Course Name: Introduction to Cryptocurrencies and Blockchain Technology

1. Introduction

The course is designed while keeping in view the sociotechnical domain of blockchain technology and its applicability in different disciplines such as finance, commerce, computer science, ICT, cryptography, distributed systems, cybersecurity, systems scalability, new innovative business models and start-up culture and so on. The objective of the course is to prepare students, Ph.D. candidates and professionals/teacher benefiting from their diverse and broad backgrounds and to provide a holistic analysis of blockchain technology, smart contracts, and digital currency systems, applications, and services. Moreover, the course is also prepared to develop a solid understanding of abstracting the essential structure, recognizing the sources of uncertainty, and applying appropriate state of art models and technical tools from blockchain environment to develop different solutions for the market.

2. Target Audience

The course is designed specifically for early career academic staff and teacher in training centres, K12 and vocational schools, who are going to teach "Blockchain technology or integrate topics.

3. Pre-requisite

Participants of this course are required general teaching skills, basic computer skills and basic English language knowledge.

4. Course Length, Hours

The course is designed for 3ECTS ~ 84 hours and will be delivered online completely. This will include pre-recorded lecture videos as well as practical and activity sessions.

5. Course Content

The following resource contains all the essential information your need to know for this course. Course content has been organized in 10 modules, which are:

Module 1: Blockchain and Consensus

Learning Outcomes

The students will learn about centralized, distributed and probabilistic consensus algorithms. They will understand why traditional, deterministic algorithms are not feasible for large scale networks and will understand the need for additional conceptual extensions for a scalable consensus. They will obtain a basic and conceptual understanding of how cryptocurrency technologies can overcome these limitations and how consensus is the core computational primitive at the root of Bitcoin, Ethereum, IOTA and other recent developments.

Content

- Deterministic consensus algorithms.
- Limitations from complexity and Brewer's theorem.
- The gist of the Nakamoto Bitcoin and of the Popov Tangle White Paper
- Advanced consensus technologies

- Concepts of blockchains, proof-of-work, and tangle

Suggested Reading

- Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System
- Serguei Popov, The Tangle.
- Shreya Agrawal, Khuzaima Daudjee: A Performance Comparison of Algorithms for Byzantine Agreement in Distributed Algorithms
- Leslie Lamport, Robert Shostak, Marshall Pease: The Byzantine Generals Problem
- Seth Gilbert, Nancy Lynch: Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services

Module 2: Basics of Smart Contracts and Creation of New Tokens

Learning Outcomes

The students will learn about the underlying principles that are required to create blockchain-based smart contracts. They will understand why such smart contracts are better than currently prevalent means of creating contracts and to create exemplary smart contracts for various applications, especially those that involve machine-to-machine and IoT based communication.

Moreover, with the rising popularity of ICOs, the students will learn how new tokens can be created on the Ethereum ecosystem. As a result of this course, the students will be equipped to evaluate as well as create smart contracts for a wide range of use-scenarios and create their own tokens when required.

Content

- Smart Contracts Basics
- Establishing Our Own Private Ethereum Network
- Smart Contracts on Solidity
- Creation of new tokens using ERC20.
- Analysis of Use Case Feasibility

Suggested Reading

- Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System Dmitry Khovratovich et al.: SecureToken Development and Deployment
- K Delmolino et al.: Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab.
- K Christidis et al.: Blockchains and smart contracts for the internet of things
- GW Peters et al.: Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money.

Module 3: Initial Coin Offerings (ICOs) – Crowdfunding on the Blockchain

Learning Outcomes

This module focuses on so-called initial coin offerings (ICOs) – a novel approach for crowdfunding of blockchain start-ups. The students will learn and understand the disadvantages of existing funding approaches and the advantages and challenges of ICOs as an alternative finance instrument. Furthermore, different strategies on how to conduct an ICO as well as analyses of successful and failed real-world ICOs will be conducted. As a result of this course, the students will obtain an understanding of the basic concepts of ICOs, issues of different conceptual approaches to ICOs as well as the advantages of blockchain-based solutions.

