Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

Auswertung der Blockchain-Konsultativabstimmung in der Stadt Zug

Inhaberinnen und Inhaber einer blockchainbasierten digitalen ID der Stadt Zug hatten vom 25. Juni bis am 1. Juli 2018 die Möglichkeit, an einer Konsultativabstimmung teilzunehmen. 72 Personen nutzten diese Gelegenheit. Mit diesem Machbarkeitsnachweis konnte ein neuer, blockchainbasierter Ansatz von E-Voting unter realistischen Bedingungen getestet werden. Dieser Schlussbericht zeigt die verschiedenen Vorteile der dezentralisierten Abstimmungslösung auf, erklärt die Architektur des Systems und gibt Aufschluss über das Feedback der Zugerinnen und Zuger, welche beim E-Voting-Test teilgenommen hatten.

Zentralisiert oder dezentralisiert, das ist die Frage!

Das dezentralisierte Abstimmungsverfahren basiert auf der Blockchaintechnologie und überzeugt mit vielen herausragenden Vorteilen im Vergleich zum zentralisierten Abstimmungsverfahren.

Bevor vertieft über Vor- oder Nachteile diskutiert werden kann, müssen die Unterschiede zwischen diesen beiden Wahlverfahren aufgezeigt werden. Das Hauptmerkmal eines dezentralen Systems beruht auf unabhängigen Instanzen, wobei keine einzelne Instanz die vollständige Kontrolle über das System hat. «Dezentralisiert» impliziert «verteilen», in diesem Zusammenhang bedeutet es eine Verteilung des gesamten Ablaufs (inklusive Rechenleistung und Datensicherung) auf mehrere Knoten – so genannte «Nodes». Das traditionelle Abstimmungsverfahren mit dem Stimmzettel aus Papier ist hingegen per Definition als zentralisiert einzustufen. Die meisten der sogenannten E-Voting-Mechanismen, ob mittels Wählautomaten oder online, sind ebenfalls als zentralisiert einzustufen, obschon diese in gewisser Weise auf verschiedene Einheiten verteilt sind. Die Entscheidungen werden schlussendlich immer noch in zentralisierter Form (von einer einzelnen Instanz) getroffen.

Das dezentralisierte Abstimmungssystem verfügt über die Vorteile eines Online-Abstimmungsverfahrens. Es weist keinerlei geographische Einschränkungen auf und die Wählerin und der Wähler können von überall her ihre elektronische Stimmabgabe tätigen, solange eine Verbindung zum Internet besteht. Diese Flexibilität führt zu einer grösseren Wahlbeteiligung. Weitere wesentliche Vorteile des dezentralisierten Abstimmungssystems sind:

Sicherheit
Der Hauptvorteil des dezentralisierten Abstimmungssystems ist seine hohe Sicherheit. Die Echtheit der Daten wird während des gesamten Wahlverfahrens garantiert durch:

1. eine effektive Identitätsfeststellung, welche es Hackern verunmöglicht, sich als einen anderen Wähler auszugeben.
2. die Technik digitaler Unterschriften, welche die Korrektheit der Daten gewährleistet und sicherstellt, dass keine betrügerischen Veränderungen während dem Datentransfer vorgenommen werden können.
3. das Blockchainsystem, welches die Unveränderbarkeit der Daten sicherstellt. Sobald eine Stimme im Blockchainsystem abgegeben wurde, kann diese nicht mehr entfernt oder verändert werden.

Die Tatsache, dass die Daten auf verschiedenen «Nodes» gespeichert werden, verunmöglicht eine böswillige Zerstörung oder Löschung der Daten – selbst wenn einer oder mehrere dieser Knoten gehackt werden sollte. Solange eine genügende Anzahl «Nodes» besteht, ist es fast unmöglich, das gesamte System zu hacken.

