



## Course Syllabus

<b>Course Code</b>	<b>Course Title</b>	<b>ECTS Credits</b>
BLOC-521	Digital Currency Programming	10
<b>Prerequisites</b>	<b>Department</b>	<b>Semester</b>
BLOC-512, BLOC-514 Programming experience	Digital Innovation	Fall/Spring
<b>Type of Course</b>	<b>Field</b>	<b>Language of Instruction</b>
Elective	Computer Science	English
<b>Level of Course</b>	<b>Lecturer(s)</b>	<b>Year of Study</b>
2 <sup>nd</sup> Cycle	Dr. Konstantinos Karasavvas	2 <sup>nd</sup>
<b>Mode of Delivery</b>	<b>Work Placement</b>	<b>Corequisites</b>
Face to face	N/A	N/A

### Course Objectives:

The main objectives of the course are to:

- Explain how bitcoin works, from when a transaction is created to when it is considered part of the blockchain
- Describe private and public keys as well as the different types of addresses and how exactly they are constructed and used
- Introduce the students to the Bitcoin Script language including developing different type of scripts using both a node's CLI as well as using Python.
- Demonstrate advanced scripting and how it can be used to handle several real-world use cases with code examples
- Expose students to the P2P network, how it operates, the different kinds of potential network forks and explain the Bitcoin's network mechanisms for maintaining and upgrading
- Expose students to advanced topics like Atomic Swaps, Hashlocks, Payment Channels and more
- Discuss promising state of the art feature development

## Learning Outcomes:

After completion of the course students are expected to be able to:

- Interpret the technology components of Bitcoin and how it really works behind-the-scenes
- Explain in detail how keys and addresses work on Bitcoin
- Develop scripts using the Bitcoin Script language and have a deep understanding of the provided API
- Develop programs using Python (the rational is the same of any programming language) to create Bitcoin scripts and interact with Bitcoin nodes
- Explain how the Bitcoin P2P network operates and how it can evolve (upgrading mechanisms)
- Explain advanced blockchain topics like Atomic Swaps, Payment Channels, Lightning Network
- Be aware of challenges and future development on the Bitcoin network (applicable in other blockchains)

## Course Content:

1. How Bitcoin works
  - a. Introduce transactions and how they are propagated
  - b. Explain how transactions form blocks
  - c. Deconstruct a block and its header and explain in detail how mining works
  - d. Demonstrate how Nakamoto consensus works and explain why previous distributed consensus algorithms were insufficient
  - e. Describe the development environment and interact with a node with examples
2. Keys and Addresses
  - a. Remind basic cryptographic primitives
  - b. Explain in detail and demonstrate how private keys, public keys and addresses are generated
  - c. Explain different types of wallets
  - d. Describe HD wallets in detail while demonstrating the benefits with real-world scenarios
  - e. Create keys and addresses using a node and programmatically
  - f. Describe payment BIPs

3. Scripting
  - a. Explain transactions in detail
  - b. Introduce Script and important opcodes
  - c. Go through details on how to create scripts
  - d. Dissect P2PKH and P2SH transaction types with examples
  - e. Examine several ways to create transactions
4. Advanced Scripting
  - a. Introduce multi-signature transactions
  - b. Describe direct and indirect ways to store data on the blockchain
  - c. Explain different types of timelock transactions with examples
  - d. Explain the Segregated Witness upgrade and how it is implemented as well as native and nested segwit transactions
  - e. Describe other network features like RBF and CFPF
5. Bitcoin Networks
  - a. Introduce the P2P network and how it operates
  - b. Explain what are soft- and hard-forks and demonstrate with examples
  - c. Describe the process of how the network is upgraded
  - d. Explain the concept of time on the network
  - e. Discuss how to talk directly at the P2P network level
6. Advanced Topics
  - a. More Scripting (Atomic Swaps, Hashlocks, Payment Channels)
  - b. Describe Lightning Network
  - c. Discussion of state of art (in development) topics

### **Learning Activities and Teaching Methods:**

Teaching material including presentations with extended descriptions and explanations, asynchronous video presentations, additional readings (journal articles and e-books), access to additional videos related to the course, synchronous meetings (Engageli), forums, interactive activities and chats.

**Assessment Methods:**
**Formative Assessments (not graded)**

Each session there will be several self-assessment exercises. These assessments are not graded but students will be encouraged to solve them, participate and discuss in the forums.

**Formative Assessments (graded)**

Regular interactive activities such as quizzes: Total 12 quizzes (one per session) containing 10 interactive questions related to the session's material. These activities, collectively, count towards 12% of the final grade.

1 Assignment after session 6 containing a programming exercise. The students have 3 weeks to submit their programs, which will count towards 28% of the final grade. Throughout this period the assignment is discussed via the forums to clarify and/or stir the students towards the right direction. Extensive feedback will be provided for the assignment to help them consolidate the material.

**Summative Assessments**

Final exam (3 hours): A minimum score of 60% is required to successfully complete the course.

**Required Textbooks / Readings:**

Title	Author(s)	Publisher	Year	ISBN
Mastering Bitcoin	Andreas Antonopoulos	O'Reilly Also Online	2017	978-1491954386 <a href="https://github.com/bitcoinbook/bitcoinbook">https://github.com/bitcoinbook/bitcoinbook</a>

**Recommended Textbooks / Readings:**

Title	Author(s)	Publisher	Year	ISBN
Programming Bitcoin	Jimmy Song	O' Reilly	2019	978-1492031499
The Science of the Blockchain	Roger Wattenhofer	CreateSpace Independent Publishing Platform	2016	978-1522751830

Other resources:

1. How does Bitcoin work? - <https://learnmeabitcoin.com/>
2. Learn Bitcoin from the command line - <https://github.com/ChristopherA/Learning-Bitcoin-from-the-Command-Line>
3. <https://www.lopp.net/bitcoin-information.html>