Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. B. Beckert
Michael Kirsten, Mihai Herda

Praxis der Softwareentwicklung, Sommersemester 2018

Aufgabenbeschreibung

Eine kurze Bemerkung vorab

Dies ist *Ihr* Projekt. Dieses Dokument ist kein Katalog von Aufgaben, der Punkt für Punkt abgearbeitet werden muss, um das Modul zu bestehen, sondern lediglich eine Reihe von Hinweisen, was wir erwarten. Wie *Ihr* Programm nachher aussieht, müssen Sie selbst entscheiden.

1 Hintergrund

Eines der Forschungsthemen an unserem Lehrstuhl ist die Spezifikation und Verifikation von Wahlverfahren, um nachzuweisen, dass diese korrekt ablaufen. Die Entwicklung von Distributed-Ledger-Technologien (bzw. Blockchains) stellt nun eine Möglichkeit dar, die Nachverfolgbarkeit der Stimmabgabe über eine Kette von Transaktionen in der Blockchain zu gewährleisten. Neben den sehr populär gewordenen Umsetzungen öffentlicher Blockchains wie Ethereum oder Bitcoin existieren außerdem sogenannte *permissioned* Ledger-Technologien, die spezialisierte Blockchains für einen begrenzten Nutzerkreis inklusive einer individuellen Rechteverwaltung ermöglichen. Innerhalb dieses Projekts wollen wir diese Technologie nun auf elektronische Wahlverfahren anwenden.

2 Aufgabenstellung

Innerhalb dieses Projekts sollen Sie ein Blockchain-basiertes E-Voting-System entwerfen und implementieren. Vorerst soll die Stimmabgabe öffentlich sein und für kleine Wahlen (bspw. für Vereinswahlen o.Ä.) funktionieren. Optional können verschiedene Abstimmungstypen (Mehrheitswahlen, Zustimmungswahlen, Präferenzwahlen, etc.) ergänzt sowie zusätzliche Konzepte wie etwa eine Stimmendelegation unterstützt werden. Hierbei erwarten wir, dass Sie sich selbstständig in das Blockchain-Framework einarbeiten. Wenn Sie gut mit dem Framework zurechtkommen, sind auch Erweiterungen auf (teil-)private Wahlen denkbar.

Im Folgenden sind einige Eckpunkte beschrieben.

2.1 Minimale Leistungsmerkmale

Stimmabgabe. Die Stimmabgabe soll mindestens so erfolgen, dass jeder Wähler einen Kandidaten wählen kann. Weitere Modi wie Zustimmungs- und Präferenzwahl sind denkbar.

Stimmenübermittlung und -auszählung. Es soll mindestens eine relative Mehrheitswahl unterstützt werden, weitere Verfahren wie bspw. ein Punktesystem, Erst-/Zweitstimme etc. sind denkbar. Eine öffentliche Übermittlung und nachverfolgbare Wahl soll möglich sein. Optional sind noch weitere Arten wie eine geheime Abstimmung denkbar. Nach entsprechender Aktivität des Wahlleiters soll die Wahl automatisch ausgezählt und veröffentlicht werden. Hier ist außerdem eine automatische Überprüfung denkbar.

Grafische Oberfläche. Ihr Programm muss über zwei grafische Benutzeroberflächen verfügen. Eine als Sicht für den Wahlleiter, eine für die Wähler. Dabei sollen für die Wähler die Auswahlmöglichkeiten sowie entsprechende Erklärungen angezeigt und die Möglichkeit zur Stimmabgabe (ggf. auf verschiedene Arten, bspw. Stimmendelegation oder geheim) gegeben werden. Als Wahlleiter soll man eine Wahl starten und beenden sowie automatisch auszählen bzw. überprüfen können. Außerdem soll, je nach dahionterliegender Implementierung, ein Wahlleiter über den genauen Wahlmodus entscheiden können.

