UNIVERSITY of NICOSIA

Course Syllabus

Course Code	**Course Title**	**ECTS Credits**
COMP-541	Digital Currency Programming	10
Prerequisites	**Department**	**Semester**
DFIN-511, DFIN-524	Computer Science	Fall
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 Konstantinos Karasavvas	1st or 2nd
Mode of Delivery	**Work Placement**	**Co-requisites**
Distance Learning	N/A	None

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

•thoroughly explain private and public keys as well as addresses and how exactly they are constructed and used

•expose the students to the Bitcoin Script language including developing different type of scripts using the provided API.

•expose students to the different kinds of forking and explain the Bitcoin's network mechanisms for maintaining and upgrading

•decompose a blockchain system's fundamental components, how they fit together and examine a modular blockchain system in more detail

•demonstrate advanced scripting and how it can be used to handle several real-world use cases with code examples

•provide a thorough understanding of smart contracts, their technical capabilities, practical applications, limitations and security constraints they operate within

•explain to students both fundamental and implied differences between Ethereum and Bitcoin protocol by covering historical, conceptual and architectural distinctions

•provide a detailed covering of the most prominent smart contract platform Ethereum and expose students to its main programming language Solidity

•raise awareness of the delicate nature of smart contracts programming, examining emerging practices for assuring the quality of decentralized applications, code patterns and security considerations

•expose students to various development environments and different approaches of managing smart contracts throughout their lifecycle.

Learning Outcomes:

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

- understand the technology components of Bitcoin and how it really works behind-the-scenes.
- explain in detail how keys and addresses work on Bitcoin
- explain in detail the architecture and the data structures of Bitcoin
- develop scripts using the Bitcoin Script language and have a deep understanding of the provided API
- create programs using several libraries to access Bitcoin nodes
- understand forking and the way the Bitcoin network evolves
- understand the architectural components of a blockchain system
- understand the inner workings of smart contracts as means for developing decentralized applications
- evaluate the multifaceted differences between specialized digital currency platforms and general purpose blockchains by comparing Bitcoin and Ethereum protocols
- understand the details of interactions between the enclosed smart contract network and the external world, be aware of further implications these interactions pose to the aspect of decentralization
- establishing deep understanding of the Ethereum model, its consensus model, code execution, operation of its network, storage options and main actors that participate on its protocol
- demonstrate developing smart contracts in Solidity for Ethereum protocol and be aware of different approaches to developing decentralized applications

Course Content:

1. The story of a transaction
a) From Transactions to Blocks
b) Blocks and Distributed Consensus
c) Basic interaction with a Bitcoin node
2. Keys and Addresses
a) Basic cryptography
b) From private keys to addresses
3. The Bitcoin Script language
a) Introduction to the Bitcoin Script language
b) Script writing and execution

c) Advanced scripting
d) Tools and libraries to access Bitcoin’s API and scripting capabilities
4. Blockchain deployment
a) Mining and forking
b) Upgrading the network
c) Related BIPsd) Segregated Witness (SegWit)
5. Blockchain architectures
a) Abstract Architecture
b) Ways to dive deeper
c) Introduction to major blockchain platforms
6. Smart contracts and Ethereum
a) Technical introduction to smart contracts
b) Ethereum overview
c) Web3 proposition for a decentralized internet
d) Using Ethereum sub-protocols, storage and ways of interacting with the external world
7. Comparing Bitcoin and Ethereum
a) Historical comparison
b) Conceptual distinction between a payment system and a decentralized applications platform
c) Differences in their architectures from security-first aspect to a rich feature set
d) Future roadmap for them, following their own paths with probable interconnections
8. Development environment
a) Multitude of clients in Ethereum
b) Production and test networks in Ethereum
c) Public, private and development deployments
9. Contract code walk-through
a) Demonstration of smart contract
b) Introduction to Solidity
c) Contract lifecycle
10. Solidity in depth
a) Building blocks
b) Popular contracts already in deployment
11. Considerations for production deployment
a) Quality of decentralized applications
b) Code patterns
c) Security
d) Other smart contract platforms
e) Discussion of future prospects

Learning Activities and Teaching Methods:

Lectures, Practical Exercises, and Projects

Assessment Methods:

Final exam, Project (individual programming), assignments

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Mastering Bitcoin	Andreas Antonopoulos	O’Reilly Publishing	2014	978-0691171692
Bitcoin: A Peer-toPeer Electronic Cash System	Satoshi Nakamoto	Online	2009	https://bitcoin.org/bitcoin.pdf
Ethereum White Paper	Vitalik Buterin	Online	2017	https://github.com/ethereum/wiki/wiki/WhitePaper

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	2016	9780691171692
The Science of the Blockchain	Roger Wattenhofer	CreateSpace Independent Publishing Platform	2016	9781522751830

Other resources:

- Bitcoin Protocol Specifications (https://en.bitcoin.it/wiki/Protocol_specification)
- Bitcoin transaction Scripting (https://en.bitcoin.it/wiki/Script)
- Majority is not Enough: Bitcoin Mining is Vulnerable (http://arxiv.org/abs/1311.0243)
- Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin (http://eprint.iacr.org/2012/248.pdf)
- Ethereum documentation (http://www.ethdocs.org/en/latest)
- Solidity documentation ((https://solidity.readthedocs.io/en/develop))