On the Viability of Open-Source Financial Rails: Economic Security of Permissionless Consensus (Joint with Rafael Pass and Elaine Shi)

Abstract:

Bitcoin showed that an open-source financial rail is possible—one where interchangeable service providers can join or leave at will. The key question, however, is whether the permissionless consensus technology that makes this possible can also meet the security standards needed for mainstream financial applications. We develop a model that integrates economic and distributed-systems constraints, define the objectives of free entry and security, and examine their joint attainability. We demonstrate the feasibility of an open and secure protocol by presenting a protocol that attains an economically meaningful notion of security while preserving Bitcoin's permissionless design. Our protocol's security does not require costly miner rewards or high energy consumption. The analysis formalizes the essential role of the user community in sustaining secure and efficient open financial rails.