World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:06, 2018

Formal Verification for Ethereum Smart Contract Using Coq

Authors : Xia Yang, Zheng Yang, Haiyong Sun, Yan Fang, Jingyu Liu, Jia Song

Abstract : The smart contract in Ethereum is a unique program deployed on the Ethereum Virtual Machine (EVM) to help manage cryptocurrency. The security of this smart contract is critical to Ethereum’s operation and highly sensitive. In this paper, we present a formal model for smart contract, using the separated term-obligation (STO) strategy to formalize and verify the smart contract. We use the IBM smart sponsor contract (SSC) as an example to elaborate the detail of the formalizing process. We also propose a formal smart sponsor contract model (FSSCM) and verify SSC’s security properties with an interactive theorem prover Coq. We found the 'Unchecked-Send' vulnerability in the SSC, using our formal model and verification method. Finally, we demonstrate how we can formalize and verify other smart contracts with this approach, and our work indicates that this formal verification can effectively verify the correctness and security of smart contracts.

Keywords : smart contract, formal verification, Ethereum, Coq
Conference Title : ICICS 2018 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 06-07, 2018

Open Science Index, Computer and Systems Engineering Vol:12, No:06, 2018 publications.waset.org/abstracts/85595.pdf