Syllabus
BLOCKASTICS: Stochastic models for blockchain analysis
Pierre-O Goffard

Course Overview

Blockchain technology emerged in 2008 as the foundational technology behind Bitcoin. Since then, it has evolved significantly, with numerous blockchain systems proposed for applications beyond cryptocurrencies. This course explores the intersection of stochastic models and blockchain systems, offering insights into the analysis and understanding of these complex decentralized networks.

Part 1: Blockchain concepts and consensus protocols
A blockchain is a distributed data ledger maintained through consensus among multiple nodes in a peer-to-peer network. Following an overview of foundational definitions and real-world applications of blockchain (like Decentralized finance) we delve into the core consensus protocols that underpin blockchain systems. Additionally, we outline three key evaluation dimensions for blockchain systems: security, decentralization, and efficiency.

Part 2: Security of blockchain systems
We review mathematical models and tools employed to assess the security of blockchain systems. Specifically, we focus on security concerns associated with the proof-of-work protocol, such as double spending. Our analysis utilizes standard models from applied probability literature, including random walks, Markov chains, and Poisson processes.

Part 3: Decentralization of blockchain systems
Decentralization measures the fairness of decision-making power distribution among peers in a blockchain network. In this section, we will examine the decentralization of proof-of-stake blockchain systems using an urn model. Additionally, we will analyze proof-of-work blockchain decentralization by applying insurance risk theory to study the formation of mining pools.

Part 4: Efficiency of blockchain systems
Efficiency refers to the capacity of a blockchain system to process data within a given time frame. In this section, we introduce a general queuing model to quantify throughputs (the number of transactions processed per time unit) and latency (the time taken for a transaction to transition from the pending state to confirmed).

Part 5: Crypto-currency returns cycles using Hidden Markov Model
The cryptocurrency market, akin to real-world assets, exhibits cyclic behaviors known as bear and bull cycles. A prevalent approach to studying these cycles involves assuming that the distribution of log returns depends on the current state of an unobservable Markov chain. In this section, we explore a simple model where log returns follow a Gaussian distribution, and we employ Bayesian algorithms to infer parameters using Bitcoin data.

Prerequisites:

- Basic knowledge on stochastic processes such as random walk, Poisson processes and Markov

chains (Some reminders will be provided during the lectures)

- The proofs will use standard combinatorial analysis, Martingale techniques and first step analysis. (Some reminders will be provided during the lectures)
- Basic knowledge of coding in Python. We will use Python to do Monte Carlo Simulations using native Python methods and bits of NumPy and SciPy. Examples and illustrations will be done using Python and Jupyter notebooks. My suggestion is to install Anaconda but one can also simply use Google Colab. Please bring your laptops!

EVALUATIONS:

You will be grouped in teams of 2-3 (depending on the number of attendees), and you will be required to deliver a presentation during the final lecture on a research paper related to the topic of blockchain mathematics. I will provide you with a selection of papers to choose from, or you may propose your own paper for approval. Your grade will be based on the quality of your oral presentation and the accompanying presentation materials (slides). The final lecture will take the form of an internal seminar.