Introduction 4

Jonathan Katz, Google / University of Maryland

Abstract:
In this lecture, I will introduce SNARKs – succinct, non-interactive arguments – and briefly discuss why they have generated so much excitement in the blockchain world. I will then cover two useful building blocks for SNARKs: the classical sum-check protocol (which can also be used to show IP=PSPACE) and the Goldwasser-Kalai-Rothblum protocol (Journal of the ACM 2015).

Biography:
Jonathan Katz is currently a Senior Staff Research Scientist at Google while on leave from the University of Maryland, where he is a Professor in the Department of Computer Science. He is a co-author of the widely used textbook “Introduction to Modern Cryptography,” now in its third edition. Katz has received numerous awards, including an Alexander von Humboldt Research Award, a UMD Distinguished Scholar-Teacher Award, and an ACM SIGSAC Outstanding Contribution Award. He is a fellow of the IACR and the ACM.