6.892

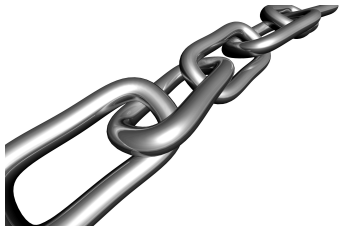
Shared Public Ledgers

Cryptocurrencies, Blockchains, and Other Marvels

Instructors: Silvio Micali and Neha Narula

Time: F 1-4

Room: 36-155



WHAT A *public ledger* is a tamperproof sequence of data that can be read and augmented by *everyone*. Shared public ledgers stand to revolutionize the way a democratic society operates. They secure all kinds of traditional transactions –such as payments, asset transfers, titling– in the exact order in which they occur; and enable totally new transactions ---such as cryptocurrencies and smart contracts. They can remove intermediaries and usher in a new paradigm for trust. As currently implemented, however, public ledgers cannot achieve their enormous potential.

HOW After describing current implementations, the course will provide new ideas and techniques for building public ledgers that are provably correct and scalable.

TOPICS Bitcoin and other cryptocurrencies, Lightning Networks, Byzantine agreement, Authenticated datastructures, Other (self-contained) cryptographic tools.

FORMAT The course will be run in seminar style with occasional guest lecturers.

REQUIREMENTS 6.033 and 6.046 (or “absolution” from the instructors)

NOTE Limited number: Register Now! ☺