



Technische  
Universität  
Braunschweig

Institut für Betriebssysteme  
und Rechnerverbund



## Seminar Distributed Systems

Blockchain: From Cryptocurrencies to Smart Contracts

**Signe Rüsçh**

October 25, 2017

# Table of Contents

Organisational

Topic Descriptions

# Organisational

- Course
  - Course held in German/English
- Language
  - Essay and presentation in either German or English
- Certificate Requirements
  - Essay (6 pages, double column)
  - Presentation of own topic (25min + discussion)
  - Active participation in discussions

# Procedure

- Not a single meeting with all presentations
- Two presentations each meeting
- Every Wednesday, starting November 22th, 3pm - 4:30pm
- The first two students have 4 weeks

# Procedure

## Procedure (4 Weeks)

Today Topic selection

W 1-3 Read the papers or find other work fitting the topic<sup>1</sup>

W 1-3 Write essay and create presentation

W 2 Presentation dry-run, first draft of essay

W 3 Presentation, receiving peer review of essay

W 3-4 Incorporate comments

W 4 Submission of essay & presentation slides

---

<sup>1</sup>How to read a paper, <http://dl.acm.org/citation.cfm?id=1273458>

# Requirements Presentation

- 25mins talks = approx. 25 slides
- Pictures  $\gg$  text
- Presentation best-practices
  - Title, author, page numbers on each slide
  - Corporate design TU Braunschweig
- Structure of presentation (recommendation)
  - Introduction, Motivation
  - Problem
  - Approach
  - Evaluation, Conclusion (one slide summary!)
- Templates: <https://www.ibr.cs.tu-bs.de/kb/templates.html>
- $\LaTeX$  is preferred

# Requirements Essay

- 6 pages (ACM Proceedings template)
- Structural components
  - Introduction & Motivation
  - Problem outline
  - Solutions, approaches tackling the problem
  - Evaluation
  - Conclusion, Discussion of results, Outlook
- Look at multiple papers and your papers' related work!
- Templates:  
<https://www.acm.org/publications/proceedings-template>

# Table of Contents

Organisational

Topic Descriptions



# Topic Descriptions

## What is a blockchain?

- Like a black board
- Blocks as messages containing transactions
- Strict ordering of messages
- Rule-based read permissions, global write
- No message modification



# Topics Overview

- General Introduction
  1. Introduction to Blockchain (BA)
  2. Current Blockchains: Bitcoin, Ethereum, and Hyperledger (BA)
  3. Architectures of Distributed Ledgers (BA)
  4. Smart Contracts (BA)
- Consensus Protocols:
  6. Consensus Protocols: Proof-of-Work (BA/MA)
  7. Consensus Protocols: Proof-of-Stake (BA/MA)
  8. Consensus Protocols: BFT (1) (BA/MA)
  9. Consensus Protocols: BFT (2) (MA)

## Topics Overview (2)

- Issues in Blockchains

- 10. Scalability of Blockchains (MA)
- 11. Anonymity in Cryptocurrencies (MA)
- 15. Social and Economic Impact (BA)

- Security in Blockchains

- 5. The DAO (BA)
- 12. Attacks on Blockchains (Nico) (BA/MA)
- 13. Networking and Network Attacks (Nico) (BA/MA)
- 14. Trusted Execution on Blockchain (Nico) (MA)

## Topics Overview (2)

- Issues in Blockchains
  - 10. Scalability of Blockchains (MA)
  - 11. Anonymity in Cryptocurrencies (MA)
  - 15. Social and Economic Impact (BA)
- Security in Blockchains
  - 5. The DAO (BA)
  - 12. Attacks on Blockchains (Nico) (BA/MA)
  - 13. Networking and Network Attacks (Nico) (BA/MA)
  - 14. Trusted Execution on Blockchain (Nico) (MA)

### Topic Assignment