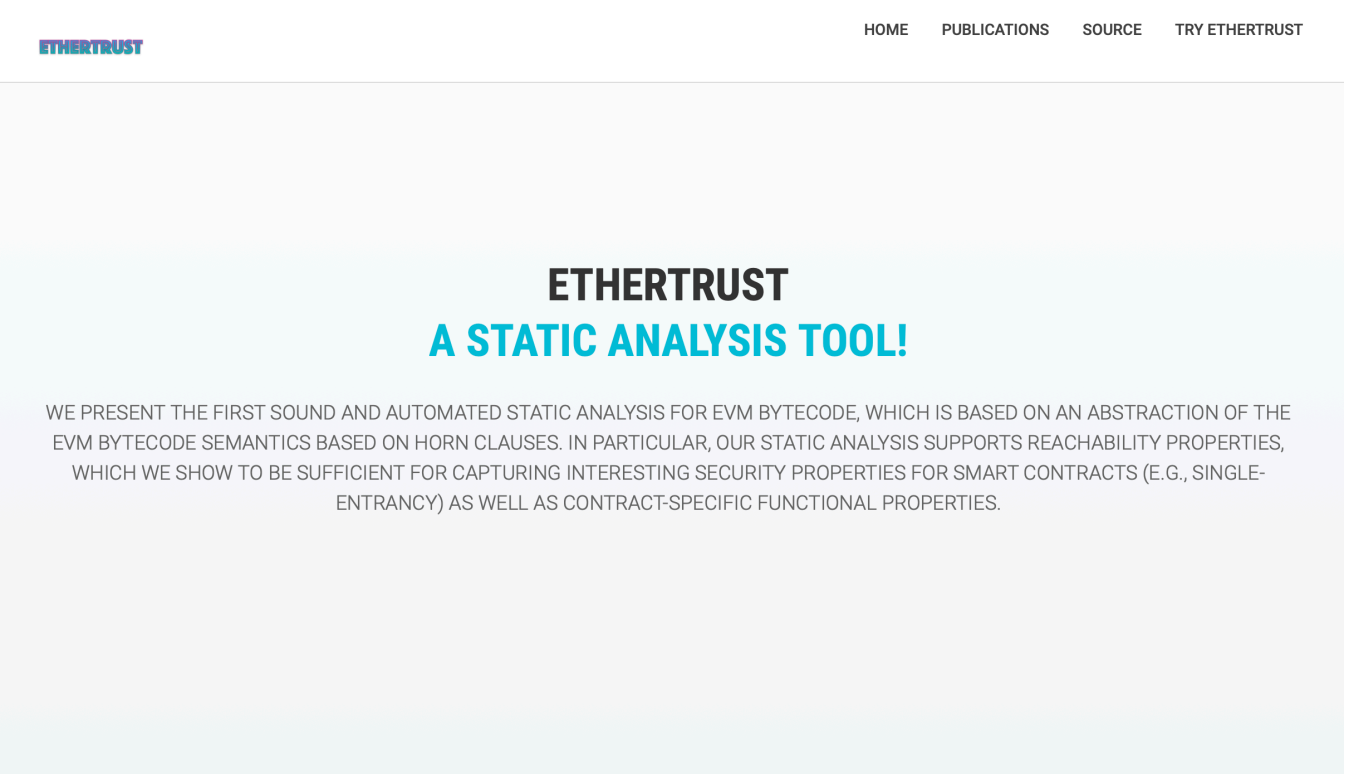
EtherTrust User Guide

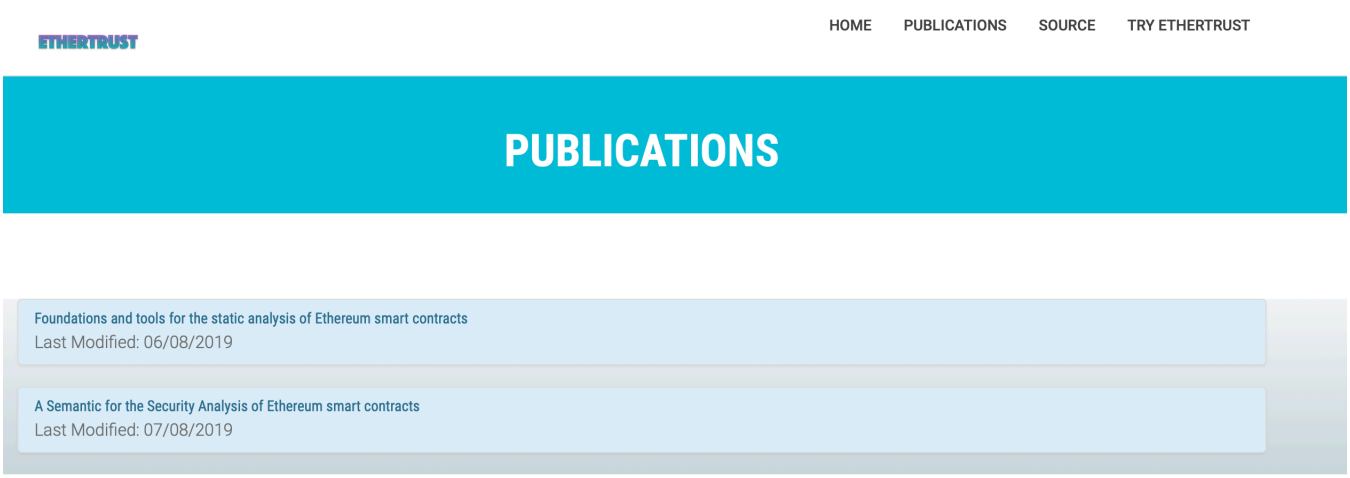
EtherTrust is a static analysis tool that implements a sound analysis of Ethereum Smart contracts. In particular, it is capable of showing wether a contract has a reentrancy flow that can lead to loss of the money stored