THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

RESEARCH SEMINAR

Insightful Mining Equilibrium

Prof. Xiaotie Deng

Chair Professor

Peking University, China

Date : 1 February 2023 (Wed)
Time : 11:00 am - 12:00 pm
Hybrid Mode: PQ703 /Zoom

Abstract

The selfish mining attack, arguably the most famous game-theoretic attack in blockchain, indicates that the Bitcoin protocol is not incentive-compatible. Most subsequent works mainly focus on strengthening the self-ish mining strategy, thus enabling a single strategic agent more likely to deviate. In sharp contrast, little at-tention has been paid to the resistant behavior against the selfish mining attack, let alone further equilibrium analysis for miners and mining pools in the blockchain as a multi-agent system.

In this work, first, we propose a strategy called insightful mining to counteract selfish mining. By infiltrating an undercover miner into the selfish pool, the insightful pool could acquire the number of its hidden blocks. We prove that, with this extra insight, the utility of the insightful pool could be strictly greater than the self-ish pool's when they have the same mining power. Then we investigate the mining game where all pools can either choose to be honest or take the insightful mining strategy. We characterize the Nash equilibrium of this mining game, and derive three corollaries: (a) each mining game has a pure Nash equilibrium; (b) honest mining is a Nash equilibrium if the largest mining pool has a fraction of mining power no more than 1/3; (c) there are at most two insightful pools under equilibrium no matter how the mining power is distributed.

About the Speaker

Prof. Xiaotie Deng got his BSc from Tsinghua University, MSc from the Chinese Academy of Sciences, and Ph.D. from Stanford University.

He is currently a chair professor at Peking University. He taught in the past at Shanghai Jiaotong University, the University of Liverpool, the City University of Hong Kong, and York University. Before that, he was an NSERC international fellow at Simon Fraser University. Deng's current research focuses on algorithmic game theory, with applications to the Internet and Blockchain Economics.

He is an ACM fellow for his contribution to the interface of algorithms and game theory, an IEEE Fellow for computing in partial information and interactive envi-ronments, and a CSIAM Fellow for contributions to game theory and blockchain. He is a foreign member of Academia Europaea.

He is one of the winners of the 2022 Test of Time Award of ACM SIGecom for set-tling the complexity of computing a Nash equilibrium.

We drive innovation through
SMART COMPUTING