Stabilität
Wie bereits erwähnt, kann die Betriebsbelastung über die dezentralisierten Rechner verteilt werden. Prozesse von überlasteten «Nodes» können auf solche mit freier Kapazität verschoben werden. Somit ist auch bei einem Ausfall eines einzelnen Knoten gewährleistet, dass es zu keinem kompletten Systemausfall kommt. Für den Nutzer und die Nutzerin bedeutet dies eine anwenderfreundliche Lösung mit einer stets zeitnahen Rückmeldung der Daten.

Vertrauen
Im dezentralisierten Abstimmungssystem wertet eine Reihe von Instanzen die Stimmabgaben aus, vor Erfassung der Daten müssen diese Instanzen zu einer Übereinstimmung kommen. Die Auswertenden können also nicht nur die Organisatoren selbst sein, wie z.B. die Staatsregierung, sondern auch verschiedene mit dieser Aufgabe betreute Institutionen – angefangen von der UN bis hin zu politischen Parteien oder sogar dem lokalen Gemeinderat. Dieses Konzept stellt sicher, dass selbst bei korrupten Staatsregierungen keine Wahlergebnisse gefälscht werden können. In anderen Worten, das dezentralisierte System ist resistent gegen betrügerische Einflussnahme aus den eigenen Reihen.

Rückversicherung
Mit der Abgabe des konventionellen Stimmzettels an der Urne – aber auch mit der schriftlichen Briefwahl – haben die Wählenden nur limitierte Informationen über den weiteren Verbleib ihres Stimmzettels. Einmal in die Urne oder in den Briefkasten geworfen, kann der Stimmzettel nicht mehr weiterverfolgt werden. Die Wählenden haben keine Möglichkeit zu prüfen, ob ihre Stimmzettel auch tatsächlich erfasst und ausgezählt wurden. Im dezentralisierten Wahlverfahren haben die Wähler die Möglichkeit, eine Rückbestätigung zu erhalten, sobald ihre Stimmzettel geprüft und erfasst worden sind. Diese Option stellt bis zu einem gewissen Grad eine Rückversicherung für die Wählerschaft dar.

Transparenz
Um Sicherheitslecks zu verhindern, ist ein zentralisiertes System im Normalfall nicht für die Öffentlichkeit zugänglich («closed-source»). Die Endnutzer haben keinerlei Transparenz über die Abläufe («black box») und tappen diesbezüglich komplett im Dunkeln. Mit dem Verfahren des dezentralisierten Wahlsystems hingegen ist eine vollständige Verifizierbarkeit der Datenverarbeitung gewährleistet («open-source»). Dies erlaubt es sowohl den Wählenden als auch den verschiedenen Instanzen, die Funktionsweise des Wahlverlaufs zu prüfen, was wiederum zu verbesserter Transparenz führt. Diese Transparenz und die Verifizierbarkeit der «open-source» Datenverarbeitung kann Softwareentwickler motivieren, ebenfalls einen Beitrag zu leisten, was wiederum das System noch sicherer macht.

Das überprüfbare elektronische Wahlsystem

E-Vote ist die nächste Generation einer Abstimmungslösung, welche mit ihrer Blockchaineigenschaft das Abstimmungsverfahren unmittelbar, anonym, sicher, transparent, verifizierbar und unveränderbar macht.

E-Vote erlaubt Behörden auf Gemeinde- und Bundesebene:

- Teilnehmende aufzustellen und über eine neue Abstimmung zu informieren sowie die Resultate innert Minuten zu verarbeiten;
- auf operationeller Stufe Kosten und Zeit einzusparen;
- mit einer sicheren Lösung unabhängig von deren Standort mehr Wählende zu erreichen;
- das Vertrauen in den Abstimmungsprozess erheblich zu verbessern, da das Blockchainverfahren keine Veränderungen der erfassten Daten zulässt.

