

# **Blockchain-basiertes E-Voting**

Artem Vasilev, Achim Kriso, Philipp Schaback, Tim Fröhlich, David Schuldes

2018-05-29

# Inhaltsverzeichnis

<b>1 Produktübersicht</b>	<b>4</b>
<b>2 Zielbestimmung</b>	<b>4</b>
2.1 Musskriterien . . . . .	4
2.2 Sollkriterien . . . . .	6
2.3 Kannkriterien . . . . .	6
2.4 Abgrenzungskriterien . . . . .	7
<b>3 Produkteinsatz</b>	<b>8</b>
3.1 Anwendungsbereiche . . . . .	8
3.2 Zielgruppen . . . . .	8
<b>4 Produktumgebung</b>	<b>8</b>
4.1 Software . . . . .	8
4.2 Hardware . . . . .	8
4.3 Orgware . . . . .	9
4.4 Schnittstellen . . . . .	9
<b>5 Funktionale Anforderungen</b>	<b>9</b>
<b>6 Produktdaten</b>	<b>12</b>
<b>7 Produktleistungen</b>	<b>13</b>
<b>8 Weitere Nicht-Funktionale Anforderungen</b>	<b>13</b>
<b>9 Qualitätsanforderungen</b>	<b>13</b>
<b>10 Globale Testfälle</b>	<b>15</b>
<b>11 Systemmodelle</b>	<b>18</b>
11.1 Use-Case-Diagramm . . . . .	18
11.2 Netzwerk . . . . .	19
11.3 Systemarchitektur . . . . .	20
<b>12 Benutzeroberfläche</b>	<b>21</b>
12.1 Wahlleiter . . . . .	21
12.2 Wähler . . . . .	28
<b>13 Spezielle Anforderungen an die Entwicklungsumgebung</b>	<b>31</b>
<b>14 Zeit- und Ressourcenplanung</b>	<b>31</b>



# 1 Produktübersicht

Bei herkömmlichen E-Voting Lösungen gestaltet es sich als problematisch, Manipulation von Wahlergebnissen zu verhindern und den Wählern zu gewährleisten, dass ihre Stimme unverändert in die Wahl eingegangen ist.

Die Blockchain E-Voting Software löst diese Probleme mithilfe der Blockchain-Technologie. Sobald ein Wähler seine Stimme abgibt wird sie im Blockchain-Ledger gespeichert und kann nicht mehr verändert werden. Über diesen Weg garantiert die Software, dass seine Stimme nicht verloren geht und unverändert gespeichert wurde.

# 2 Zielbestimmung

## 2.1 Musskriterien

**M1**

### **Unterstützte Wahlformen**

Implementiert durch: F3

Die Software unterstützt das Mehrheitswahl-Prinzip. Es ist möglich eine Wahl aufzusetzen, bei der der Gewinner nach dem Prinzip der Relativen Mehrheitswahl ermittelt wird. Es wird sichergestellt, dass der Wähler nur eine Stimme abgeben kann.

**M2**

### **Erstellung einer Wahl**

Implementiert durch: F1 F2 F4 F5 F6 F7 F8

Ein Wahlleiter kann eine Wahl über seine Benutzeroberfläche konfigurieren. Wenn eine Wahl gestartet ist können nur Wähler die als wahlberechtigt authentifiziert sind die Wahl in ihrer Benutzeroberfläche sehen.

**M3**

### **Teilnahme an einer Wahl**

Implementiert durch: F9 F10 F11 F12

Wenn ein Wähler wahlberechtigt ist hat er die Möglichkeit, abhängig von dem Auszählungsverfahren, einen oder mehrere Kandidaten in seiner Benutzeroberfläche auszuwählen. Wenn beispielsweise das Instant-Runoff-Voting ausgewählt ist kann der Wähler mehrere Kandidaten bewerten, während bei den Mehrheitswahlen nur ein Kandidat ausgewählt werden kann. Wenn der Wähler seine Auswahl bestätigt wird sie vom Klient an das Netzwerk übermittelt.

**Rückmeldung bei Stimmabgabe****M4**

Implementiert durch: F13

Wenn ein Wähler seine Stimme abgegeben hat wird er über seine Benutzeroberfläche informiert, ob seine Stimmabgabe erfolgreich war oder nicht. Eine Stimmabgabe ist genau dann erfolgreich, wenn die Stimme im Blockchain-Ledger eingetragen wurde.

**Stimmenübermittlung****M5**

Implementiert durch: F9 F12

Ist die Stimmabgabe eines Wählers erfolgreich garantiert die Software, dass seine Stimme unverändert zum Blockchain-Ledger hinzugefügt wurde.

**Stimmenauszählung****M6**

Implementiert durch: F14 F15

Sobald eine Wahl beendet ist werden alle erfolgreich abgegebenen Stimmen mit einem Auszählungsverfahren ausgezählt. Das Auszählungsverfahren wird bei der Wahlkonfiguration festgelegt.

**Graphische Benutzeroberfläche für Wahlleiter****M7**

Implementiert durch: F1 F2 F3 F4 F5 F6 F7 F8

Der Wahlleiter kann über seine Benutzeroberfläche eine Wahl konfigurieren. Ist eine Wahl gestartet wird der aktuelle Wahlstand auf seiner Benutzeroberfläche angezeigt. Ist die Wahl beendet wird das Ergebnis der Auszählung auf der Benutzeroberfläche angezeigt.

**Graphische Benutzeroberfläche für Wähler****M8**

Implementiert durch: F9 F10 F11 F13

Die Benutzeroberfläche des Wählers bietet Informationen über die Kandidaten, erlaubt es für einen Kandidaten zu stimmen. Ihm werden außerdem die Beschreibung der Wahl, als auch die Beschreibungen der Kandidaten angezeigt.

## 2.2 Sollkriterien

**S1**

### Absolute Mehrheitswahl

Implementiert durch: F3

Wahlen können mit dem Auszählungsverfahren der Absoluten Mehrheitswahl ausgewertet werden. Die Absolute Mehrheitswahl ist dementsprechend eine Option die dem Wahlleiter zur Verfügung gestellt wird. Sollte zum Ende der Wahl keiner der Kandidaten 50% erreicht haben gibt es keinen Gewinner. In diesem Fall wird dem Wahlleiter die Möglichkeit geboten die Wahl erneut zu starten.

**S2**

### Speichern der Konfiguration

Implementiert durch: F1 F5 F7

Der Wahlleiter kann eine Konfiguration in einer Datei abspeichern und wieder laden. Diese Funktionalität ist in dem Konfigurationsmenü erreichbar. Das Laden einer solchen Datei überschreibt alle Informationen die schon in dem Konfigurationsmenü eingegeben wurden.

**S3**

### Dynamische Peer-Verbindung

Implementiert durch: F16

Beim Verbindungsauflauf eines Klienten zum Blockchain-Netzwerk verbindet sich dieser mit dem Peer der die niedrigste Latenz aufweist. Der Klient ermittelt erst die Latenz aller Peers und verbindet sich dann mit demjenigen, der die niedrigste Latenz aufweist.

## 2.3 Kannkriterien

**K1**

### Instant-Runoff-Voting

Implementiert durch: F3

Das Auszählungsverfahren Instant-Runoff-Voting kann benutzt werden um eine Wahl auszuwerten und wird dem Wahlleiter zur Auswahl gestellt.

**K2**

### Geheime Wahlen

Implementiert durch: F2

Wähler können ihre Stimmen abgeben, so dass sie nur für den Wahlleiter der Wahl einsehbar ist. Das wird mit einem asymmetrischen Verschlüsselungsverfahren erreicht. Das Wahlergebnis kann am Ende der Wahl vom Wahlleiter an die Wähler propagiert werden.

**Verteilung von Zugangsdaten****K3**

Implementiert durch: F4

Der Wahlleiter kann die Zugangsdaten von Wählern (dessen Zertifikat) für die Wahl per Email an die Wähler zu verteilen.

**Automatisches Wahlende****K4**

Implementiert durch: F14

Bestimmung einer weiteren Endbedingung bei der Wahlkonfiguration deren Erfüllung die Wahl automatisch beendet. Eine Wahl ist beendet, wenn der bei der Wahlkonfiguration festgelegte Endzeitpunkt der Wahl erreicht ist oder wenn die zusätzlich festgelegte Endbedingung erreicht ist. Die zusätzlichen Endbedingungen sind:

- Ein bei der Wahlkonfiguration festgelegter Prozentsatz an Wählern hat seine Stimme erfolgreich Stimmabgabeabgegeben.
- Ein Kandidat hat einen bei der Wahlkonfiguration festgelegten Prozentsatz an insgesamt zugelassenen Wählern erreicht.

