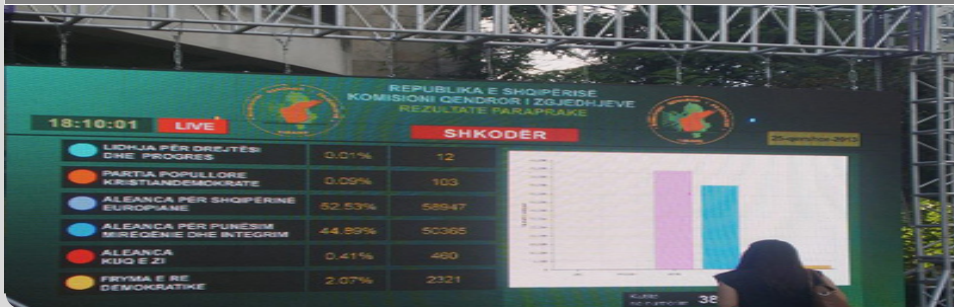


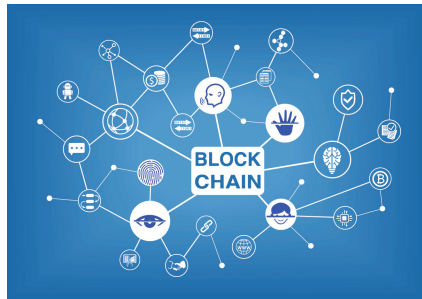
Thema: Blockchain-basiertes E-Voting

Praxis der Softwareentwicklung im Sommersemester 2018

Prof. Bernhard Beckert, Mihai Herda, Michael Kirsten | 04.05.2018

INSTITUT FÜR THEORETISCHE INFORMATIK, KIT





Aufgabe

Entwicklung eines Blockchain-basierten E-Voting-Systems

- Kleine Wahlen
- Öffentliche Stimmen
- *Optional*: verschiedene Abstimmungstypen, Stimmendelegation, ...

Anforderungen

- Funktionalität für Wähler und Wahlleiter
- Stimmen im Ledger gespeichert
- Automatische Überprüfung und Auszählung mit Smart Contracts
- Zwei graphische Benutzeroberflächen

Technischer Rahmen

- Hyperledger Fabric als Blockchain-Framework
- Implementierung der Clients in Java
- Smart Contracts in Java oder Go

Mihai Herda

herda@kit.edu – Raum 227

Michael Kirsten

kirsten@kit.edu – Raum 228

Webseite

formal.iti.kit.edu/teaching/pse/2018/

- Termine
- Dokumente

Vorstellung: Wer sind Sie? Vorwissen? Motivation für Thema?

Mihai Herda

herda@kit.edu – Raum 227

Michael Kirsten

kirsten@kit.edu – Raum 228

Webseite

formal.iti.kit.edu/teaching/pse/2018/

- Termine
- Dokumente

Vorstellung: Wer sind Sie? Vorwissen? Motivation für Thema?

- Wann haben Sie Zeit für ein wöchentliches Treffen?
- Welche Klausuren schreiben Sie dieses Semester? Wann?

Ergebnis

- Wochentermin: Freitag 15:45 - 17:15 Uhr in Raum 211, Geb. 50.34 (zweiter Stock)
- Abgabe der Artefakte:
Jeweils Mittwoch 11:00 Uhr vor dem Kolloquium im SVN-Repository
- Klausurenpause: t.b.a.

Bitte per E-Mail Klausurentermine/Urlaubspläne senden!

Phase	Dauer	Kalenderwoche	Jahr
Einlesen	ca. 1 Woche	18 – 19	2018
Pflichtenheft	3 Wochen	20 – 22	2018
Entwurf	4 Wochen	23 – 26	2018
Implementierung	4 Wochen	27 – 30	2018
Klausurpause	2 Wochen	31 – 32	2018
Qualitätssicherung	3 Wochen	33 – 35	2018
Interne Abnahme		36	2018
Abschlusspräsentation		37/38 ?	2018

Phase	Dauer	Kalenderwoche	Jahr
Einlesen	ca. 1 Woche	18 – 19	2018
Pflichtenheft	3 Wochen	20 – 22	2018
Entwurf	4 Wochen	23 – 26	2018
Implementierung	4 Wochen	27 – 30	2018
Klausurpause	2 Wochen	31 – 32	2018
Qualitätssicherung	3 Wochen	33 – 35	2018
Interne Abnahme		36	2018
Abschlusspräsentation		37/38 ?	2018

Phasenverantwortlicher

- koordiniert die Arbeit
- präsentiert die Ergebnisse im Kolloquium
- Zuteilung liegt bei Ihnen

Kolloquium

- Abschluss einer Phase
- Vortrag vom Phasenverantwortlichen
- Fragenrunde

Abgaben (Artefakte)

- Abgaben mit den geforderten Artefakten stets per SVN (Link schicken wir Ihnen per E-Mail)
- Teil der Prüfungsleistung
- Abgabe ca. 48 Stunden vor Kolloquium (jeweils Mittwoch 11 Uhr)
- Abgabe pünktlich, muss eindeutig im SVN erkenntlich sein

Kolloquium

- Teil der Prüfungsleistung (Vortrag und Fragerunde)
- Wichtig: Anwesenheit ist Teil der Prüfungsleistung

Gewichtung

Pflichtenheft 10%, Entwurf 30%, Implementierung 30%,
Qualitätssicherung 20%, Abschlusspräsentation 10%

Werkzeug-gestützte SW-Entwicklung

Verwendung von

- Repository (GIT oder SVN)
- Issues Tracker
- Continuous Integration
- Build-Skripte (Maven, Ant, ...)

Repositories angeboten von:

- ATIS (SVN)
- Github, Bitbucket, etc.
- SCC (<https://git.scc.kit.edu>)

Den Betreuern ist Zugriff zu gewähren. Überprüfung von Commits.

1. Phase: Pflichtenheft

Artefakt: Pflichtenheft im Umfang: ca. 30-40 Seiten

Inhalte:

- Systemmodell und -umgebung
- Zielbestimmungen (Muss-, Wunsch- und Abgrenzungskriterien)
- Vollständige funktionale Anforderungen; Qualitätsanforderungen
- GUI-Entwürfe
- Ausführliche Testfallszenarien
- Phasenverantwortliche

- Austausch der Kontaktinformationen
- Anlegen des Repository
- Festlegung der Phasenverantwortlichen
- Anlegen einer Instanz auf BW-Cloud (<https://www.bw-cloud.org>)
- Ausprobieren von Hyperledger Fabric und Tutorials auf <http://hyperledger-fabric.readthedocs.io/>
- Einlesen in E-Voting, GUI Programmierung in Java

Bis zum nächsten Treffen!

Vielen Dank
für die Aufmerksamkeit!

Gibt es Fragen?

Vielen Dank
für die Aufmerksamkeit!

Gibt es Fragen?