in a contract, hence it is of interest to Smart contract developers and users.

Preliminaries

EtherTrust does not need an installation and can be used via its online interface.

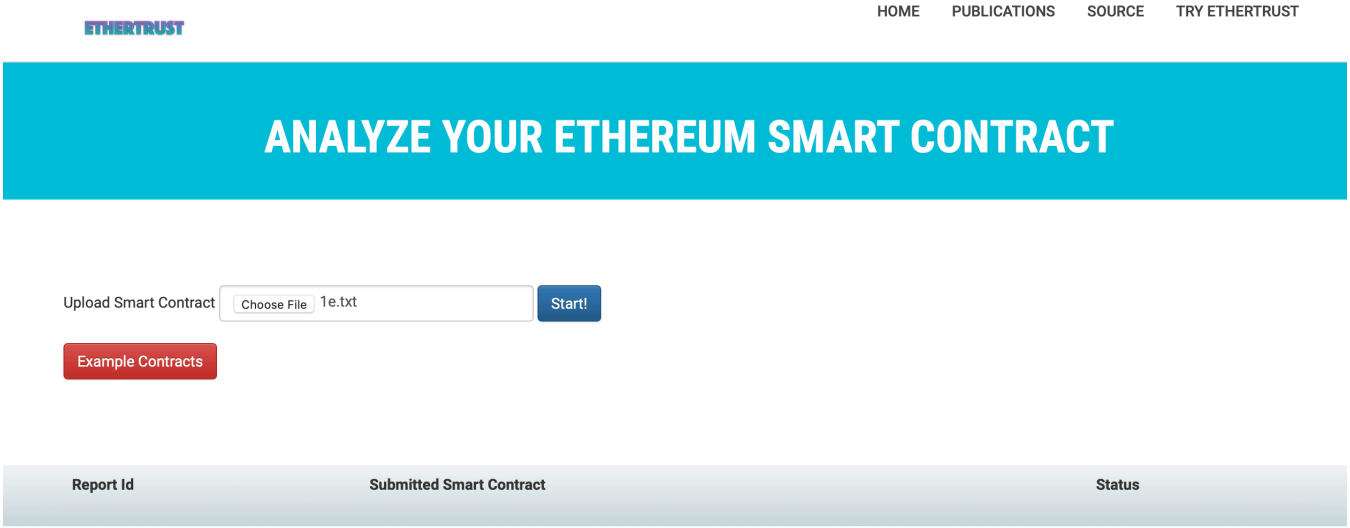


All publication materials about the theoretical foundations driving EtherTrust are also available online

