HS19

DISTRIBUTED SYSTEMS ADVANCED & BLOCKCHAIN

Administration

T. Bocek

thomas.bocek@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

- **Module Description**

Distributed Systems Advanced & Blockchain

Kurzzeichen:	M_DSA
Durchführungszeitraum:	HS/18-HS/19
ECTS-Punkte:	4
Lernziele:	Genaue Details werden zu Semesterstart bekannt gegeben. Mögliche Themen sind:

- Blockchains Theorie & Praxis
- Grundlagen von verteilten Algorithmen und Datenstrukturen
- Grundlagen von Peer-To-Peer Systemen und Distributed Ledger Technologie
- Architekturen von vollständig verteilten Peer-to-Peer Systemen
- Fehlertoleranz und Konsistenz Peer-to-Peer Systemen
- Sicherheit und Konsens in Peer-To-Peer Systemen
- Algorithmen und Mechanismen für Blockchain Technologien

Verantwortliche Person:	Bocek Thomas
Empfohlene Module:	Verteilte SW-Systeme (M_Vss, FS/16-FS/20)
Zusätzlich vorausgesetzte Kenntnisse:	keine

DSA Administration – VSS Retrospect FS19

- **Remoting (Netzwerkprogrammierung):**
  - Synchrone Kommunikation: TCP/IP, QUIC, Remote Procedure Calls, HTTP Web Services
  - Asynchrone Kommunikation
  - weitere Message Exchange Patterns und Kommunikationsprotokolle im Überblick
  - NAT
- **Anwendung verteilter Systeme. Zum Beispiel:**
  - BitTorrent
  - Bitcoin / Ethereum (ERC20/Solidity)
  - Rsync / Tor
- **Zentrale Konzepte für den Entwurf verteilter Systeme:**
  - Naming
  - Synchronization
- **Verteilte Algorithmen und Datenstrukturen:**
  - Namensauflösung
  - Verteilte Hash-Tabellen, Similarity Search, Replication
  - Bloomfilter
  - Lamport-Uhr
  - Vektor-Uhr

VSS knowledge is good to have

- **Website: dsl.hsr.ch**
- **Genaue Details werden zu Semesterstart bekannt gegeben. Mögliche Themen sind:**
  - Blockchains Theorie & Praxis
  - Grundlagen von verteilten Algorithmen und Datenstrukturen
  - Grundlagen von Peer-To-Peer Systemen und Distributed Ledger Technologie
  - Architekturen von vollständig verteilten Peer-to-Peer Systemen
  - Fehlertoleranz und Konsistenz Peer-to-Peer Systemen
  - Sicherheit und Konsens in Peer-To-Peer Systemen
  - Algorithmen und Mechanismen für Blockchain Technologien

Beschreibung HS20

- **Titel: Advanced Distributed Systems & Blockchain (DS2) (Nachfolger von: DSA)**
  - Prüfungsdauer: Schriftliche Prüfung, 60min.
  - Zulassungsbedingungen zur Prüfung: Erfolgreiche Abgabe gelöster Übungsaufgaben nach Ankündigung.
  - Modulverantwortlicher DS2: Thomas Bocek
  - Voraussetzung: DS1
- **HS20: In den Übungen entwickeln Studentengruppen eine erweiterte verteile Applikation (Challenge Task II), welche diverse Requirements erfüllen müssen für eine Erfolgreiche Abgabe der Übung und als Zulassung zur Prüfung. Ein Beispiel aus dem HS18 war es eine vollständige verteilte P2P Applikation zu erstellen, welche mithilfe einer Blockchain Nachrichten notariell beglaubigen kann.**
- **Verteilte Systeme sind allgegenwärtig in beruflichem und privatem Alltag; sie führen Konzepte und Technologien aus unterschiedlichen Bereichen der Informatik zusammen. Die Themengebiete umfassen:**
  - Synchronization in Distributed Systems (Causality, Lamports Clock, Vector Clocks)
  - **Blockchain Security Considerations and Cryptography**
  - **DHTs** (Chord, Kademlia)
  - Distributed Systems with **WebRTC**
  - Distributed Batch Processing with Apache Spark
  - **Ethereum**, IOTA, **NEO**
  - **Consensus Mechanisms, Atomic Swaps**

