NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Is Bitcoin Stable, Secure, and Scalable?**

Speaker: Professor Roger Wattenhofer
Information Technology and Electrical Engineering Department,
ETH Zurich, Switzerland

Date/Time: 4 December 2015, Friday, 03:00 PM to 04:30 PM

Venue: Seminar Room @ LT19
COM2, Level 1

Chaired by: Dr Gilbert, Seth Lewis, Dean's Chair Assistant Professor, School of
Computing
(gilbert@comp.nus.edu.sg)

Registration: https://goo.gl/Lk8NmX

Refreshment provided; Limited seats: 40 pax; First come first serve

Abstract:

I will first give a short introduction to the Bitcoin system, explaining some of the basics such as transactions and the block chain. Then, I will discuss some interesting technical aspects in more detail, regarding the stability, security, and scalability of Bitcoin. Regarding stability, I will discuss Bitcoin's eventual consistency, and the related problem of double spending. Regarding security, I will shed some light into our findings regarding the bankruptcy of MtGox, previously the dominant Bitcoin exchange service. Finally, I will discuss scalability, and present duplex micropayment channels. Apart from scalability, these channels also guarantee end-to-end security and instant transfers, laying the foundation of a network of payment service providers.

Biodata:

Roger Wattenhofer is a full professor at the Information Technology and Electrical Engineering Department, ETH Zurich, Switzerland. He received his doctorate in Computer Science in 1998 from ETH Zurich. From 1999 to 2001 he was in the USA, first at Brown University in Providence, RI, then at Microsoft Research in Redmond, WA. He then returned to ETH Zurich, originally as an assistant professor at the Computer Science

Department.

Roger Wattenhofer's research interests are a variety of algorithmic and systems aspects in computer science and information technology, currently in particular wireless networks, wide area networks, mobile systems, social networks, and physical algorithms. He publishes in different communities: distributed computing (e.g., PODC, SPAA, DISC), networking (e.g., SIGCOMM, MobiCom, SenSys), or theory (e.g., STOC, FOCS, SODA, ICALP).

About Advanced Systems Seminar (ASS):

ASS is a new seminar series comprising of prominent researchers working in systems areas. It's a low-volume seminar series, with about 1 talk per month, and will overlap with important school talks (e.g. faculty candidate talks). We will have a mix of folks from industry and academia, on topics of emerging interests. The series is open to all invitees and School of Computing - NUS members. All graduate students working in systems, PL/ SE, networking, security, OS, architecture, databases and allied areas are strongly encouraged to attend these talks and converse with the speakers.