# Cyber security regulation

## Proff. Ferdinando Ametrano; Giuseppe D’Agostino

Part of course: **Bitcoin and Blockchain Technology** (Prof. Ferdinando M.Ametrano)

***COURSE AIMS AND INTENDED LEARNING OUTCOMES***

The course is about bitcoin, the associated blockchain technology, and their relevance in the field of cyber security regulation.

Bitcoin is introduced as ingenious breakthrough fintech innovation.

Its game theory, computer science (distributed systems, distributed consensus), and monetary theory elements are examined in the attempt to properly convey the interdisciplinarity of the topic and appreciate its relevance.

Technical and programming elements about digital signatures, blockchain, Merkle tree, addresses, transactions, and timestamping are also provided to assess features and limits of the Bitcoin protocol.

***COURSE CONTENT***

* Cash, Electronic Money, Central Bank Money, eCash
* Internet Money
* Bitcoin Transactions
* About Money
* Private Money and the Centralization Dilemma
* The Double Spending Problem
* Bitcoin as Digital Gold
* Bitcoin as Investment Asset
* Bitcoin Financial Services
* Discrete Logarithm Problem on Finite Cyclic Groups
* Modular Arithmetic
* Finite Fields
* Elliptic Curves Over Real Numbers
* DLP on Elliptic Curves Over Finite Fields
* Hash Functions
* Partial Hash Inversion
* Hash Pointer Data Structures: Blockchain and Merkle Tree
* Design of A Simplified Digital Currency
* Distributed Consensus
* Mining
* P2P Network
* Protocol Governance
* Elliptic curve digital signature algorithm
* Elliptic curve Schnorr signature algorithm: Mu(lti)Sig(nature), threshold signature, batch verification
* Addresses and WIFs
* Hierarchical deterministic wallets: BIP32, BIP43, BIP44
* Mnemonic phrase: BIP39 and Electrum
* TxIns, TxOs, UTxO, nLockTime
* Bitcoin script language
* Transactions
* Blocks
* Wallets and Bitcoin Core
* Testnet, regtest, and wallet workshop
* Money and innovation: monetary and token engineering
* Hayek money and dual asset ledger money
* Blockchain beyond bitcoin
* Finance and blockchain
* Timestamping, notarization, and anchoring
* Smart contracts
* Distributed ledger technology

***READING LIST***

Python library

[https://btclib.org](https://btclib.org/)  
<https://github.com/btclib-org/btclib>

Python scripts, Excel spreadsheets, and regtest lab material

[http://github.com/btclib-org/bbt](https://github.com/btclib-org/bbt)

Introductory reading

* Ferdinando M. Ametrano,  
  *“Bitcoin: oro digitale, finanza e tulipani”*,  
  <https://docs.google.com/document/d/1gecm0uT43tl8d4WFYNs9H_v3p70PPfPmQITR4GxSWkE>

Technology references

* Satoshi Nakamoto,  
  *“Bitcoin: A Peer-to-Peer Electronic Cash System”* (2008),  
  <https://bitcoin.org/bitcoin.pdf>
* Andreas M. Antonopoulos,  
  *“Mastering Bitcoin: Programming the Open Blockchain”* (2nd edition, 2017),  
  Oreilly & Associates Inc, 978-1491954386,  
  <https://github.com/bitcoinbook/bitcoinbook>
* Jimmy Song,  
  *“Programming Bitcoin: Learn How to Program Bitcoin from Scratch”* (2020)  
  Oreilly & Associates Inc, 978-1492031499,  
  <https://github.com/jimmysong/programmingbitcoin>
* A. Narayanan, et al.,  
  *“Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”* (2016),  
  Princeton University Press, 978-0691171692,  
  <https://www.coursera.org/learn/cryptocurrency>, <http://bitcoinbook.cs.princeton.edu/>, <https://lopp.net/pdf/princeton_bitcoin_book.pdf>
* Pedro Franco,  
  *“Understanding Bitcoin: Cryptography, Engineering and Economics”* (2014),  
  Wiley, 978-1119019169
* Ferdinando M. Ametrano,  
  *“Bitcoin, Blockchain, and Distributed Ledgers: Between Hype and Reality”* (2017),  
  <https://ssrn.com/abstract=2832249>
* Roger Wattenhofer,  
  *“Blockchain Science: Distributed Ledger Technology”* (3rd edition, 2020),  
  Independently published, 978-1793471734