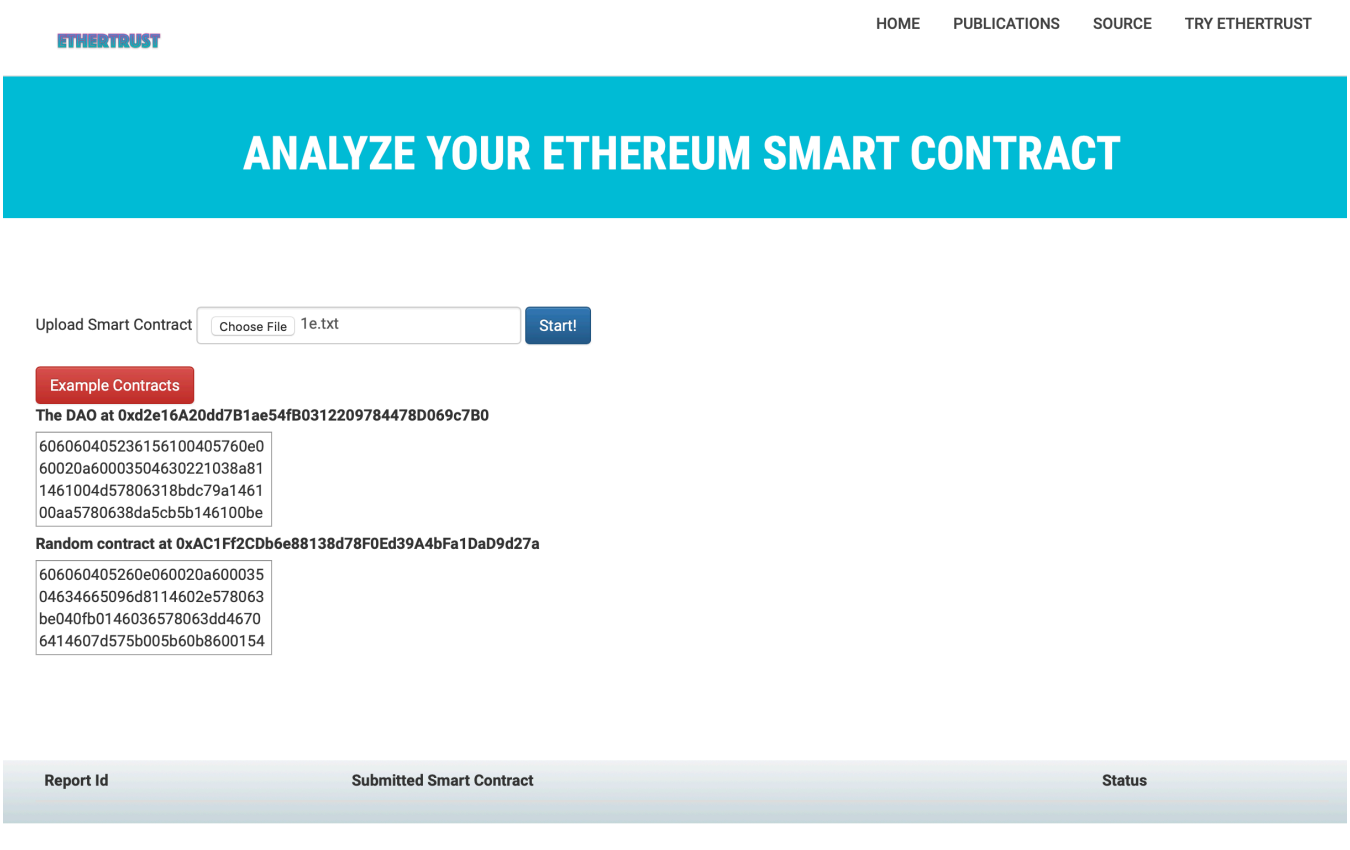


Analyzing contracts

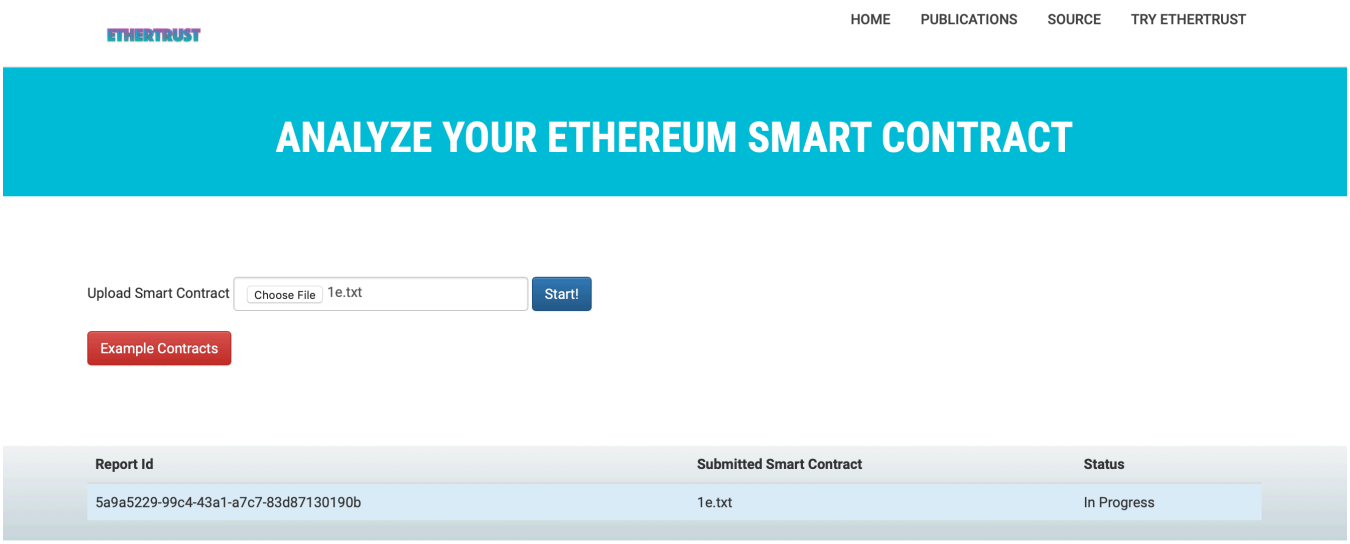
Currently, the web interface accepts contracts with size <=100kb. Users are free to submit their contracts saved in a text file. Contracts are expected to be submitted in a form they are stored in a blockchain, i.e., bytecodes.



