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.

References

[1] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Performance Evaluation*, vol. 104, pp. 23–41, 2016.

[2] V. Buterin, "A next-generation smart contract and decentralized application platform," *https://github.com/ethereum/wiki/wiki/White-Paper*, 2014.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." Available at https://bitcoin.org/bitcoin.pdf, 2008.

[4] P.-O. Goffard, "Fraud risk assessment within blockchain transactions," *Advances in Applied Probability*, vol. 51, pp. 443–467, jun 2019. https://hal.archives-ouvertes.fr/hal-01716687v2.

[5] L. Schilling and H. Uhlig, "Some simple bitcoin economics," *Journal of Monetary Economics*, vol. 106, pp. 16–26, oct 2019.

[6] J. Pfeffer, "An (institutional) investor's take on cryptoassets," *Medium*, 2017.

[7] R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Modeling and analysis of block arrival times in the bitcoin blockchain," *Stochastic Models*, vol. 36, pp. 602–637, jul 2020.

[8] S. Asmussen and H. Albrecher, *Ruin Probabilities*. WORLD SCIENTIFIC, sep 2010.

[9] L. W. Cong, Z. He, and J. Li, "Decentralized mining in centralized pools," *The Review of Financial Studies*, vol. 34, pp. 1191–1235, apr 2020.

[10] L. W. Cong, Y. Li, and N. Wang, "Tokenomics: Dynamic adoption and valuation," *The Review of Financial Studies*, vol. 34, pp. 1105–1155, aug 2020.

[11] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Financial Cryptography and Data Security*, pp. 436–454, Springer Berlin Heidelberg, 2014.

[12] X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: mechanism, design and applications," *Science China Information Sciences*, vol. 64, nov 2020.

[13] S. P. Gochhayat, S. Shetty, R. Mukkamala, P. Foytik, G. A. Kamhoua, and L. Njilla, "Measuring decentrality in blockchain based systems," *IEEE Access*, vol. 8, pp. 178372–178390, 2020.

[14] Y. Kawase and S. Kasahara, "Transaction-confirmation time for bitcoin: A queueing analytical approach to blockchain mechanism," in *Queueing Theory and Network Applications*, pp. 75–88, Springer International Publishing, 2017.

[15] OECD, "The tokenisation of assets and potential implications for financial markets," tech. rep., 2020.

[16] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011.

[17] F. Saleh, "Blockchain without waste: Proof-of-stake," *The Review of Financial Studies*, vol. 34, pp. 1156–1190, jul 2020.

[18] I. Roşu and F. Saleh, "Evolution of shares in a proof-of-stake cryptocurrency," *Management Science*, vol. 67, pp. 661–672, feb 2021.

[19] Q.-L. Li, J.-Y. Ma, and Y.-X. Chang, "Blockchain queue theory," in *Computational Data and Social Networks*, pp. 25–40, Springer International Publishing, 2018.

[20] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "Sok: Decentralized finance (defi)," 2021.

[21] W. Liu, X. Liang, and G. Cui, "Common risk factors in the returns on cryptocurrencies," *Economic Modelling*, vol. 86, pp. 299–305, mar 2020.

[22] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *Financial Cryptography and Data Security*, pp. 477–498, Springer Berlin Heidelberg, 2017.

[23] M. Chaudhry and J. Templeton, "The queuing system m/GB/l and its ramifications," *European Journal of Operational Research*, vol. 6, pp. 56–60, jan 1981.

[24] N. T. J. Bailey, "On queueing processes with bulk service," *Journal of the Royal Statistical Society: Series B (Methodological)*, vol. 16, pp. 80–87, jan 1954.

[25] D. R. Cox, "The analysis of non-markovian stochastic processes by the inclusion of supplementary variables," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 51, pp. 433–441, jul 1955.

[26] M. Rosenfeld, "Analysis of hashrate-based double spending," *arXiv preprint arXiv:1402.2009*, 2014.

[27] D. Blackwell and J. B. MacQueen, "Ferguson distributions via polya urn schemes," *The Annals of Statistics*, vol. 1, mar 1973.

[28] J. Lansky, "Possible state approaches to cryptocurrencies," *Journal of Systems Integration*, vol. 9, pp. 19–31, jan 2018.

[29] J. Hargrave, N. Sahdev, and O. Feldmeier, "How value is created in tokenized assets," in *Blockchain Economics: Implications of Distributed Ledgers*, pp. 125–143, WORLD SCIENTIFIC (EUROPE), jan 2019.

[30] W. J. Baumol, "The transactions demand for cash: An inventory theoretic approach," *The Quarterly Journal of Economics*, vol. 66, p. 545, nov 1952.