Cryptography references

* Christof Paar, Jan Pelzl,  
  *“Understanding Cryptography”*,  
  Springer, 978-3642041006 <http://www.crypto-textbook.com/>, <http://wiki.crypto.rub.de/Buch/en/slides.php>, <https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg/videos>
* Dan Boneh, *“A Graduate Course in Applied Cryptography”*,  
  Stanford University  
  <https://www.coursera.org/learn/crypto>, <https://toc.cryptobook.us/>
* Lawrence C. Washington,  
  *“Elliptic Curves: Number Theory And Cryptography”* (2008),  
  Chapman and Hall, 978-1420071467
* Standards for Efficient Cryptography Group  
  SEC 1: Elliptic Curve Cryptography, March 2009. Version 2.0.  
  <http://www.secg.org/sec1-v2.pdf>
* Standards for Efficient Cryptography Group  
  SEC 2: Recommended Elliptic Curve Domain Parameters, March 2009. Version 2.0.  
  <http://www.secg.org/sec2-v2.pdf>
* Guidelines for Efficient Cryptography  
  GEC 2: Test Vectors for SEC 1, September 1999. Version 0.3.  
  <http://read.pudn.com/downloads168/doc/772358/TestVectorsforSEC%201-gec2.pdf>

Monetary theory references

* Friedrich A. Hayek,  
  *“Denationalisation of Money: The Argument Refined”*,  
  <https://mises.org/library/denationalisation-money-argument-refined>
* Saifedean Ammous,  
  *“The Bitcoin Standard: The Decentralized Alternative to Central Banking”* (2018),  
  Wiley, 978-1119473862
* Ferdinando M. Ametrano,  
  *“Hayek Money: The Cryptocurrency Price Stability Solution”* (2014),  
  <https://ssrn.com/abstract=2425270>
* Robert Sams,  
  *“A Note on Cryptocurrency Stabilisation: Seigniorage Shares”* (2015),  
  <https://github.com/rmsams/stablecoins/blob/master/paper.pdf>
* Ferdinando M. Ametrano,  
  *“Bitcoin: oro digitale per nuovi standard monetari* (2020),  
  published in “Dal sesterzio al bitcoin”, Rubettino Editore (edited by Angelo Miglietta, and Alberto Mingardi)  
  [http://bit.ly/2NQg9VJ](https://bit.ly/2NQg9VJ)

***TEACHING METHOD***

* Slide based lessons with associated bibliography
* Python 3 programming assignments and technology assignments
* Workshop labs on Bitcoin Core, Electrum, and OpenTimestamps.

***ASSESSMENT METHOD AND CRITERIA***

Students are asked to solve the homework assignments for each lesson. Please send the homeworks to the e-mail that will be indicated with subject **BBT202010-BRESCIA #1** for the first lesson, **BBT202010-BRESCIA #2** for the second lesson, etc.

The exam will be a multiple choice online live test.

***NOTES AND PREREQUISITES***

*Warnings and prerequisites:*

There are no strict prerequisites, even if a computer science mindset and some familiarity with algebra and finance might help to appreciate the course. While a rigorous formal approach is almost impossible in a course touching on so many and so different knowledge areas, intellectual curiosity is stimulated about the interplay between maths, cryptography, economic incentives, technology, monetary theory, regulatory issues, and politics.

If you have an e-mail *@unicatt.it* please join the 202010-brescia channel in the Slack [BBT workspace](https://join.slack.com/t/bbt-training/signup) using your first and last name (no nicknames); a profile picture would be appreciated, but is not mandatory. Details and updates about the course will be posted in the Slack channel.

