Hello everyone!

We are working on our Solidity smart contract state analyzer and extractor tool "SmartMuv". The purpose of this post is to get valuable feedback from the community.

"SmartMuv" can analyze and extract the complete state of a Solidity smart contract using static analysis techniques. The feature that separates it from other static analysis tools is the "Key Approximation Analysis"

of mapping keys, which can retrieve all keys of a mapping variable.

It uses ASTs to analyze the Slot Layout of the smart contract and performs "Key Approximation Analysis" on CFGs. It consists of two steps:

Reach Analysis

It is a data-flow analysis that statically determines which definitions may reach a given point in the code. During this analysis, we mark all the nodes where a key is appended/added to a mapping variable.

Key Backtracking

In backtracking, we use Reach Analysis results to reach the source of marked key variables.

We then extract the values of all the approximated mapping keys and then calculate their respective slots to extract their values from the chain.

We have tested our tool on 70K unique smart contracts extracted from XBlock dataset. SmartMuv can analyze all types of variables including mapping variables, multi-dimensional arrays, and structs.

Uses

- Slot Analysis

of a smart contract, to get a complete storage layout of a smart contract

.

- Smart contract storage audit

.

- Can be used for Dapp/Blockchain data explorers.
- State extraction (snapshot)

of smart contracts up to the latest or a certain block number.

- Redeployment/upgrade

of smart contracts along their existing state/data

.

- Migration

of smart contracts along with contract data

i.e. L1 to L2 or L2 to L2 migrations.

We have worked on "Interprocedural Analysis" and "Event Analysis" to ensure we do not miss any mapping key source, and retrieve every possible value that can be used as a mapping key. These analyses need to be integrated into our public repo.

Our [research work](link) has been published

at ACM TOSEM

, kindly check out our [GitHub repo

](https://github.com/WaizKhan7/SmartMuv), any feedback will be really appreciated!