Master Engineering ELITE Programme **Sabatino Costanzo & Loren Trigo**
University of Toronto

BLOCKCHAIN TECHNOLOGIES AND ITS APPLICATIONS TO CRYPTOCURRENCIES (APS 1050)

--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, tokens) and applications that are relevant for businesses and other users. Students become acquainted with the history and typology of Blockchain technologies; develop and apply a set of selection criteria for the evaluation of Blockchain consensus strengths, weaknesses and risks; 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 where the use of cryptography is essential. For this reason, this course includes a gentle but complete introduction to cryptography that covers all the essentials from asymmetric encryption to "zero-knowledge-proof-of-knowledge" proofs. On a practical level, participants acquire a concrete understanding of Blockchain technologies through the installation, operation and modification of a number of Blockchain technologies that operate in real-world testnet networks: starting from the operation/modification of a simple Bitcoin node; moving on to the operation of Bitcoin and Ethereum wallets, and to the operation/modification of Ethereum clients or DApps providing a business service, and ending with the trading of a cryptocurrency account. For more details please go to the Course Layout Section below.

COURSE PRE-REQUISITES:

There are no prerequisites for this course, but previous course-work or experience in programming would be helpful.

COURSE STRUCTURE & CONTENT:

Cryptocurrencies and other Blockchain Technologies is divided into five parts and 12 modules:

- The first theme: Introduction and Economics
- The second theme: Bitcoin Technology
- The third theme: Blockchain Technologies
- The fourth theme: Cryptography Essentials
- The fifth theme: Valuing and Trading Bitcoin

LEARNING OBJECTIVES:

The course presents:

1. An annotated blueprint of current Blockchain designs with special attention to Bitcoin and Ethereum and their technical features
2. A conceptual frame for the benchmarking of Blockchain models with respect to selection criteria relevant to business activity
3. The possible path for the adoption of Blockchain, the emergence of new business segments and of decentralized technology communities and organizations
4. The operation of Blockchain related technologies: networks, nodes, wallets, and Blockchain related demos relevant to diverse business areas, including Internet of Things, asset tokenization, payment systems, auditing etc.
5. Simple valuation models for Bitcoin.

LEARNING OUTCOMES:

The student will acquire the capacity to:

1. Install and correctly use programs implementing cryptographic key manipulation, simulated consensus algorithms, Blockchain wallets and Blockchain DApps (distributed applications) operating in testnet networks.
2. Understand the cryptography and consensus algorithms underlying the Blockchain with enough rigor (from concrete mathematical examples and from the parsing of programs, not metaphors) so as to be able to confidently read and understand Blockchain related white-papers and related business models.
3. Identify a Blockchain consensus algorithms' strengths, weaknesses and risks with respect to: networked integrity, distributed power, value as incentive, security, privacy, rights preserved and inclusion.
4. Program from scratch/modify and operate a Blockchain DApp: a multi-layered distributed application having a testnet Ethereum Blockchain as the back-end and a web page user interface as the front-end, so as to be able to confidently read and understand DApp white-papers and related business models. Technologies learned: Solidity smart contracts, asynchronous Javascript (Web3), and JQuery, using the Truffle framework + Ganache Blockchain simulator.
5. Setup, operate and trade a Bitcoin account safely.

--COURSE LAYOUT--

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.

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; Birthday paradox and collisions.

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

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 TECHNOLOGIES

Session 5

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 6

Guidelines for Projects (Personal and Team). Research materials (presentations) on Internet of Things (IoT) , the DAO Hack, and Polkadot.

Ethereum: Ethereum Virtual Machine, Bitcoin Ethereum Similarities & Contrasts, Ethereum Components, Ethereum Transactions, Nonce, Gas Cost and Price, Ethereum Smart Contracts, Programming an Ethereum Smart Contract with Solidity, Truffle Framework, Calls vs Transactions, Promises, Web3 Object Tutorial, Asynchronous Javascript Tutorials, Election DApp Tutorial, Pet Shop DApp Tutorial, Faucet Tutorial, Python IOT Tutorial, Ethereum DApp Minicourse.

Session 7

Research materials (presentations) on: Ricardian contracts and Game theory, Stablecoins, Are Tokens Securities?

D'Apps and Tokens in Ethereum: What is a D'App, Web3, IPFS, Oracles, Tokens, Ethereum Tokens, Asset Tokenization, Token Fungibility, Types of Tokens (Utility vs Equity), ERC20 Token Standard Interface, Launching your own ERC20 Token, Interaction with an ERC20 Token (METoken Tutorial) with Metamask, Ganache & Truffle, Web3 1.x.x and Metamask changes, The Async Await Javascript construct.

PART FOUR: CRYPTOGRAPHY ESSENTIALS

Session 8

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 9

Cryptography two. RSA theorem, Homomorphic encryption: the concept, Pedersen commitment; ZK-SNARK: ZK proof of identity, ZK proof of knowledge. 1.InteractiveZeroKnowledgeProof_Python_DEMO 2.HomomorphicEncryption_Python_DEMO 3.ZeroKnowledgeProof-Javascript_DEMO

Session 10

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

PART FIVE: VALUING AND TRADING CRYPTOCURRENCIES

Session 11

Bitcoin Metcalfe valuation, sketch of other valuation models

Session 12

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/

HOMEWORK ASSIGNMENTS AND FINAL PROJECT:

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

9. Cryptography homework

10. Final Project: the programming of an Ethereum Dapp or the writing of a Case study about a Blockchain white paper.

REQUIRED TEXTBOOKS:

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

OTHER SOURCES:

4. The Bitcoin Developer Guide: https://bitcoin.org/en/developer-guide
5. Arvind Narayanan (2016), Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction Kindle Edition.https://www.amazon.ca/Arvind-Narayanan-ebook/dp/B01GGQJ2XW/ref=sr_1_fkmr1_1?keywords=bitcoin+isbn+blockchain+arvind+narayanan&qid=1590352046&sr=8-1-fkmr1
6. Andreas Antonopoulos and Gavin Wood (2019) Mastering Ethereum.
7. bitcoin-notes-v0.1 (distributed in the first lecture)

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)

CASE STUDIES:

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

6. CASE STUDY: Steemit a New Social Media, Ramon Casadesus-Masanell et. al. 2019, https://hbsp.harvard.edu/product/720428-PDF-ENG

--COURSE INSTRUCTORS—

Sabatino Costanzo-Alvarez:

He 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 IESA Institute, 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., one of the largest Investment Firms in Latin America, 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.