netidee

PROJEKTE

Bürgerchain

Zwischenbericht | Call 12 | Projekt ID 2092

Inhalt

1 Einleitung

Im Projekt „Bürgerchain“ soll eine webbasierte e-Voting Plattform für Vereine, Parteien und Privatpersonen umgesetzt werden. Die Arbeit an dem Projekt startete im Januar 2018, dieser Zwischenbericht gibt einen Überblick über den Projektstand mit Ende Juni 2018.
Ziel bei Projektstart war es, zu diesem Zeitpunkt mit mindestens zwei interessierten Organisationen einen Anforderungskatalog erstellt zu haben, der Grundlage für die weitere Entwicklung sein soll. Auf Grundlage dieses Anforderungskatalogs sollte ein Bedienkonzept für die Plattform erarbeitet werden.
Ein weiteres Ziel war es, Technologien auf ihre Praktikabilität für den Einsatz in diesem Projekt hin zu evaluieren. Konkret betraf das die Bereiche der Backend-Entwicklung, Frontend-Entwicklung, Datenspeicherung, Server-Umgebung und die eingesetzten kryptographischen Methoden sowie die verwendete Blockchain.
Bei einem Teil der Arbeitspakete kam es zu Verzögerungen, mit einigen der geplanten Aktivitäten wurde später begonnen als ursprünglich geplant. Das größte Arbeitspaket, das die tatsächliche Umsetzung der e-Voting Plattform betrifft, ist dafür schon etwas weiter fortgeschritten als geplant.
Eine detaillierte Auflistung der Arbeitspakete sowie der jeweiligen Status folgt im nächsten Abschnitt dieses Berichts.

2 Status der Arbeitspakete

2.1 Arbeitspaket 1 – Kunden für die Nutzung der Bürgerchain gewinnen

Im Rahmen dieses Arbeitspakets wurden Organisationen gesucht, die Interesse am Einsatz einer e-Voting-Plattform haben. Im Zuge dieser Aktivitäten wurden Parteien und größere Vereine in Österreich kontaktiert. Während von einigen Vereinen bzw. Parteien Absagen kamen, äußerten die Landesorganisation einer Partei und ein Verein konkretes Interesse am Einsatz der Bürgerchain.
Mit diesen beiden Organisationen wurden Anforderungen an eine e-Voting-Plattform formuliert, die für einen Einsatz zwingend umgesetzt werden müssten.
Eine wesentliche Erkenntnis aus den Gesprächen mit den Organisationen war, dass der Ablauf von Abstimmungen nicht so trivial ist wie ursprünglich gedacht. In der ursprünglichen Planung war davon ausgegangen worden, dass eine Wahl einen relativ strikten, klaren Ablauf hat:

- Eine im Vorhinein feststehende Liste von Fragen kommt zur Abstimmung
- Wahlberechtigte haben ein Zeitfenster von mehreren Stunden oder gar Tagen, in dem sie abstimmen können
- Nach Ablauf der festgelegten Zeit gibt es ein Ergebnis

Beide Organisationen hatten jedoch die Anforderung, dass während einer Wahl laufend neue Fragen gestellt bzw. Fragen umformuliert werden können und dass das Zeitfenster für die Beantwortung der Fragen nur wenige Minuten groß ist. Abhängig vom Ergebnis einer Abstimmung sollte es auch möglich sein, mehrere Wahlgänge durchzuführen. Der interessierte Verein hatte zusätzlich die Anforderung, dass Wahlberechtigte unterschiedliche Stimmgewichte haben sollten.
Diese Anforderungen wurden in Arbeitspaket 3 in einem Use-Case Dokument erfasst, das beschreibt, welche Anwendungsfälle durch die Bürgerchain abgedeckt werden sollen. Dieses Dokument war

einerseits Grundlage für die weiteren Aktivitäten in den Arbeitspaketen 2 und 3, in denen die im Projekt eingesetzten Technologien ausgewählt werden bzw. die Benutzerschnittstelle designt wird.
Bei beiden interessierten Organisationen brachten die Gespräche leider auch etwas Ernüchterung: Der Verein hat sehr spezielle Anforderungen an die technische Umsetzung, die im Rahmen dieses Projekts nicht erfüllt werden können. Die Partei, die Interesse zeigt, sieht den Einsatz einer e-Voting-Plattform als langfristiges Ziel, das wohl frühestens 2019 angegangen wird.
Der Abschluss dieses Arbeitspakets hat sich durch die länger andauernden Gespräche mit Partei bzw. Verein etwas verzögert, mit 15.5. wurde die Use-Case-Liste aber vorerst abgeschlossen. Sollten sich im Laufe des Projekts neue Anforderungen ergeben, wird die Use-Case-Liste erweitert bzw. angepasst.