## 2.4 Abgrenzungskriterien

**Unveränderbarkeit einer Stimme****A1**

Sobald der Wähler eine Stimme abgegeben hat, kann er diese nicht mehr ändern. Das gilt insbesondere auch wenn die Wahl noch läuft.

**Kein Speichern von Wahlverhalten****A2**

Der Blockchain-Ledger, der die Stimmabgaben enthält wird nach finalem Beenden der Wahl durch den Wahlleiter gelöscht. Deswegen ist das Wahlverhalten (die Stimmabgaben eines Wählers aus früheren Wahlen) für keinen Benutzer der Software einsehbar.

**Vertrauen in den Wahlleiter****A3**

Die Legitimität einer Wahl beruht auf der Vertrauenswürdigkeit des Wahlleiters. Wenn der Wahlleiter seine Wahl manipulieren möchte, so sind keine Maßnahmen im System vorhanden die ihn davon stoppen können. Beispielsweise könnte der Wahlleiter im Namen der Wähler wählen, da er alle Zertifikate der Wähler besitzt.

## **3 Produkteinsatz**

### **3.1 Anwendungsbereiche**

Die Software wird zur Durchführung von kleinen Wahlen oder Abstimmungen im Rahmen von Vereinen, Firmen oder Parlamenten verwendet.

### **3.2 Zielgruppen**

1. Wähler
2. Wahlleiter

## **4 Produktumgebung**

### **4.1 Software**

Die Software soll für das Erstellen und Verwalten der Blockchain das Hyperledger Fabric Framework verwenden. Das Framework bietet eine auf dem Consensus-Verfahren basierende Blockchain-Implementierung. Hierfür wird die Hauptanwendung in Java 7 geschrieben und das Hyperledger Fabric Java SDK verwendet. Für das erstellen von Chaincodes soll Go verwendet werden. Um die Funktionalität von Hyperledger Fabric zu gewährleisten wird ebenso eine Installation von GoLang benötigt.

### **4.2 Hardware**

Es werden Computer für die Wähler und den Wahlleiter benötigt. Diese Computer müssen mit einer Internetverbindung ausgestattet sein und mindestens Java 7 installiert haben.

## **4.3 Orgware**

1. Installation der Software, die für das Funktionieren von Hyperledger erforderlich ist.  
(siehe <http://hyperledger-fabric.readthedocs.io/en/release-1.1/prereqs.html>)
2. Anlegen des Netzwerks, wenn es keines gibt.

## **4.4 Schnittstellen**

Die Wahl eines Wählers wird im Blockchain-Ledger gespeichert und über das Blockchain-Netzwerk verteilt.

## **5 Funktionale Anforderungen**

### **Erstellung einer Wahl**

**F1**

Getestet durch: T1 Implementiert: M2 M7 S8

Der Wahlleiter kann eine neue Wahl erstellen. Es existiert immer nur eine Wahl zu einem Zeitpunkt. Zudem kann eine Vorher abgespeicherte Wahlkonfiguration geladen werden. Hierbei öffnet sich das Konfigurationsmenü mit den geladenen Einstellungen in der Übersichtsseite. Der Wahlleiter wird durch die Erstellung geführt. Es sind folgende Schritte notwendig:

### **Allgemeine Konfiguration der Wahl**

**F2**

Getestet durch: T1 T3 Implementiert: M2 M7 K2

Der Wahlleiter legt den Namen und einen Beschreibungstext der Wahl fest. Er setzt den Start- und Endzeitpunkt der Wahl.

**F3**

### **Auswahl des Auszählungsverfahrens**

Getestet durch: T1 Implementiert: M1 M7 S8 K1

Die Festlegung eines Auszählungsverfahrens ist möglich. Es stehen die folgenden zur Verfügung:

- Relative Mehrheitswahl
- Absolute Mehrheitswahl
- Instant-Runoff-Voting

**F4**

### **Hinzufügen von Wählern**

Getestet durch: T1 Implementiert: M2 M7 K3

Der Wahlleiter fügt die Wähler mit ihrem Namen hinzu. Das System generiert automatisch die erforderlichen Zertifikate. Die Zertifikate werden im Netzwerk verteilt. Nur die hinzugefügten Wähler sind zur Teilnahme berechtigt.

Der Wahlleiter kann außerdem die Zertifikate per Email an die Wähler senden.

**F5**

### **Importieren der Wahlkonfiguration**

Getestet durch: T4 Implementiert: M2 M7 S8

Der Wahlleiter hat beim aufsetzen einer neuen Wahl im Konfigurationsmenü die Möglichkeit eine existierende Konfigurationsdatei zu benutzen um die Wahl zu erstellen. Die Konfigurationsdatei enthält Einstellungen um eine neue Wahl aufzusetzen. Sie kann vom Wahlleiter aus einer bereits aufgesetzten Wahl erzeugt werden.

**F6**

### **Hinzufügen von Kandidaten**

Getestet durch: T1 Implementiert: M2 M7

Der Wahlleiter fügt die Kandidaten mit ihrem Namen hinzu. Es ist außerdem möglich jedem Kandidaten eine Beschreibung zu geben, die den Wählern in ihrer GUI angezeigt wird. Das System propagiert die Kandidaten automatisch an das Netzwerk.

**F7**

### **Exportieren der Wahlkonfiguration**

Getestet durch: T4 Implementiert: M2 M7 S8

Der Wahlleiter hat die Möglichkeit seine vorgenommenen Einstellungen in einer Datei zu exportieren. Es wird ein Dateibrowser geöffnet in welchem der Speicherort für die Konfigurationsdatei festgelegt werden kann. Die gespeicherte Konfigurationsdatei beinhaltet alle Einstellungen der Wahl.

**Aktivierung der Wahl****F8**

Getestet durch: T1 Implementiert: M2 M7

Der Wahlleiter bestätigt seine Einstellungen zur Wahl. Mit der Bestätigung beginnt die Übertragung der Informationen in das Netzwerk. Die Wahl startet zum festgelegten Zeitpunkt.

**Wahlfunktion für Wähler****F9**

Getestet durch: T1 T2 Implementiert: M3 M5 M8

Der Wähler kann an der laufenden Wahl teilnehmen. Er durchläuft dazu folgende Schritte:

**Authentifizierung mittels Zertifikat****F10**

Getestet durch: T1 Implementiert: M3 M8

Der Wähler authentifiziert sich gegenüber dem Netzwerk mit seinem Zertifikat. Ist er zur Wahl nicht berechtigt oder hat schon gewählt wird er darauf hingewiesen. Andernfalls kann er wählen.

**Auswählen eines Kandidaten****F11**

Getestet durch: T1 Implementiert: M3 M8

Dem Wähler stehen die vom Wahlleiter festgelegten Kandidaten zur Auswahl. Der Wähler kann einen der Kandidaten auswählen. Er kann seine Auswahl beliebig oft ändern.

**Übermittlung der Stimme****F12**

Getestet durch: T1 Implementiert: M3 M5

Bestätigt er seine Wahl, so wird die Stimme in den Blockchain-Ledger geschrieben. Sie ist hiermit final übernommen und kann nicht länger geändert werden.

**Rückmeldung an den Wähler****F13**

Getestet durch: T1 Implementiert: M8 M4

Wenn die Stimme erfolgreich im Blockchain-Ledger aufgenommen wurde, erhält der Wähler eine Bestätigung über seine GUI. Sonst erhält der Wähler eine Benachrichtigung, dass seine Wahl fehlschlug. Er kann dann zur Auswahl der Kandidaten zurückkehren und seine Stimme erneut abgeben.

**F14**

**Beenden der Wahl**

Getestet durch: T1 Implementiert: M6 K4

Die Wahl endet zum eingestellten Zeitpunkt (oder bei Erreichen des zusätzlichen Kriteriums) automatisch. Stimmabgaben der Wähler sind nicht länger möglich/gültig. Die Auswertung der Wahl beginnt:

**F15**

**Auszählung der Stimmen**

Getestet durch: T1 Implementiert: M6

Die Auszählung findet in jedem Klienten statt. Dieser fragt die Stimmen von seinem Peer ab und bestimmt, abhängig vom dem Auszählungsverfahren, welcher Kandidat gewonnen hat. Das Ergebnis der Auszählung wird daraufhin auf den GUIs des Wählers als auch des Wahlleiters dargestellt.

