of preferences happen in 4% of the time. Vanilla FCFS compared with FBA-FCFS, will be bearing extra negative externalities (e.g., centralization, higher fees, worse UX, etc,.) from 12x more conflict of preferences.

Bursts of conflict of preferences are significant, and just adding some partial ordering in FCFS mitigates most.

If we compared 3EV of vanilla-FCFS with FBA-FCFS:

Mafia: same, 0%, (assuming programmable privacy)

Moloch: much more, from uncoordination and a naive ultra-simplified social choice function that does not coordinate burst period MEV (permissionless, price discovery, atomic)

Monarch: much less (by def), also it throned the wrong king (AWS, Google Cloud), the Monarch is not incentive aligned and is more centralizing

Transformation of 3EV

Spread charged by Market Maker bridges

If miners go rogue and steal bundles

When you go from public mempool to vanilla-FCFS

A malicious coordinator that pockets all surplus

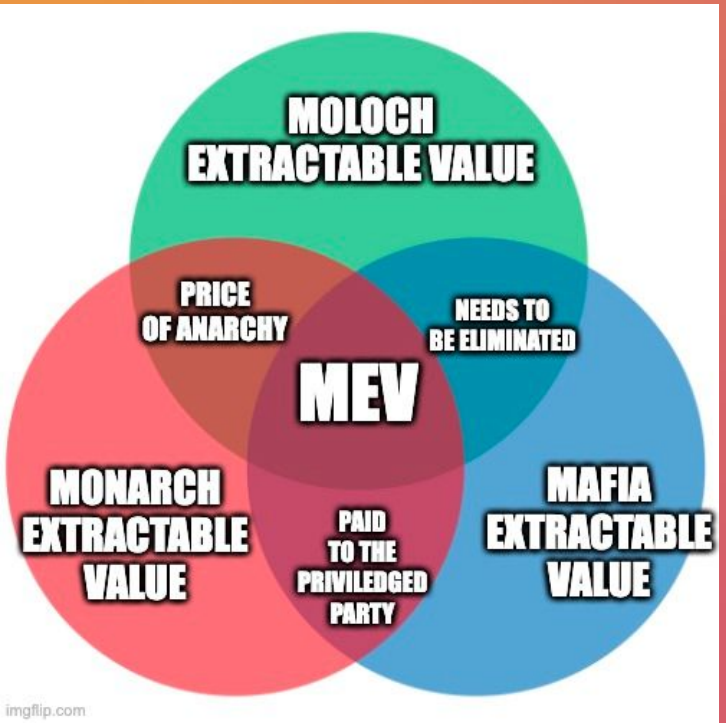
Programmable privacy

DAO governance (non-monotonic decentralization)

Concretization

Implications

Implications



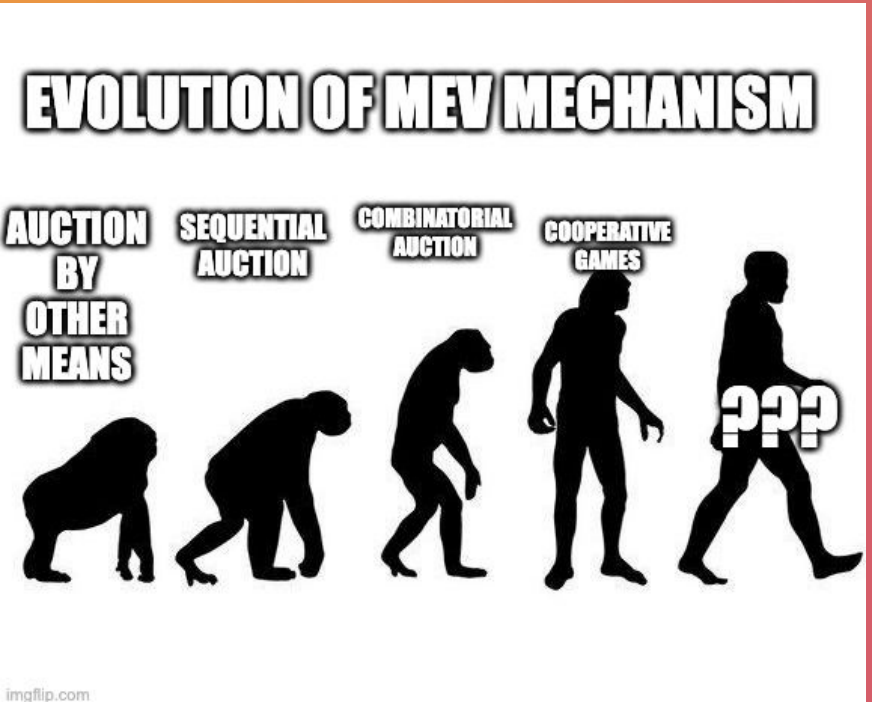
How to achieve 0%, 0%, and a distributed 100%?

