

SMT-based Gas Consumption Computation for Smart Contracts

Matteo Marescotti, Martin Blich, Antti E. J. Hyvärinen, Sepideh Asadi, Natasha Sharygina



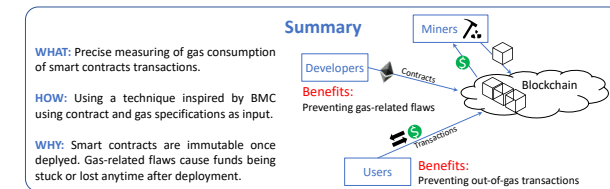
Università della Svizzera Italiana

Faculty of Informatics
Formal Verification and Security Lab

Matteo Marescotti, Martin Blich, Antti E. J. Hyvärinen, Sepideh Asadi, Natasha Sharygina

- Smart contracts are **immutable** once deployed.
- Gas-related flaws cause **money losses, DoS**, etc.
- Effects are **anytime** after deployment.

SMT-based Gas Consumption Computation for Smart Contracts



THIS WORK

- **Analysing** gas consumption.
- Using a technique inspired by **BMC**.
- Contract **model** and gas **specification** as input.