**F16**

**Dynamische Peer-Verbindung**

Getestet durch: T1 T2 T3 Implementiert: S8

Der Klient verbindet sich automatisch mit einem Peer im Blockchain-Netzwerk. Dabei beachtet er die Latenzen aller Peers und wählt den mit der kleinsten Latenz aus.

## **6 Produktdaten**

Die Stimmabgaben der Wahlteilnehmer werden auf einem Blockchain-Ledger gespeichert. Die Zertifikate der Wähler werden in Datenbanken im Netzwerk gespeichert. Diese Daten gehen verloren sobald der Blockchain-Ledger gelöscht wird. Es werden keine weiteren Benutzerdaten gespeichert.

## 7 Produktleistungen

Die Software muss die abgegebene Wahl eines jeden Wählers zählen. Eine abgegebene Stimme ist unverfälscht im Wahlergebnis enthalten. Jede abgegebene Stimme muss in der Auszählung der Wahl vertreten und somit dargestellt sein.

Die Software muss dem Wähler auf der Benutzeroberfläche deutlich machen ob seine Wahl erfolgreich war oder nicht.

Die Abgabe einer Stimme dauert nicht länger als 5 Minuten. Die GUI reagiert hierbei sofort um dem Benutzer Rückmeldung über seine Aktion geben.

Die Auszählung einer Wahl unter einer Stimmenzahl von 10.000 Wählern dauert nicht länger als 5 Minuten.

## 8 Weitere Nicht-Funktionale Anforderungen

### Einfache Benutzung

N1

Die Wahl sollte für einen Benutzer mit nur geringen Computerkenntnissen möglich sein.

### Verifizieren der Wahlberechtigung

N2

Es soll nur denjenigen Benutzern möglich sein an einer Wahl teilzunehmen, welche die hierzu notwendigen Berechtigungen haben.

### Manipulation der Wahl

N3

Es soll nicht möglich sein die Wahl eines Anderen zu ändern, Stimmen zu löschen oder anderweitig das Ergebnis der Wahl zu manipulieren.

## 9 Qualitätsanforderungen

### Korrektheit der Wahlergebnisse

Q1

Sofern ein Wähler seine Stimme erfolgreich abgegeben hat, ist diese garantiert im Wahlergebnis enthalten. Sie wurde dem Kandidaten, für den gewählt wurde, angerechnet.

## **Q2      Protokollierung des Netzwerkes**

Ereignisse und Probleme auf dem Blockchain-Netzwerk werden in einer Logdatei chronologisch protokolliert. Diese Logdatei ist für den Wahlleiter einsehbar.

## **Q3      Unveränderbarkeit der Wahl**

Sobald die Wahl vom Wahlleiter einmal aufgesetzt wurde, können die Einstellungen dieser Wahl von niemandem (insbesondere vom Wahlleiter) mehr verändert werden.

## **Q4      Vermeidung von unlogischen Eigenschaften der Wahl**

Während dem festlegen der Einstellungen der Wahl wird der Wahlleiter auf Probleme in der Konfiguration hingewiesen. Folgende Fehler werden berücksichtigt:

- Kein oder nur ein Kandidat wurde eingetragen.
- Kein oder nur ein Wähler wurde eingetragen.
- Einem Wähler oder Kandidaten wurde kein Name gegeben.
- Der Wahl wurde kein Name gegeben.
- Die Wahl endet vor oder demselben Zeitpunkt an dem sie startet.

## **Q5      Verhinderung des Double-Spending-Problems**

Jeder Wähler kann nur einmal seine Stimme erfolgreich abgeben. Eine erneute Abgabe seiner Stimme resultiert in einer Fehlermeldung auf der Benutzeroberfläche des Wählers, die ihn auf das Problem hinweist.

## **Q6      Vermeidung von ungewollten Enthaltungen**

Falls ein Wähler seine Wahl auf seiner GUI bestätigen möchte, ohne dass dieser für einen der Kandidaten gestimmt hat, wird eine Warnung angezeigt die darauf hinweist.

## **Q7      Warnungen bei Netzwerkproblemen**

Bei Problemen die Stimme eines Wählers in das Blockchain-Netzwerk zu übertragen, wird dieser Wähler in seiner GUI darüber informiert. Er hat dann die Möglichkeit seine Stimme erneut abzugeben.

## 10 Globale Testfälle

T1

### Ablauf einer Wahl

Testet: F1 F2 F3 F4 F6 F8 F9 F10 F11 F12 F13 F14 F15 F16

T1.1 **Stand:** Wahlleiter „Fritz Müller“ hat die GUI geöffnet um eine neue Wahl aufzusetzen.

**Aktion:** Fritz gibt den Namen „Vorstandswahl 2018“ an, wählt als Wahlsystem die Relative Mehrheitswahl aus und fügt eine passende Beschreibung hinzu.

Fritz fügt „Max Mustermann“, „Anna Meier“, „Erich Schmitt“ und 10 andere Wähler hinzu.

Zuletzt werden „Johannes Heinzhof“, „Wolfgang Rudolf“ und „Sabine Scholl“ als Wahlmöglichkeiten von Fritz festgelegt,

**Reaktion:** Die Zertifikate für alle zugelassenen Wähler werden generiert.

T1.2 **Stand:**

**Aktion:** Fritz wählt aus, dass die Wahl am 1. August 2018 beginnt und am 31. August 2018 endet. Er bestätigt seine Eingaben.

**Reaktion:** Die Wahl ist jetzt im Blockchain-Netzwerk aktiv.

T1.3 **Stand:** Max Mustermann startet die Wähler GUI am 1. August 2018

**Aktion:** Max gibt seinen Namen und sein Authentifizierungs Zertifikat an.

**Reaktion:** Die GUI updatet sich und zeigt alle Wahlmöglichkeiten an

T1.4 **Stand:**

**Aktion:** Max wählt „Sabine Scholl“ aus den Wahlmöglichkeiten aus und bestätigt seine Wahl.

**Reaktion:** Die GUI schickt seine Stimme ab und informiert ihn dass diese erfolgreich gezählt wurde.

T1.5 **Stand:** Der 31. August 2018 ist erreicht.

**Aktion:** Die Wahl beendet sich auf dem Blockchain-Netzwerk.

**Reaktion:** Die Wahlergebnisse können auf den GUIs eingesehen werden.

**T2**

## **Verhinderung von Angriffsversuchen auf die Wahl**

Testet: F9 F16

T2.1 **Stand:** Wiederholung des Schritte von T1 1.1-1.4

**Aktion:** Max startet erneut eine Wähler GUI und gibt seine Namen und Zertifikat an.

**Reaktion:** Die GUI teilt ihm mit, dass seine Stimme schon gegeben wurde und bricht den Wahlvorgang ab.

T2.2 **Stand:**

**Aktion:** Max startet erneut eine Wähler GUI und gibt den Namen „Anna Meier“ und sein ursprüngliches Zertifikat an.

**Reaktion:** Die GUI teilt ihm mit, das sein Zertifikat ungültig für den gegebenen Namen ist und bricht den Wahlvorgang ab.

**T3**

## **Fehlerhafte Wahlkonfigurationen**

Testet: F2 F16

T3.1 **Stand:** Wahlleiter „Hans Werner“ hat seine GUI geöffnet um eine neue Wahl aufzusetzen

**Aktion:** Hans drückt den „Weiter“ Button solange, bis der „(Fertigstellen) Abschnitt erscheint.

**Reaktion:** Der GUI-Bereich in dem normalerweise der Wahlname eingetragen ist, enthält eine Fehlermeldung die auf den fehlenden Wahlnamen hinweist.

Neben der Liste der Kandidaten erscheint eine Fehlermeldung die auf die fehlenden Kandidaten hinweist.

Neben der Liste der Wähler erscheint eine Fehlermeldung die auf die fehlenden Wähler hinweist.

Der „Bestätigen“ Button ist ausgegraut.

### T3.2 Stand:

**Aktion:** Hans drückt den „Allgemein“ Button. Er gibt der Wahl den Namen „Beste Blockchain“. Er drückt daraufhin zweimal den „Weiter“ Button.

Hans fügt den drei Kandidaten hinzu. Der erste Kandidat bekommt den Namen „Bitcoin“ und der zweite Kandidat den Namen „Cryptokitties“. Der letzte Kandidat bekommt keinen Namen.

Zuletzt fügt Hans die vier Wähler „Martin Schleier“, „Peter Ente“ und „Jürgen Gans“ hinzu. Für den vierte Wähler trägt Hans keinen Namen ein. Hans drückt den „Weiter“ Button.

