Efficient Blockchain-Driven Multiparty Computation Markets at Scale

Noyes, Charles

My project addresses a long-standing problem at the intersection of computer science, cryptography, and game theory. A truly efficient system for secure multiparty computation (sMPC) has been sought after for over three decades, and here I present a novel sMPC scheme that is fast enough to be feasible for real usage. The core innovation of this project is the novel combining of blockchains, the data stores on top of which cryptosystems like Bitcoin are built, with securely homomorphic computation and verification schemes. Recent innovations in the field have resulted in blockchains that allow for the canonical and deterministic execution of Turing-complete code on top of their decentralized networks. However, this computation is extremely slow. This project offloads the computation step onto a network of peer-processors, to which any internet enabled device can contribute power, and utilizes the blockchain only for the much simpler verification step. Compared to the most recent academic efforts to create fast sMPC systems, this project was orders of magnitude faster. For moderate network sizes, the average speed increased 100-1000x, the gap growing as the network scaled. Perhaps the most exciting result was in the comparison to Hadoop; this project approached overheads of only 20%, at 5 sigma confidence, when adapting the scheduler to deploy sMPC tasks. The implications of this project are vast; a global computational cloud to which any individual can contribute power would decrease the price of generic processing radically. On a broader scale, the entire idea of the computational power of hardware being processor dependent will be rendered obsolete, the very limit of what we can achieve with our ‘existing technology’ will be rendered obsolete.

Awards Won:

Intel ISEF Best of Category Award of $5,000

First Award of $5,000

Intel Foundation Cultural and Scientific Visit to China Award

National Security Agency Research Directorate : Second Award of $1,500