BLOCKCHAIN AND CRYPTOCURRENCIES

Instructors: *Dean Fantazzini and Rostislav Berezovsky*

Syllabus

1. Course Description

a. **Pre-requisites:** We assume that the students have a background in statistics and econometrics. An introduction to the basic concepts of financial modelling will be provided.

b. **Abstract:** The course studies the basics of decentralized financial protocols which are one of the fastest growing and innovative topics in modern finance. The goal of this course is to introduce the main concepts related to blockchains and cryptocurrencies. It includes a deep dive into blockchain technology underlying Bitcoin and Ethereum networks, scalability solutions, network consensus mechanics, encryption basics. Special focus is made on the architecture and models of decentralized exchanges, borrowing and lending protocols, stablecoins and prediction markets solutions. The course wants to bridge the gap between theory and practice and the applied aspects of financial models are emphasized throughout the course. The practical part contains many real-world cases using the R software.

2. Program of the course

a. Blockchain technology: blocks, addresses, transactions, consensus algorithm

b. Ethereum: decentralized virtual machine architecture, scalability

c. Consensus protocols: results about different consensus algorithms, most widespread models comparison

d. Confidentiality in blockchain: symmetric and asymmetric encryption, elliptic curves, zero knowledge proofs

e. DeFi: key decentralized financial primitives, models of automatic market makers and lending protocols

f. Financial modelling of Bitcoin and other cryptocurrencies using R

g. Credit Risk Management for cryptocurrencies and examples with R

3. Learning Objectives & Outcomes

At the conclusion of the course, students should have:

- Understanding of blockchain technology basics, application of blockchain to digital transformation of the financial industry, and relevant research directions in the field.
- Capability of self-development of new research methods, changing the scientific and production profile of activities.
- Ability to use modern information technologies and software in professional activities, to set tasks for specialists in the development of R software for solving professional problems.

4. Methods of Instruction

Lectures: 26 hours. 18 (Rostislav Berezovsky), + 8 (Dean Fantazzini)

5. Reading List

a. Required:

- Lecture slides (provided in advance before the lecture)
- Antonopoulos, Andreas M. (2014). Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O'Reilly Media, Inc, ISBN:978-1-4493-7404-4
- Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.
- Fantazzini, D. (2019), *Quantitative Finance with R and Cryptocurrencies*. Amazon KDP, ISBN-13 978-1090685315
- Würtz, D., Lam, L., Ellis, A., Chalabi, Y. (2010). *Basic R for Finance*. Finance Online Publishing.

b. Optional: see the references below for each specific topic.

6. Special Equipment and Software Support (if required)

• Equipment: computer, Internet connection (the lectures will take place online using Zoom)
• Software needed: R, RStudio (last version!)

7. Grading System and Examination Type[1]

- The final grade will be based on a home assignment.
- The home assignment contains two parts:
    - blockchain theory assignment (50% of the final grade)
    - financial modelling assignment (50% of the final grade)

8. Teaching Language: Russian/English

9. Timetable: Lectures: February-April 2022.

[1] Sample materials for knowledge assessment are available in ICEF Information system at https://icef-info.hse.ru.

Course Outline – Rostislav Berezovsky

1. Blockchain technology [2 hours]

1.1 DLT, public and private blockchains

1.2 How Bitcoin works: address, transaction, node, consensus, forks, script language

References

- Antonopoulos, Andreas M. (2014). Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O'Reilly Media, Inc, ISBN:978-1-4493-7404-4
- Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com

2. Ethereum [4 hours]

2.1 Ethereum 1.0 network architecture and EVM

2.2 Blockchain scalability 1st nd 2nd layer solutions: sharding, state channels, sidechains, roll-ups, DAGs, BDN

2.3 Ethereum 2.0 current development

References

- Antonopoulos, A. M., & Wood, G. (2018). Mastering Ethereum: building smart contracts and dapps. O'reilly Media Inc, ISBN: 978-1-4919-7194-9
- Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32.
- Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020, February). SoK: Layer-two blockchain protocols. In International Conference on Financial Cryptography and Data Security (pp. 201-226). Springer, Cham.

