UNIVERSITY of NICOSIA

Course Syllabus

Course Code	Course Title	ECTS Credits
COMP-537DL	Digital Currencies	10
Prerequisites	**Department**	**Semester**
COMP-514DL, COMP-515DL	Computer Science	Spring
Type of Course	**Field**	**Language of Instruction**
Required for Blockchain Technologies concentration	Computer Science	English
Level of Course	**Lecturer(s)**	**Year of Study**
2nd Cycle	Dr Harald Gjermundrød Dr Dmitry Apraksin	1st
Mode of Delivery	**Work Placement**	**Corequisites**
Distance Learning	N/A	None

Course Objectives:

The main objective of this course are to:

- provide a deep understanding of decentralized digital currencies and the underlying blockchain technology
- cover in detail the underlying cryptographic technologies which are used in order to devise a blockchain framework
- provide deep knowledge of the architecture of the bitcoin system, including the data structure used for the bitcoin blockchain
- provide deep knowledge of mining in blockchain infrastructures by comparing the different roles, contributions, and motivations of the entities involved in maintaining the consistency of the decentralized ledger.
- expose the students to the Bitcoin Script language including developing different type of scripts using the provided API.
- compare and contrast the different wallets types that are available for the bitcoin system with respect to security, privacy, and convenience to the user.
- make students aware of various deployment scalability issues related to the bitcoin system, and different proposed approaches and experiments of haw to address them.

Learning Outcomes:

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

1. understand the technology components of blockchain-based digital currencies, the process of currency issuance, proof-of-work, consensus and distributed ledger
2. understand the underlying cryptographic technology utilized in blockchain-based digital currencies
3. explain in detail the architecture and the data structure of the bitcoin digital currency
4. critically compare and evaluate different approaches/implementations of digital currencies
5. critically assess the importance of the miners in blockchain deployments and their motives
6. compare and contrast the different categories of miners
7. develop scripts using the Bitcoin Script language and have a deep understanding of the provided API
8. demonstrate an understanding of the different digital currency wallet types and be able to conduct transactions using different types of wallets
9. be aware of problems and challenges in blockchain deployments, especially with relation to scalability issues, and have a deep understanding of the different tradeoffs that proposed solutions entails.

Course Content:

1. Introduction to digital currencies and blockchain technology
   a) Basic description of digital currency and blockchain technology
   b) History of digital currency
   c) Transactions in digital currencies
2. Cryptographic technologies used in digital currencies systems
   a) Hashing algorithms
   b) Digital signatures
   c) Asymmetric cryptographic techniques
3. Bitcoin network architecture
   a) Distributed consensus
   b) Proof-of-Work (PoW)
   c) Data structure of the bitcoin blockchain
   d) Operation on the bitcoin blockchain
4. Blockchain verification and consensus, i.e. mining
   a) Role of the different nodes in a blockchain deployment
   b) Full nodes vs. SPV (Simplified Payment Verification) nodes
   c) Mining economics
5. The Bitcoin Script language
   a) Introduction to the Bitcoin Script language
   b) Script writing and execution
6. Bitcoin wallets
   a) Different types of wallets
   b) Security implications of the different type of wallets

7. Blockchain deployment scalability issues
   a) Mining pools
   b) Centralization
   c) Types of attacks
   d) Bitcoin Improvement Proposal (BIP)
   e) Segregated Witness Benefits (SegWit)

Learning Activities and Teaching Methods:

Lectures, Practical Exercises, and Projects.

Assessment Methods:

Projects, Exercises, Quizzes, Final Exam.

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Mastering Bitcoin	Andreas Antonopoulos	O'Reilly Publishing	2014	978-1-4493-7404-4
Bitcoin: A Peer-to-Peer Electronic Cash System	Satoshi Nakamoto	Online	2009	https://bitcoin.org/bitcoin.pdf

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction	A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder	Princeton University Press	2016	978-0691171692

The Science of the Blockchain	Roger Wattenhofer	CreateSpace Independent Publishing Platform	2016	978-1522751830

Other resources:

1. Bitcoin Protocol Specifications (https://en.bitcoin.it/wiki/Protocol_specification)
2. Bitcoin transaction Scripting (https://en.bitcoin.it/wiki/Script)
3. Majority is not Enough: Bitcoin Mining is Vulnerable (http://arxiv.org/abs/1311.0243)
4. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin (http://eprint.iacr.org/2012/248.pdf)