Content

- Traditional start-up funding approaches

- Fundamentals of ICOs
- Different strategies and approaches to conduct an ICO.
- Create your own token on the blockchain.
- Analyses of successful and failed ICOs

Suggested Reading

- Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System
- Gavin Wood: Ethereum: A Secure Decentralised Generalised Transaction Ledger
- Christian Catalini, Joshua S. Gans: Initial Coin Offerings and the Value of Crypto Tokens
- John P. Conley: blockchain and the Economics of Cryptotokens and Initial Coin Offerings

Module 4: Blockchain and the Law

Learning Outcomes

The students will learn about the legal implications of blockchain based transactions, reaching from controversies about the forming of contracts (declaration of intent), accountability, representation, and liability for non-performance. Students will obtain basic skills and knowledge to identify legal requirements to be considered when setting up blockchain based transaction systems, and they will gain awareness of liability risks and provided procedural measures to cope with them.

Content

- Formation of contracts in civil law and common law systems
- A mistake in contract contents and its impact
- Non-performance of contracts and legal remedies
- Interpretation of blockchain-generated contracts under European private law
- Smart contracts and restricted legal capacity
- Outlook: Accountability challenges of contracts concluded by autonomous systems

Suggested Reading

Primavera De Filippi, Aaron Wright: blockchain and the Law, Harvard University Press 2018, ISBN 9780674976429

Module 5: Authentication and Digital Identities on the Blockchain

Learning Outcomes

This module focuses on digital identities and blockchain-based authentication solutions. The students will learn and understand the challenges of digital identities and issues of existing (de)centralized authentication and identity solutions. As a result of this module, the students will obtain an understanding of the basic concepts of digital identities, issues of different conceptual approaches to digital identities as well as the advantages of blockchain-based solutions.

Content

- Digital Identities
- Challenges and limitations of digital identities
- Existing (de)centralized authentication systems and their limitations
- (Self-Sovereign) blockchain-based Identity solutions

Suggested Reading

- Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System
- Christian Lundkvist: uPort: A Platform for Self-Sovereign Identity
- Guy Zyskind: Decentralizing Privacy: Using Blockchain to Protect Personal Data

- Guy Zyskind: Enigma: Decentralized Computation Platform with Guaranteed Privacy
- Authcoin

Module 6: Business Process Management (BPM) and Blockchain

Learning Outcomes

The students will get essential concepts of business process management and the way how they can be supported by blockchain concepts. The focus of the module is the concepts of business process management and their blockchain support. The goal is to enable students to specify business processes with BPM and to translate them into blockchain concepts.

Content

- Essentials of business process management
- Modelling business processes with BPMN
- Business process management systems
- Blockchain support of business processes

Suggested Reading

Dumas, La Rosa, Mendling, Reijers: Fundamentals of business process management. 2nd Edition, 2018.

Module 7: Blockchain and Privacy

Learning Outcomes

The privacy of blockchain participants and the confidentiality of on-chain data are an underestimated problem in most current blockchain implementations. If not addressed properly, many proofs-of-concepts will not have the possibility to mature into production. Legacy blockchain implementations like Bitcoin rely on all the transaction data being stored in plain text on the blockchain for them to be validated by the network. This module will highlight the false promises of pseudo anonymity, why most current blockchains offer the opposite of privacy and current solutions to the identified problems.

Content

- Off-chain storage, sidechains, state channels (lightning, perun, raiden, ...)
- Address deriving schemes.
- 1-time payment addresses
- Stealth addresses
- zk-SNARKs
- Mixing

Suggested Reading

- Vitalik Buterin: Privacy on the blockchain (Ethereum Blog)
- Ahed Kosba et al.: Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts
- Guy Zyskind et al.: Enigma: Decentralized Computation Platform with Guaranteed Privacy
- Ian Miers et al.: Zerocoin: Anonymous Distributed ECash from Bitcoin
- R3 research: Survey of Confidentiality and Privacy-Preserving Technologies for Blockchains
- CryptoNote Whitepaper (now Monero, uses Ring Signatures forPrivacy)

Module 8: Advanced Module on Smart Contracts

Learning Outcomes

The students will learn about the state of the art in three specific aspects pertaining to smart contracts.