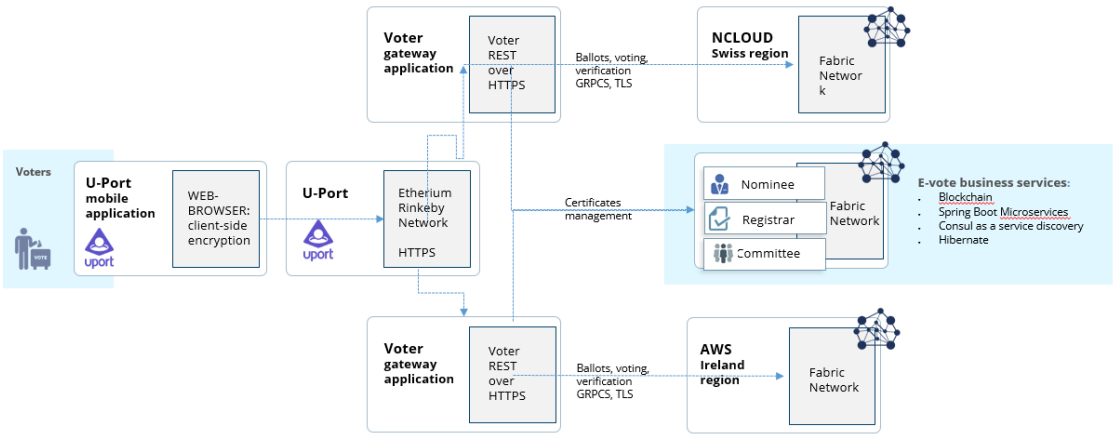
E-Vote verbessert den Abstimmungsprozess mit den folgenden Eigenschaften:

- Durch den anonymisierten Prozess werden keine persönlichen Informationen der Wählerinnen und Wähler preisgegeben und das Stimmgeheimnis bleibt gewahrt.
- Wählerinnen und Wähler können Ihre abgegebene Stimme jederzeit einsehen oder ändern, solange der Abstimmungsprozess im Gange ist.
- Ein externes Identitätssystem prüft die Rechtmässigkeit der Stimmabgabe und trotzdem bleiben die Wählenden anonym. Jede Person kann die abgegebenen Stimmen resp. deren Rechtmässigkeit überprüfen.
- Eine komplette Verschlüsselung der Abstimmungsdaten sichert diese gegen Eingriffe und Manipulationen.

E-Vote vereint die folgenden Technologien:

- Homomorphe Verschlüsselung – das Kryptosystem erlaubt den Nutzenden, verschlüsselte Daten zu berechnen, wie wenn diese nicht verschlüsselt wären, jedoch ohne diese Daten Preis zu geben. Beispiel: Nutzerinnen und Nutzer können verschlüsselte Zahlen addieren ohne diese zu entschlüsseln. E-Vote nutzt das Paillier-Kryptosystem für homomorphe Verschlüsselungen.
- Digitale Unterschrift – ein unwiderlegbarer mathematischer Beweis, dass die unterzeichnende Person Daten ins System übermittelt hat. Die Unterschrift garantiert, dass die Daten während des Transfers ins Blockchainsystem nicht verändert wurden.
- Nutzerseitige Verschlüsselung – die Verschlüsselung seitens der Wählenden (für private Datenverschlüsselung) wird direkt auf deren PCs isoliert.
- «Zero-Knowledge-Beweis» (Kenntnisfreier Beweis) – eine Methode, durch die eine Partei einer anderen Partei beweisen kann, dass eine gegebene Aussage wahr ist, ohne jedoch irgendwelche Informationen preiszugeben, ausser der Tatsache, dass die Aussage tatsächlich wahr ist.

Wie funktioniert die E-Vote Lösung?



Erklärung des Abstimmungsprozesses:

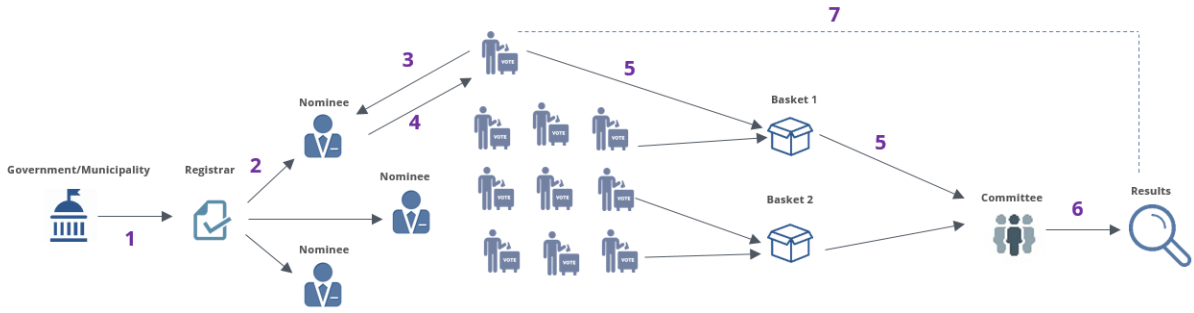
Rollen:

- Der «Verwalter» ist die Institution/Behörde, welche die Wahl oder Abstimmung auslöst und leitet.
- Der «Wahlbeauftragte» ist die Institution/Behörde, welche die Wahlberechtigung der Wählenden überprüft und bestätigt (Überprüfung der digitalen ID) und diesen ihre Stimmrechtsausweise bereitstellt.
- Der «Wähler» ist diejenige Person, welche über eine digitale ID verfügt und abstimmt.
- Das «Wahlkomitee» ist die Institution/Behörde, welche die Stimmrechtsausweise auszählt, überprüft und die Wahlergebnisse vorlegt.

Bedingungen:

- Die Abstimmunterlagen umfassen verschiedene Fragen zu einer bestimmten Wahlvorlage.
- Ein Stimmrechtsausweis (einmalig für jede einzelne wählende Person) beinhaltet die Stimmabgaben der Wählerin oder des Wählers.
- Urnen sind dezentralisierte, unveränderbare Datenverwahrstellen, wo die Wählenden ihre Stimmabgaben übermitteln.

Wie sieht der Wahlprozess aus?



Schritt 0
Bevor die Abstimmung beginnt, erhält jede wahlberechtigte Person eine bestätigte digitale uPort-ID von der Regierung/Gemeinde.

Schritt 1
Die Regierung oder Gemeinde löst eine Wahl- oder Abstimmungsvorlage aus und schickt alle nötigten Informationen zu dieser Abstimmung an den Verwalter.

Schritt 2
Der Verwalter erarbeitet die Wahl- oder Abstimmungsvorlage (mit einer Liste von Fragen und Antwortmöglichkeiten sowie Angabe über die Abstimmdauer etc.) auf dem blockchainbasierten Kanal und bestimmt den Wählerkreis, den Wahlbeauftragten sowie das Wahlkomitee.

Schritt 3
Eine wählende Person kann sich in ein dafür vorgesehenes Wahlportal[1] einwählen, um eine unübertragbare Stimme abzugeben. Sie hat die Wahl zwischen einem privaten oder öffentlichen

[1] Falls eine wählende Person keiner der verfügbaren Parteien vertraut, kann sie einen privaten Blockchain-«Node» führen.

«Node»[2]. Der private Schlüssel wird in der eigenen Brieftasche («wallet») verwahrt, der öffentliche Schlüssel hingegen wird zusammen mit einer Anfrage für einen Stimmzettel an den Wahlbeauftragten geschickt.

Mit einem öffentlichen Schlüssel können die Wahlberechtigten ihre Identifikation auf der Blockchain nachweisen und sicherstellen, dass ihre Stimmabgabe mit ihrer Identität verknüpft bleibt, ohne jedoch den Inhalt ihrer Stimmabgabe oder ihrer Identität preiszugeben. Mit einem privaten Schlüssel unterzeichnen die Wählenden den Stimmzettel um zu beweisen, dass dieser mit ihrer ID zusammenpasst.

Schritt 4
Der Wahlbeauftragte authentifiziert die Wählenden, welche die digitale ID von uPort verwenden und stellt ihnen einen persönlichen Stimmzettel aus.