**Reaktion:** Neben der Liste der Kandidaten erscheint eine Fehlermeldung die darauf hinweist, dass für einen Kandidat kein Name eingetragen wurde.

Neben der Liste der Wähler erscheint eine Fehlermeldung die darauf hinweist, dass für einen Wähler keinen Namen eingetragen wurde.

### T3.3 Stand:

**Aktion:** Hans drückt den „Kandidaten“ Button. Er trägt den Namen „HyperLedger Fabric“ für den dritten Kandidaten ein und drückt „Weiter“.

Er trägt den Namen „Martina Storch“ für den vierten Wähler ein und drückt „Weiter“.

**Reaktion:** Es erscheint keine Fehlermeldung mehr und der „(Bestätigen)“ Button ist anklickbar.

## Import/Export Funktionalität

**T4**

Testet: F5 F7

**T4.1 Stand:** Wahlleiter Konrad Quack hat seine GUI gestartet und hat eine Wahl konfiguriert.

**Aktion:** Im „Fertigstellen“ Abschnitt drückt er den „Exportieren“ Button.

**Reaktion:** Es erscheint eine Dialogbox zum Auswählen von Dateien.

### T4.2 Stand:

**Aktion:** Konrad wählt einen Speicherplatz.

**Reaktion:** Eine Datei die die Wahlkonfiguration enthält wird an diesem Speicherplatz abgespeichert.

**T4.3 Stand:** Konrad hat seine GUI erneut eröffnet.

**Aktion:** Er wählt den „Importieren“ Button.

**Reaktion:** Es erscheint eine Dialogbox zum Auswählen von Dateien.

#### T4.4 Stand:

**Aktion:** Konrad wählt die Wahlkonfigurationsdatei aus.

**Reaktion:** Die Konfigurations-GUI öffnet sich, mit den Einstellungen aus der Datei in die GUI eingetragen.

## 11 Systemmodelle

### 11.1 Use-Case-Diagramm

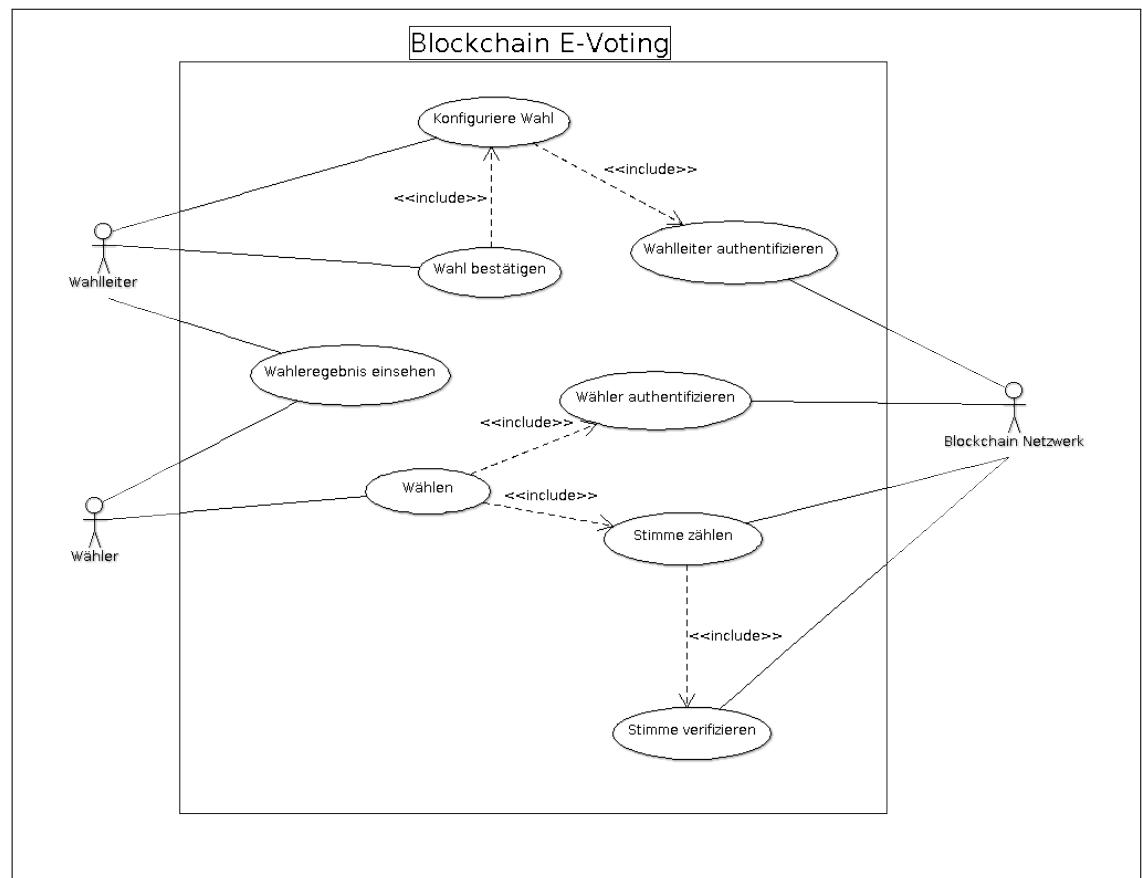


Abbildung 1: Ein Use-Case-Diagramm mit den typischen Funktionen der Software.

## 11.2 Netzwerk

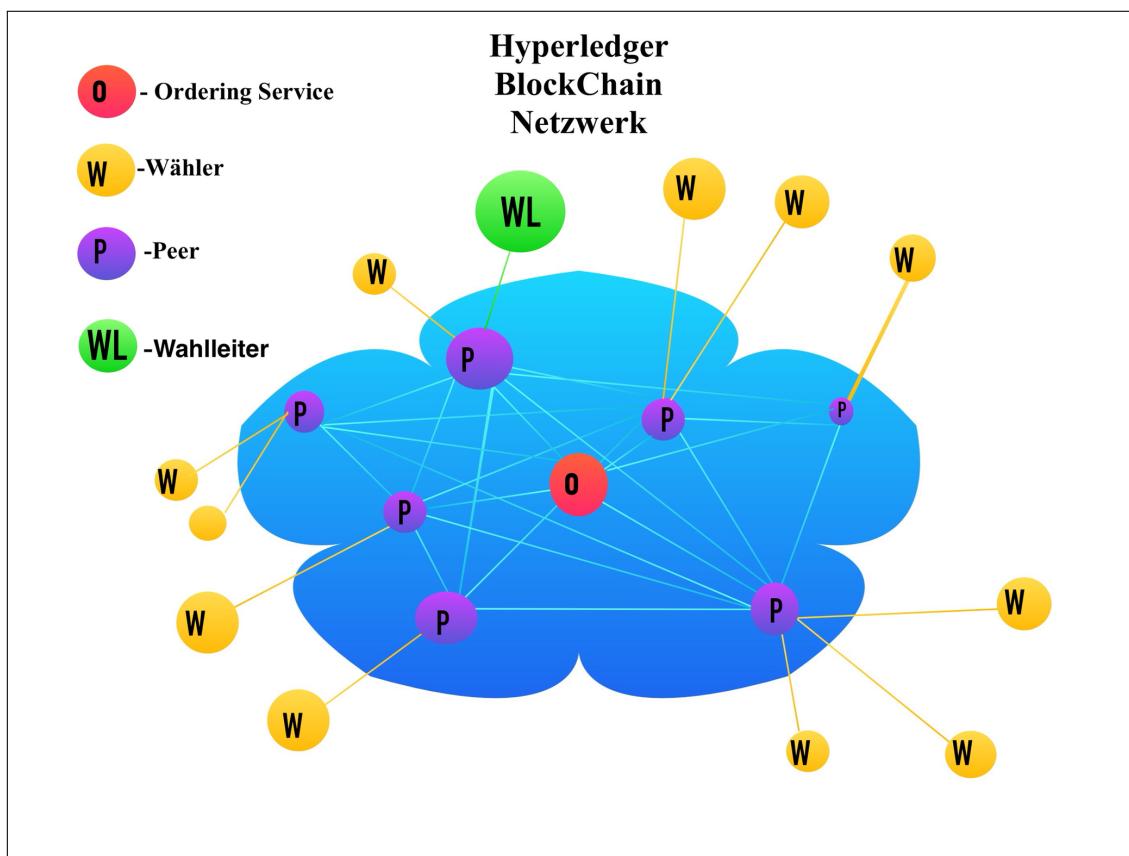


Abbildung 2: Darstellung des Blockchain Netzwerkes.

