UNIVERSITY of NICOSIA

Course Syllabus

Course Code	Course Title	ECTS Credits
BLOC-514	Emerging Topics in Blockchain and Digital Currency	10
Prerequisites	**Department**	**Semester**
N/A	Digital Innovation	Fall/Spring
Type of Course	**Field**	**Language of Instruction**
Required	Blockchains and Information Systems	English
Level of Course	**Lecturer(s)**	**Year of Study**
2nd Cycle	Dr. Elias Iosif	2nd
Mode of Delivery	**Work Placement**	**Corequisites**
Face to face	N/A	N/A

Course Objectives:

The main objective of this course is to provide students with a conceptual framework and applied competencies that will assist them explain, apply, assess and manage blockchain-based systems and resources supporting the implementation or utilization of digital currencies as well as other decentralized applications. Those topics will be presented within the context of the latest advances in the field of blockchain technologies. The course is structured around three broad sections:

1. Bitcoin blockchain: technological aspects of the most widely used blockchain (i.e., Bitcoin blockchain) with particular reference and use of the latest release of the Bitcoin Core;
2. Advances in core technological aspects of blockchains: network security and anonymity, scalability and interoperability, forks and consensus mechanisms;
3. Emerging decentralized applications and other related technological areas: indicative use cases of emerging applications (prediction markets and exchanges) along with related issues (e.g., digital identities), as well as the relation of blockchains with Internet-of-Things and Artificial Intelligence in conjunction with their application for societal good.

Learning Outcomes:

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

- Interpret and use the Bitcoin Core for a number of applications that go beyond the two-parties transactions;

- Compare, critically assess and evaluate different blockchain systems;
- Explain and analyze fundamental mechanisms of blockchain systems including consensus and forks;
- Critically assess blockchain implementations in terms of network security and anonymity;
- Outline technological challenges such as scalability and interoperability;
- Assess and acquire knowledge on decentralized applications based on blockchains and critically assess the respective services towards the broader challenge of Decentralized Autonomous Organizations (DAOs);
- Identify technologies that can be combined with blockchains (e.g., Internet-of-Things and Artificial Intelligence) in combination with their high-level integration;
- Identify and analyze use cases where the application of blockchains exhibits a positive societal contribution.Understand and analyze fundamental mechanisms of blockchain systems including consensus and forks
- Critically assess blockchain implementations in terms of network security and anonymity
- Explain technological challenges such as scalability and interoperability
- Assess and acquire knowledge on decentralized applications based on blockchains and critically assess the respective services towards the broader challenge of Decentralized Autonomous Organizations (DAOs)
- Identify technologies that can be combined with blockchains (e.g., Internet-of-Things and Artificial Intelligence) in combination with their high-level integration
- Identify and analyze use cases where the application of blockchains exhibits a positive societal contribution.

Course Content:

1. Emerging topics in Bitcoin Script and Bitcoin Core
2. Network protection
3. Anonymity and fungibility
4. Bitcoin scalability: Lightning network
5. Ethereum scalability: sharding
6. Forks
7. Consensus mechanisms
8. Blockchain interoperability
9. Self-sovereign identities
10. Decentralized markets and Decentralized Autonomous Organizations (DAOs)
11. How blockchain can contribute to the advancement of Artificial Intelligence, Intelligence Augmentation
12. Societal implications of blockchain technologies (e.g., human trafficking, human rights)

Learning Activities and Teaching Methods:

Teaching material including PowerPoint (PPT) presentations with extended descriptions and explanations, asynchronous video presentations, additional readings (journal articles and/or e-books), access to additional videos related to the course, synchronous meetings (Engageli), forums, chats, case studies and other formative and summative assessments.

Assessment Methods:

Formative Self-Assessment (not graded)

A number of formative self-assessment questions (not graded) will be provided during each lecture. An indicative sample is provided in the last part of this Guide along with the respective answers.

