Abstract:
What gives a currency value? Do banks play an inalienable role in transaction settlement? Must governments be associated with the fate of a viable currency? Is digital commerce consistent with privacy? Do we need a judicial branch of government to interpret and enforce financial contracts? And...who can you trust?

In this talk, we will not answer any of these questions. However, we will describe a technical framework for maintaining financial ledgers that has upended classical thinking about these fundamental questions. We will describe Bitcoin, explain some of its features and shortcomings, and survey recent techniques for developing improved ledgers.