BLOCKCHAIN TECHNOLOGIES AND ITS APPLICATIONS TO CRYPTOCURRENCIES (APS 1050 H)

Important Notice:

Be advised that, due to the circumstances surrounding this edition of the course, ALL of the following administrative and academic guidelines are subject to adjustments and/or changes

Lectures:

Mondays / 3:00 PM to 6:00 PM / May 25 to Aug 24 / 2020.

Instructors:

Sabatino Costanzo & Loren Trigo

Office Hours:

Every week on the day of the class we'll be available 'live' during 6 hours answering questions in 'Piazza' (from noon time to 6:00 PM). We may open another channel (conversation-oriented technology still to be selected) for less technical and/or less formal questions. Private and/or administrative questions will be handled through a dedicated email that will be provided on the first day of class.

Communication:

- The class slides and the careful transcription of the instructor's detailed comments on the slides (as well as the corresponding optional voice-over) will be uploaded to Quercus on the day of the class, at the time the class starts
- Technical questions will be addressed via 'Piazza'.
- Administrative issues of a more private nature will be addressed via a dedicated email address that will be provided by the instructors during the first class.
- General administrative questions may be addressed via an interactive 'voice' technology, still to be selected.

References:

The main literature will be comprised by the lecture slides and the meticulous transcriptions of the accompanying explanatory comments made by the instructors during previous live editions of this course. If needed, these transcriptions can be 'listened-to' via the 'text-to-voice' option uploaded with the written course material. In short, there are no required textbooks for this course; the slides and the transcriptions of the slides' comments will suffice as such, and a bibliography will be provided.

Grading Scheme:

- Weekly Homeworks (Cumulative): 40%
- In-class Summary Exercises (Cumulative): 10%
- Final Project Deliverables: 50%

Homework:

- We will have homework assignments on most weeks.
- Homeworks will usually drill the techniques learned during the week in which the homework was assigned.
- You can work by yourself or as part of a team.
- Homeworks are very important because they give you the opportunity to apply the theory you've learned.

Teams:

We'll start the course with a survey that will allow us to build (and suggest to you) possible 'skill-balanced' teams, but you'll always have the option of working as an individual or coming-up with your own.

Attendance & In-Class Summary Exercises:

- We'll consider that you have "attended" the 'nth' class, as far as you can show that you have gone through the session corresponding to week 'n', and this is how you are expected to do it:
- We'll upload the 'nth session' of this course to Quercus on the day and at the time at which the session starts. Therefore, from that moment on you'll have available: (i) An extensive presentation of the topic planned for that week (ii) The transcripts of the comments we used to make in class on each one of the slides (iii) The option of activating a voice-over to read the explanatory text for you while you go through the slides making notes.
- As you go through the nth class (Slides & Text), once every few slides you'll be asked (in the text) to summarize in your own words (and to jot them down in word-pad or a similar text file), the main take away idea(s) presented so far and the main question(s) --if any-- that you may like to ask later in 'Piazza'.
- Once the class is over and you have completed the summary exercises corresponding to that class (each exercise should take about 10 minutes to complete), **you'll have until midnight of the next day** to upload them (all together in a single document or txt file) to Quercus.
- Uploading **all** of the summary exercises you did on that day 'on time' (**i.e., before midnight of the next day**), guarantees to us that: (i) You went through the whole class attentively (ii) You stopped, reflected and wrote down periodically your insights and your questions at the crucial moments of the class.
- Typically, there will be 3 to 5 of those summary exercises per class, and their total cumulative value will constitute 10% of your final grade.

- To make sure that everything goes smoothly on the day of the class, we'll be present, answering questions 'live' in 'Piazza', from noon to 6:00 PM.
- At a certain point we were considering teaching this class 'live' online in order to maximize its 'interactive nature', but after testing the technology available we felt that giving a 'recitation' lecture through an imperfect audio system, an often unstable connection and having as an illustration resource a lagging computer screen, could hardly become a positive interactive experience.
- So we thought that it would be much more effective (and efficient) to provide an exhaustive account of [the best content from our class slides] + [the notes of our explanations & comments about those slides, meticulously collected along many editions of this course], and make the package available to you (the slides, the comments and a voice-over of those comments), so that you could control the speed of the information flow--, while, at the same time, on the day of the class, we made ourselves available 'live' for 6 straight hours to give support and answer questions about the content.

Final Project:

- The Final Project is definitely the highest point of the course.
- As soon as the theoretical bases have been covered in the first 6 or 7 class sessions and the basic practical experience has been acquired by doing the first 6 or 7 homeworks, the student will be ready to start deciding the subject of their Final Project.
- In due time we'll provide a vast, detailed list of possible projects to choose from, but we'll be always be open to listen to and to evaluate the viability of a student's own proposed project.
- Details about the expected deliverables regarding those projects will also be provided in due time.