Summative Assessments

Assignment: 16%

Short summative activities: 12 sessions x 2% = 24%. Overall, the short summative activities are designed to exhibit a clear interactive character. In total, four different approaches are utilized for this purpose as follows:

Interactive discussions during the class

Interactive use of command line tools (including simulators) or related computational tools

Interactive quiz (questions)

Interactive use of wiki for sharing content developed by students.

For each session, the specific combination of the above approaches is reported in the respective section of this guide.

Final exam, assessed out of 100, 60% of the total mark.

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
"Mastering Bitcoin: Programming the Open Blockchain". 2nd Edition	Andreas M. Antonopoulos	Sebastopol: O'Reilly Media	2017	

“Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”	Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder	Princeton University Press	2016	
“Bitcoin and Blockchain Security”	Ghassan Karame and Elli Audroulaki	Artech House, Inc., Norwood, MA, USA	2016	

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
“Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security	Gennaro, R., Goldfeder, S., and Narayanan, A	In Proc. of International Conference on Applied Cryptography and Network Security (pp. 156-174). Springer, Cham	2016	

Selected Online Readings:

Mauro Conti, Sandeep Kumar E, Chhagan Lal and Sushmita Ruj (2017). “A survey on security and privacy issues of bitcoin” arXiv preprint [URL: https://arxiv.org/pdf/1706.00916.pdf]

Kyle Croman et al. (2016). “On Scaling Decentralized Blockchains” [URL: http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf]

Joseph Poon and Thaddeus Dryja (2016). “The Bitcoin Lightning Network”

Shaan Ray (2017). “Blockchain Forks” [URL: https://hackernoon.com/blockchain-forks-b0dca84db0b0]

Vaibhav Saini (2018). “ConsensusPedia: An Encyclopedia of 30 Consensus Algorithms A complete list of all consensus algorithms”. [URL: https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f]

Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra,Jorge Timón, and Pieter Wuille (2014). “Enabling Blockchain Innovations with

Pegged Sidechains» [URL: http://kevinriggen.com/files/sidechains.pdf]

Vitalik Buterin (2016). “Chain Interoperability” [URL: http://www.r3cev.com/s/Chain-Interoperability-8g6f.pdf]

“The Inevitable Rise of Self-Sovereign Identity”, (2017). A white paper from the Sovrin Foundation [URL: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf)]

Koutroumpis Pantelis, Aija Leiponen, and Llewellyn DW Thomas (2017) “The (Unfulfilled) Potential of Data Marketplaces”. No. 53. The Research Institute of the Finnish Economy [URL: https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-53.pdf)]

Chrisjan Pauw (2018). “Prediction Markets, Explained” [URL: https://cointelegraph.com/explained/prediction-markets-explained]

Jon Buck (2017). “Blockchain Oracles, Explained” [URL: https://cointelegraph.com/explained/blockchain-oracles-explained]

S. Makridakis, A. Polemitis, G. Giaglis and S. Louca (2018). “Blockchain: The Next Breakthrough in the Rapid Progress of AI”, Robotics & Automation Engineering Journal [URL: https://juniperpublishers.com/raej/pdf/RAEJ.MS.ID.555592.pdf]

Massimo Bartoletti and Livio Pompianu (2017). “An analysis of Bitcoin OP_RETUR metadata” (https://arxiv.org/pdf/1702.01024.pdf)

Philipp Frauenthaler, Michael Borkowski, and Stefan Schulte (2019). “A Framework for Blockchain Interoperability and Runtime Selection”. arXiv preprint arXiv:1905.07014 (https://arxiv.org/abs/1905.07014)

Marinos Themistocleous, Kypros Stefanou, Christos Megapanos, and Elias Iosif (2018). “To Chain or Not to Chain? A Case from Energy Sector”. In European, Mediterranean, and Middle Eastern Conference on Information Systems, pp. 31-37. Springer, Cham, 2018.