

Grosser Gemeinderat, Vorlage

Interpellation "E-Voting in der Stadt Zug – ein trügerischer Erfolg?"

Antwort des Stadtrats vom 14. Mai 2019

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Am 6. März 2019 hat die glp-Fraktion die Interpellation „E-Voting in der Stadt Zug – ein trügerischer Erfolg?“ eingereicht. Sie stellt darin dem Stadtrat eine Reihe von Fragen. Wortlaut und Begründung des äusserst umfangreichen Vorstosses sind aus dem vollständigen Interpellationstext im Anhang ersichtlich.

Frage 1

Welche Ziele verfolgt der Stadtrat mit solchen E-Voting-Versuchen? In der Annahme, dass nicht jede Gemeinde und jeder Kanton ihr eigenes E-Voting System entwickeln und in der Zukunft einsetzen wird, möchte die Stadt damit einen wissenschaftlichen Beitrag für die Allgemeinheit leisten, oder ist eine eigene, autonome E-Voting Lösung für die Stadt geplant?

Antwort

In den vergangenen Jahren hat die Stadt Zug im Bereich der Blockchaintechnologie verschiedentlich Pionierleistungen erbracht. Bei sämtlichen Projekten ging es in erster Linie darum, als Verwaltung in niederschweligen Projekten Erfahrung mit der neuen Technologie zu sammeln. Dies im Bestreben, dass die Stadt Zug als Zentrum des sogenannten "Crypto Valley" einerseits versteht, was die Technologie auch für eine Verwaltung bedeuten kann. Andererseits ging und geht es bei diesen Projekten auch darum, dass die Stadtverwaltung die Bestrebungen verschiedener Player im "Crypto Valley" nach Möglichkeiten unterstützt und sich als Teil des Ökosystems versteht. Im Rahmen von verschiedenen, klar abgegrenzten Pilotprojekten hat sich die Stadtverwaltung deshalb als Anwendungspartner zur Verfügung gestellt. So auch in diesem Fall: Die Hochschule Luzern kam auf der Suche nach einem Anwendungspartner für ein Forschungsprojekt im Rahmen von blockchainbasierten E-Voting-Systemen auf die Stadt Zug zu. Diese bot sich als Anwendungspartner für dieses Projekt geradezu an, hatte zuvor die Stadt Zug doch bereits Erfahrungen im Rahmen einer blockchainbasierten digitalen Identität gesammelt. Diese bildet Basis für das vorliegende E-Voting-System. Hinzu kam, dass Jan Gerlach, welcher für die Abteilung Informatik der Stadt Zug arbeitet, im Frühling 2017 eine Diplomarbeit zum Thema "E-Voting System auf Grundlage der Blockchain Technologie" verfasst hatte und so in diesem Bereich schon grosse Erfahrungen vorweisen konnte. Es war damit naheliegend, dass sich die Stadt Zug als Partner für weitere Forschungsarbeiten der Hochschule Luzern auf diesem Gebiet zur

Verfügung stellte. Das grundlegende Ziel dieses Versuchs lag denn darin, ein realistisches E-Voting Szenario abzubilden, welches neue, vielversprechende Technologien wie Blockchain und digitale Identitäten integriert und für den Benutzer einfach zu gebrauchen ist.

Es ging damit zu keinem Zeitpunkt darum, für die Stadt Zug ein eigenes E-Voting-System zu entwickeln. Vielmehr wollte die Stadt Zug mit dieser Testabstimmung einerseits eigene Erfahrungen über mögliche zukünftige Abstimmungssysteme sammeln und einen Diskussionsbeitrag leisten. So zeigt sich gerade im Rahmen der aktuell laufenden Diskussionen zum E-Voting, dass ein blockchainbasiertes System gegenüber einem zentral ausgestalteten System gewisse Vorteile haben könnte.

Frage 2

Wer ist der Verfasser / die Verfasserin des Schlussberichtes? Über dem Titel werden die Firma «Luxsoft», die Hochschule Luzern und die Stadt Zug aufgeführt, es bleibt jedoch unklar, wer welche Teile verfasst, oder darauf Einfluss genommen hat.

Antwort

Es handelt sich um ein Gemeinschaftswerk mit dem Ziel, die gemachten Erfahrungen zu verschriftlichen. Von Seiten der Stadt Zug wurde der Bericht von der Abteilung Informatik mitverfasst, unter der Federführung von Jan Gerlach. Konkret wurde der letzte Teil des Berichtes mit der Auswertung der Umfrage durch die Abteilung Informatik beschrieben. Von der Firma Luxoft wurden vom Chefentwickler der Software die technischen Details und die Architektur des Systems erläutert. Die konzeptionellen Ausführungen des E-Voting-Systems stammen von der Hochschule Luzern.