[31] J. R. Gan, G. Tsoukalas, and S. Netessine, "Initial coin offerings, speculation, and asset tokenization," *Management Science*, vol. 67, pp. 914–931, feb 2021.

[32] slush pool, "Reward system specifications," 2021.

[33] C. Bertucci, L. Bertucci, J.-M. Lasry, and P.-L. Lions, "Mean field game approach to bitcoin mining," 2020.

[34] H. Alsabah and A. Capponi, "Bitcoin mining arms race: R&d with spillovers," *SSRN Electronic Journal*, 2018.

[35] Z. Li, A. M. Reppen, and R. Sircar, "A mean field games model for cryptocurrency mining," 2019.

[36] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Financial Cryptography and Data Security*, pp. 515–532, Springer Berlin Heidelberg, 2017.

[37] C. Grunspan and R. Pérez-Marco, "ON PROFITABILITY OF NAKAMOTO DOUBLE SPEND," *Probability in the Engineering and Informational Sciences*, pp. 1–15, feb 2021.

[38] J. Jang and H.-N. Lee, "Profitable double-spending attacks," *Applied Sciences*, vol. 10, p. 8477, nov 2020.

[39] M. Brown, E. Peköz, and S. Ross, "BLOCKCHAIN DOUBLE-SPEND ATTACK DURATION," *Probability in the Engineering and Informational Sciences*, pp. 1–9, may 2020.

[40] C. GRUNSPAN and R. PÉREZ-MARCO, "DOUBLE SPEND RACES," *International Journal of Theoretical and Applied Finance*, vol. 21, p. 1850053, dec 2018.

[41] C. Grunspan and R. Pérez-Marco, "On profitability of selfish mining," 2019.

[42] J. Göbel, H. Keeler, A. Krzesinski, and P. Taylor, "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Performance Evaluation*, vol. 104, pp. 23–41, oct 2016.

[43] J. D. C. Little, "A proof for the queuing formula:L= λW," *Operations Research*, vol. 9, pp. 383–387, jun 1961.

[44] Q.-L. Li, J.-Y. Ma, Y.-X. Chang, F.-Q. Ma, and H.-B. Yu, "Markov processes in blockchain systems," *Computational Social Networks*, vol. 6, jul 2019.

[45] Y. Kawase, , and S. Kasahara, "Priority queueing analysis of transaction-confirmation time for bitcoin," *Journal of Industrial & Management Optimization*, vol. 16, no. 3, pp. 1077–1098, 2020.

[46] H. L. Smith, *An introduction to delay differential equations with applications to the life sciences.* Springer, New York, 2011.

[47] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, pp. 382–401, July 1982.

[48] J.-P. Abegg, Q. Bramas, and T. Noël, "Blockchain using proof-of-interaction," in *Networked Systems*, pp. 129–143, Springer International Publishing, 2021.

[49] E. Anceaume, A. Guellier, R. Ludinard, and B. Sericola, "Sycomore: A permissionless distributed ledger that self-adapts to transactions demand," in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, IEEE, nov 2018.

[50] B. Biais, C. Bisière, M. Bouvard, and C. Casamatta, "The blockchain folk theorem," *The Review of Financial Studies*, vol. 32, pp. 1662–1715, apr 2019.

[51] J. Xu, N. Vavryk, K. Paruch, and S. Cousaert, "Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols," 2021.

[52] P. Labs, "Filecoin: A decentralized storage network," *White paper*, 2017. https://filecoin.io/filecoin.pdf.

[53] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, (USA), p. 173–186, USENIX Association, 1999.

[54] S. Al-Kuwari, J. H. Davenport, and R. J. Bradford, "Cryptographic hash functions: Recent design trends and security notions." Cryptology ePrint Archive, Report 2011/565, 2011. https://ia.cr/2011/565.

[55] A. Antonopoulos, *Mastering Bitcoin*. O'Reilly UK Ltd., July 2017.

[56] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *whitepaper*, 2012.

[57] R. van der Hofstad and M. Keane, "An elementary proof of the hitting time theorem," *The American Mathematical Monthly*, vol. 115, pp. 753–756, oct 2008.

[58] M. Renault, "Four proofs of the ballot theorem," *Mathematics Magazine*, vol. 80, pp. 345–352, dec 2007.

[59] L. Takács, "A generalization of the ballot problem and its application in the theory of queues," *Journal of the American Statistical Association*, vol. 57, pp. 327–337, jun 1962.

[60] C. Lefèvre and P. Picard, "A new look at the homogeneous risk model," *Insurance: Mathematics and Economics*, vol. 49, pp. 512–519, nov 2011.