### 11.3 Systemarchitektur

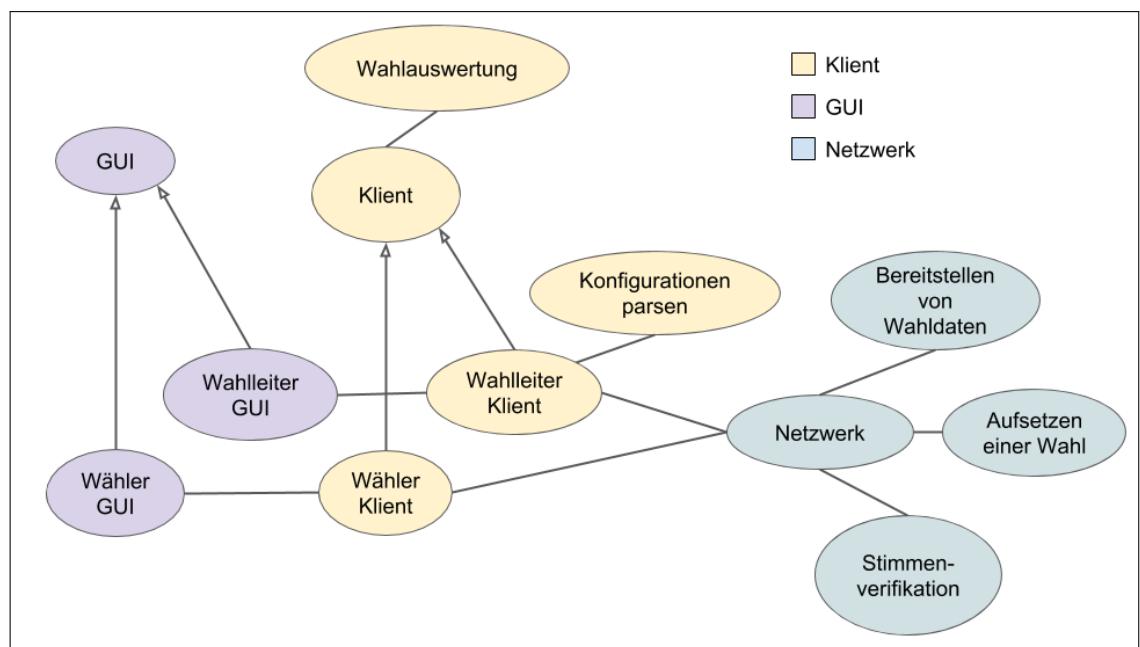


Abbildung 3: Veranschaulichung der vorgesehenen Systemarchitektur.

## 12 Benutzeroberfläche

### 12.1 Wahlleiter

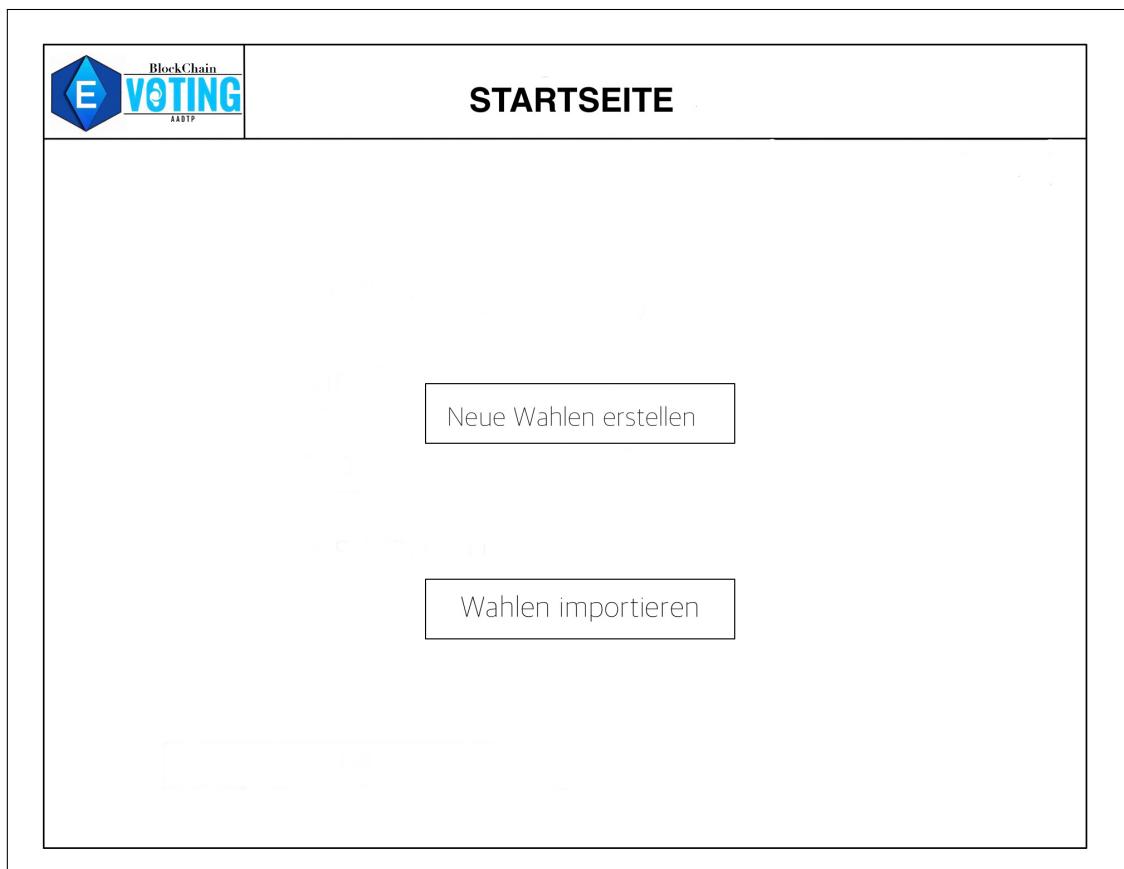


Abbildung 4: Die Startseite der Wahlleiter Benutzeroberfläche;

Der Wahlleiter kann über den „Wahlen importieren“ Button eine bereits konfigurierte Wahl laden oder über „(„Neue Wahlen erstellen) eine neue Wahl konfigurieren.

		<b>Wahlname</b>
<b>Allgemein</b>  <b>Zeitraum</b>  <b>Kandidaten</b>  <b>Wähler</b>  <b>Fertigstellen</b>	Name <input type="text"/>  Wahlsystem <input type="text"/> <input type="button" value="▼"/>  Beschreibung <div style="border: 1px solid black; height: 100px; width: 100%;"></div>	<input type="button" value="Abbrechen"/> <input type="button" value="Weiter"/>

Abbildung 5: Allgemeine Einstellungen einer Wahl.

Der Wahlleiter kann einen Namen für die Wahl eintragen und das zu verwendende Auszählungsverfahren Wahlsystem in einem Dropdown-Menü auswählen. Er kann der Wahl eine Beschreibung hinzufügen, es wird aber nicht vorausgesetzt um die Wahl zu starten. Der „Abbrechen“ Button beendet den Konfiguration, verwirft alle Einstellungen und schließt das Konfigurationsmenü. Bei betätigen des „Weiter“ Buttons wechselt er zum nächsten Schritt der Wahlkonfiguration.

 <h2 style="text-align: center;">Wahlname</h2>	
<b>Allgemein</b>  <b>Zeitraum</b>  <b>Kandidaten</b>  <b>Wähler</b>  <b>Fertigstellen</b>	<p>Anfang <input type="text" value="xx/xx/yyyy"/> <input type="text" value="00:00"/> <input type="button" value="sofort"/></p> <p>Ende <input type="text" value="xx/xx/yyyy"/> <input type="text" value="00:00"/></p> <p><input type="button" value="Extrabedingungen"/> ▽</p> <p style="text-align: right;"><input type="button" value="Abbrechen"/> <input type="button" value="Weiter"/></p>

Abbildung 6: Einstellungen um den Zeitraum der Wahl zu bestimmen.

Der Wahlleiter kann den Anfang und das Ende des Wahlvorgangs bestimmen. Dabei kann er das Datum und die Uhrzeit wählen. Um die Wahl direkt nach der Konfiguration zu starten, kann der Wahlleiter den „sofort“ Button drücken. Die Anfangs Eingabeflächen werden daraufhin auf das derzeitige Datum und Uhrzeit gesetzt. In dem Dropdown-Menü „Extrabedingung“ kann er eine alternative Endbedingung für die Wahl auswählen. Abhängig davon welche der Wahlleiter wählt, erscheinen unter dem Dropdown-Menü noch zusätzliche Optionen für die ausgewählte Extrabedingung.

