
Woke Fuzzer
EthPrague 2022
Dominik Teiml, Michal Převrátil

Contents

Intro

- Ackee Blockchain is a blockchain security firm based in Prague, Czech Republic.
- Dominik Teiml: Ethereum Tech Lead @ Ackee Blockchain.
  - Fml. Gnosis, CertiK, Trail of Bits
- Michal Převrátil: Woke Developer @ Ackee Blockchain.

History of Woke

I think we all feel the unmaturity of existing Ethereum tooling.

This is usually NOT the fault of the developers.

Making great tools requires:

- a lot of experience with Ethereum,
- experience with the implementation language,
- a lot of expended effort,

and the gains (at least for the developer) are not immediately super high.

Sometime in October 2021, Dom saw enough possible improvements for Slither to warrant building a new tool.

History of Woke II

So originally, the idea was just to build a better Slither.

Later, we realized that if we have that, we can easily implement a lot of other features:

- a state-of-the-art language server,
- research new methods of contract visualization, both on the static level (source code) and dynamic (transaction execution)
- a line-by-line debugger for Solidity contracts,

and many others. We got to work.

History of Woke III

First, we implemented a config parser, a Solidity version manager, a regex parser for versions and imports, and a compilation manager.

Sometime in March, Dom implemented a simple fuzzer during a smart contract audit.

We then used it during several audits and it found several high-severity bugs.

History of Woke IV

Fork?

•

Merge?

Echidna