Hi, we are doing research related to MEV and smart contract analysis and would like to ask for your opinion about how our work can contribute to the MEV community.

Recently we have been working on proposing an automated static detection technique for front-running and MEV opportunities in smart contracts.

Different from previous studies that measure the amount of MEV extracted in the transaction history, we are trying to find potential MEV opportunities before the contract is interacted with by users or even before deployment.

We see that current projects, like MEV-explore, only collect historical, already-extracted MEV data for a limited, manually collected set of protocols and contracts, limiting the coverage to only a small portion of the theoretical total extractable value.

With our approach, we hope we can help the community discover a larger range of potential MEV opportunities even before the MEV is exposed to the public.

For instance, if one transaction a user is about to submit will expose MEV to the public, our approach can give warnings before the transaction is submitted to the public mempool. The user can be advised to submit the transaction privately to miners/validators to avoid being front-run by various MEV bots in the wild.

Our approach achieves this by statically analyzing the contract code and using symbolic execution to find functions and the corresponding calling transactions that can expose MEVs.

To sum up, our approach may have the following benefits:

1. Help the community to increase the coverage of MEV measurement. Our approach can automatically help to find more newly-emerging protocols and contracts that expose MEV opportunities.

2. Provide early warnings to blockchain users of the MEVs that will be exposed by their transactions. Our approach can analyze the contract and warn users whether their about-to-submit transactions can be attacked by front-running bots in public mempool, e.g., displacement/insertion/suppression front-running attacks. Currently, users can choose to submit transactions privately to mev-geth nodes, but it requires a solid understanding and rich experience to decide whether a transaction can be front-run and should be submitted privately. Our approach is meant to make this decision much easier for users.

We create this post to ask for your opinion on our research.

- Do you think our research is useful and beneficial to the community?

- Do you think our approach can make the aforementioned two contributions to the community?

- What other contributions related to smart contract code analysis do you think we can make to the MEV community?

Thanks for everyone’s opinions and comments in advance.