URL: b.socrative.com/student/

Room: HSR

DSA: Plan 2019

Nr	Date	Vorlesung*	Dozent
01	18.09.19	Admin / Miniproject / Repetition VSS	Bocek
02	25.09.19	Repetition VSS / P2P Basics	Bocek
03	02.10.19	WebRTC / TomP2P recap	Bocek
04	09.10.19	Security Considerations / Ethereum	Bocek
05	16.10.19	Ethereum II / Security	Bocek
06	23.10.19	ICOs / NEO	Bocek
07	30.10.19	IOTA / Bazo PoS and Bazo Sharding	Bocek
08	06.11.19	Protocol Details - Noise, RLPx, QUIC / Kademlia broadcast	Bocek
09	13.11.19	vDHT / Raft / Paxos / Applied Cryptography	Bocek
10	20.11.19	Monero	Bocek
11	27.11.19	Bitcoin Advanced	Bocek
12	04.12.19	Crypto Mining/Admin(challenge task, exam, feedback)	Bocek
13	11.12.19	Challenge Task Presentations	you
14	18.12.19	Fragestunde und Feedback	Bocek
15	08.01.20	Beratungswoche	Bocek

* topics may change

Modulbewertung

Bewertungsart:	Note von 1 - 6

Leistungsbewertung

Während der Prüfungssession:	Schriftliche Prüfung, 120 Minuten
Zulassungsbedingungen zur Prüfung:	Erfolgreiche Abgabe gelöster Übungsaufgaben nach Ankündigung.
Während des Semesters:	
Bewertungsart:	keine Note oder Wertung

DSA Exercises

- **Wednesday lecture: 08:10 – 09:50**
  - Room: 1.201
- **Wednesday exercise u11: 10:10 – 11:50**
  - Room: 1.201
- **Wednesday exercise u12: 13:10 – 14:50**
  - Room: 1.201

- **"Mini" Project (description of HS18) – Challenge Task**
  - I will be here during exercise hours, but you are **not required** to be **physically present**
  - If nobody shows up, I'm in room **in room 1.169**
  - **Starts 25.09.2019 (lecture 2)**
    - **No exercises today!**

- **Goal: practical application of P2P concepts and tools**

DSA Administration / “Mini” Project / Challenge Task

- **Design and implementation of a fully-distributed game, with a gambling aspect**
  1. Board games, e.g., tic-tac-toe, four-in-a-row, poker, UNO, …
     - Waiting room, random numbers, chat
  2. Gambling, before start, e.g., pay in pot, winner gets it, …

- **Milestone: 06.11.2019**
  - Send code to us, include instructions
  - If we cannot run your code, you will be disqualified from CT,
  - Resubmit 1 week later, if we cannot run your code, **cannot write exam**

- **Each student's group is free to decide about specifics of building the P2P gaming and gambling application and how to organize the information within the distributed network.**

- **Requirements**
  1. Full decentralization and P2P for the board game (e.g., WebRTC, TomP2P, libp2p)
  2. Waiting room with chat
  3. Fully decentralized and P2P mechanisms for gambling (e.g., Bitcoin/Ethereum)
  - The solution may use existing libraries and code, but those must be allowed to be published under an open software license.
  - The final presentation shall outline the application and architecture.

- **Requirements not met = cannot write exam**

DSA Administration / “Mini” Project / Challenge Task (19 Students)

- **Deliverables, 11.12.2019**
  - Well documented code of the application
  - Presentation (slides) and demo of the application, also showing the architecture and design decisions
- **Libraries and tools**
  - P2P: TomP2P in Java, GoP2P is wip, WebRTC as an option
  - Allowed to use any language or framework. However, the supervisors are familiar with those: Java, Golang, and a bit JavaScript
  - Ethereum is the most popular public blockchain for smart contracts (Remix)
- **Organization**
  - n groups of 2 people, if group members found, send email to thomas.bocek@hsr.ch
  - During the challenge task, the group shall meet every week during exercise hours to work on the task and discuss the next steps.
  - The groups shall utilize their homework times to work on the CT, besides the exercise time slots assigned on Wednesday.
  - You do not have be physically present at the exercises. Supervisors will be available **on Wednesday.**
  - The groups shall determine and set-up an internal project plan
  - Distribute the workload so that each group member gets a fair load of work