2.2 Arbeitspaket 2 – Technologien für die Umsetzung des Projekts auswählen

Im Rahmen dieses Arbeitspakets wurde festgelegt, mit welchen Technologien das Projekt Bürgerchain umgesetzt werden sollte:

- *Hosting*: Evaluiert wurden Amazons Elastic Compute Cloud (EC2), Googles App Engine Standard und App Engine Flexible sowie Hosting auf einem dedizierten Server. Die wichtigsten Entscheidungskriterien waren
    - Niedriger Wartungsaufwand, einfache Bedienung
    - Niedrige Kosten für Hosting
    - Ausfallsicherheit
    - Skalierbarkeit
    - Einfache, kostengünstige Möglichkeit, ein SSL-Zertifikat zu installieren

  Schließlich fiel die Entscheidung, den überwiegenden Teil der Bürgerchain-Anwendung in **Googles App Engine Flexible** zu hosten, weitere Teile in **Googles App Engine Standard**
- *Backend/Web App Framework*: Für das Backend wurden Python/Flask, Java/Spring MVC und C#/ASP.NET Core evaluiert. Die Entscheidungskriterien waren:
    - Einarbeitungsaufwand
    - Portierbarkeit der Anwendung
    - Entwicklungswerkzeuge und Tools, Integration des gewählten Hosting-Providers

  Unter den oben angeführten Gesichtspunkten wurde entschieden, die Bürgerchain mit C#/ASP.NET-Core umzusetzen, kleine Teile werden in Python implementiert. Vom Einsatz von Angular wurde nach kurzer Testphase abgesehen.
- *Web-Frontend*: Für das Frontend wurden Bootstrap und Material Lite sowie die Möglichkeit, das User Interface von Grund auf selbst zu implementieren evaluiert. Für das Frontend wird hauptsächlich auf Material Lite gesetzt.
- *Blockchain*: In den Vergleich der Blockchain-Technologien floss am meisten Zeit, hier wurden zahlreiche Blockchains (Ethereum, Ardor, NXT, Artis, IOTA, …) anhand folgender Gesichtspunkte evaluiert:
    - Kosten – es soll günstig sein, Daten in der Blockchain zu speichern. Im Rahmen einer Wahl kann es sein, dass mehrere 1000 Transaktionen in der Blockchain gespeichert werden, Transaktionskosten müssen daher niedrig sein.
    - Geschwindigkeit – Transaktionen sollen innerhalb weniger Sekunden bestätigt werden, um den Anforderungen nach schnell durchführbaren Abstimmungen gerecht zu werden
    - Reife und Sicherheit – Die Blockchains sollten schon einen gewissen Reifegrad erreicht haben, das Konzept dahinter sollte stimmig und sicher sein
    - Möglichkeit, Daten anonymisiert in der Blockchain zu speichern

Leider erfüllte keine der evaluierten Blockchains alle Anforderungen in einem zufriedenstellenden Maß. Daher wurde entschieden, auf eine nicht-verteilte, Blockchain-artige Speicherung der Daten, abgesichert durch Zeitstempel externer Timestamp-Server zu setzen. Der Austausch dieser für die Speicherung der Wahlergebnisse gewählten Methode durch eine Blockchain-basierte Methode sollte aber in Zukunft einfach möglich sein, falls sich eine Blockchain in Zukunft für diesen Einsatz anbietet.

- *Kryptographische Methoden*: Für die Umsetzung der Wahl an sich wurde eine Reihe von Verfahren evaluiert, die einerseits eine anonyme Stimmabgabe, die Nachvollziehbarkeit der korrekten Stimmzählung sowie einen Identitätsnachweis ermöglichen sollen. Am Ende wurde ein einfaches Verfahren unter Verwendung der Bürgerkarte ausgewählt.

Auch im Rahmen dieses Arbeitspakets kam es zu Verzögerungen. Einerseits waren die dafür zuständigen Projektteammitglieder Michael Faschinger und Felix Klengel anderweitig bis Anfang Juni mehr gebunden als geplant, andererseits hatten die Verzögerungen aus Arbeitspaket 1 und Arbeitspaket 3 Auswirkungen auf die Zeitpunkte, zu denen Technologieentscheidungen gefällt wurden. Dieses Arbeitspaket wurde erst Ende Juni statt wie ursprünglich geplant mit Ende Mai abgeschlossen.

2.3 Arbeitspaket 3 – User Interface Prototyp erarbeiten

Ziel dieses Arbeitspakets ist es, ein Bedienkonzept für die Bürgerkarten-Webseite zu erstellen. Grundlage dafür waren die in Arbeitspaket 1 identifizierten Anforderungen. In einem ersten Schritt wurde eine Übersicht aller verfügbaren Seiten (z.B. zum Erstellen einer Wahl, zum Abstimmen, zur Ansicht der Ergebnisse) erstellt und deren Beziehung untereinander beschrieben. Derzeit läuft die erste Design-Iteration, in der für die Startseite sowie einige der Unterseiten ein User Interface entworfen wird. Erste Drafts sind bereits verfügbar.
Auch in diesem Arbeitspaket kam es zu Verzögerung aufgrund der fehlenden Verfügbarkeit von Michael Faschinger sowie wegen Verzögerungen aus Arbeitspaket 1. Ein Abschluss des Arbeitspakets ist mit Ende Juli geplant.