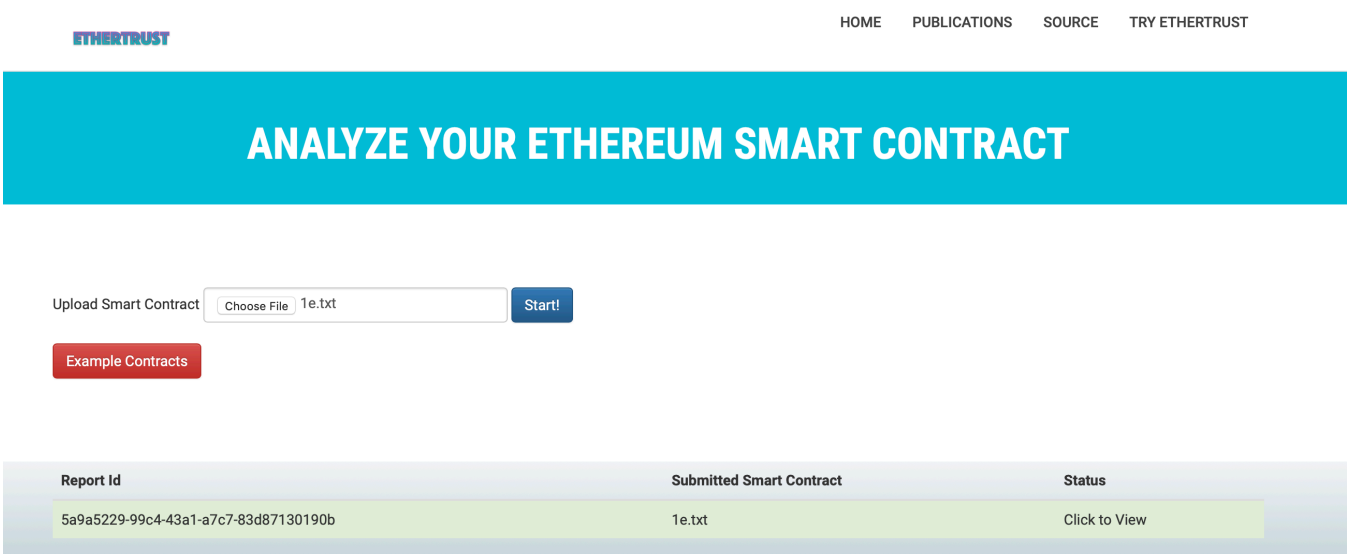
In case a user does not have a contract to analyze, still would like to try the service, we provide two example contracts, one (0xd2e16A20dd7B1ae54fB0312209784478D069c7B0) which exhibits a reentrancy flow and a safe contract with respect to reentrancy property (0xAC1Ff2CDb6e88138d78F0Ed39A4bFa1DaD9d27a).



After pressing a **Start!** button analysis is executed. Each analysis task gets assigned a Report Id - a unique hash value. This value can be used if a user leaves website, but still would like to check the results later.



When analysis is done the webpage changes and a user is welcomed to see the results. Our website fetches the results of analysis automatically, there is no need to refresh the page to observe the behavior. And happens it to be the case that the webpage was closed, analysis results still can be retrieved using the Report Id.



Results

For each analyzed contract there can be multiple results, each of them corresponds to a possible reentrancy flow in a contract.

EtherTrust can establish two kinds of result: SATISFIABLE (sat) and UNSATISFIABLE (unsat).

Sat means that there is a satisfying assignment found that corresponds to the reentrancy flow. In other words, if sat result is derived it might be the case that the analyzed contract might have a reentrancy bug.

Unsat means that EtherTrust managed to show the impossibility of having a reentrancy bug for a particular contract. In other words, it mens that the analyzed contract is guaranteed to be safe with respect to the reentrancy flow.