Winner Group of CT in 2012

- **Fully-distributed, P2P online radio with recommendation**
- **Group 4 – Radiommender**

- **Submitted research result to P2P12 in Tarragona, Spain**
- **Radiommender: P2P on-line radio with a distributed recommender system**
  - http://www.csg.uzh.ch/csg/en/news/p2p12.html

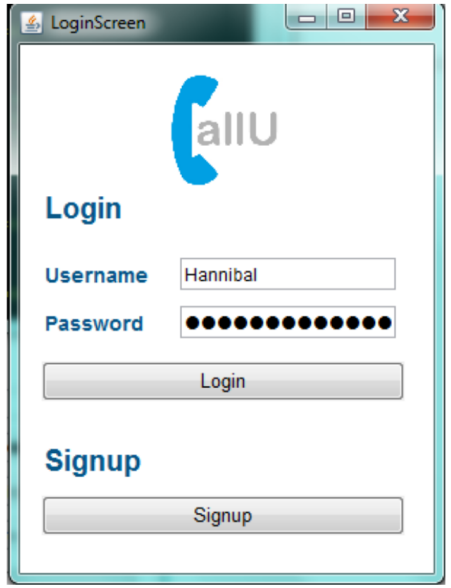
Challenge Task 2013

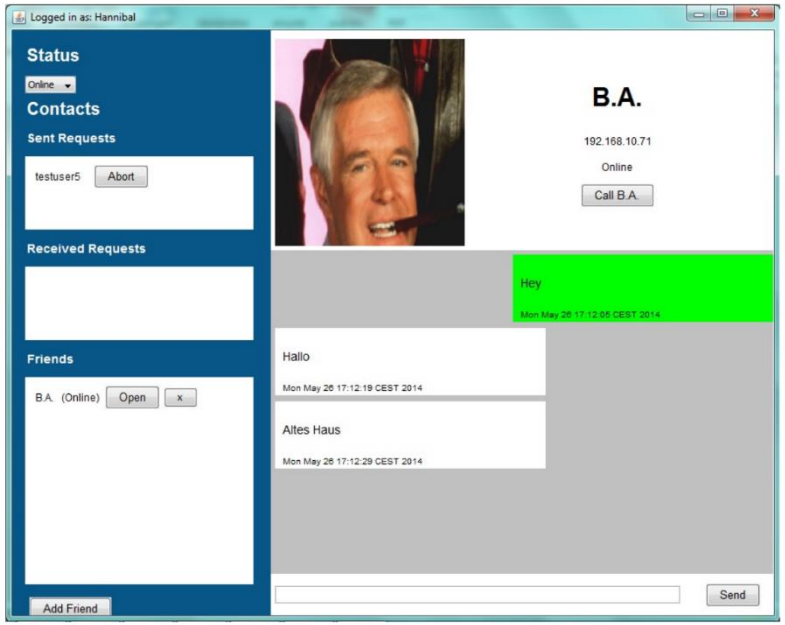
- **Winner Group of CT in 2013**
- **Fully-distributed, P2P synchronization application**
- **Group 2: Box2Box - A P2P-based file-sharing and synchronization application**

- **Submitted research result to P2P13 in Trento, Italy**
- **Demo paper**
  - https://ieeexplore.ieee.org/document/6688736/