--COURSE DESCRIPTION—

Bitcoin is a particular implementation of Blockchain technology that has led to a disruptive "product": a set of digital cryptocurrencies with the potential to compete with fiat currencies. This course will provide students with the concepts and mechanics of the Blockchain technologies starting from Bitcoin. Unlike **ECE1770**, this course is not focused on middleware software design per se, but on how the Blockchain middleware can serve as a platform that supports products (cryptocurrencies) and applications that are relevant for businesses and other users. The course will focus on identifying business relevant benchmarking criteria for Blockchain technologies in accordance with their current and future impact on business processes. On a practical level, the course will enable students to set up a Bitcoin account that follows rigorous safety protocols, so as to enable students to become familiar with this revolutionary technology.

This course will enable students to:

1. Acquire a concrete understanding of Blockchain technologies through the installation, operation and modification (by coding changes or the addition of pseudocode) of a simplified Blockchain program in each student's computer.
2. Become acquainted with the history and typology of Blockchain technologies: the landscape of cryptocurrencies and hyper currencies
3. Develop and apply a set of selection criteria for the evaluation of Blockchain strengths, weaknesses and risks with respect to: networked integrity, distributed power, value as incentive, security, privacy, rights preserved and inclusion
4. Trace a likely path for the adoption of Blockchain technologies-- beginning with the identification of processes where Blockchain ledgers lead to efficiencies, to the emergence of new business models and ending with the need for constraints/regulation.
5. Learn to setup, operate and trade a Bitcoin account safely.

CORE READING LIST

1. Andreas Antonopoulos(2017) Mastering Bitcoin (free), https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf
2. P. Kravchenko and others (2018) Blockchain and Decentralized Systems in 3 volumes ($24 total): https://www.amazon.ca/Blockchain-Decentralized-Systems-Pavel-Kravchenko-ebook/dp/B07M9PD1K9/ref=sr_1_1?keywords=blockchain+and+decentralized+systems+by+kravchenko&qid=1588959687&sr=8-1
3. Joseph Bambara and others (2018) Blockchain, A practical Guide to Developing Business, Law and Technology solutions ($37): https://www.amazon.ca/Blockchain-Practical-Developing-Technology-Solutions/dp/1260115879/ref=sr_1_fkmr0_1?keywords=Joseph+Bambara+%282018%29+Blockchain%2C&qid=1588960116&sr=8-1-fkmr0

Another very useful source:

4. The Bitcoin Developer Guide: https://bitcoin.org/en/developer-guide

There are no mandatory prerequisites but previous course work or experience in programming would be helpful.

Course Structure and Content

Cryptocurrencies and other Blockchain Technologies is divided into four themes and 12 modules:

- The first theme: Economics of Cryptocurrencies
- The second theme: Bitcoin Technology
- The third theme: Blockchain Disintermediation & New Business Models

- The fourth theme: Owning and Trading Bitcoin

Learning outcomes

1. An annotated blueprint of current Blockchain designs with special attention to Bitcoin and Ethereum and their technical features
2. A benchmarking of Blockchain models (cryptocurrencies and hypercurrencies) with respect to selection criteria relevant to business activity
3. A possible path for the adoption of Blockchain, the emergence of new business segments and of decentralized technology communities and organizations
4. A working Bitcoin account as a learning tool.

--COURSE LAYOUT--

REQUIRED Textbooks:

5. Andreas Antonopoulos(2017) Mastering Bitcoin (free), https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf
6. P. Kravchenko and others (2018) Blockchain and Decentralized Systems in 3 volumes ($24 total): https://www.amazon.ca/Blockchain-Decentralized-Systems-Pavel-Kravchenko-ebook/dp/B07M9PD1K9/ref=sr_1_1?keywords=blockchain+and+decentralized+systems+by+kravchenko&qid=1588959687&sr=8-1
7. Joseph Bambara and others (2018) Blockchain, A practical Guide to Developing Business, Law and Technology solutions ($37): https://www.amazon.ca/Blockchain-Practical-Developing-Technology-Solutions/dp/1260115879/ref=sr_1_fkmr0_1?keywords=Joseph+Bambara+%282018%29+Blockchain%2C&qid=1588960116&sr=8-1-fkmr0

Another very useful source:

8. The Bitcoin Developer Guide: https://bitcoin.org/en/developer-guide

PART ONE: INTRODUCTION AND ECONOMICS

Session 1

Bitcoin intro: Importance of Bitcoin as ledger, protocol and platform; Bitcoin as alternative currency; 4 converging views of Bitcoin; projections for Bitcoin and blockchains; birthday paradox and collisions.

