

I.BA_MOVK_MM – Kryptographie

Übung: Blockcahin

Dr. Ladan Pooyan-Weihs

Semesterwoche 13

Aufgabe 1: Blockchain

Erläutern Sie, inwiefern die dezentrale Architektur des Blockchain-Netzwerkes zu dessen Sicherheit beiträgt.

Aufgabe 2: Elektronische Zahlungsverkehr

Woran unterscheidet sich E-Bargeld von Bitcoin? Nennen Sie mindestens 2 Punkte und begründen Sie Ihre Antwort.

Aufgabe 3: Bitcoin

Nennen Sie die verwendeten kryptographischen Elemente für Bitcoin und beschreiben Sie welche Funktionen sie erfüllen?

- a) Erläutern Sie, wie das Problem *double-spending* für Bitcoin gelöst wird?
- b) Wie beurteilen Sie die ökologischen Aspekte in Bezug auf Energieverbrauch für Mining?
- c) Was passiert im Jahre 2141, wenn kein Bitcoin mehr im Lauf gebracht wird?
- d) Wie sicher ist Bitcoin gegen Cyberattacken? Kann Bitcoin verloren gehen?

Aufgabe 4: Transaktion im Bitcoin-Netzwerk

Warum wird der Hash-Wert des öffentlichen Schlüssels einer Teilnehmerin als der Adressname des eigenen Computers genutzt?

Viel Vergnügen!