[61] B. Q. Ta, "Probabilistic approach to appell polynomials," *Expositiones Mathematicae*, vol. 33, no. 3, pp. 269–294, 2015.

[62] P.-O. Goffard and C. Lefèvre, "Duality in ruin problems for ordered risk models," *Insurance: Mathematics and Economics*, vol. 78, pp. 44–52, jan 2018.

[63] B. Avanzi, H. U. Gerber, and E. S. Shiu, "Optimal dividends in the dual model," *Insurance: Mathematics and Economics*, vol. 41, pp. 111–123, jul 2007.

[64] P.-O. Goffard and C. Lefèvre, "Boundary crossing of order statistics point processes," *Journal of Mathematical Analysis and Applications*, vol. 447, pp. 890–907, mar 2017.

[65] H. Albrecher and P.-O. Goffard, "On the profitability of selfish blockchain mining under consideration of ruin," *Operations Research*, vol. 70, pp. 179–200, jan 2022.

[66] J. F. C. Kingman, *Poisson Processes*. OXFORD UNIV PR, Jan. 1993.

[67] H. Albrecher, D. Finger, and P.-O. Goffard, "Blockchain mining in pools: Analyzing the trade-off between profitability and ruin," *Insurance: Mathematics and Economics*, vol. 105, pp. 313–335, jul 2022.

[68] G. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang, "Compounding of wealth in proof-of-stake cryptocurrencies," in *Financial Cryptography and Data Security*, pp. 42–61, Springer International Publishing, 2019.

[69] P.-O. Goffard, S. Loisel, and D. Pommeret, "Polynomial approximations for bivariate aggregate claims amount probability distributions," *Methodology and Computing in Applied Probability*, vol. 19, pp. 151–174, nov 2015.

[70] P.-O. Goffard, S. Loisel, and D. Pommeret, "A polynomial expansion to approximate the ultimate ruin probability in the compound poisson ruin model," *Journal of Computational and Applied Mathematics*, vol. 296, pp. 499–511, apr 2016.

[71] S. Asmussen, P.-O. Goffard, and P. J. Laub, "Orthonormal polynomial expansions and lognormal sum densities," in *Risk and Stochastics*, pp. 127–150, WORLD SCIENTIFIC (EUROPE), apr 2019.

[72] P.-O. Goffard and P. J. Laub, "Orthogonal polynomial expansions to evaluate stop-loss premiums," *Journal of Computational and Applied Mathematics*, vol. 370, p. 112648, may 2020.

[73] K. Barigou, P.-O. Goffard, S. Loisel, and Y. Salhi, "Bayesian model averaging for mortality forecasting using leave-future-out validation," *International Journal of Forecasting*, mar 2022.

[74] P.-O. Goffard, "Two-sided exit problems in the ordered risk model," *Methodology and Computing in Applied Probability*, vol. 21, pp. 539–549, nov 2017.

[75] P.-O. Goffard and P. J. Laub, "Approximate bayesian computations to fit and compare insurance loss models," *Insurance: Mathematics and Economics*, vol. 100, pp. 350–371, sep 2021.

[76] M. Levine, "The crypto story." Bloomberg business week, Oct. 2022. https://www.bloomberg.com/features/2022-the-crypto-story/?leadSource=uverify%20wall.

[77] A. Lipton and A. Treccani, *Blockchain and Distributed Ledgers*. WORLD SCIENTIFIC, apr 2021.

[78] A. Dembo, S. Kannan, E. N. Tas, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni, "Everything is a race and nakamoto always wins," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ACM, oct 2020.

[79] E. Bayraktar, A. E. Kyprianou, and K. Yamazaki, "ON OPTIMAL DIVIDENDS IN THE DUAL MODEL," *ASTIN Bulletin*, vol. 43, pp. 359–372, jul 2013.

[80] F. Avram, Z. Palmowski, and M. R. Pistorius, "On the optimal dividend problem for a spectrally negative lévy process," *https://doi.org/10.1111/j.1467-9868.2009.00736.x*, vol. 17, feb 2007.

[81] F. Avram, A. Horváth, S. Provost, and U. Solon, "On the padé and laguerre–tricomi–weeks moments based approximations of the scale function w and of the optimal dividends barrier for spectrally negative lévy risk processes," *Risks*, vol. 7, p. 121, dec 2019.

[82] C. Andrieu, A. Doucet, and R. Holenstein, "Particle markov chain monte carlo methods," *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, vol. 72, pp. 269–342, jun 2010.

[83] P.-O. Goffard, "Sequential monte carlo samplers to fit and compare insurance loss models," *Scandinavian Actuarial Journal*, pp. 1–23, nov 2022.