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 45 minutes lectures on the topic of stochastic models in relation to the analysis of blockchain systems.

Part 1: Blockchain concepts
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, we introduce the *proof-of-work* and *proof-of-stake* consensus protocols which are at the core of public and permissionless blochchains (like the bitcoin and ethereum ones). We further define three dimensions according to which a blockchain system may be evaluated including (1) efficiency, (2) decentralization and (3) security.

Part 2: Simple models for blockchain performance analysis
A review of the mathematical models and tools used so far to assess 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: Risk models and blockchain mining
Mining blocks on a blockchain equipped with a proof of work consensus protocol is well-known to be resource-consuming. A miner bears the operational cost, mainly electricity consumption and IT gear, of mining, and is compensated by a capital gain when a block is discovered. The profitability of mining is studied via stochastic model and tools borrowed from insurance risk theory. We consider the case of solo mining, pool mining and selfish mining.

Part 4: Decentralized finance and cryptoasset pricing
Blockchain creates an environment where multiple parties can interact directly and transparently. It is therefore immediately relevant to banks and financial institutions which incur huge middlemen costs in settlements and other back office operations. Decentralized finance (DeFi) offers a new financial architecture that is non-custodial, permissionless, openly auditable, pseudo-anonymous and with potential new capital efficiencies. An overview of the existing cryptoasset is provided and model to value such assets are discussed.

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." working paper or preprint, https://hal.archives-ouvertes.fr/hal-02649025, May 2020.

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

[24] 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.