

Ausgewählte Kapitel der Systemsoftware (AKSS)

Einführung

23.04.2025

Dr. Christian Berger

Lehrstuhl für Informatik 4
Friedrich-Alexander-Universität Erlangen-Nürnberg



Lehrstuhl für Verteilte Systeme
und Betriebssysteme



FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

TECHNISCHE FAKULTÄT

Organisatorisches

- Arbeitsweise, Zeitlicher Ablauf und Meilensteine
- Erlaubte Arbeitsmittel
- Benotung

Organisatorisches

- Arbeitsweise, Zeitlicher Ablauf und Meilensteine
- Erlaubte Arbeitsmittel
- Benotung

Inhalte des Seminars

- Einführung
- Überblick über die Vorträge
- Semesterplan

Organisatorisches

- Arbeitsweise, Zeitlicher Ablauf und Meilensteine
- Erlaubte Arbeitsmittel
- Benotung

Inhalte des Seminars

- Einführung
- Überblick über die Vorträge
- Semesterplan

Werkzeuge

- Empfohlene Werkzeuge
- Vorsicht: Arbeiten mit AI-Tools (Grammarly vs. ChatGPT)

Organisatorisches

Dr. Christian Berger



berger@cs.fau.de

- **Termin:** Mittwochs, 16:15, Aquarium (0.031)
- **Webseite:** sys.cs.fau.de/lehre/ss25/akss
- **Mailingliste** an alle Teilnehmer & Betreuer
akss@lists.informatik.uni-erlangen.de
- **Mailing** an Betreuer
berger@cs.fau.de

23.04.2025 Organisation, Einführung und Themen

30.04.2025 Arbeitstechniken

07.05.2025 Papierdiskussion

14.05.2025 Vortragstechniken

21.05.2025 Konferenzvortragsdiskussion

28.05.2025 – *entfällt* –

04.06.2025	Präsentationen (Slot 1)
11.06.2025	Präsentationen (Slot 2)
18.06.2025	Präsentationen (Slot 3)
25.06.2025	Präsentationen (Slot 4)
02.07.2025	Präsentationen (Slot 5)
09.07.2025	Präsentationen (Slot 6)
16.07.2025	Präsentationen (Slot 7)
23.07.2025	Abschluss- und Feedbackrunde

Einarbeitung

- Eigenständiges Bearbeiten eines Themas
- Literaturrecherche: Vorgegebenes Papier als Ausgangsbasis
- Treffen mit Betreuer:in zur Besprechung der Ergebnisse

Einarbeitung

- Eigenständiges Bearbeiten eines Themas
- Literaturrecherche: Vorgegebenes Papier als Ausgangsbasis
- Treffen mit Betreuer:in zur Besprechung der Ergebnisse

Ausarbeitung

- Erstellen einer Ausarbeitung (6 bzw. 4 Seiten)
- ACM Standard Proceedings Template (ACM SIG style)
- Berücksichtigen der Wissensbasis
- Sprache: Deutsch oder Englisch

Anforderungen an die Ausarbeitung

Was sie nicht sein sollte

- *keine* reine Nacherzählung/Übersetzung
- direkte Übernahme von Abbildungen vermeiden

Was sie sein sollte

- Aufgreifen und Vertiefen einzelner Aspekte
- Herausarbeiten eigener Fragestellung
- eigene Literaturrecherche
 - Recherche alternativer Arbeiten
 - vergleichende Darstellung
 - insbesondere Masterstudierende
- Einschätzung und Beurteilung des konkreten Themas
- Erste Version: *roter Faden*

Vortrag

- Foliensatz zur Ausarbeitung
- *Optional: i4-Beamertemplate* (neo)
- Berücksichtigen der Hinweise zur Erstellung der Folien
- Sprache: Deutsch oder Englisch
- Vortrag im Rahmen des Seminars
 - 25-minütiger Vortrag
 - 10-minütige Diskussion zum Vortrag

- **Einstieg: Treffen zur Besprechung des Themas [E]**
 - **Vier Wochen** vor der Präsentation
 - Papiere wurden detailliert gelesen und Literaturrecherche hat stattgefunden
- **Erste Version der Ausarbeitung [A]**
 - **Drei Wochen** vor der Präsentation
 - Feedback von Betreuer