Schritt 5
Die Wählenden geben Ihre Stimme ab, wobei die Stimmabgabe durch den öffentlichen Schlüssel des Wahlkomitees verschlüsselt wird. Der öffentliche Schlüssel wird für jede Abstimmung verwendet und basiert auf dem «Paillier»-Verschlüsselungssystem. Die Wählerinnen und Wähler unterzeichnen ihren Stimmzettel mit ihrem persönlichen Schlüssel und übergeben ihn der Blockchain. Die Stimmzettel werden in dezentralisierten Urnen gesammelt und zwischen den «Nodes» auf der Blockchain abgeglichen.

Schritt 6
Sobald die Abstimmung beendet ist, ruft das Wahlkomitee sämtliche anonymisierten und verschlüsselten Stimmzettel von der Blockchain ab, verifiziert deren Echtheit, indem alle Unterschriften geprüft werden (es werden zudem diverse weitere kryptographische Prüfungen vorgenommen), und berechnet das Abstimmungsresultat. Im Anschluss daran übermittelt das Wahlkomitee die Auswertung der Stimmen auf die Blockchain zusammen mit einem «Zero-Knowledge-Beweis» (einem kenntnisfreien Beweis), welcher den verschlüsselten Stimmzetteln und den entschlüsselten Resultaten entspricht.

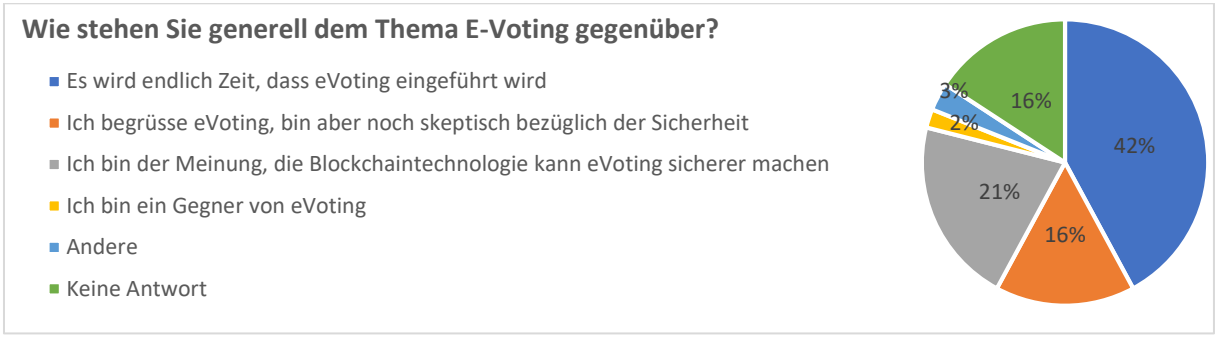
Schritt 7
Alle Blockchainteilnehmenden können die Resultate überprüfen, indem sie einen mathematischen Beweis anwenden, (also einen öffentlichen Schlüssel des Wahlkomitees benützen) und dann eine Summe von entschlüsselten Wahlresultaten erfassen. Eine Wählerin oder ein Wähler kann auch überprüfen, ob der eigene Stimmzettel erfasst und ausgezählt wurde, indem ein öffentlicher Schlüssel verwendet wird. Somit ist gewährleistet, dass niemand die individuell übermittelten Stimmzettel von anderen Stimmberechtigten entschlüsseln kann, aber trotzdem die Garantie hat, dass die Resultate nicht manipuliert wurden.