 <h2 style="text-align: center;">Wahlname</h2>	
<b>Allgemein</b>  <b>Zeitraum</b>  <b>Kandidaten</b>  <b>Wähler</b>  <b>Fertigstellen</b>	<p>1. Name <input type="text" value="Kobe Bryant"/> <input type="button" value="Beschreibung"/> <input type="button" value="-"/></p> <p>2. Name <input type="text" value="Kevin Durant"/> <input type="button" value="Beschreibung"/> <input type="button" value="-"/></p> <p style="text-align: center;"><input type="button" value="+"/></p> <p style="text-align: right;"><input type="button" value="Abbrechen"/> <input type="button" value="Weiter"/></p>

Abbildung 7: Hinzufügen der Kandidaten.

Der Wahlleiter kann über den „+“ Button einen neuen Kandidaten hinzufügen. Auf der Benutzeroberfläche erscheint daraufhin eine neue Zeile. In dem Eingabefeld wird der Name des Kandidaten eingegeben. Der „Beschreibung“ Button ermöglicht es, dem Kandidaten eine optionale Beschreibung zu geben. Dieser Button öffnet ein neues Fenster mit einem Textfeld in das die Beschreibung eingegeben werden kann. Der „-“ Button in jeder Zeile löscht den jeweiligen Kandidaten.

 <b>Allgemein</b>	<h3>Wahlname</h3>	
	1. Name	<input type="text"/> -
	2. Name	<input type="text"/> -
<b>Zeitraum</b>	<input type="button" value="+"/>	
<b>Kandidaten</b>		
<b>Wähler</b>		
<b>Fertigstellen</b>	<input type="button" value="Abbrechen"/> <input type="button" value="Weiter"/>	

Abbildung 8: Hinzufügen der Wähler.

Der Wahlleiter kann nach gleichem Prinzip Wähler hinzufügen und entfernen. Er kann hierbei nur die Namen der Wähler angeben.

<b>Wahlname</b>	
<b>Allgemein</b>	Zeitraum: von _____ bis _____ Beschreibung: <div style="border: 1px solid black; height: 100px; width: 100%;"></div>
<b>Zeitraum</b>	
<b>Kandidaten</b>	Kandidaten: 1.Kobe Bryant 2. Kevin Durant 3. Lebron James 4. James Harden <div style="border: 1px solid black; height: 20px; width: 100%;"></div>
<b>Wähler</b>	Wähler: 1. Max Musterberg 2. Mark Swagman 3. Josy Stalinberg 4. Heinz Lenin <div style="border: 1px solid black; height: 20px; width: 100%;"></div>
<b>Fertigstellen</b>	<div style="text-align: right;"> <input type="button" value="Export"/>  <input type="button" value="Abbrechen"/> <input type="button" value="Bestätigen"/> </div>

Abbildung 9: Übersicht über alle Einstellungen.

Der Wahlleiter sieht alle vorgenommenen Einstellungen seiner Wahl:

1. Den Start- und Endzeitpunkt der Wahl.
2. Die optionale zusätzliche Endbedingung der Wahl.
3. Alle zur Wahl verfügbar stehenden Kandidaten inkl. Name und Beschreibung.
4. Alle zur Wahl berechtigten Wähler und deren Namen.

Bei betätigen des "Export" Buttons kann der Wahlleiter die Konfiguration der Wahl speichern. Bei betätigen des "Bestätigen" Buttons wird die Wahl erstellt.

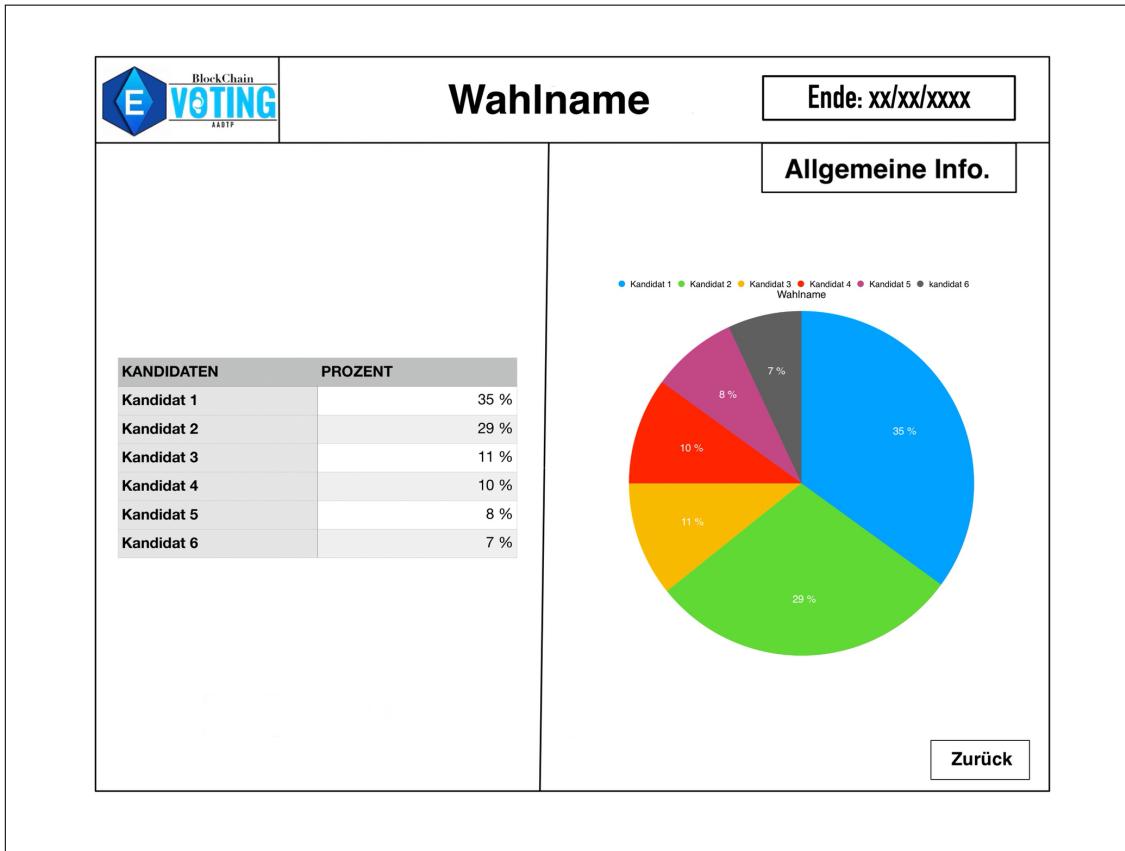


Abbildung 10: Übersicht über den aktuellen Wahlstand.

Der Wahlleiter bekommt während dem Ablauf der Wahl tabellarisch und in Form eines Diagrammes den aktuellen Stand seiner Wahl dargestellt. Über den „Allgemeine Info.“ Button wird die Beschreibung der Wahl anstatt des Diagrammes angezeigt.

