UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Laboratory: Bitcoin, Crypto-assets and Blockchain

2223-E1803M-EXT-LABBIT

Learning objectives

The course is about bitcoin, crypto-assets, and the associated blockchain technology.

Game theory, computer science (distributed systems, distributed consensus), and monetary theory elements are examined in the attempt to properly convey the interdisciplinarity of the topics and appreciate their relevance.

Contents

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

Detailed program

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

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, and politics.

Teaching methods

Slide based lessons with associated bibliography

Assessment methods

Multi-choice question test

Textbooks and Reading Materials

Ferdinando M. Ametrano,
“Bitcoin: oro digitale, finanza e tulipani”,
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

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

Semester

March 8 - May 10 2023

Teaching language

English

Sustainable Development Goals

PEACE, JUSTICE AND STRONG INSTITUTIONS