
- Master-/Bachelorarbeit -
**Zahlungsströme als komplexes
Netzwerk in Bitcoin**



Bitcoin (<http://www.bitcoin.org>) ist eine P2P-Währung, die durch eine OpenSource-Software-Infrastruktur versucht, alternative Bezahlmethoden zu etablieren. Als technische Lösung kommt eine dezentrale Datenbank aller Transaktionen zum Einsatz, die getätigt wurden und durch die Teilnehmer „zertifiziert“ werden (durch ein sog. proof-of-work Konzept).

Es sollen in zwei M.Sc./B.Sc.-Projekten folgende Fragen beantwortet werden (Projekte sind je nach Aufwand als Master- oder Bachelor-Arbeiten auslegbar):

1. Data Mining on Transactions

Alle Transaktionen formen einen (bipartiten) Graphen. Dieser kann rekonstruiert werden aus den „signierten“ proof-of-work Daten bzw. durch einen crawler, der online als Client-Ersatz am bitcoin-Netzwerk teilnimmt und mitprotokolliert, welche Ereignisse auftreten. Es soll in diesem Projekt ein Crawler programmiert werden, der die Zeitreihen von Transaktionen und den Transfer der Daten an die Mitglieder des P2P-Netzwerks ermittelt und in gängigen Datenformaten erfasst (PostgreSQL, CSV, etc.)

2. statistische Modellierung des Zahlungsnetzwerks.

Neben der Topologie des Netzwerks (gibt es dominante „Geldgeber“? Wer kontrolliert den Zahlungsfluß? Wird tatsächlich eine zentrale Instanz vermieden?) sind vor allem potenzielle Betrugsversuche von Interesse (versucht jemand sog. double-spending, indem er den proof-of-work schneller erledigt?). Zudem kann die Dynamik der Netzwerkbildung untersucht werden, etwa, ob es wiederkehrende Zahlungsströme gibt, ob Empfänger sich eine Art Reputation aufbauen können etc.

In diesem Projekt sollen die oben erhobenen Daten mit Hilfe statistischer Modellierung und Zeitreihenanalyse einer genauen Betrachtung unterzogen werden. Kenntnisse in R und Netzwerkanalyse-Tools wären hier von Vorteil.

Kontakt: Prof. Dr. Kay Hamacher (hamacher@bio.tu-darmstadt.de)
Prof. Dr. Stefan Katzenbeisser (skatzenbeisser@acm.org)