Software-Architektur. Eine saubere Trennung zwischen kritischen (z.B. Stimmenübermittlung) und unkritischen (z.B. GUI) Komponenten ist von immenser Bedeutung. Entwerfen Sie austauschbare Komponenten mit minimalen, wohldefinierten Schnittstellen.

2.2 Technische Eckpunkte

- Programmiersprachen: Java und Go.
- GUI-Bibliothek: z.B. Swing
- Versionsverwaltung: Subversion und GIT. (siehe unten)
- Entwurfs- und Entwicklungsumgebung: nach Wunsch, z.B. ArgoUML
- Unit-Test-Rahmenwerk: z.B. JUnit
- Dokumenterstellung: nach Wunsch, bevorzugt LaTeX (Abgabe aber immer als PDF)

3 Organisatorisches

3.1 Technische Ausstattung

Die Website zur Veranstaltung findet sich unter `https://formal.iti.kit.edu/teaching/pse/2018`. Dort werden in Zukunft weitere organisatorische Information bereitgestellt.

Wir stellen ein SVN-Repository bereit, in dem alle Artefakte (insbesondere Abgaben) abgelegt werden sollen. Vor der Nutzung müssen Sie sich erst registrieren, dazu besuchen Sie folgende Website: `https://svnserver.informatik.kit.edu/i57/login/` und loggen sich mit Ihrem ATIS-Account (`s_...`) ein; der Account wird dann von uns freigeschaltet.

3.2 Bewertung

Die Benotung Ihres Systems richtet sich nach folgenden Kriterien:[1]

- Qualität aller abgegebenen Dokumente
- Qualität der Kolloquien
- Qualität der Abschlusspräsentation
- Erfüllen der minimalen Leistungsmerkmale (s.o.)
- *Sinnvolle*[2] Erweiterungen über diese Merkmale hinaus
- Qualität des erstellten Programms (das schließt u.A. Benutzbarkeit und Robustheit ein)

[1] Diese Liste hat keine Reihenfolge, die einer Gewichtung entspricht. Es gibt sicherlich weitere Punkte, die als selbstverständlich gelten und sich bei Nichterfüllen negativ auswirken.

[2] Sie tun Sich selbst und dem Projekt nichts Gutes wenn Sie sich zu sehr verkünsteln.

Die Gesamtnote errechnet sich dann nach der im Modulhandbuch genannten Gewichtung:

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

Nach jeder Phase findet (im Rahmen der regelmäßigen Treffen) ein Kolloquium statt, in dem die Ergebnisse der Phase *selbstständig* (in 15 Minuten) vorgestellt, sowie anschließend diskutiert werden sollen. Jedes Team-Mitglied muss einmal präsentieren.[3] Die Benotung jeder einzelnen Phase wird nach dem entsprechenden Kolloquium besprochen.

3.3 Treffen

Treffen finden wöchentlich im Raum 211 statt. Auch wenn gerade kein Kolloquium ansteht, raten wir Ihnen dringend, jede Woche über Ihren Fortschritt zu berichten. Nur dann können wir unverbindliche, gezielte Kommentare abgeben. Sorgen Sie daher bitte auch dafür, dass alle erforderlichen Dokumente rechtzeitig im SVN verfügbar sind. Die Abgabeversion soll eindeutig identifizierbar sein. Halten Sie sich an den vereinbarten Abgabeschluss. Eine Woche vor Abgabe ist eine Vorversion einzureichen.

Darüber hinaus sollten Sie sich natürlich auch noch regelmäßig in der Gruppe besprechen. Sie können dazu Raum 211 nutzen falls er frei ist (vor der Tür hängt ein Kalender mit Reservierungen; bitte nehmen Sie Rücksicht darauf, dass MitarbeiterInnen Priorität genießen).

[3] Dennoch müssen sich selbstverständlich *alle* Team-Mitglieder in *allen* Phasen einbringen.