

Module	Blockchain and Consensus
Lecturer	Prof. Dr. rer. nat. Clemens H. Cap
Language	English
Teaching Method:	Lecture
Credit Points / Duration	0.25 ECTS / 4 Lectures of 90 minutes each
Attendance Requirements	Basics in computer science and mathematics; Some background in distributed algorithms is helpful
Goals / Skills:	<p>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.</p> <p>They will obtain a basic and conceptual understanding 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.</p>
Content	<ul style="list-style-type: none"> • 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
Media Used	Electronic presentation, blackboard illustrations, discussion, practical demonstrations
Suggested Reading	<ul style="list-style-type: none"> • 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