## 12.2 Wähler

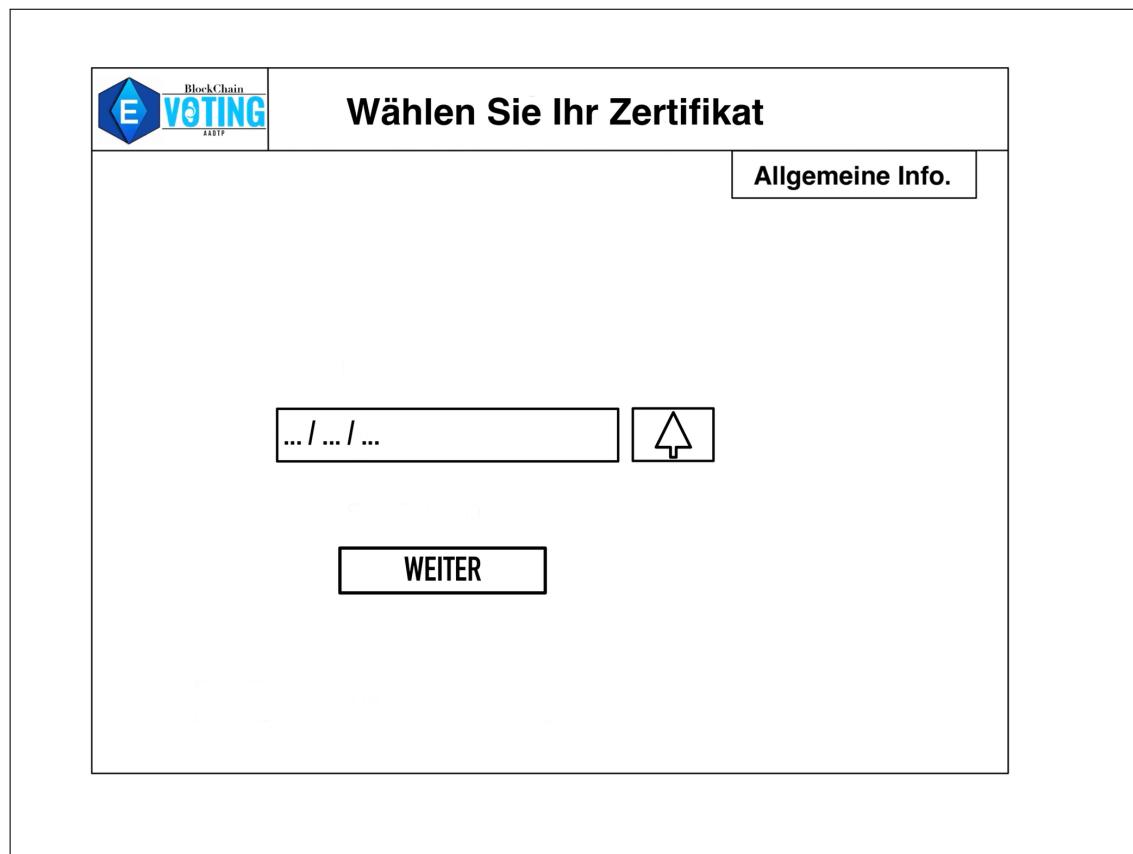


Abbildung 11: Anfangs-GUI die das Zertifikat des Wählers anfragt.

Der Wähler kann sein Zertifikat auswählen indem er den Button mit dem Pfeil nach oben drückt. Es erscheint ein Dateibrowser mit dem er seine Zertifikats-Datei auswählt. Er bestätigt seine Auswahl bei betätigen des „Weiter“ Buttons. Bei erfolgreicher Authentifizierung wird er zur Wahl weiter geleitet.

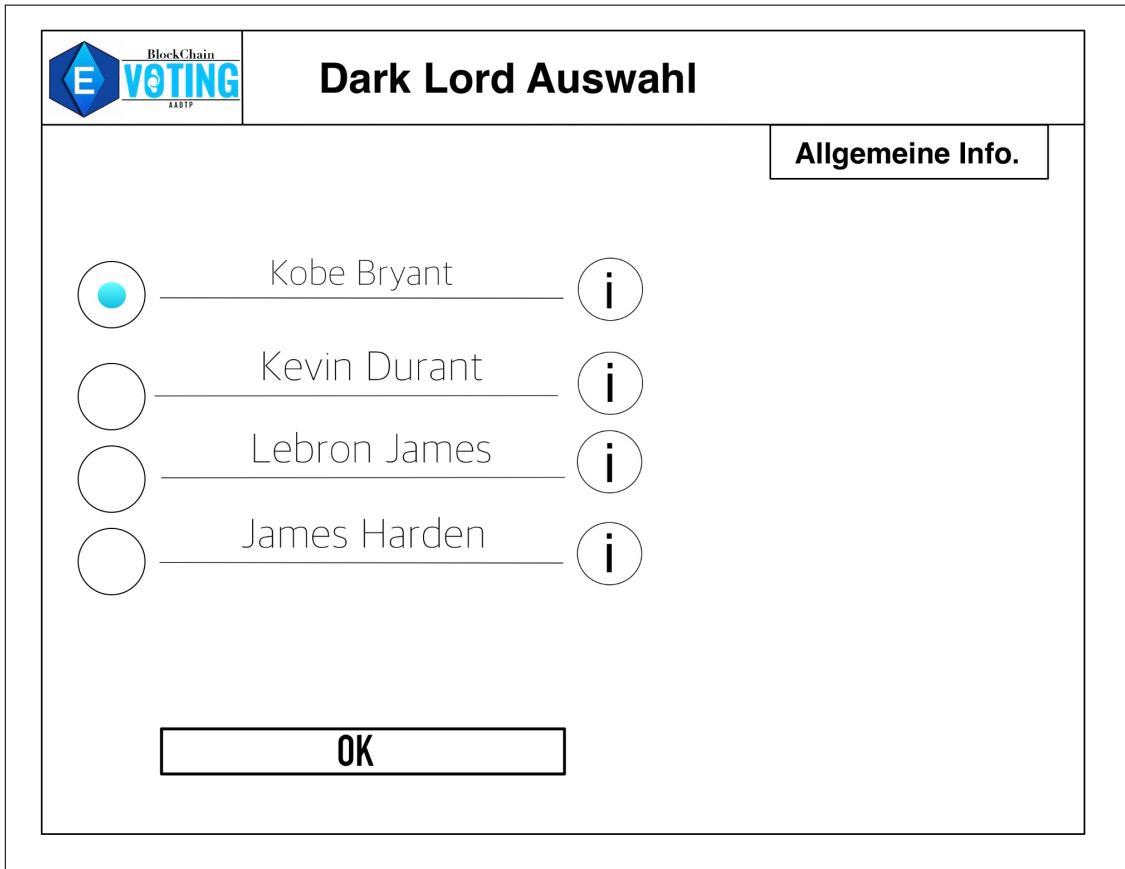


Abbildung 12: Auswahl der Kandidaten.

Der Wähler kann einen oder mehrere Kandidaten auswählen und seine Auswahl beliebig oft ändern. Das anwählen des "i" Buttons zeigt die Beschreibung des entsprechenden Kandidaten im rechten, leeren Bereich der Benutzeroberfläche. Der „Allgemeine Info.“ Button zeigt die Beschreibung der Wahl im rechten, leeren Bereich der Benutzeroberfläche an. Wenn dieser Bereich schon mit einer anderen Beschreibung gefüllt ist, wird diese ersetzt. Bei betätigen des "OK" Buttons wird die Wahl bestätigt.

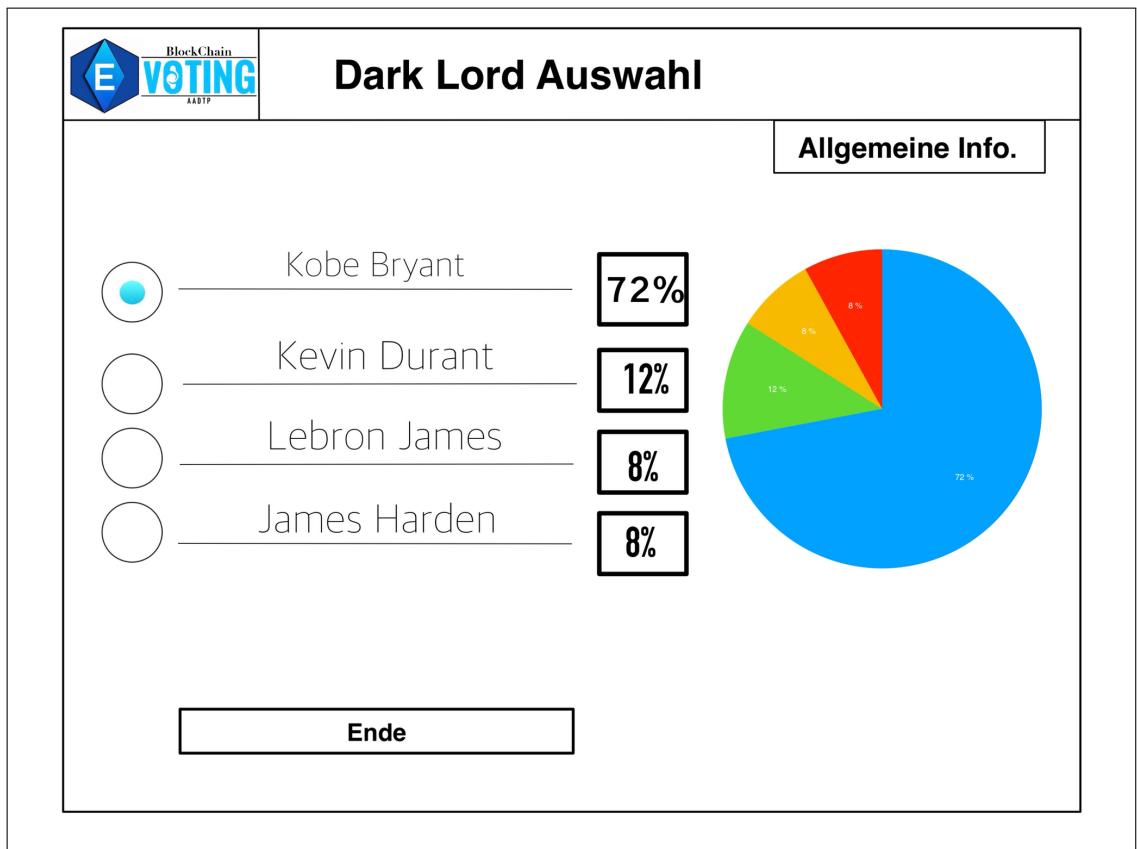


Abbildung 13: Ergebnisse der Wahl.