Frage 3

Der Schlussbericht in der Form, in welcher er auf der Webseite veröffentlicht wurde, entspricht leider kaum wissenschaftlichen Standards. So wird beispielsweise die Tatsache, dass es sich bei den Teilnehmenden wahrscheinlich um sehr technikaffine Personen handelt nicht einmal erwähnt, auch scheint die Auswahl der Fragen einseitig und willkürlich, zusätzlich werden Hypothesen ohne Quellenangabe, als erwiesene Tatsachen dargestellt z.B. Auf Seite 1: Evoting führt zu einer höheren Stimmbeteiligung. Es fehlen sowohl Stichproben-, als auch Methodenbeschreib, von einer kritischen Würdigung oder Quellenangaben ganz zu schweigen. Wie schätzt der Stadtrat die wissenschaftliche Validität der Erhebung und des veröffentlichten Berichtes ein?

Antwort

Seitens Stadt Zug war zu keinem Zeitpunkt ein wissenschaftlicher Bericht beabsichtigt. Wenn schon hätte alleinig die Hochschule Luzern an einem solchen Interesse. Seitens Stadt Zug war wichtig, dass ein Abschlussbericht vorliegt, welcher über wesentliche Aspekte des Projektes Auskunft gibt. Dies erscheint dem Stadtrat mit dem vorliegenden Bericht als erfüllt; der Bericht erklärt, was überhaupt getestet wurde und hat informierenden Charakter. Im Übrigen kann die Vermutung, dass es sich bei den Teilnehmenden um technikaffine Personen handelt, nicht bestätigt werden. Vielmehr setzt sich der Benutzerkreis der digitalen Identität höchst divergent zusammen.

Frage 4

Wir nehmen an, dass es sich hierbei nicht um den eigentlichen Schlussbericht, sondern um eine Kurzzusammenfassung handelt. Aufgrund der Wichtigkeit des Themas für die Öffentlichkeit, möchten wir den Stadtrat anfragen, ob er bereit wäre dieser Kurzzusammenfassung auch den vollständigen Abschlussbericht anzuhängen?

Antwort

Der Stadtrat war immer bestrebt, den Aufwand bei den verschiedenen Versuchsprojekten möglichst gering zu halten. Ein umfassender Abschlussbericht würde dieser Absicht zuwiderlaufen. Die Durchführung von Abstimmungen und Wahlen sind zudem letztlich Sache von Bund und Kantonen. Ein detaillierter Abschlussbericht zum Thema E-Voting seitens Stadt Zug würde denn zu weit führen. Es sei an dieser Stelle nochmals erwähnt, dass dieses Projekt nicht zum Ziel hatte, einen wissenschaftlichen Diskurs zum Thema E-Voting zu lancieren. Vielmehr war beabsichtigt, mit einem Proof-of-Concept einen Diskussionsbeitrag zu leisten für die Durchführung einer elektronischen Abstimmung auf Grundlage der Blockchaintechnologie. Dies scheint gelungen.

Frage 5

Das erklärte Ziel des Schlussberichtes ist, ausschliesslich die Vorteile der dezentralen Abstimmungslösung aufzuzeigen. Warum?

Antwort

Da das getestete E-Voting-System eine dezentrale Abstimmungslösung darstellt, werden dementsprechend die Vorteile einer solchen – dezentralen- Lösung aufgezeigt.

Frage 6

Gibt es aus der Sicht des Stadtrats / der beteiligten Institutionen wirklich keinerlei Nachteile bei der eingesetzten Technologie? In der Annahme, dass jede Technologie ihre Nachteile hat, warum wurden diese Nachteile zwecks Ausgewogenheit nicht in den Bericht mitaufgenommen?

Antwort

Die Frage ist berechtigt. Im Sinne der Ausgewogenheit hätte der Bericht auch mögliche Nachteile aufzeigen sollen. Im Rahmen der vorliegenden Beantwortung der Interpellation wurden deshalb nochmals Abklärungen zu möglichen Nachteilen gegenüber zentralen Lösungen gemacht. Solche konnten jedoch nicht eruiert werden, was jedoch nicht heisst, dass eine blockchainbasierte Lösung absolut fehlerunanfällig ist bzw. dass sich zu einem späteren Zeitpunkt nicht auch Nachteile zeigen können. So haben sich beim "normalen" E-Voting grössere Sicherheitsbedenken auch erst ergeben, als die Lösung einem Stresstest unterzogen wurde. Vorliegend ist geplant, den Quellcode der E-Voting-Lösung zu veröffentlichen. Dieser kann so von technikaffinen Leuten einer Prüfung unterzogen werden.

Frage 7

Gemäss Bericht ist es nicht möglich ein solches E-Voting-System zu hacken. Konkret beschreibt er von der Unmöglichkeit sich als eine/n andere/n Wähler/lin auszugeben. Ist der Stadtrat ebenfalls der Überzeugung, dass das getestete System unmöglich zu hacken oder anderweitig zu manipulieren ist?

