1154-68-2613 **Swanand Kadhe*** (swanand.kadhe@berkeley.edu) and **Kannan Ramchandran** (kannanr@berkeley.edu). *How can a coding theorist make blockchains more efficient and scalable?*

In this talk, we will highlight how coding theory can play an instrumental role in addressing some of the fundamental challenges in the emerging field of blockchains, and in turn, demonstrate how blockchains open up novel code design problems. In the first half, we will focus on blockchain storage requirements that are growing near-exponentially. We will describe a 'Secure Fountain (SeF)' architecture, based on fountain codes, that enables users to encode blocks into a small number of coded blocks, thereby reducing storage costs by orders of magnitude. We demonstrate that the peeling decoder admitted by fountain codes turns out to be crucial for security against adversarial users that can provide maliciously formed coded blocks. Specifically, it enables us to introduce error-resiliency by leveraging the hash-chain structure of the blockchain. Further, the rateless property of fountain codes helps in achieving high decentralization and scalability. In the second half, we describe how codes can be used to mitigate data withholding attacks in blockchains. We analyze the requirements that a code must satisfy to ensure high availability guarantees, and demonstrate that generalized low density parity check (GLDPC) codes are excellent candidates. (Received September 17, 2019)