

HS18

DISTRIBUTED SYSTEMS ADVANCED & BLOCKCHAIN

Administration

T. Bocek

thomas.bocek@hsr.ch

■ Module Description

Distributed Systems Advanced & Blockchain

<i>Kurzzeichen:</i>	M_DSA
<i>Durchführungszeitraum:</i>	HS 2018 - HS 2018
<i>ECTS-Punkte:</i>	4
<i>Lernziele:</i>	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
<i>Verantwortliche Person:</i>	Thomas Bocek
<i>Empfohlene Module:</i>	-
<i>Zusätzlich vorausgesetzte Kenntnisse:</i>	keine

■ Charakteristische Eigenschaften verteilter Software-Systeme:

- Verteilungsdimensionen, Kopplungsarten, Designherausforderungen
- VSS-Anwendungsgebiete in der Praxis, z.B. Unternehmensanwendungen, Distributed Control Systems, World-Wide Web (WWW)
- Wichtige Architekturstile und Anwendungstopologien: Client-Server, Hub-and-Spoke, Peer-to-Peer

■ Remoting (Netzwerkprogrammierung):

- Synchrone Kommunikation: TCP/IP Sockets, Remote Procedure Calls, HTTP Web Services
- Asynchrone Kommunikation
- weitere Message Exchange Patterns und

Kommunikationsprotokolle im Überblick

■ Zentrale Konzepte für den Entwurf verteilter Systeme:

- Naming
- Synchronization

■ Verteilte Algorithmen und Datenstrukturen:

- Namensauflösung
- Verteilte Hash-Tabellen
- Lamport-Uhr
- Vektor-Uhr

■ Anwendung verteilter Systeme. Zum Beispiel:

- BitTorrent
- Bitcoin / Ethereum
- Rsync / Tor

■ **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

■ **Website: dsl.hsr.ch**

■ **Thesis section:**

- <https://dsl.hsr.ch/res/>
- Online quiz

URL: b.socrative.com/student/

Room: HSR

DSA: Plan 2018

Nr	Date	Vorlesung*	Dozent
01	18.09.18	Admin / Miniproject / Repetition VSS	Bocek
02	25.09.18	Repetition VSS / Security Considerations	Bocek
03	02.10.18	Bitcoin Script Language / UTXO	Bocek
04	09.10.18	Ethereum Internals I	Bocek / Blum
05	16.10.18	Ethereum Internals II	Bocek / Blum
06	23.10.18	Consensus PoS with Bazo	Blum / Bocek
07	30.10.18	Sharding with Bazo	Blum / Bocek
08	06.11.18	Map/reduce / Protocol Details - Noise / KPC / NAT	Bocek
09	13.11.18	vDHT / Raft / Paxos	Bocek / Blum
10	20.11.18	Network Coding	Bocek
11	27.11.18	Broadcast / Kademlia broadcast	Bocek
12	04.12.18	Voting / Applied Cryptography	Bocek / Blum
13	11.12.18	Challenge Task Presentations	you
14	18.12.18	Fragestunde und Feedback	Bocek / Blum
15	08.01.19	Beratungswoche	Bocek / Blum

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

- **Tuesday lecture: 08:10 – 09:50**

- Room: 3.114

- **Tuesday exercise u11: 10:10 – 11:50**

- Room: 1.263

- **Tuesday exercise u12: 13:10 – 14:50**

- Room: 1.263

- **Tuesday exercise u13: 15:10 – 16:50**

- Room: 1.263

- **Wednesday exercise u14: 08:10 – 09:50**

- Room: 1.257

- **“Mini” Project ([description](#)) – Challenge Task**

- We will be here during exercise hours (Wednesday on-demand), but **not required** to be **physically present**

- If nobody is in the exercise room, **we are in room 1.169**

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

- Implementation of a P2P application based on a P2P toolkit

- **Design and implementation of a fully-distributed, P2P messaging application with an integrated, blockchain-based notary service.**

1. Instant messaging app similar to Bleep, Signal, Telegram
 - Contact list, group chat, offline / online status, offline messages (optional)
2. Fully decentralized notary service (Eingeschriebener Brief)

- **Milestone: 06.11.2018**

- 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 messaging application and how to organize the information within the distributed network.