3. Consensus protocols [2 hours]

3.1 Raft, Paxos, dBFT, pBFT, fBFT, PoS, DPoS, LPoS, PoA

3.2 Vulnerabilities in consensus: double spending, selfish mining, long range attacks, nothing at stake

References

- Antonopoulos, Andreas M. (2014). Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O'Reilly Media, Inc, ISBN:978-1-4493-7404-4
- Castro, M., & Liskov, B. (1999, February). Practical byzantine fault tolerance. In OSDI (Vol. 99, No. 1999, pp. 173-186).
- Hinz, J. (2020). Resilience Analysis for Double Spending via Sequential Decision

Optimization. Applied System Innovation, 3(1), 7.

4. Confidentiality in blockchain [2 hours]

4.1 Zero knowledge proof

4.2 zk-SNARK, zk-STARK, Bulletproof

References

- Rafael Pass, Abhi Shelat (2008) A course in cryptography. Lecture notes, Cornell https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf
- Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: Decentralized anonymous payments from bitcoin. In 2014 IEEE Symposium on Security and Privacy (pp. 459-474). IEEE.
- Zcash knowledge base, https://z.cash/technology/

5. Decentralized Finance: design and examples [8 hours]

5.1 Lending and borrowing, interest rate models

5.2 Decentralized oracles, synthetic assets, and prediction markets

5.3 Stablecoins: pegged assets, crypto backed assets, algorithmic stablecoins

5.4 Decentralized exchanges: CMFFs, IL, concentrated liquidity, stableswap

5.5 DeFi vulnerabilities and attacks, flash loans

References

- Darren Lau, Daryl Lau, Sze Jin Teh, Kristian Kho, Erina Azmi, TM Lee, Bobby Ong (2020) How to DeFi. CoinGecko, ISBN 979-8-6405-7910-9
- Klages-Mundt, A., & Minca, A. (2019). (In) Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks. arXiv preprint arXiv:1906.02152
- Evans, A. (2020). Liquidity provider returns in geometric mean markets. arXiv preprint arXiv:2006.08806
- Adams, H., Zinsmeister, N., & Robinson, D. (2020). Uniswap v2 core. URl: https://uniswap. org/whitepaper. pdf.
- Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2021). Uniswap v3 core. Tech. rep., Uniswap.
- Evans, A., Angeris, G., & Chitra, T. (2021). Optimal fees for geometric mean market makers. arXiv preprint arXiv:2104.00446.
- Angeris, G., Evans, A., & Chitra, T. (2021). Replicating Market Makers. arXiv preprint arXiv:2103.14769.
- Angeris, G., Agrawal, A., Evans, A., Chitra, T., & Boyd, S. (2021). Constant function market makers: Multi-asset trades via convex optimization. arXiv preprint arXiv:2107.12484.
- Evans, A. (2020). Liquidity provider returns in geometric mean markets. arXiv preprint arXiv:2006.08806.

Course Outline - Dean FANTAZZINI

1. Financial modelling of Bitcoin and other cryptocurrencies using R [4 hours]

1.1 Where to get (free) Bitcoin and cryptocurrencies data?

1.2 What is bitcoin's fundamental value? A review of financial and economic approaches

1.3 Modelling bitcoin price dynamics (VAR/VEC/BVAR/VAR-lasso)

References

- **Fantazzini, D. (2019) *Quantitative Finance with R and Cryptocurrencies*. Amazon KDP, ISBN-13 978-1090685315: chapters 2,4,7**. https://sites.google.com/view/quafirc
- McNeil, A., Frey, R., Embrechts, P., *Quantitative Risk Management: Concepts, Techniques, and Tools*, Princeton University Press, 2005: chapters 1-4.

2. Credit Risk Management for cryptocurrencies and examples with R [4 hours]

2.1 An introduction to classical credit risk management

2.2 Credit risk for Small and Medium-sized Enterprises (SMEs): the case of crypto-exchanges and crypto-currencies

2.3 Forecasting the Probability of Default (PD) of exchanges: Expert and credit rating systems

2.4 Forecasting the Probability of Default (PD) of exchanges: Credit Scoring Systems

2.5 Forecasting the Probability of Default (PD) of exchanges: Machine learning

2.6 Model Evaluation: ROC, AUC and Loss Functions (**time permitting*)

References

- **Fantazzini, D. (2019) *Quantitative Finance with R and Cryptocurrencies*. Amazon KDP, ISBN-13 978-1090685315: chapter 13**. https://sites.google.com/view/quafirc
- McNeil, A., Frey, R., Embrechts, P., *Quantitative Risk Management: Concepts, Techniques, and Tools*, Princeton University Press, 2005: chapter 8.