Auswertung der Abstimmung durch die Stadt Zug

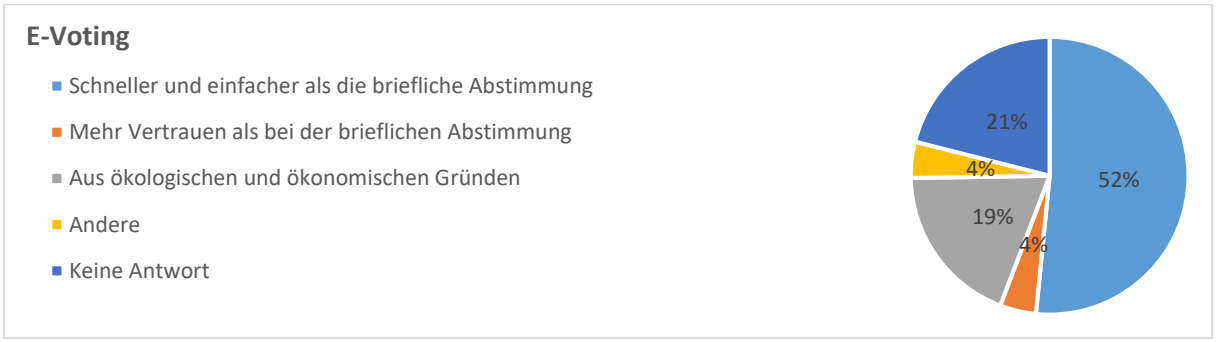
Die Umfrage der Stadt Zug bei den Einwohnerinnen und Einwohnern mit einer digitalen ID zeigt ein klares Ergebnis: Mehr als drei Viertel der Befragten begrüssen die Einführung von E-Voting und 21 Prozent sind der Meinung, dass Blockchaintechnologie elektronische Abstimmungen sicherer machen kann. Nur 2 Prozent möchte die Einführung von E-Voting verhindern. Trotz einer grundsätzlich grossen Zustimmung sind einige noch skeptisch, was die Sicherheit von E-Voting anbelangt. Zudem sind viele Umfrageteilnehmenden der Meinung, dass die Zuger Bevölkerung neben der Möglichkeit

[2] Der öffentliche Schlüssel der Wählerin oder des Wählers ist während der Überprüfung der Wahlberechtigung vom Wahlbeauftragten auf dem Blockchainkanal registriert. In diesem Prozess werden sämtliche Daten der wählenden Person vom Wahlbeauftragten anonymisiert.

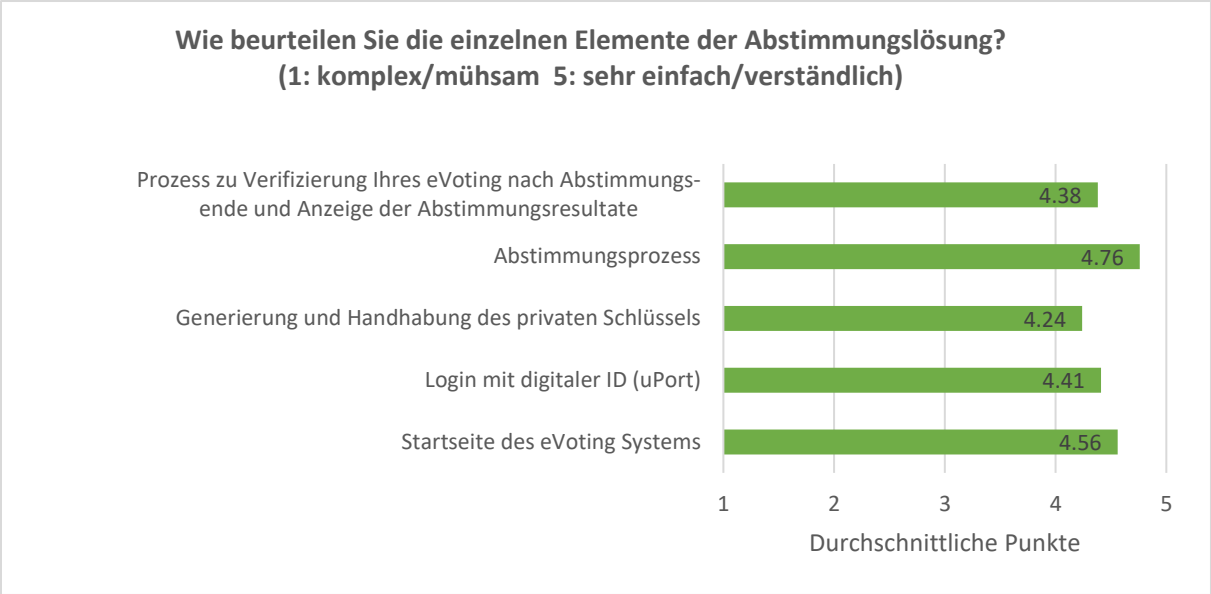
des E-Votings die Wahl haben sollte, weiterhin brieflich abzustimmen. Mehr als drei Viertel aller Teilnehmenden hatten bereits im Vorfeld eine digitale ID, somit hat sich rund ein Viertel der Teilnehmerinnen und Teilnehmer eine digitale ID für die Testabstimmung zugelegt.