- Erste Version der **Präsentation** (Folien) [P]
 - **Zwei Wochen** vor der Präsentation
 - Feedback von Betreuer
- Finale Version der Ausarbeitung [F]
 - **Eine Woche** vor der Präsentation
 - Betreuer verteilt die Ausarbeitung über die Mailingliste

Zeitlicher Ablauf im Semester

23.04.2025

30.04.2025

07.05.2025

14.05.2025

21.05.2025

28.05.2025

04.06.2025

11.06.2025

18.06.2025

25.06.2025

02.07.2025

09.07.2025

16.07.2025

23.07.2025

E										
A	E									
P	A	E								
F	P	A	E							
V1	F	P	A	E						
	V2	F	P	A	E					
		V3	F	P	A	E				
			V4	F	P	A				
				V5	F	P				
					V6	F				
						V7				

Arbeitsmittel

- Verwendung von Git empfohlen
→ <https://gitlab.cs.fau.de/>
- Abgabe der Ausarbeitung/Folien per Git oder E-Mail

Arbeitsmittel

- Verwendung von Git empfohlen
→ <https://gitlab.cs.fau.de/>
- Abgabe der Ausarbeitung/Folien per Git oder E-Mail

Organisation

- Beim Seminar gilt **Anwesenheitspflicht**:
Bei Abwesenheit bitte (per E-Mail) Bescheid geben, z.B. bei Krankheit
- **Technikcheck** rechtzeitig vor der Präsentation
- Veröffentlichung der (finalen) Folien und Ausarbeitung auf der Seminarwebseite
(Falls nicht gewünscht, bitte Bescheid geben)

Erlaubte bzw. empfohlene Arbeitsmittel

- Versionsverwaltung (Git)
- Rechtschreib- und Grammatikchecker (e.g. Grammarly)
- Latexumgebung (TexStudio, Overleaf, etc)
- Literaturverwaltung (Zotero)
- Literaturrecherche (Google Scholar, Semantic Scholar, ..)

Erlaubte bzw. empfohlene Arbeitsmittel

- Versionsverwaltung (Git)
- Rechtschreib- und Grammatikchecker (e.g. Grammarly)
- Latexumgebung (TexStudio, Overleaf, etc)
- Literaturverwaltung (Zotero)
- Literaturrecherche (Google Scholar, Semantic Scholar, ..)

Vorsicht

- KI-generierter Inhalt ins Papier kopieren nicht erlaubt!

Bestehen

Voraussetzungen:

- Seminararbeit wurde abgegeben und mit **bestanden** bewertet
- Vortrag wurde gehalten und mit **bestanden** bewertet

Achtung

- Beide Leistungen müssen zwingend erbracht und bestanden werden
- Eine nicht abgegebene Arbeit oder ein nicht gehaltener Vortrag führt automatisch zum Nicht-Bestehen

Endnote ist eine “Portfoliobewertung“

Wie setzt sich die Seminarnote zusammen?

- *Finale* Abgabe der Seminararbeit
- Präsentation *im Seminar*
 - Beide Leistungen zählen jeweils zu *gleichen Proportionen*
- Aber: Aktive **Mitarbeit** zählt auch (Diskussionsrunde)

Endnote ist eine “Portfoliobewertung“

Wie setzt sich die Seminarnote zusammen?

- *Finale* Abgabe der Seminararbeit
- Präsentation *im Seminar*
 - Beide Leistungen zählen jeweils zu *gleichen Proportionen*
- Aber: Aktive **Mitarbeit** zählt auch (Diskussionsrunde)

Grobe Daumenregel zur Orientierung

- Bewertungsanteile A:P:M in etwa 40:40:20

Replizierte Systeme und Blockchain-Systeme

- Die folgenden Themengebiete werden betrachtet:
 - Grundlagen replizierter Systeme anhand von Beispielen erklärt (Bitcoin, PBFT)
 - Skalierbarkeit von Replikationsprotokollen (#Nodes)
 - Performance und Modularität von replizierten Systemen
 - Validierungstechniken (Korrektheit der Algorithmen)
 - Byzantinische Fehlertoleranz in der Praxis
 - Neue Ansätze zu Proof-of-Work Systemen

