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

APS-CMC

BLOCKCHAIN TECHNOLOGIES AND CRYPTOCURRENCIES

(AP1050H Summer 2019)

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. Pedro Franco (2015) Understanding Bitcoin, John Wiley & Sons.
   https://openlibrary.org/works/OL17802119W/Understanding_Bitcoin
   Franco (2015) can be partially substituted with: https://bitcoin.org/en/developer-guide
2. Arvind Narayanan et. al. (2016) Bitcoin and Cryptocurrency Technologies, Princeton University Press (draft), http://bitcoinbook.cs.princeton.edu/
3. Peter Lipovyanov (2019) Blockchain for Business 2019 (5$ at Packt, 48 hour fire sale)
4. Dan Tapscott et. Al (2016) Blockchain Revolution, Penguin. ($14 at Amazon)

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.

PART ONE: INTRODUCTION AND ECONOMICS

Session 1 [3.42]

Foundational Themes: The 4 meanings of Bitcoin, Significance of Bitcoin as a Currency, 4 converging views of Bitcoin, Significance of Bitcoin as a Technology (Blockchain), Challenges, Possible outcomes

Readings & homework: Franco (2015) 1, 2 & 3
How Blockchain Will Change Organizations Don Tapscott Alex Tapscott 2017
The Truth About Blockchain Marco IansitiKarim R. Lakhani 2018

PART TWO: BITCOIN TECHNOLOGY

Session 2 [3.16]

Encryption: Transactions, Hash Functions, Digital Signatures, Bitcoin Addresses, Transaction Validation Scripts, The Double Spending Problem, Proof-of-work consensus, Security Challenges, Scalability problems

Readings & homework:
Franco (2015) 5 & 7
Homework 1 due (see list below)

DEMO: SMALL PYTHON BLOCKCHAIN INSTALL & RUN

Session 3 [2.58]

Bitcoin Wallets & Exchanges

Readings & homework:
Franco (2015) 8

15 minute Quiz on class 2 contents
WALLET DEMO: Cryptocurrency Account Setup: A System for Owning Cryptocurrencies: Tails, Electrum & Bitcoin Core, Testnet

Session 4 [3.02]

The Power of Script: Elements of a Transaction, Transaction Script Types, Bond Based Contracts, Pay-to-script-hash Escrow, Op-return, Smart Property, Colored Coins, Hashed Commitments, Oracles, Prediction Markets, Payment Relays, Payment Channels (Lightning Network)

Readings & homework:
Franco (2015) 4, 6, 12
The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments
A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels
Homework 2 due (installation and running only, see list below)

Session 5 [3.20]

Privacy: Loss of Privacy via Transaction Analysis & Side Channel Analysis, Mixing, The Bitcoin Privacy Model , Cryptographic Alt-Coins (Monero, Zcash)

Readings & homework:
Franco (2015) 13
Homework 2 due (results, see list below)

Session 6 [1.02]

Bitcoin Mining & Governance

Readings & homework:
Franco (2015) 9
Homework 3 due (see list below)

PART THREE: BLOCKCHAIN

Session 7 [4.13]

Blockchain: Changing Bitcoin (Block Size, Puzzle, Consensus), Alternative Protocols for Distributed Consensus (Practical Byzantine Fault Tolerance, Proof-of-Stake), Distributed Ledger Technologies, Use Cases of DLTs

Readings & homework:
Gervais et. al, On the Security of Proof of Work Blockchains, (2016).
Nelson, The Byzantine General's Problem (2007).
Bano et. al SoK: Consensus in the Age of Blockchains (2017).
Nussbaum, Blockchain Project Ecosystem Market Map and Musings on the State of the Ecosystem, (2017)

Session 8 [4.04]

Ethereum, Ethereum Dapps, The_DAO, The SEC: Token vs. Coins vs. Stocks

Readings & homework:
Franco (2015) 12.7.3
Overview of Ethereum: White Paper
Homework 4 due (see list below)

Session 9 [1.29]

IoT&Blockchain, Altoins: Stability and Interoperability

Readings & homework:
Franco (2015) 14
Dan Tapscott et. al (2016) 1, 2, 3, 4
Driscoll, Surveying Blockchain Tech For Enterprise (2017)
Homework 5 due (see list below)

PART FOUR: OWNING AND TRADING BITCOIN

Sessions 10

Trading: Trading Cryptocurrency Pairs using Statistical Arbitrage: A Python program for trading crypto currency pairs will be provided and explained.

Portfolio selection: Principles of portfolio selection for crypto-currencies.

Readings & homework:
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 6 due

Sessions 11 & 12

Presentations by Students

Readings & homework:
Dan Tapscott et. al (2016) 5 & 6
Driscoll, Surveying Blockchain Tech ForEnterprise (2017)

Homework 7 due (Session 11)
Presentations due (Session 11)
Presentations due (Session 12)

Individual Papers due on 'final exams week'

Course Grading: The components of the final course grade will be weighted as follows:
Student evaluation will be based on the following criteria:

Session 3: Quiz……5%

Team Homeworks (all software to be provided to students)……70 %

1. Session 2: Installation, successful use and description of results of digital signature & asymmetric encryption software
2. Session Session 4 & 5: Installation, running, description of results and optional modification of a Blockchain program
3. Session 6: Installation, successful use of Tails, Electrum testnet Bitcoin wallet, Bitcoin Core & Bitcoin blockchain browser
4. Session 8: Installation & description of results under stipulated conditions of a program that solves the Byzantine General's Problem
5. Session 9: Installation, successful use of testnet Ethernet wallet Metamask & Ethernet blockchain browser
6. Session 10: Writing (by copy and paste), publication and description of results of faucet smart contract on Ethereum blockchain
7. Session 11: Evaluation of possible status (Token vs. Coin vs. Stock) of a short list of cryptocurrencies

Sessions 11 & 12: Team Presentation on a blockchain use case/case study/crypto valuation method……15%

Final Exams Week: Individual final paper on the aspect of the team presentation developed by each student……..10%

Note: these statements are guidelines subject to change.

Textbooks:

1. Pedro Franco (2015) Understanding Bitcoin, John Wiley & Sons.
   https://openlibrary.org/works/OL17802119W/Understanding_Bitcoin
   Franco (2015) can be partially substituted with: https://bitcoin.org/en/developer-guide
2. Arvind Narayanan et. al. (2016) Bitcoin and Cryptocurrency Technologies, Princeton University Press (draft), http://bitcoinbook.cs.princeton.edu/
3. Dan Tapscott et. Al (2016) Blockchain Revolution, Penguin. ($14 at Amazon) This one is ESSENTIAL.

Cases (to be presented by students):

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

Articles (to further contextualize the cases to be presented):

1. Ethreum: 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)