PART TWO: BITCOIN TECHNOLOGY

Session 2

Bitcoin architecture and security: Bitcoin building blocks, transactions, UTXOs, blocks, hash chains; digital signatures and fingerprints; authorization scripts, proof-of-work; scalability problems; double spending probability

Session 3

Bitcoin Script language from simple smart contracts up to Lightning Network: transaction primitives; transaction types; smart contract examples; Open Assets; Lightning Network

Session 4

Cryptography one: Symmetric encryption: one time pad; Asymmetric encryption: Diffie-Hellman-Elgamal encryption protocol: private key, public key, shared secret; RSA encryption protocol; encryption protocol based on elliptic curves over prime fields

Session 5

Bitcoin wallets: extended network, wallet functions, synchronization and transaction security, key management, key generation with elliptic curves, python implementation, paper wallets and Electrum wallet

PART THREE: BLOCKCHAIN

Session 6

Consensus Algorithms: Oral Messages algorithm, PBFT, digital ledger technologies, comparison with proof-of-work, proof-of stake, hybrid consensus, evaluation table of consensus protocols, tasks that complement or hinder the application of blockchain technologies

Session 7

Ethereum: platform description, use cases: Ipfs, Golem, Maersk supply chain, Grid+, Innogy share and charge, Slock.it, blockchain IOT python demo, Ethereum d'apps, Ethereum client setups for programming a D'app, PetShop Dapp Demo.

Session 8

Cryptography two: Homomorphic encryption: the concept, Pedersen commitment; ZK-SNARK: ZK proof if identity, ZK proof of knowledge; homomorphic encryption medical demo, zero knowledge proof of knowledge homomorphic graph demo, ZKledger Pedersen commitment presentation and demo

Session 9

Privacy: Bitcoin de-anonymization techniques, Bitcoin mixing, stealth addresses, the Bitcoin privacy model, privacy altcoins; internet privacy limitations

Session 10

Smart contracts: Ricardian contracts vs smart contracts, the DAO, synergy between smart contracts and game theory, stable coins, asset tokenization

Sessions 11

Cryptography three: Digital signatures, proof of identity revisited, the digital signature algorithm; hashing.

PART FOUR: VALUING AND TRADING CRYPTOCURRENCIES

Session 12

12. Bitcoin Metcalfe valuation, sketch of other valuation models

13. Crypto arbitrage, trading demo, co-integration demo

Suggested Readings:
Rohrbach, Janick and Suremann, Silvan and Osterrieder, Joerg, Momentum and Trend Following Trading Strategies for Currencies Revisited - Combining Academia and Industry (June 6, 2017). Available at SSRN: https://ssrn.com/abstract=2949379 or http://dx.doi.org/10.2139/ssrn.2949379
Corbet, Shaen and Meegan, Andrew and Larkin, Charles James and Lucey, Brian M. and Yarovaya, Larisa, Exploring the Dynamic Relationships between Cryptocurrencies and Other Financial Assets (November 13, 2017). Available at SSRN: https://ssrn.com/abstract=3070288 or http://dx.doi.org/10.2139/ssrn.3070288

Corbet, Shaen and Lucey, Brian M. and Yarovaya, Larisa, Datestamping the Bitcoin and Ethereum Bubbles (December 1, 2017). Available at SSRN: https://ssrn.com/abstract=3079712 or http://dx.doi.org/10.2139/ssrn.3079712
https://blog.patricktriest.com/analyzing-cryptocurrencies-python/

HOMEWORKS

We believe one cannot learn a technology by just reading about it, one must use it. These are hands-on homeworks.

1. Homework using Kleopatra or similar software to sign documents with digital signatures

2. Homework simulating a blockchain in Python to analyze the operation of hash chains

3. Homework simulating the Bitcoin blockchain in Python to analyze the impact of block size and block interval on security

4. Homework using two wallets, Bitcoin Core and Electrum in the Testnet Bitcoin network

5. Homework using Tails, Tor and Electrum in the Testnet Bitcoin network

6. Homework using tools to measure lack of browser privacy.

7. Homework using an Ethereum remote Metamask client setup to publish and operate a Testnet faucet smart contract

8. Homework using an Etherum simulated blockchain Ganache plus Truffle client setup to publish and operate a PetShop smart contract

References:

1. Ethereum: White Paper, https://github.com/ethereum/wiki/wiki/White-Paper
2. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, https://lightning.network/lightning-network-paper.pdf
3. How Blockchain Will Change Organizations Don Tapscott Alex Tapscott 2017, Sloan Management Review, https://sloanreview.mit.edu/article/how-blockchain-will-change-organizations/
4. The Truth About Blockchain Marco Iansiti Karim R. Lakhani 2018, https://hbr.org/2017/01/the-truth-about-blockchain
5. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels, https://www.tik.ee.ethz.ch/file/716b955c130e6c703fac336ea17b1670/duplex-micropayment-channels.pdf
6. Formalizing and Securing Relationships on Public Networks, http://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First
7. On Decentralizing Prediction Markets and Order Books, http://www.econinfosec.org/archive/weis2014/papers/Clark-WEIS2014.pdf
8. Bitcoin faces a crossroads, needs an effective decision-making process, https://freedom-to-tinker.com/2015/05/11/bitcoin-faces-a-crossroads-needs-an-effective-decision-making-process/
9. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf
10. Bitcoin: A First Legal Analysis, http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf
11. Letter of support for A.B. 1326 (CoinCenter), https://coincenter.org/entry/letter-of-support-for-ab-1326-to-california-state-senate
12. A License to Kill Innovation: Why A.B. 1326 is Bad for Business, Innovation, and Privacy, https://www.eff.org/deeplinks/2015/08/license-kill-innovation-why-ab-1326-californias-bitcoin-license-bad-business

13. Peterson, Timothy, Metcalfe's Law as a Model for Bitcoin's Value (January 22, 2018). Available at SSRN: https://ssrn.com/abstract=3078248 or http://dx.doi.org/10.2139/ssrn.3078248

14. Rohrbach, Janick and Suremann, Silvan and Osterrieder, Joerg, Momentum and Trend Following Trading Strategies for Currencies Revisited - Combining Academia and Industry (June 6, 2017). Available at SSRN: https://ssrn.com/abstract=2949379 or http://dx.doi.org/10.2139/ssrn.2949379

15. Corbet, Shaen and Meegan, Andrew and Larkin, Charles James and Lucey, Brian M. and Yarovaya, Larisa, Exploring the Dynamic Relationships between Cryptocurrencies and Other Financial Assets (November 13, 2017). Available at SSRN: https://ssrn.com/abstract=3070288 or http://dx.doi.org/10.2139/ssrn.3070288

16. Corbet, Shaen and Lucey, Brian M. and Yarovaya, Larisa, Datestamping the Bitcoin and Ethereum Bubbles (December 1, 2017). Available at SSRN: https://ssrn.com/abstract=3079712 or http://dx.doi.org/10.2139/ssrn.3079712

17. Gervais et. al, On the Security of Proof of Work Blockchains, (2016). https://eprint.iacr.org/2016/555.pdf

18. Nelson, The Byzantine General's Problem (2007). http://www.cs.kzoo.edu/cs480/homework/MarkNelsonBG.pdf

19. Bano et. al SoK: Consensus in the Age of Blockchains (2017). https://arxiv.org/pdf/1711.03936.pdf

20. Nussbaum, Blockchain Project Ecosystem Market Map and Musings on the State of the Ecosystem, (2017) https://medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940ababaf27

21. Driscoll, Surveying Blockchain Tech ForEnterprise (2017)

Cases:

1. CASE STUDY: Bitcoin: The Future of Digital Payments? Andrei Hagiu, Nathan Beach 2014, Harvard Business School Case, https://www.hbs.edu/faculty/Pages/item.aspx?num=47472

2. CASE STUDY : Deutsche Bank: Pursuing Blockchain Opportunities (A) and (B) by Lynda M. Applegate, Roman Beck and Christoph Müller-Bloch 2017, Harvard Business School Case, https://www.hbs.edu/faculty/Pages/item.aspx?num=52628

3. CASE STUDY : Bitfury: Blockchain for Government by Mitchell Weiss and Elena Corsi 2017 Harvard Business School Case, https://www.hbs.edu/faculty/Pages/item.aspx?num=53445

4. CASE STUDY: BitGold: Turning Digital Currency into Gold? Jean-Philippe VergneBrady Burke 2015, Harvard Business School Case, https://hbr.org/product/bitgold-turning-digital-currency-into-gold/W15608-PDF-ENG