First, the students will learn about problems of oligopoly formation in proof-of-stake formation and mitigation with the use of mobile smart contracts. Next, the current state of the art of smart-contract languages with their pros and cons will be explored. Finally, we move from intra-organizational smart contracts to cross-organizational smart contracts and explore how an additional multi-agent system layer on top of smart-contracts helps to facilitate collaboration.

Content

- Proof of stake problems and mobile smart contracts
- Pros and cons of currently existing smart-contract languages
- Cross-organizational collaboration models for legally relevant smart contracts
- Multi-agent-systems to facilitate cross-organizational smart contracts collaboration.
- Advanced cross-organizational topics such as conflict management, e-governance, rollbacks of collaborations.

Suggested Reading

The students will get a list of specific research papers for each topic.

Module 9: Legally Intended Smart Contracts

Learning Outcomes

The students shall understand the interaction between law and the design of legally intended smart contracts. The students will learn about design challenges, pattern and modelling tools.
The focus of this module in on teaching the complexity of understanding legal terms and transferring them into code considering legal frameworks. The goal is to understand the need for close cooperation with lawyers to write correct legal code. Additionally, the student shall learn about modelling techniques and tools for legally binding code.

Content

- Introduction into basic legal terminology and processes by the example of a simple sales and delivery contract
- Development of legal primitives (atomic elements) and transfer into programmable objects; learning using modelling tools.
- Analysis of an existing legally binding smart contract regarding the elements above
- Design of a new (simple) legally binding smart contract

Suggested Reading

- Grigg, I.: The ricardian contract. In Proceedings of the First IEEE International Workshop on Electronic Contracting, pages 25–31. IEEE, 2004.
- Grigg, I.: On the intersection of ricardian and smart contracts, 2015.
- C. D. Clack, V. A. Bakshi, und L. Braine, “Smart Contract Templates: essential requirements and design options”, 2016.
- R3 and Norton Rose Fulbright. Can smart contracts be legally binding contracts? 2016.

Module 10: Blockchain: A Decentralized Political Technology

Learning Outcomes

This module focuses on explaining the origin and original use of Blockchain. The students will understand and argument if blockchain originates in Political economy.

Content

- (Austrian) Economics

- (Private) Law
- (Voluntary) Governance
- Two Methodology: Trivium & Deconstructivism

Suggested Reading/Material

- X3 Early Coin white papers
- X3 Foundational documents
- X3 Austrian Economic texts
- Watch three Videos (Argon+ Friedman+Seasteads)

6. Course Duration

The course has been setup as self-paced course. This means that participants have the full responsibility of their progress, thus the course is flexible within a wide time frame. The time you need to complete this course has been estimated to 84 hours, and you have 2 months from your registration to complete the course. This includes mandatory reading material and activity.

7. Course Assessment

Each week contains a mandatory reading activity.

To move on to the next Module, you need to complete the reading activity. Upon the successful completion of each module a small badge will be automatically awarded to you.

Having successfully completed all the 10 modules, you will be allowed to download your certificate, as well as the course badge.

Communication within the Course

Although the course is self-paced you may feel the need to communicate with teachers or your peers. That is why the two following forums are offered. The Announcements is only for teachers' announcements, while the Coffee Shop is the forum you may use to reach your peers or teachers.

Announcements Forum (News forum)

Your teachers may use this forum to share general news and announcements regarding the course. Posts created in this forum are also automatically sent to your inbox.

Coffee Shop Forum (Forum)

Feel free to use this forum to reach your peers or teachers. You may use it to share a quick introduction of you, ask a query, or share a story!