MafiaEV: programmable privacy, which allows full expressivity and agents control how their information is used along the path of determination of outcome by M.

MolochEV: efficiency, Price of Anarchy elimination via refinement of society ie specialization. Slack v.s., Eula.

MonarchEV: value division in a way such that maximizes welfare/future returns. Don't focus on tiny kickbacks to existing 1x users, focus on onboarding the invisible 99x users, as MonarchEV grows superlinearly (dMEVdt). For example, investments into wallets, or retroPGF.

Evolution



How to achieve 0%, 0%, and a distributed 100%?

3EV was defined by source of value

Sink of value is different, e.g., MafiaEV sinks to Monarch

Sink of value impacts the source of value

Controlling sink allows controlling source, via the magic of credible commitments

- Builder as rollup (zk/op, optimistic social sequencing)
- Expressivity of bidding language (incompleteness theorem), semantics lattice
- Decentralization of building (parametrized Themis)
- SGX, tokens, revelation principles, etc,.

But all of this conditions on a low enough inter-domain coalition factor, i.e., high enough competition (contestable).

Utterance

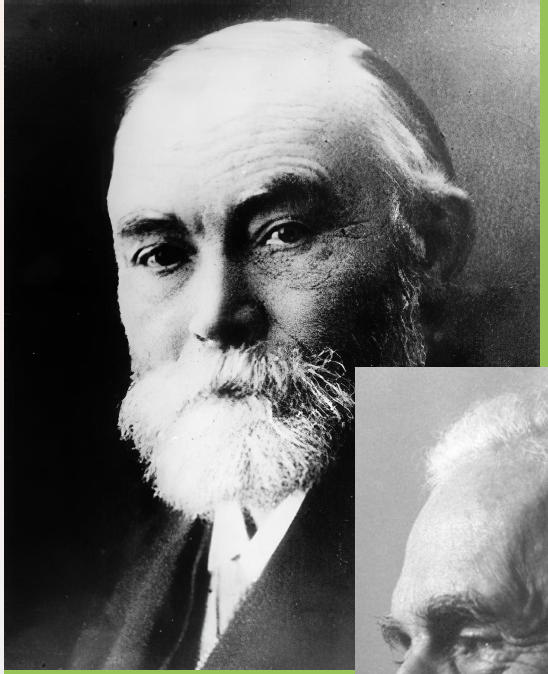
Philosophical Foundation For “This is NOT MEV”

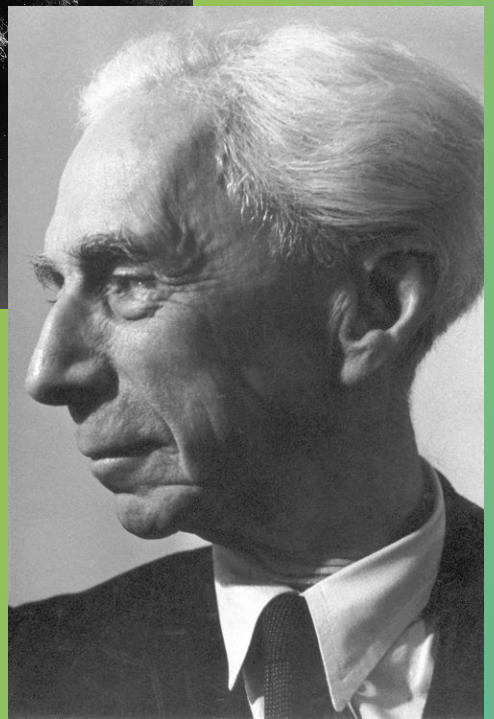
Presuppositions and Utterances

“X is MEV”

