Module	**Blockchain and Privacy**
Lecturer	Dipl.-Math. Sebastian Stammler
Language	English
Teaching Method	Lecture + Tutorial
Credit Points / Duration	0.25 ECTS / 4 Lectures of 90 minutes each
Attendance Requirements	Basics in computer science, mathematics and blockchain; A background in cryptography is helpful.
Goals / Skills	The privacy of blockchain participants and confidentiality of on-chain data are an underestimated problem in most current blockchain implementations. If not addressed properly, many proof-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 lecture will highlight the false promises of pseudonymity, why most current blockchains offer the opposite of privacy and current solutions to the identified problems.
Content	• Off-chain storage, side-chains, state channels (lightning, perun, raiden, ...) • Address deriving schemes • 1-time payment addresses • stealth addresses • zk-SNARKs • mixing
Media Used	Electronic presentation, blackboard illustrations, discussion, practical exercises
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 E-Cash from Bitcoin • R3 research: Survey of Confidentiality and Privacy Preserving Technologies for Blockchains • CryptoNote Whitepaper (now Monero, uses Ring Signatures for Privacy)