National Blockchain Talk Series

Department of Computer Science and Engineering

Indian Institute of Technology Kanpur

Date: Monday September 10, 2018

Time: 10:15 – 11:30 am

Venue: KD 101

Title:

Analyzing Safety of Smart Contracts using Zeus

Speaker:

Dr. Mohan Dhawan

IBM India Research Lab

Abstract: A smart contract is hard to patch for bugs once it is deployed, irrespective of the money it holds. A recent bug caused losses worth around $50 million of cryptocurrency in the Ethereum Blockchain. We present *Zeus*---a sound fault detection framework to verify smart contracts. Zeus leverages both abstract interpretation and symbolic model checking, along with the power of constrained horn clauses to quickly verify contracts for safety. We have built a prototype of Zeus for Ethereum and the Hyperledger Fabric blockchain platforms and evaluated it with over 22,400 smart contracts. Our evaluation indicates that about 94.6% of contracts (containing cryptocurrency worth more than $0.5 billion) are vulnerable. Zeus is sound with zero false negatives and has a low false positive rate, with an order of magnitude improvement in analysis time as compared to any prior attempt at verifying smart contracts.

Bio: Mohan is a Researcher Staff Member with IBM Research, India. He is broadly interested in Systems, Security and Program Analysis, with a current focus on Blockchain. Mohan has published several papers in high impact conferences. He earned his PhD in Computer Science from Rutgers University in 2013.