- **Requirements**

1. Full decentralization and P2P mechanisms
 2. Send messages between peers
 3. Quickly and easily verify messages
- 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 (56 Students)

■ Deliverables, 11.12.2018

- Well documented code of the application
- Presentation (slides) and demo of the application, also showing the architecture and design decisions

■ Libraries and tools

- Using TomP2P as the P2P library recommended (we know how it works)
- Allowed to use any language or framework. However, the supervisors are familiar with those: C#.NET (Roman), Swift (Roman), Java (Thomas), and Golang (Thomas)
- Ethereum is the most popular public blockchain for smart contracts ([Remix](#))

■ Organization

- n groups of 3 people, [register here](#)
- 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 Tuesday or Wednesday.
- You do not have to be physically present at the exercises. Supervisors will be available in **office 1.169 on Tuesday** during the exercise time, and on **Wednesday only by request**.
- 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](http://www.csg.uzh.ch/csg/en/news/p2p12.html)
- 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



SignupScreen

allU

Signup

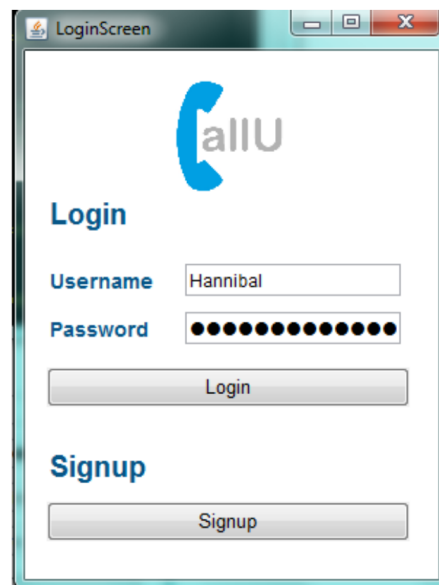
Username: Hannibal

Password: ●●●●●●●●●●

Fullname: Just Hannibal

Location: Everywhere

Signup



LoginScreen

allU

Login

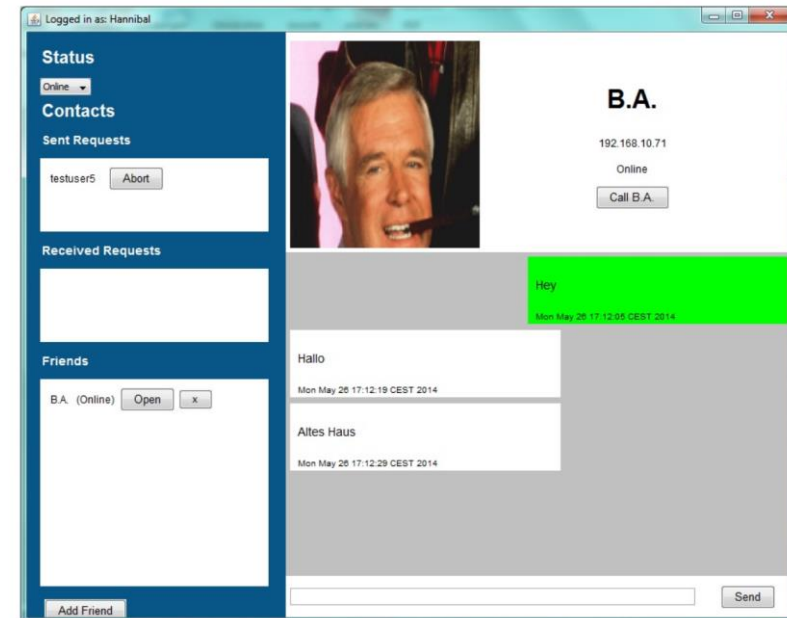
Username: Hannibal

Password: ●●●●●●●●●●

Login

Signup

Signup



Logged in as: Hannibal

Status
Online

Contacts

Sent Requests

testuser5 [Abort]

Received Requests

[Empty box]

Friends

B.A. (Online) [Open] [x]

Chat Area:

B.A.
192.168.10.71
Online
[Call B.A.]