Die Gründe, welche für E-Voting sprechen, sind vielfältig. Dass die Abstimmungen dadurch gegenüber einer brieflichen Abstimmung viel schneller und einfacher durchgeführt werden können, war für 52 Prozent der Befragten der Hauptgrund, weshalb E-Voting eingeführt werden sollte. Ökologische und ökonomische Argumente wurden ebenfalls mehrfach genannt.



Auch wenn die meisten Teilnehmenden mit dem Ablauf der Testabstimmung sehr zufrieden waren, gibt es noch einige Faktoren, die verbessert werden müssen, um den reibungslosen Ablauf einer Abstimmung sicherzustellen. Einige Personen waren mit technischen Problemen ihrer digitalen ID konfrontiert, die es ihnen verunmöglichten, an der Abstimmung teilzunehmen. Die einzelnen Elemente der Abstimmungslösung bewerteten die teilnehmenden Personen sehr positiv. Der Abstimmungsprozess wurde dabei als besonders einfach und verständlich taxiert und auch die Startseite des Systems hat den Stimmenden zugesagt. Verbesserungspotenzial besteht bei der Handhabung des privaten Schlüssels sowie bei den Erklärungen zu den einzelnen Schritten.



Die Möglichkeit für Bemerkungen am Schluss der Befragung wurde rege genutzt. Bemängelt wurde, dass über die Durchführung der Abstimmung in den Medien nicht genug berichtet wurde. Viele Umfragenteilnehmerinnen und -teilnehmer beklagten sich darüber, nichts von der Abstimmung vernommen zu haben oder erst im letzten Moment. Einige berichteten, dass sie erst im Nachhinein von der Abstimmung in Kenntnis gesetzt wurden. Leider ist es aus technischen Gründen nicht möglich, Inhaberinnen und Inhaber einer digitalen ID der Stadt Zug über die uPort-App im Hinblick auf eine bevorstehende Abstimmung zu benachrichtigen. Über die uPort-App laufen weltweit noch andere Anwendungen. Für die Pilotphase hat die Stadt Zug aus Kostengründen keine eigene App-Variante entwickeln lassen.

Die digitale ID der Stadt Zug wurde am 15. November 2017 eingeführt und befindet sich in einer Pilotphase. Neben der E-Voting-Lösung sind für die Inhaberinnen und Inhaber einer digitalen ID verschiedene andere Anwendungen in der Evaluation bzw. bereits als Pilotprojekt in Betrieb, so das Ausleihen von Stadtvelos nach dem Free-Floating-Prinzip über eine spezielle App. Demnächst folgt das Ausleihen von Büchern in der Bibliothek ohne Bücherausweis.

Fazit und Ausblick

Der Machbarkeitsnachweis war ein Erfolg. Sämtliche technische Erwartungen wurden erfüllt und die Teilnehmenden empfanden den Abstimmungsprozess einfach und verlässlich. Es konnten wertvolle Erkenntnisse gewonnen werden, die zu weiteren Verbesserungen führen werden. Projekte wie dieses sind unentbehrlich, um den Weg zu einem sicheren und verlässlichen E-Voting-System zu ebnen. Ein Link zum Code wird auf diversen Kanälen öffentlich zugänglich gemacht. So zum Beispiel auf der Website der Stadt Zug, auf der Website des Blockchain Lab der Hochschule Luzern und auf der Seite der Firma Luxoft. Sämtliche Projektteilnehmerinnen und -teilnehmer tragen dazu bei, die E-Voting-Lösung weiter zu verbessern, zusätzliche Anwendungsbereiche zu finden und die Ergebnisse mit der Gemeinschaft zu teilen.

Zug, 30. November 2018