DISSERTATION PROPOSAL

Zahra Ebrahimi

"Essays in FinTech"

Friday, December 11, 2020
10:00am EST
Zoom: https://cmu.zoom.us/j/99242627651?pwd=dVJpcjV1elVTakM2ZllTT0N1cWIrQT09

In the first chapter, we develop a new, game-theoretic formulation of any blockchain where each user decides how to update a distributed ledger. Blockchains are useful only in so far as the updating strategies of users attain consensus - users agree on which version of the ledger is "correct" - and permanence - users do not have incentives to omit or modify past data. While currently-implemented strategies - longest chain rules - do not achieve consensus or permanence when users are sufficiently heterogeneous, we prove existence of new equilibrium strategies that attain both consensus and permanence for any degree of heterogeneity. In practice, these equilibrium strategies are robust to so-called 51% attacks. Our results shed light on the important role economic incentives play in determining the resilience of blockchain ledgers.

In the second chapter, I propose to study the systemic risk posed by cyber incidents to overall financial stability. Correlated cyber risk may arise through common financial market infrastructures and service providers, as well as common exposure to systematically important financial institutions. I model this interconnectedness as two graphs, one capturing the connections formed by banks through interbank borrowing and lending relationships, and the other, capturing the connections formed by banks through various infrastructures and service providers. I will study how a cyber incident involving a service provider with several bank clients can unfold in the financial network, potentially triggering a funding liquidity cascade. Taking the financial network as given, I aim to investigate the equilibrium as well as efficient set of connections that arises in this setting.

In the third chapter, I propose to estimate the losses incurred due to a cyber attack on financial institutions connected through service providers using data available on past cyber events to account for direct losses, and Fedwire data to account for losses due to contagion effects.