
# Aggelos Kiayias

akiayias@inf.ed.ac.uk
www.kiayias.com


# Scaling Bitcoin Securely

*Monday, May 30 2016, 11-12:30pm*

In this lecture we will present a framework for analyzing formally blockchain protocols against a fairly general class of adversaries. The framework is based on standard cryptographic models proposed in the context of secure multiparty computation appropriately modified to fit the setting of bitcoin where the mode of communication is anonymous unreliable broadcast. In this framework we will cast the basic properties of blockchain protocols, termed *persistence* and *liveness*. We will demonstrate how these properties interact with the synchronization assumption between nodes and we will explain how they address commonly considered attacks in practice such as double-spending and denial of service against transactions. We will then examine the problem of scaling these protocols with particular emphasis on transaction processing time. How fast can a blockchain grow before security breaks? How many blocks does one need to wait before a transaction is confirmed? We will provide a mathematical toolset for investigating such questions.

**Reading:**


- Juan Garay and Aggelos Kiayias and Nikos Leonardos, The Bitcoin Backbone Protocol: Analysis and Applications, Cryptology ePrint Archive: Report 2014/765, https://eprint.iacr.org/2014/765