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

In 2008, Blockchain was introduced to the world as the underlying technology of the Bitcoin electronic cash system. After more than a decade of development, various blockchain systems have been proposed with application going beyond the creation of a cryptocurrency. This course is organized around four chapters on the theme of stochastic models in relation to the analysis of blockchain systems.

Part 1: Blockchain concepts and consensus protocols
A blockchain is a distributed data ledger maintained by achieving consensus among a number of nodes in peer-to-peer network. After providing some preliminary definitions and discussing some real world applications of blockchain, we introduce the various consensus protocols at the core of blockchain systems. We further define three dimensions according to which a blockchain system must be evaluated including (1) security, (2) decentralization and (3) efficiency.

Part 2: Security of blockchain systems
A review of the mathematical models and tools used so far to assess the security of blockchains systems. We address here security issues linnked to the *proof-of-work* protocol, including double spending and selfish mining. the performance of blockchain systems is provided. They consist of standard models from the applied probability literature like random walks, Markov chains, urns and queues.

Part 3: Decentralization of blockchain systems
Decentralization measures the fairness of the decision power distribution among the blockchain network peers. We are going to study the decentralization of *proof-of-stake* based blockchain via stochastic processes with reinforcement and of *proof-of-work* based blockchain with the formation of mining pool.

Part 4: Efficiency of blockchain systems
Efficiency is the amount of data that a blockchain systems can processed per time unit. A general queueing model is introduced to provide numerical indicators of throughputs (the number of transactions being processsed per time unit) and latency (the time it takes for a transaction to go from the state pending to confirmed).

Prerequisites:

- Basic knowledge on stochastic processses 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. (Once again some reminders will be provided during the lessons)
- Basic knowledge of coding in python. We will use Python to do Monte Carlo Simulations using native python methods and bit 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 uses Google collab. Please bring your laptops!

Evaluations:
You will be gathered in groups of 2-3 and you will have to give a presentation (during the very last lecture) on a research paper in relation to the topic of blockchain mathematics. I will give you some papers to choose from. You may also find your own paper and I will let you know whether it is adequate. The grade will be based on the quality of the oral presentation and the presentation support (the slides).

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] H. Albrecher and P.-O. Goffard, "On the profitability of selfish blockchain mining under consideration of ruin," *To appear in Operations Research*, May 2021. https://arxiv.org/abs/2010.12577.

[5] 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.

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

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

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

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

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

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

[20] 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.

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

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

[23] 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.

[24] 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.

[25] 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.

[26] 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.

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

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

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

[30] 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.

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

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

[33] H. Albrecher, D. Finger, and P.-O. Goffard, “Blockchain mining in pools: Analyzing the trade-off between profitability and ruin,” 2021. https://arxiv.org/abs/2109.03085.

[34] slush pool, “Reward system specifications,” 2021.

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

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

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

[38] 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.

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

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

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

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

[43] C. Grunspan and R. Pérez-Marco, “On profitability of selfish mining,” 2019.

[44] 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.

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

[46] 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.

[47] 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.