5. CASE STUDY: Bitcoin CASE STUDY Jean-Philippe VergneKen Mark 2014, https://hbr.org/product/bitcoin/W14336-PDF-ENG

--COURSE INSTRUCTORS—

Sabatino Costanzo-Alvarez

Sabatino Costanzo-Alvarez holds a Masters in Economics and Finance from Brandeis University as well as a Magister Scientiarum, a Magister Philosopharum and a Ph.D. in Mathematics from Yale University, where in 1990 achieved a significant breakthrough by solving a mathematical conjecture which had remained unsolved for more than 3 decades. Taught Mathematics of Finance at Boston University as an Associated Professor for 5 years and later co-founded the Boston Trading Group LLC, designed the trading systems used in the firm's daily Futures Trading Operations and acted as head trader of the team. Holds the licenses "Registered Representative NYSE/NASDAQ" (Series 7), "Registered Financial Advisor", "Registered Uniform State Law Securities Agent", "Registered Managed Futures Fund Representative" in the U.S. and "Canadian Securities Course" & "Conduct and Practices" in Canada, as well as products training at Morgan Stanley in Boston, and later at Merrill Lynch in New York. Chaired the Advanced Management Program for Senior Executives (PAG), an Executive MBA at the US Accredited IESA Institute in Caracas, where he taught Financial Engineering and Investment Management as an Associate Professor, and tutored over 70 MBA dissertations. Acted as Head of Research at Econo Invest C.A., the largest Investment Firm in Venezuela, leading the Investment Strategy Team in charge of generating and executing the U.S. & E.U. investment strategies for Commodities, Fixed Income Instruments and Equities for the firm (published weekly in Bloomberg), as well as generating and maintaining the Sovereign Fixed Income Indexes of Brazil, Colombia, Mexico, Peru, Chile, Uruguay and Venezuela to be used in the design of international financial products. Acted as an Investment Advisor for the International Wealth Management Groups at Morgan Stanley (Boston), Merrill Lynch (NY) and the Royal Bank of Canada(Toronto), and is now a Senior Partner at the Toronto boutique Investment Firm Inter Alea, where he provides state-of-the-art mathematical modeling solutions to portfolio and risk management problems for a select group of corporate and high net worth private clients, designing and managing their investment portfolios based on their specific risk & return requirements. He teaches Portfolio Management, Statistics & Mathematical Modelling and Business Mathematics Courses at the Pilon School of Business, and is the founder and advisor of the Sheridan Students Trading and Investment Association. He is a Lecturer at the U of T Graduate School, where he is teaching Portfolio Management, Blockchain Technology, Cryptocurrencies and Artificial Intelligence applied to Finance.

Rosario Lorenza Trigo-Ferre

Holder of a B. A. in Philosophy (Magna Cum Laude) from Yale University -where she also received training in Math & Physics-, a Ph.D. in Generative Linguistics from Massachusetts Institute of Technology (MIT) and a M. Sc. in Management of Information Systems from Boston University ("Beta Gamma Sigma Honors" award), she was a Professor at Boston University for 8 years. While a Programmer Analyst at Boston University, she designed and developed an application for the management of accounts trading stock and currency futures and co-designed financial applications under the direction of Professor Zvie Bodie at B.U. Co-founder and Trader at the Boston Trading Group and Certified Programmer Analyst in e-commerce by the University Computer Careers Program, she generated the trading signals for currencies and metals futures used in the BTG's market operations; developed an application maximizing the efficiency of trading system for currency and metal futures, and designed a client-server application for the management and operation of trading accounts. Has designed and developed many multi- tiered e-commerce applications dynamically generated from databases. Project leader and senior programmer analyst at IngeDigit, designed and developed internet applications for banking accounts management & operation, and for international transactions between banking accounts and credit cards. She was a Professor at the Department of Production and Technical Innovation of the IESA Institute, the top -only US accredited- Venezuelan Business School, where taught courses in Information Systems, Simulation in Finance, Operations and Database Marketing. She is the author of many scientific papers in refereed journals and a Permanent Consultant for an international development bank (C.A.F, The Andean Region Development Bank), where she has designed the financial models used to evaluate the profitability, coverage and socio-economic impact of projects like the inclusion of fiber-optic cable in highways in Colombia and Peru. These models led to the enactment of new laws making such inclusion mandatory in the Andean region. Also designed the financial models used to evaluate the profitability of projects in satellite technology in Argentina (specifically the ARSAT program) by estimating the future regional demand for transponders and the impact of the project in the input-output matrix of the country, and is now a Partner at the boutique Investment Firm InterAlea, where she designs, develops, tests and implements trading and risk management strategies based on the entropy analysis of price signals, executed on stock quote-data processed through SQL-Server. She is a Lecturer at the U of T Graduate School, where she is teaching Portfolio Management, Blockchain Technology, Cryptocurrencies and Artificial Intelligence applied to Finance.