[Profile picture of B.A.]

Hey
Mon May 26 17:12:05 CEST 2014

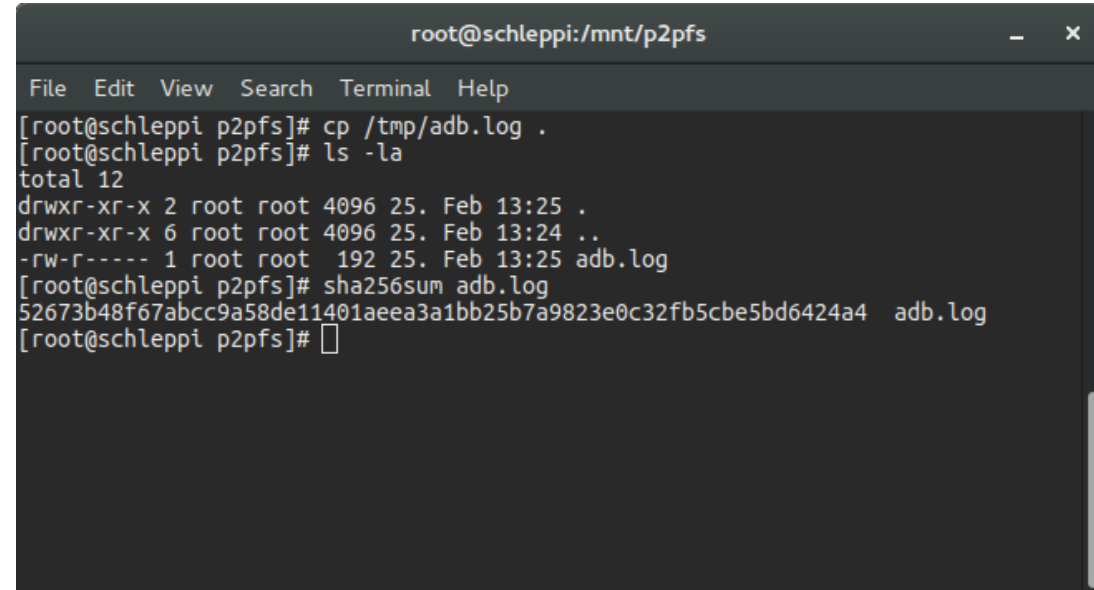
Hallo
Mon May 26 17:12:19 CEST 2014

Altes Haus
Mon May 26 17:12:29 CEST 2014

[Add Friend] [Send]

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: Smart contract-driven tic-tac-toe



```
root@schleppi:/mnt/p2pfs
File Edit View Search Terminal Help
[root@schleppi p2pfs]# cp /tmp/adb.log .
[root@schleppi p2pfs]# ls -la
total 12
drwxr-xr-x 2 root root 4096 25. Feb 13:25 .
drwxr-xr-x 6 root root 4096 25. Feb 13:24 ..
-rw-r----- 1 root root 192 25. Feb 13:25 adb.log
[root@schleppi p2pfs]# sha256sum adb.log
52673b48f67abcc9a58de11401aeea3a1bb25b7a9823e0c32fb5cbe5bd6424a4  adb.log
[root@schleppi p2pfs]#
```

■ 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
- ~1/2 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 Tuesday Morning – 08:10
- Mini project – challenge task, [register](#)
 - Work on challenge task during exercise hours and at home
 - Supervisors will be here in the office 1.169 on Tuesday and can relocate if required
 - Exercise on Wednesday on demand
- 3 requirements to be met
 1. Full decentralization and P2P mechanisms
 2. Send messages between peers
 3. Quickly and easily verify received messages
- To write exam all 3 requirements must be fulfilled
- Milestone 1: send source code to until 06.11.2018
- Final hand-in with presentation and demo: 11.12.2018
- HSR Challenge Task Winner 2018
 - 18.12.2018



Questions?

Prof. Dr. Thomas Bocek thomas.bocek@hsr.ch
Roman Blum roman.blum@hsr.ch