DIPARTIMENTO
DI INFORMATICA
SAPIENZA
UNIVERSITÀ DI ROMA

DISTINGUISHED LECTURE

Lecturer: Prof. Lorenzo Alvisi
(Cornell University)
Title: Order! A tale of money, intrigue, and specifications
Location: Aula Alfa (Via Salaria 113)
Date: December 2, 2021
Time: 16.00-17.00 (CET)

Abstract: Mistrust over traditional financial institutions is motivating the development of decentralized financial infrastructures based on blockchains. In particular, Consortium blockchains (such as the Linux Foundation Hyperledger and Facebook's diem) are emerging as the approach preferred by businesses. These systems allow only a well-known set of mutually distrustful parties to add blocks to the blockchain; in this way, they aim to retain the benefits of decentralization without embracing the cyberpunk philosophy that informed Nakamoto's disruptive vision.

At the core of consortium blockchains is State Machine Replication, a classic technique borrowed from fault tolerant distributed computing; to ensure the robustness of their infrastructure, consortium blockchains actually borrow the Byzantine-tolerant version of this technique, which guarantees that the blockchain will operate correctly even if as many as about a third of the contributing

parties are bent on cheating. But, sometimes, "a borrowing is a sorrowing".

I will discuss why Byzantine-tolerant state machine replication is fundamentally incapable of recognizing, never mind preventing, an ever present scourge of financial exchanges: the fraudulent manipulation of the order in which transactions are processed - and how its specification needs to be expanded to give it a fighting chance.

But is it possible to completely eliminate the ability of Byzantine parties to engage in order manipulation? What meaningful ordering guarantees can be enforced? And at what cost?