NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

SEMINAR ANNOUNCEMENT

Basic Properties of the Blockchain

Dr Juan Garay
Yahoo Research

Date: 27 April 2017 (Thursday)
Time: 11.00am to 12.00pm
Venue: MAS Executive Classroom 2, MAS-03-07
School of Physical and Mathematical Sciences

Abstract

As the first decentralized cryptocurrency, Bitcoin has ignited much excitement, not only for its novel realization of a central bank-free financial instrument, but also as an alternative approach to classical distributed computing problems, such as reaching agreement distributedly in the presence of misbehaving parties, as well as to numerous other applications—contracts, reputation systems, name services, etc. The soundness and security of these applications, however, hinges on the thorough understanding of the fundamental properties of its underlying *blockchain* data structure, which parties ("miners") maintain and try to extend by generating "proofs of work" (POW, aka "cryptographic puzzle").

In this talk we formulate such fundamental properties of the blockchain—common prefix, chain quality, chain growth—and show how applications such as consensus and a robust public transaction ledger can be built ``on top'' of them, assuming the adversary's hashing power (our analysis holds against arbitrary attacks) is strictly less than ½ and high network synchrony:

The above properties hold assuming that all parties—honest and adversarial—"wake up" and start computing at the same time, or, alternatively, that they compute on a common random string (the "genesis" block) only made available at the exact time when the protocol execution is to begin. In this talk we also consider the question of whether such a trusted setup/behavioral assumption is necessary, answering it in the negative by presenting a Bitcoin-like blockchain protocol that is provably secure without trusted setup, and, further, overcomes such lack in a scalable way—i.e., with running time independent of the number of parties [4].

A direct consequence of our construction above is that consensus can be solved directly by a blockchain protocol without trusted setup assuming an honest majority (in terms of computational power).

Speaker Biography

Juan Garay is currently a Sr. Principal Research Scientist at Yahoo Research. Previously, after receiving his PhD in Computer Science from Penn State, he was a postdoc at The Weizmann Institute of Science, and held research positions at IBM T.J. Watson Research Center, Bell Labs and AT&T Labs – Research. His research interests include both foundational and applied aspects of cryptography and information security. Dr. Garay has published extensively in the areas of cryptography, network security, distributed computing, and algorithms; has been involved in the design, analysis and implementation of a variety of secure systems; and is the recipient of over two dozen patents. He has served on the program committees of numerous conferences and international panels—including co-chairing Crypto 2013 and 2014, the discipline's premier conference.

Host: Division of Mathematical Sciences, School of Physical and Mathematical Sciences

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES
DIVISION OF MATHEMATICAL SCIENCES
SPMS-MAS-03-01, 21 NANYANG LINK, SINGAPORE 637371
TEL: +65 6513 7470