Challenge Task 2014

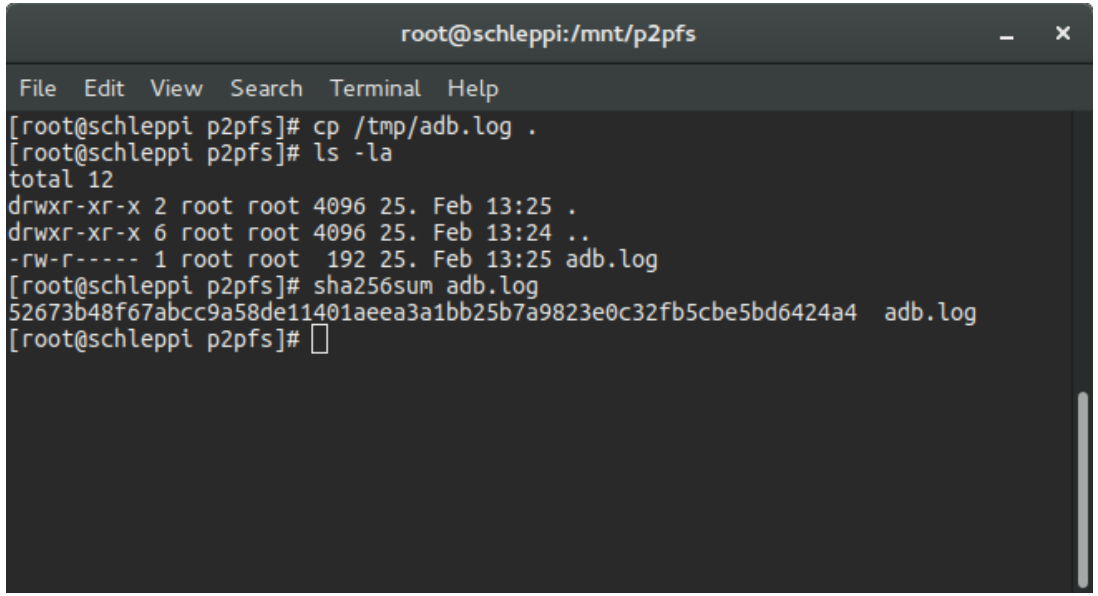
- **Fully decentralized Skype clone**
  - Codec: Opus
  - Every group could establish a phone call, all groups passed the 3 requirements





Challenge Task 2015

- **P2P-based file system**
- **Idea: scale up/down by adding/removing peers**
- **Mount with FUSE (Mac/Linux), no Windows ☹**
- **Challenges: consistency, availability (churn)**
- **Deployment: 10-15 ODroid U1 with attached USB storage**



- **Only one group managed to store/retrieve file with churn (winner)**
  - One group failed completely

Challenge Task 2018

- **Design and implementation of a fully-distributed, P2P messaging application with an integrated, blockchain-based notary service**
- **Requirements**
  1. Full decentralization and P2P
  2. Send messages between peers
  3. Quickly and easily verify messages
- **Each winner: 0.01311 BTC (50CHF)**
  - They used the IOTA blockchain as a signaling layer for WebRTC.
  - Everything decentralized

DSA Recommendation

- **Follow the lecture closely**
  - Lecture slides contain relevant
  - Reading further literature is recommended
    - Link are provided in the slides
- **Post-processing the lecture**
  - If topics or statements from the lecture are not clear, research and resolve them
  - Discussion and reviews in learning groups
- **Actively participate in the mini project**
  - Trying to understand it theoretically is not enough – hands-on is key!
  - If its not working, **read logs**, try to figure it out by yourself. If its still not working, ask.
  - Do not miss the opportunity of discussing details with your supervisor

- **12 lectures**
  - (29h = 24h + 5h; ca. 2.5h / week)
  - ~2h frontal teaching
  - ~½ h post-processing
- **Exercises / mini project**
  - (56h = 28h + 28h, ca. 4.5h / week)
  - ~4h challenge task
  - ~0.5h post-processing
- **Exam**
  - ~35h exam preparation
- **4 ECTS = 120h**
- **Prüfung:**
  - Closed book 2h, no coding, Hilfsmittel: none

Summary

- **Lectures Wednesday Morning – 08:10**
- **Mini project – challenge task, 2 group members: send to thomas.bocek@hsr.ch until next week**
  - Work on challenge task during exercise hours and at home
  - Supervisors will be here and in the office 1.169
- **3 requirements to be met**
  1. Fully decentralized game
  2. Waiting room, chat
  3. Fully decentralized gambling
- **To write exam all 3 requirements must be fulfilled**
- **Milestone 1: send source code to until 06.11.2019**
- **Final hand-in with presentation and demo: 11.12.2019**
- **HSR Challenge Task Winner 2019**
  - 18.12.2019

Questions?

Dr. Thomas Bocek thomas.bocek@hsr.ch