UNIVERSITY *of* GUELPH

COLLEGE *of* ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PHD.CSCI Seminar

Monday January 25, 2021 at 10:00AM on Zoom

Achieving Fairness in an Automated, Distributed and Decentralized Trustless Environment

Muhammad Rehman

Advisor: Dr. Charlie Obimbo
Co-Advisor: Dr. Getu Hailu (Department of F.A.R.E)
Advisory Committee: Dr. Xiaodong Lin
Advisory Committee: Dr. Hassan Khan

ABSTRACT:

For a transaction, the involved parties have to trust a neutral entity that could ensure a trustful transaction and deal with any situation in a fair manner acceptable to all stake holders. In our real life we achieve this by having some authoritative entity in the middle, e.g. notary, to oversee the transaction. However, it is a challenge in an e-transaction in a distributed environment which is essentially considered a trustless system where transacting parties do not need to have a middleman to ensure the fairness. Blockchain offers trustless transaction in a distributed environment without the need of a trusted middle entity but it is limited to cryptocurrency transactions. What if we want to have a property sale in the same fashion i.e. automated, decentralized and trustless way without involving a middle entity? Smart contract is a set of self-executable code on underlying blockchain that ensures the fulfillment of terms and conditions set between the parties without involving an authoritative facilitator. However, sometimes in smart contracts, fairness becomes questionable if one or more parties are inclined to cheat.

Fairness is a key ingredient in any financial transaction. Transactions can't work properly unless a rigid fairness policy is in place. Fairness could have been achieved differently in unique situations with the presence of pre-defined terms and conditions aka rules. What we have to have in an automated blockchain smart contract system that allows us to achieve fair outcome when unknown parties, who do not trust each other, want to execute a transaction without involving any intermediaries to enforce their rules for fairness? This could be achieved in the presence of a set of rules developed using special security protocols, encryption/decryption techniques, cryptographic hashes and zero knowledge proof to build a game-like solution that ensures the fairness without having any ruling authority.