“There exists a game E and an allocation mechanism/ordering protocol M, and that within (M, E) using the 3EV definitions we can indeed see X is constituted by a type (or multiple types) of 3EV.”

Utterance of “X is MEV” has a presupposition of the existence condition of E and M and X being indeed in the set 3EV(E, M). Thus, if there does not exists such E and M (*absent of the Monarch*), then the utterance is false. X is NOT MEV



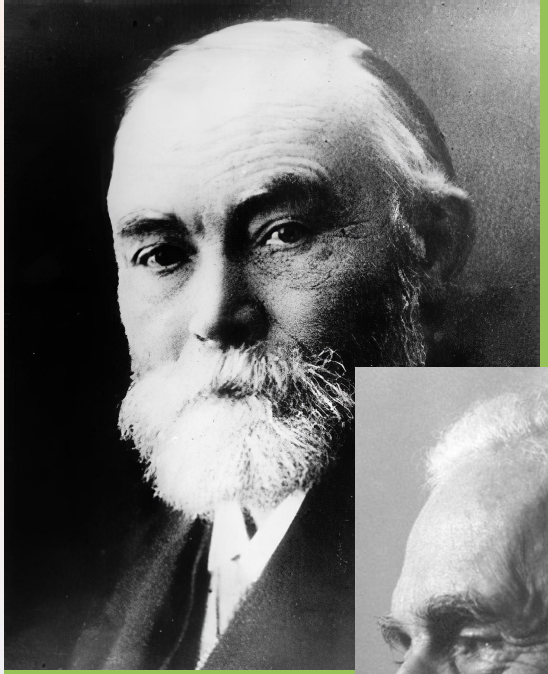


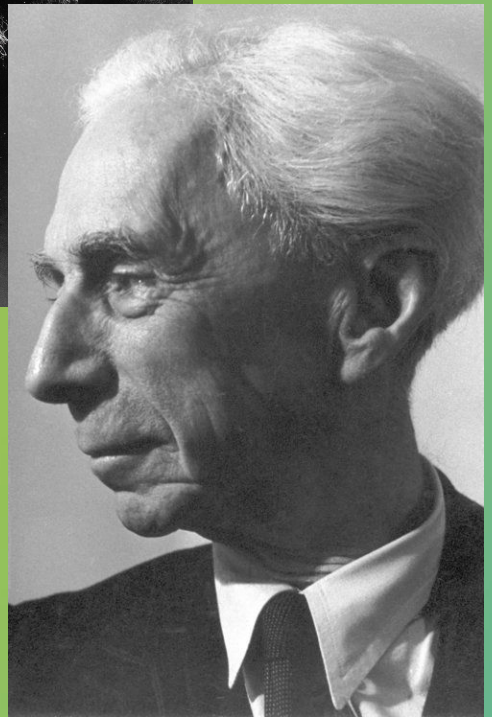
Example

The value Kim and Don is extracting absent a Monarch, i.e., (1,1), is NOT MEV

Kim \ Don	Silent	Betray
Silent	2,2	0,3
Betray	3,0	1,1

Kim & Don playing simple Prisoner Dilemma





Language Games

“X is MEV”

The sentence might be true, as the context of the utterance is social and we might agree on some notion of the game.

If the sentence is presented without context, then the sentence is nonsense and has no truth value.

