



UNIVERSITÀ  
DEGLI STUDI DI MILANO-BICOCCA

## SYLLABUS DEL CORSO

### Laboratory: Bitcoin, Crypto-assets and Blockchain

2223-E1803M-EXT-LABBIT

---

#### Obiettivi formativi

Il corso riguarda bitcoin, cripto-asset e la tecnologia blockchain associata.

Teoria dei giochi, informatica (sistemi distribuiti, consenso distribuito) e elementi di teoria monetaria vengono esaminati nel tentativo di trasmettere adeguatamente l'interdisciplinarietà degli argomenti e apprezzarne la rilevanza.

#### Contenuti sintetici

Bitcoin as Digital Gold  
Hash Functions  
Blockchain, Mining, and Distributed Consensus  
Timestamping and the OpenTimestamps Protocol  
Wallets and Custody  
Beyond Bitcoin: Between Hype and Reality  
The Cryptocurrency Frontier in Monetary Engineering

#### Programma esteso

Bitcoin as Digital Gold

- Internet Money
- Bitcoin Transactions
- About Money

- Private Money and the Centralization Dilemma
- The Double Spending Problem
- Bitcoin as Digital Gold
- Bitcoin as Investment Asset
- Financial Services

## Hash Functions

- Hash Functions and Their Properties
- Puzzle Friendliness and Partial Hash Inversion
- Hash-based Data Structures

## Blockchain, Mining, and Distributed Consensus

- Simplified Digital Coin
- Distributed Consensus
- Proof-of-Work (PoW)
- Mining
- P2P Network
- Protocol Governance

## Timestamping and the OpenTimestamps Protocol

- Blockchain Immutability
- Timestamping
- The OpenTimestamps standard
- Use Cases

## Wallets and Custody

- Key Management and UTXO Database Access
- Wallets as Collection of Keys
- Custody

## Beyond Bitcoin: Between Hype and Reality

- Other Cryptocurrencies
- Smart Contracts
- Initial Coin Offering
- Non-Fungible Tokens (NFT)
- Decentralized Finance (DeFi)
- Traditional Finance for Crypto Assets
- Blockchain Without Bitcoin
- Distributed Ledger Technology
- Financial Products and Services

## The Cryptocurrency Frontier in Monetary Engineering

- Cash, eMoney, Central Bank Money, and eCash
- Stable Coins
- Hayek Money: Elastic Non-discretionary Policy
- Hayek Money: Dual Asset Ledger and Proof-of-Payment

## Prerequisiti

Non ci sono prerequisiti rigidi, anche se una mentalità informatica e una certa dimestichezza con l'algebra e la finanza potrebbero aiutare ad apprezzare il corso. Mentre un approccio formale rigoroso è quasi impossibile in un corso che tocca aree di conoscenza così tante e così diverse, viene stimolata la curiosità intellettuale per l'interazione tra matematica, crittografia, incentivi economici, tecnologia, teoria monetaria e politica.

## Metodi didattici

Lezioni basate su slide con bibliografia associata

## Modalità di verifica dell'apprendimento

Test con domande a scelta multipla

## Testi di riferimento

Ferdinando M. Ametrano,  
"Bitcoin: oro digitale, finanza e tulipani",  
[https://docs.google.com/document/d/1gecm0uT43tl8d4WFYNs9H\\_v3p70PPfPmQITR4GxSWkE](https://docs.google.com/document/d/1gecm0uT43tl8d4WFYNs9H_v3p70PPfPmQITR4GxSWkE)

Satoshi Nakamoto,  
"Bitcoin: A Peer-to-Peer Electronic Cash System" (2008),  
<https://bitcoin.org/bitcoin.pdf>

A. Narayanan, et al.,  
"Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction" (2016),  
Princeton University Press, 978-0691171692,  
<https://www.coursera.org/learn/cryptocurrency>, <https://bitcoinbook.cs.princeton.edu>,  
<https://bitcoinbook.cs.princeton.edu>, [https://www.lopp.net/pdf/princeton\\_bitcoin\\_book.pdf](https://www.lopp.net/pdf/princeton_bitcoin_book.pdf)

Pedro Franco,  
"Understanding Bitcoin: Cryptography, Engineering and Economics" (2014),  
Wiley, 978-1119019169

Friedrich A. Hayek,  
"Denationalisation of Money: The Argument Refined",  
<https://mises.org/library/denationalisation-money-argument-refined>

## Periodo di erogazione dell'insegnamento

8 marzo - 10 maggio 2023

## **Lingua di insegnamento**

Inglese

## **Sustainable Development Goals**

PACE, GIUSTIZIA E ISTITUZIONI SOLIDE

---