Der Wähler kann seine abgegebene Auswahl einsehen. Sobald der Wahlvorgang beendet wird sieht er zusätzlich die Ergebnisse der Wahl in der Form vom Prozenten und eines Diagramms. Der „Allgemeine Info.“ Button zeigt die Beschreibung der Wahl an der Stelle des Diagramms. Durch betätigen des „Ende“ Buttons schließt sich die Benutzeroberfläche des Wählers.

## 13 Spezielle Anforderungen an die Entwicklungsumgebung

Zur Entwicklung werden die IntelliJ oder Eclipse IDE verwendet. Zudem wird ein Linux basiertes Betriebssystem verwendet.

## 14 Zeit- und Ressourcenplanung

Das System lässt sich grob in drei Schichten aufgliedern: Benutzeroberfläche, Klient und Blockchain-Netzwerk. Hierfür sind folgende Verantwortlichen vorgesehen:

Benutzeroberfläche - Achim

Klient - David und Artem

Blockchain-Netzwerk - Philipp und Tim

Die zeitliche Einteilung ist wie folgt vorgesehen:

01.06. - 27.06. Entwurf und Entwicklung eines Prototypen.

29.06. - 25.07. Implementierung

10.08. - 29.08. Qualitätssicherung

05.09. Interne Abnahme

## 15 Glossar

### Glossar

**Absolute Mehrheitswahl** Auszählungsverfahren, bei dem der Kandidat gewinnt, der über 50% der Stimmen hat. Ansonsten hat niemand gewonnen. Ein Wähler kann seine Stimme genau einmal abgeben und für genau einen Kandidaten Stimmen. 3, 4, 7

**Auszählungsverfahren** Eine Methode um zu bestimmen, welcher Kandidat bei einer Wahl gewonnen hat. 4, 5, 7, 9

**Benutzer** Eine Person die mit der Software interagiert. 9, 10

**Benutzerdaten** Daten, die für einen Benutzer spezifisch sind. Beispielsweise Name, Geburtsdatum, Herkunftsland und Geschlecht. 9

**Benutzeroberfläche** Grafische Benutzerschnittstelle zu einem Computer, welche eine leichte und intuitiver Benutzung der Software ermöglicht. 3, 4, 8, 9, 11, 12

**Blockchain** Datenbanktechnologie bei der die einzelnen Datensegmente verknüpft werden um so Eigenschaften wie Unveränderbarkeit und Dezentralisierung zu erreichen. 6

**Blockchain-Ledger** Datenbank in einer Blockchain, welche alle Transaktionen, die auf der Blockchain ausgeführt wurden, enthält. In dem Kontext unserer Wahl sind die Transaktionen einzelne Stimmen. Jeder Peer in dem Netzwerk besitzt einen Ledger. 3, 7–9

**Blockchain-Netzwerk** Menge an verknüpften Peers, die zusammen einen synchronisierten Blockchain-Ledger verwalten. 10–12

**Chaincode** Programme die auf der Blockchain laufen und als Schnittstelle eines Peers zur Blockchain dienen. 6

**Double-Spending-Problem** Die mehrfache, erfolgreiche Abgabe einer Stimme in einem Wahlsystem. Die erfolgreiche Stimmabgabe darf pro Wähler maximal einmal erfolgen. 11

**Instant-Runoff-Voting** Auszählungsverfahren, bei dem der Wähler die Kandidaten nach Präferenz ordnet. Sei  $n$  die Anzahl der zur Auswahl stehenden Kandidaten, das Verfahren ist für Wahlen mit 3 oder mehr Kandidaten geeignet:

1. Jeder Wähler kann jedem Kandidaten einen Wert von 1 bis  $n$  zuweisen. Werte dürfen nicht mehrfach vergeben werden. Kandidaten müssen nicht bewertet werden.
2. Bei der Auszählung wird bestimmt welcher Kandidat die wenigsten Stimmen mit Wert 1 bekommen hat. Dieser Kandidat wird dann aus allen Listen entfernt. Die Werte der Kandidaten auf den nachfolgenden Plätzen werden jeweils um 1 abgezogen.
3. Schritt 2 wird so lange wiederholt bis nur noch 2 Kandidaten übrig sind. Der Kandidat mit den meisten ersten Stimmen hat gewonnen.

5, 7

**Kandidat** Eine Entität, für die ein Wähler bei einer Wahl stimmen kann. 4, 8, 9, 17

**Klient** Das Programm das auf den Computern der Wählern und des Wahlleiter läuft. Es stellt die GUI bereit und verwaltet die Kommunikation mit dem Blockchain-Netzwerk. 9

**Konfiguration** Feste Belegung der einstellbaren Eigenschaften eines Systems (hier i.d.R die Wahl). 3, 4, 10

**Konfigurationsmenü** Die Benutzeroberfläche des Wahlleiters in der er eine Wahl konfigurieren kann. 4

**Linux** Beliebtes Unix-like Betriebssystem. 24

**Logdatei** Datei welche alle Ereignisse (Informationen, Warnungen und Fehler) in einem System protokolliert. 10

**Peer** Computer der eine Kopie des Ledgers enthält, diese mit anderen Peers synchronisiert und eine Schnittstelle zwischen Chaincode und Software bereitstellt. 9

**Relative Mehrheitswahl** Auszählungsverfahren, bei dem der Kandidat mit den meisten Stimmen gewinnt. Ein Wähler kann seine Stimme genau einmal abgeben und für genau einen Kandidaten Stimmen. 3, 7

**Stimmabgabe** Hat ein Wähler über die Benutzeroberfläche einen Kandidaten gewählt bestätigt er seine Auswahl. Seine Stimme wird dann vom Klienten an das Blockchain-Netzwerk gesendet. Sofern die Stimme gültig ist wird sie in den Ledger eingetragen. Ansonsten wird die Stimme verworfen. Eine Stimme ist genau dann gültig wenn der Wähler sich als Wahlberechtigt authentifizieren konnte und seine Stimme noch nicht abgegeben hat. 3–5, 9

**Stimme** Eine Zähleinheit, die im Auszählungsverfahren zur Ermittlung des Wahlergebnisses benutzt wird. 3, 5, 9, 10, 12

**Stimmenauszählung** Das Auslesen der Stimmen aus der Blockchain um zu bestimmen wer die Wahl gewonnen hat. Dabei wird beachtet welches Wahlverfahren für die Wahl definiert wurde. 4

**Wahl** Eine Sammlung von Stimmen für die Bestimmung eines Kandidaten. 3–5, 7–12

**Wahl-Ende** Sobald die in der Wahl Konfiguration eingestellte Endbedingung erfüllt ist, beendet sich die Wahl. Es ist nicht mehr möglich gültige Stimmen abzugeben. Die

Ergebnisse der Wahl werden für jeden Wähler auf dessen Klienten ausgewertet und in der GUI angezeigt. 4

**Wahlberechtigt** Vom Wahlleiter als Wähler zugelassen und somit im Besitz eines gültigen Zertifikats zur Authentifizierung. 3, 10

**Wahlleiter** Administrator der Wahl, legt die Einstellungen, Wähler und Kandidaten der Wahl fest. 3–11

**Wahlstand** Das Auswertungsergebnis der Wahl, bei dem alle bisher erfolgreich abgegebenen Stimmen ausgezählt werden. 4

**Wähler** Person die bei einer Wahl einen bestimmten Kandidaten wählt und die hierfür nötigen Berechtigungen hat. 3–9, 11, 12, 18

**Zertifikat** Digitaler Datensatz, der die Authentizität und Integrität von Personen oder Objekten durch kryptografische Verfahren nachweist. 5, 7–9, 11, 12