Thus, ultimately the test of MEV conditions on which philosophical interpretation of language you agree with, if you are Wittgenstein and believes that the utterance is within the context where it is socially agreed that the Monarch is existent (which is often the case, as we can say *physics* is the Monarch), then that value is indeed MEV.

Let's change the "Language Game"

Aren't you tired of "Miner" or "Maximal?" (where the grammar isn't even correct, we say maximal MEV all the time)

We should just say MEV, and it conveniently represents a short hand for the sum type of

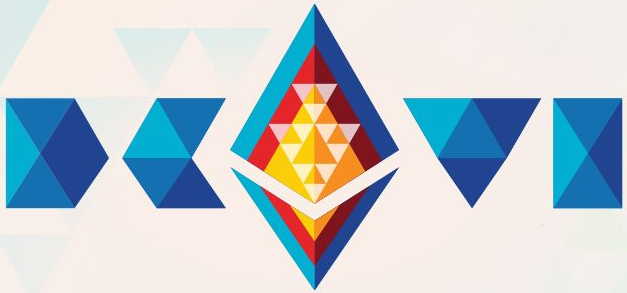
{Mafia, Moloch, Monarch} Extractable Value

MEV = {Mafia,Moloch,Monarch}
Extractable Value

Benefits:

- Distinct values (source)
- Formalizable (social process)
- Settles “bad” MEV
- Tradeoff (transform) space clear
- Implies clear solution recipe
  - Research MonarchEV distribution!
  - Research programmable privacy!
- Presupposition test (context clear)


ƷEV ƷEV ƷEV ƷEV ƷEV ƷEV ƷEV ƷEV ƷEV ƷEV
ƷEV ƷEV ƷEV ƷEV ƷEV
ƷEV ƷEV ƷEV ƷEV ƷEV
ƷEV ƷEV ƷEV ƷEV ƷEV
ƷEV ƷEV ƷEV ƷEV ƷEV
ƷEV ƷEV ƷEV ƷEV ƷEV
ƷEV ƷEV ƷEV ƷEV ƷEV
ƷEV ƷEV ƷEV ƷEV ƷEV
ƷEV ƷEV ƷEV ƷEV ƷEV