Replikation

Replizierte Systeme

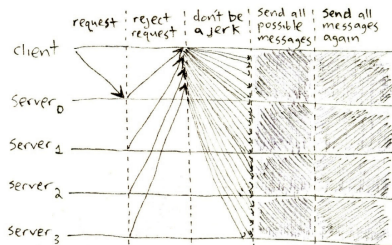
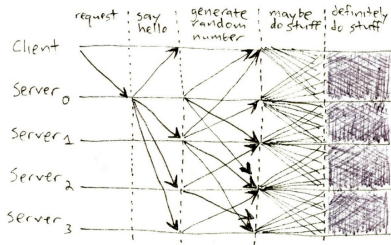
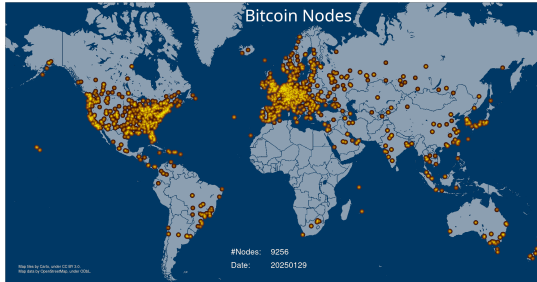


Abbildung 1: Source: The Saddest Moment

<https://scholar.harvard.edu/files/mickens/files/thesaddestmoment.pdf>

- *Redundante Ausführung mehrerer Kopien* eines Dienstes auf verschiedenen Knoten
- Ziele: Verfügbarkeit, Fehlertoleranz und Sicherheit
 - Latenz, Lastverteilung
- Beispiele: Cloud-Dienste, verteilte Datenbanken, Blockchain



Entwurfskriterien

- Konsistenz (Quorum-basiert oder Proof-of-Work)
- Hohe Skalierbarkeit und Geographische Verteilung
- Durchsatz und Latenz
- Transaktionsmodell und Programmierbarkeit



Ein Fehlermodell

- Willkürliches Fehlverhalten von Knoten, Intrige
- Modellierung mithilfe eines Angreifers

Vortragsslots

- 12 Themen wurden nach dem “First-come-first-serve” Prinzip vergeben
- Idee: Vorbesprechungen der Themen schon vor Semesterbeginn
 - Bessere Lastverteilung und niedrigere Abbrecherquote?
 - Oder: “sunk cost fallacy”
- Vortragstermin richtet sich nach Thema
 - 7 Vortragstermine
 - etwa zwei Präsentationen pro Termin
- 1 Thema ist noch offen (“The Lightning Network”)

Präsentationsslot 1

Tag: **04.06.2025**

Fundamentals of Replicated Systems

- Byzantine Fault-Tolerant Replication [R.S.]
- Blockchain and Proof-of-Work [O.M.]

Präsentationsslot 2

Tag: **11.06.2025**

Enhancing the Scalability of BFT Protocols

- Communication, Batching and Pipelining in BFT Protocols [S.Ü.]
- Committee-based Consensus, Gossiping and Randomized Sampling [S.H.]

Präsentationsslot 3

Tag: **18.06.2025**

Performance, Modularity and Liveness of BFT Protocols

- Internet Computer Consensus: The ICC Protocol Family [F.W.]
- Optimizations & their Impact on Liveness in BFT Protocols [E.B.]

A DAG instead of a Blockchain?

Präsentationsslot 4

Tag: **25.06.2025**

A DAG instead of a Blockchain?

- A Directed Acyclic Graph instead of a Blockchain?
Mempool Construction & Efficient BFT Consensus [F.M.]
- Can Directed Acyclic Graph-based BFT Protocols Have Low Latency? [A.W.]

Buggy BFT? Techniques to Validate the Correctness of BFT Protocols

Präsentationsslot 5

Tag: **02.07.2025**

Buggy BFT? Techniques to Validate the Correctness of BFT Protocols

- Uncovering the Malicious Strategies of Byzantine Generals: The Twins Approach [T.W.]
- BFT-Fuzzing, Lasso Detection and Hot States in BFT Protocol Execution [D.L.]

Bitcoin and its Performance Bottleneck: Approaches to Boost Performance!

Präsentationsslot 6

Tag: **09.07.2025**

Bitcoin and its Performance Bottleneck: Approaches to Boost Performance!