The course if for the students of Università Cattolica del Sacro Cuore only; anyone else, please consider <https://dgi.io/workshop>.

Part of course: **FINTECH** (Prof. Giuseppe D’Agostino)

***COURSE AIMS AND INTENDED LEARNING OUTCOMES***

The first part of the course is focused on the analysis of Fintech phenomenon (literally technology applied to finance) in the economic and regulatory perspectives. Students will be provided with a general understanding of Fintech activities and services within the wider digital transformation of the economy and society driven by data, artificial intelligence and ICT developments. In this context, a specific market strategy analysis of the Big-Tech firms will be carried out to grasp their scale and reach projections on financial services world.

A part of the course will be dedicated to examining some innovative forms of financial markets: digital financial marketplaces, token exchange systems based on DLT and smart contract deployment. Moreover, great attention will be paid to the EU regulatory strategy on Fintech with a focus on the Digital Finance Package. In this context, we will provide students with an analysis of the EC proposal for Digital Operational Resilience Act (DORA), which creates a unified legal framework to address ICT governance issues for all actors within the financial system, as well as a view on the EU cybersecurity legal framework.

To complete, structural elements of the EU institutional and regulatory policy on FinTech will be assessed in relation to European data and artificial intelligence strategies, in particular by examining the logic of the new EU proposal for a regulation on Artificial Intelligence, fundamental legal discipline destined to become a milestone for the development of the digital economy.

At the end of the course, students will have a good knowledge of the logic behind FinTech developments, its global, inter-sectoral and multidimensional nature. Students will also have the ability to understand the structure of the digital markets for services and their main problems - in the public interest perspective - related to competition law, innovation policy and data protection matters.

Moreover, students will be able to assess effectiveness and feasibility of the European Union's regulatory and operational strategy on Fintech, through an in-depth knowledge of the complex of variables involved and possible trends. Students will also learn to look at the world of data and related artificial intelligence techniques in the financial market from the fairness and ethics point of view.

***COURSE CONTENT***

* + 1. The Digital Data Economy: Information, Artificial Intelligence and Technology
    2. The Big-Data Era: information as new economic asset and the Artificial Intelligence systems as new decision-making tools
    3. The microeconomics of the digital platforms for the exchange of goods and services (*digital marketplaces*)

1. Financial intermediation in the new technological scenario: Fintech
2. Some areas of Fintech development:

## 5.1 Digital Financial Marketplaces: micro-structures and functioning

## 5.2 DLT, Smart Contracts and Cryptoassets: the "tokenitation"

1. FinTech: strategic and regulatory design of the European Commission
   1. From the Capital Markets Union Action Plan to the FinTech Action Plan
   2. The "Digital Single Market Strategy for Europe"
   3. An overview of the EU regulatory package on Digital Finance.
2. The Digital Operational Resilience Act for the financial sector and the EU cybersecurity legal framework.
3. The international debate on Artificial Intelligence deployment in financial services: black-box effects, ethics and liabilities.
4. The EC proposal for a regulation on Artificial Intelligence: the new frontier for Artificial Intelligence system governance.

***READING LIST***

During the lessons, the lecturer will provide papers and documents in English produced by international public or private institutions or university research centers or other international research fora.

***TEACHING METHOD***

Face-to-face lessons. Case-studies. Team-works.

***ASSESSMENT METHOD AND CRITERIA***

The exam consists of an oral test through which the student will demonstrate that he has acquired the basic notions and concepts of the subject and that he will be able to illustrate independently, appropriately and consistently the economic and regulatory issues present in the European debate on Fintech, which were studied in depth during the teaching course. The mark given on this part of the program will contribute 50% to the composition of the final mark.

***NOTES AND PREREQUISITES***

*Warnings and prerequisites*

Being an introductory course, teaching does not require prerequisites for content.

*Time and Place to meet students*

My office time is the hour following lesson at the Catholic University premises in Brescia.