3EV: {Monarch, Moloch, Mafia} Extractable Value

Xinyuan Sun

Research, Flashbots ⚡🤖

xinyuan@flashbots.net

@sxysun1

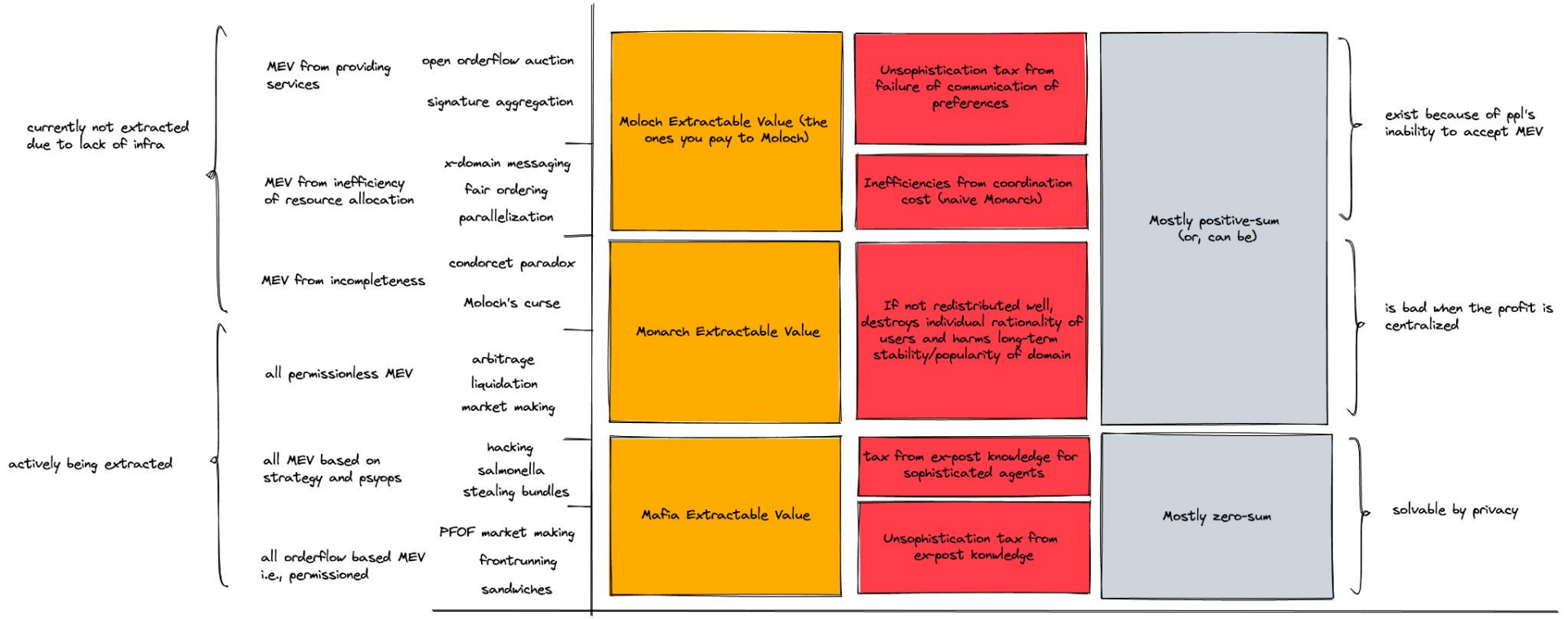
Improvements

- **Robustness**
  - instability <> dishonesty is encouraged with minimal risk
  - long-term prosperity <> honesty <> incentive alignment and recognizing monarchy
- **Fairness**
  - Creates centralization which harms geographical decentralization, network security, censorship resistance and liveness
  - Externality channeled by sophisticated users to unsophisticated users in the form of a less efficient market and worse UX
  - Thrones AWS/Google as Monarch, who isn't incentive aligned with crypto in the prosperity of the domain and its long-term value accrue/user acquisition

Vanilla-FCFS
v.s.
FBA-FCFS

Concretization

Taxonomy


currently not extracted due to lack of infra
actively being extracted
MEV from providing services
MEV from inefficiency of resource allocation
MEV from incompleteness
all permissionless MEV
all MEV based on strategy and psyops
all orderflow based MEV i.e., permissioned
open orderflow auction
signature aggregation
x-domain messaging
fair ordering
parallelization
condorcet paradox
Moloch's curse
arbitrage
liquidation
market making
hacking
salmonella
stealing bundles
PFOF market making
frontrunning
sandwiches
Moloch Extractable Value (the ones you pay to Moloch)
Monarch Extractable Value
Mafia Extractable Value
Unsophistication tax from failure of communication of preferences
Inefficiencies from coordination cost (naive Monarch)
If not redistributed well, destroys individual rationality of users and harms long-term stability/popularity of domain
tax from ex-post knowledge for sophisticated agents
Unsophistication tax from ex-post knowledge
Mostly positive-sum (or, can be)
Mostly zero-sum
exist because of ppl's inability to accept MEV
is bad when the profit is centralized
solvable by privacy

Abstraction

Formalization

Axiomatic Approach

Sophistication Semantics

- Collusion
- Knowledge
- Strategic

Axioms

- Opaque Coordinator
- Colluding Monotonicity
- Self-awareness
- Strategic Coordinator

Axiomatic Approach

(Coalitional) Extortion

- $$\kappa(\alpha, \beta) = \max_{s_i \in S_{\alpha \cup \beta}} W_{\alpha \cup \beta}(s_i) - \max_{s_i \in S_{\alpha \cup \mu}} W_{\alpha}(s_i) - \min_{s_j \in S_{\alpha \cup \mu}} W_{\beta}(s_j)$$

(Coalitional) Stealing

- $$\zeta(\alpha) = \max_{s_i \in S_{\alpha \cup \mu}} W_{\alpha}(s_i)$$