HACETTEPE ÜNİVERSİTESİ

MATEMATİK BÖLÜMÜ

GENEL SEMİNER

6 KASIM 2025

15.00

YAŞAR ATAMAN SALONU

Murat Osmanoğlu

Ankara Üniversitesi, Bilgisayar Mühendisliği Bölümü, Türkiye

Exploring Proof-of-Stake Based Consensus Mechanisms Through the Ouroboros Protocol

This presentation examines the transition from Proof-of-Work (PoW)-based to Proof-of-Stake (PoS)–based consensus mechanisms, addressing the fundamental limitations of PoW-based systems such as excessive energy consumption. PoS-based protocols offer an energy-efficient alternative by assigning block creation rights proportionally to participants' stake, rather than their computational power. Within this paradigm, Ouroboros stands out as the first provably secure Proof-of-Stake blockchain protocol that provides formal guarantees of persistence and liveness. The talk will outline how Ouroboros introduces a mathematically rigorous framework for stake-based leader election, mitigates vulnerabilities like grinding attacks, and incorporates an incentive-compatible reward structure proven to approximate Nash equilibrium behavior.

mat.hacettepe.edu.tr