SAND2017-7564C

The Center for Cyber Defenders

Expanding computer security knowledge

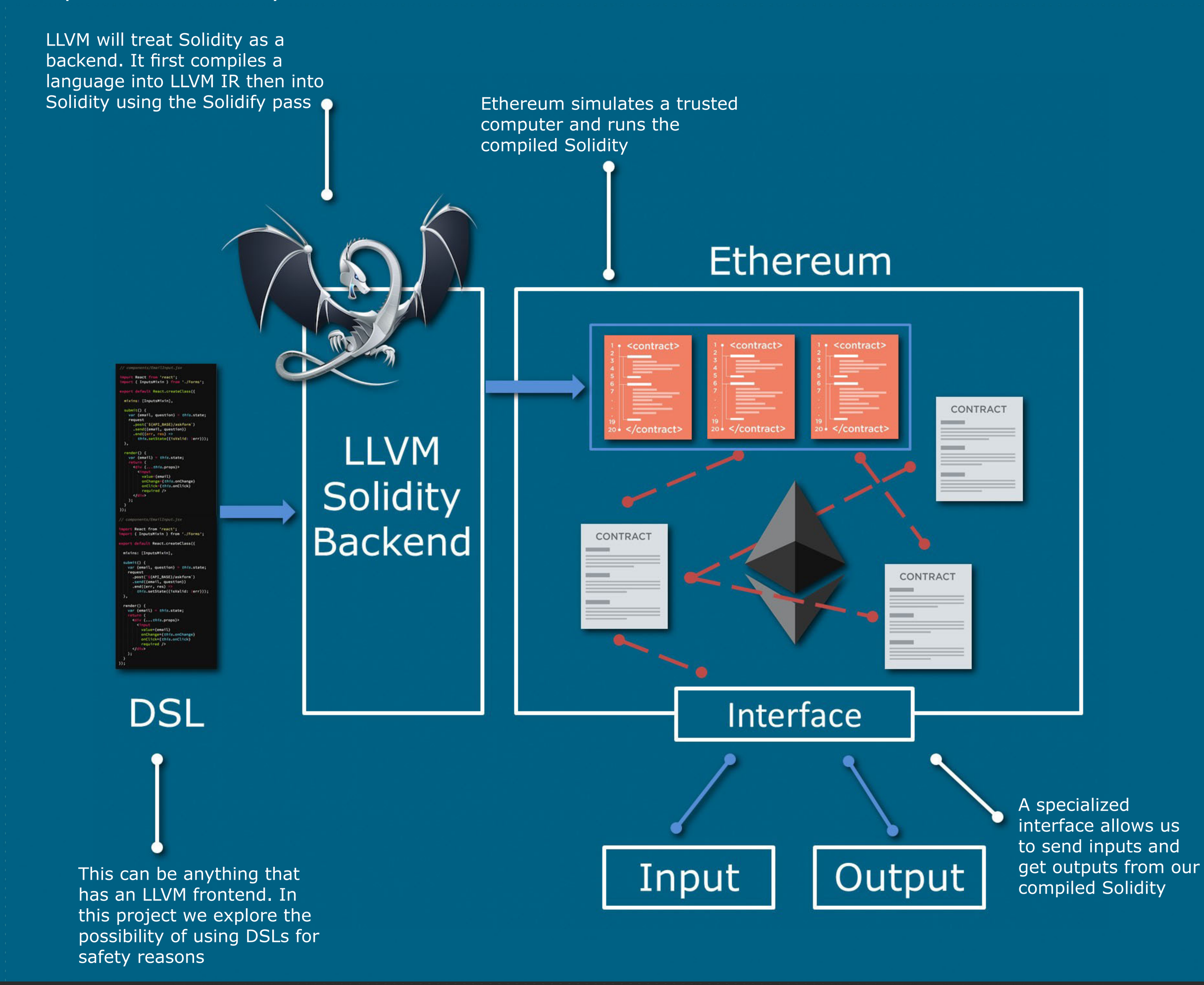
Bring Domain Specific Languages to Ethereum

Abhiram Kothapalli, University of Illinois at Urbana-Champaign

Project Mentors: Nick Pattengale, Org. 5824 and Kasimir Gabert, Org. 5838

Abstract

In this project we explore the feasibility of bringing Domain Specific Languages to the Ethereum blockchain. Ethereum can be thought of as a global, public, cloud computer where programs in the form of smart contracts have their own storage space on the blockchain. A Smart contract is designed to execute in a decentralized fashion, where no single entity can modify the results of its execution. This allows anybody to trust the integrity of a smart contracts computation without having to place trust in any third party. While smart contracts are secure in theory, they are very difficult to program safely in practice. By creating a toolchain to compile lightweight domain-specific languages into Ethereum's dominant language, Solidity, we allow non-specialists to effectively develop safe and useful smart contracts. For example lawyers from a certain firm can have a proprietary DSL that codifies basic laws safely converted to solidity to be securely executed on the blockchain. In another example, a simple provenance tracking language can be compiled and securely executed on the blockchain.



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.