Harnessing SMT Solvers for Reasoning about DeFi Protocols

Mooly Sagiv
Certora and Tel Aviv University
Tel Aviv, Israel
msagiv@acm.org

***Abstract*—DeFi (Decentralized Financial) Protocols implement financial programs using low-level programming. DeFi adoption started to go parabolic in 2020, and it's still very robust in different market conditions in 2024. Today, DeFi assets exceed 300 billion USD. A fundamental principle behind DeFi is that small open-source software called "smart contracts" precisely define the trading conditions and create an open global economy not controlled by governments and people.**
However, smart contracts are difficult to implement correctly since their behavior can radically change in different market conditions. Moreover, hackers constantly try to abuse the code to drain the money stored in the smart contracts. On the positive side, it is pretty natural to write high-level formal specifications of smart contracts since their economical utilities are well understood. Indeed, this is a unique domain where software developers are eager to write formal specifications.
I will describe the challenges of harnessing existing SMT solvers for reasoning about smart contracts.

https://doi.org/10.34727/2024/isbn.978-3-85448-065-5_4