2.4 Arbeitspaket 4 – Umsetzung und Realisierung

Nachdem in Arbeitspaket 2 die Entscheidung für den Hosting-Provider sowie für das Applikationsframework gefallen war, wurden bereits erste Teile des Backends umgesetzt. Dadurch wurde auch die Evaluierung der Frontend-Bibliotheken bzw. der Bedienkonzepte erleichtert.
Derzeit ist ein erheblicher Teil des Backends, der der Verwaltung von Wahlen und Abstimmungen dient, bereits umgesetzt. Es ist derzeit bereits möglich, Wahlen anzulegen, zu bearbeiten, Fragen zu Wahlen hinzuzufügen und zu bearbeiten. Die implementierten Komponenten werden automatisiert mit Unit-Tests sowie manuell getestet. Der aktuelle Stand der Entwicklung ist im Github-Repository der Bürgerchain auf https://github.com/michivo/buergerchain zu sehen.
Nach dem Abschluss der Arbeitspakete 2 und 3 wird das Hauptaugenmerk auf Arbeitspaket 4 liegen. Eine zeitgerechte Umsetzung dieses Arbeitspakets ist nach wie vor realistisch.

2.5 Arbeitspaket 5 – Öffentlichkeitsarbeit und Dokumentation

Im Februar 2018 wurde im Rahmen eines Berichts über das netidee-Förderjahr 2017 ein Interview mit Michael Faschinger im Ars Electronica Blog veröffentlicht (siehe https://www.aec.at/aeblog/de/2018/02/12/netidee-2017/).
Im Mai 2018 hielt Michael Faschinger im Rahmen der Linuxwochen Wien 2018 einen Vortrag zum Thema „Bürgerchain – e-Voting mit der Blockchain: Die Suche nach der richtigen Blockchain“. Wie

der Titel schon sagt, ging es bei dem Vortrag vor allem darum, unter welchen Gesichtspunkten eine Blockchain für das Projekt „Bürgerchain“ gesucht wurde und welche Probleme dabei aufgekommen sind. Sowohl der Vortrag als auch die anschließende Diskussion mit den Zuhörern waren eine interessante und aufschlussreiche Möglichkeit für einen aktiven Austausch mit der Open Source Community.
Die Dokumentation für die bisher durchgeführten Arbeiten sowie die Entwicklerdokumentation werden in den nächsten Wochen im Projekt-Wiki auf https://github.com/michivo/buergerchain/wiki veröffentlicht.

3 Zusammenfassung Planaktualisierung

Wie unter Punkt 2 schon erläutert, gibt es bei einigen Arbeitspaketen Verzögerungen, die jedoch kein großes Risiko für den Erfolg des Gesamtprojekts darstellen. Konkret ergeben sich zum ursprünglichen Projektplan folgende Veränderungen:
Meilenstein 2 wurde am 15.5. statt am 15.3.2018 erreicht.
Meilenstein 3 wird voraussichtlich am 27.7. statt am 27.4.2018 erreicht.
Arbeitspaket 2 wurde mit 30.6. statt wie geplant mit 31.5. abgeschlossen.
Arbeitspaket 3 wird voraussichtlich mit 31.7. statt wie geplant mit 31.5. abgeschlossen.
Bezüglich der geplanten Aufwände je Arbeitspaket gab es geringfügige Abweichungen (Verschiebungen zwischen den Personen, zeitliche Abweichungen), die sich im für so ein Projekt üblichen Rahmen bewegen.

Hauptgrund für die Verzögerungen war, dass Michael Faschinger neben seiner Tätigkeit für das Projekt in den vergangenen Monaten als Lehrender an einer Fachhochschule tätig war und daher nicht im erwarteten Ausmaß für das bürgerchain-Projekt arbeiten konnte. In den kommenden Monaten wird Michael Faschinger sich vollständig dem bürgerchain-Projekt widmen können, weitere Verzögerungen sind daher nicht zu erwarten.

4 Öffentlichkeitsarbeit/ Vernetzung

Wie in Punkt 2.5 schon erwähnt war das Projekt bürgerchain im Ars Electronica-Blog mit einem Interview und bei den Linuxwochen Wien 2018 mit einem Vortrag vertreten.
Ob und in welcher Form das Projekt beim Ars Electronica Festival in Linz im September 2018 vertreten sein wird, wird in den nächsten Tagen geklärt.