- Bitcoin and BFT: Is it a Match? Leader Election and Quorum Certification in PoW Systems [M.B.]
- Generalized Nakamoto Consensus [J.L.]

Approaches to Boost Bitcoin Performance (Part II): The Lightning Network

Präsentationsslot 7

Tag: **16.07.2025**

Approaches to Boost Bitcoin Performance (Part II): The Lightning Network

- The Lightning Network [*offenes Thema*]

Semesterplan - Update 23.04.2025

Semesterplan - Mittwoch

23.04.2025	Organisation, Einführung und Themen
30.04.2025	Arbeitstechniken
07.05.2025	Papierdiskussion
14.05.2025	Vortragstechniken
21.05.2025	Konferenzvortragsdiskussion
28.05.2025	— <i>entfällt</i> —
04.06.2025	Fundamentals of Replicated Systems
11.06.2025	Enhancing the Scalability of BFT Protocols
18.06.2025	Performance, Modularity and Liveness of BFT
25.06.2025	A DAG instead of a Blockchain?
02.07.2025	Buggy BFT? Techniques to Validate BFT
09.07.2025	Bitcoin and its Performance Bottleneck
16.07.2025	The Lightning Network
23.07.2025	— <i>Abschluss- und Feedbackrunde</i> —

Werkzeuge

Google Scholar (und Alternativen)

- Guter Ausgangspunkt, findet Papiere anhand von *Stichwörtern*
- Falls relevantes Papier gefunden, *Literaturverzeichnis* (References) um rekursiv weiter zu suchen
- *Reverse Search*: Von welchen Arbeiten wurde ein Papier später zitiert?

Google Scholar (und Alternativen)

- Guter Ausgangspunkt, findet Papiere anhand von *Stichwörtern*
- Falls relevantes Papier gefunden, *Literaturverzeichnis* (References) um rekursiv weiter zu suchen
- *Reverse Search*: Von welchen Arbeiten wurde ein Papier später zitiert?

Achtung

- Literatur oft hinter **Paywall** (ACM Library, IEEE Xplore)
- An kostenlosen Unizugang denken!

Latex Umgebung

- TexStudio oder TexMaker + Git für Versionsverwaltung
- Alternativ auch Overleaf geeignet
- ACM Standard Proceedings Template (ACM SIG style)

Grammar & Spellchecking

- Tools wie Grammarly und Language Tool
- Checks für Rechtschreibung und Grammatik + Korrektur
- Keine *generative* (Inhalts-erzeugende) Funktionen nutzen

Wie kann ich dir helfen?

Summarize and rephrase the following text: "Consensus algorithms allow a collection of machines to work as a coherent group that can survive the failures of some of its members. Because of this, they play a key role in building reliable large-scale software systems. Paxos [13, 14] has dominated the discussion of consensus algorithms over the last decade: most implementations of consensus are based on Paxos or influenced by it, and Paxos has become the primary vehicle used to teach students about consensus. Unfortunately, Paxos is quite difficult to understand, in spite of numerous attempts to make it more approachable."



Suche



Deep Research



Wie kann ich dir helfen?

Summarize and rephrase the following text: "Consensus algorithms allow a collection of machines to work as a coherent group that can survive the failures of some of its members. Because of this, they play a key role in building reliable large-scale software systems. Paxos [13, 14] has dominated the discussion of consensus algorithms over the last decade: most implementations of consensus are based on Paxos or influenced by it, and Paxos has become the primary vehicle used to teach students about consensus. Unfortunately, Paxos is quite difficult to understand, in spite of numerous attempts to make it more approachable."



Suche



Deep Research



Warnung

- Übernahme von KI-generiertem Inhalt ist verboten!
- Wie Plagiat => Führt zu Nicht-Bestehen des Seminars

Beispiele für “legitime” Nutzung im Sinne des Seminars

- Enthält mein Satz Rechtschreibfehler?
- Welche Papiere sind thematisch verwandt zu ..? (Double Checking von Ergebnissen eurer Literaturrecherche)
- Ich hab einen Formatierungsfehler in einer Latex Tabelle:
- Mein Latex Code kompiliert nicht. Was bedeutet dieser Fehler:

Achtung: Das waren nur Beispiele!

- Im Zweifelsfall nicht nutzen! Oder: Betreuer vorher fragen
- ChatGPT nicht blind vertrauen!

Fragerunde
