PURDUE UNIVERSITY | Elmore Family School of Electrical and Computer Engineering

# *Permissionless Blockchains: Fundamental Trade-offs in Throughput, Latency, and Safety*

Dongning Guo
Northwestern University

Monday, August 26, 2024
11:00 AM • MSEE 112

**Abstract**
Blockchain technology has revolutionized the concept of digital trust, facilitating secure peer-to-peer transactions without the need for a central authority. However, questions remain about the security and speed of these transactions. In this talk, we will explain the basic mechanics of the Nakamoto consensus protocol for permissionless blockchains, which relies on the longest-chain fork choice rule. We will examine the challenges of reaching consensus in the presence of adversarial miners and network delays. We will build a minimal mathematical model from scratch and analyze the safety of a transaction as a function of its depth in the longest chain, the rates of honest and adversarial mining, and a network delay parameter. Assuming proof-of-work mining, the results will be presented as a pair of closed-form "finite-blocklength" achievability and converse theorems. We will discuss the implications of these findings, focusing on the key trade-off between transaction throughput, confirmation latency, and safety in permissionless blockchains.

**Bio**
Dongning Guo received his Ph.D. degree in Electrical Engineering from Princeton University in 2004. He then joined the faculty of Northwestern University, Evanston, IL, where he is currently a Professor in the Department of Electrical and Computer Engineering and, by courtesy, a Professor of Computer Science. He was an R&D Engineer at the Center for Wireless Communications in Singapore from 1998 to 1999. He has served as Associate Editor of IEEE Transactions on Information Theory and IEEE Transactions on Wireless Communications, Editor of Foundations and Trends in Communications and Information Theory, and Guest Editor for the IEEE Journal on Selected Areas in Communications. He received the National Science Foundation CAREER Award in 2007, the IEEE Marconi Prize Paper Award in Wireless Communications in 2010, the Best Paper Award at the IEEE Wireless Communications and Networking Conference in 2017, and the 2023 Bitcoin Research Prize. He also lead teams that reached the final matches of the DARPA Spectrum Challenges in both 2014 and 2019. He was elected Fellow of IEEE in 2020. His research interests include blockchain and decentralization, information theory, machine learning, and wireless networks.

**Host**
Professor Husheng Li, husheng@purdue.edu