Antwort

Die Aussage in der Frage entspricht nicht den Tatsachen. Im Bericht steht wörtlich: "Solange eine genügende Anzahl «Nodes» besteht, ist es fast unmöglich, das gesamte System zu hacken". Es besteht durchaus das Risiko, dass ein Knoten gehackt werden kann. Solange jedoch nicht die Mehrheit der Knoten kompromittiert wurde, ist die Sicherheit im System gewährleistet. Oder wie es seitens Hochschule Luzern beschrieben wurde: "Die Daten werden verschlüsselt und in mehreren sogenannten Knoten gespeichert. Die Daten auf den Knoten können zwar manipuliert und gelöscht werden, weil aber auf anderen Knoten auch eine Kopie liegt, kann im Konsens zwischen den Knoten entschieden werden, was der Wahrheit entspricht und was nicht. Sprich, die falschen oder manipulierten Knoten werden ignoriert, was die Abstimmung sehr sicher macht".

Frage 8

Auf Seite 2 des Berichts wird der Vorteil des Vertrauens beschrieben. «Dieses Konzept stellt sicher, dass selbst bei korrupten Staatsregierungen keine Wahlergebnisse gefälscht werden können.». Dies mag vielleicht zutreffen, wenn das System ordentlich installiert, betrieben und überwacht wird, aber genau daran könnte ein solches System scheitern. Da man sich im Bericht auf die Eventualität einer korrupten Staatsregierung einlässt, erlauben wir uns auch diesbezüglich eine Frage: Wie kann der Stadtrat eine Fake-Simulation ausschliessen, bei der es nur so scheint, als würde das System ordentlich funktionieren, insbesondere bei einer möglichen, korrupten Staatsregierung?

Antwort

Da das getestete System auf einer sogenannten "permissioned Blockchain" aufbaut, sind die einzelnen Instanzen genau definiert. Konkret bedeutet dies, dass jeder Knoten, der Validierungen der Transaktionen durchführen kann, im System hinterlegt und bekannt ist. Damit ein solches System ordnungsgemäss betrieben werden kann, muss gewährleistet sein, dass die Knoten für die Validierung von vertrauenswürdigen Personen bzw. Organisationen betrieben werden. Dies kann zum Beispiel neben einer staatlichen Stelle auch ein Notariat sein. Zudem ist der Quellcode der Software – wie bereits dargelegt – öffentlich zugänglich. Man kann also leicht nachweisen, ob eine manipulierte Version der Software im Einsatz ist oder nicht. Ein weiterer Vorteil der vorliegenden Open Source Lösung ist, dass Fehler in der Software, seien diese absichtlich als Hintertüren implementiert worden oder nicht, durch sogenanntes "peer Review" einfacher entdeckt werden können. Kurz: Das System scheint Fehlern und Missbrauch wirksam vorzubeugen. Ebenso klar ist indes, dass Korruption und Kriminalität auch in Zukunft ihre Wege suchen und finden werden.

Frage 9

Falls der Stadtrat eine mögliche Manipulation nicht vollkommen ausschliessen möchte, wie könnten Unregelmässigkeiten entdeckt und nachgeprüft werden und was würde die Stadt bei begründeten Zweifeln unternehmen?

Antwort

Falls unterschiedliche Versionen der Abstimmungsergebnisse auf den Knoten vorhanden sind kommt der Konsensmechanismus zum Zuge. Die Mehrheit der Knoten im System entscheidet, welcher Stand der Richtige ist. Falls es doch irgendwie passieren würde, dass die Mehrheit der Knoten im System kompromittiert wäre, würde man dies trotzdem mittels Analyse und Monitoring feststellen können und könnte eine elektronische Abstimmung nachträglich für ungültig erklären bzw. im schlimmsten Falle wiederholen. Nur der Vollständigkeit halber ist zu erwähnen, dass Unregelmässigkeiten auch beim heutigen, analogen System nicht vollständig ausgeschlossen werden können.

Frage 10

Auf Seite 5 des Berichtes wird beschrieben, dass der öffentliche Schlüssel des Wahlkomitees mithilfe des «Paillier-Kryptosystems» verschlüsselt wird. Es handelt dabei um ein asymmetrisches Kryptosystem, das wie die meisten anderen Verschlüsselungsverfahren auf der Schwierigkeit der Primfaktorzerlegung und der Berechnung diskreter Logarithmen beruht. Ausreichend starke Quantencomputer werden mit hoher Wahrscheinlichkeit bereits in naher Zukunft solche asymmetrischen Kryptographie-Verfahren entschlüsseln können. Eine Lösung für dieses Problem würden symmetrische Kryptosysteme bieten, die jedoch selber andere Gefahren beinhalten, z.B. sichere Übermittlung eines Zweitschlüssels. Auch wenn die breite Öffentlichkeit mittelfristig kaum Zugang zu leistungsstarken Quantencomputern haben wird, werden andere Interessengruppen z.B. Geheimdienste, diese Möglichkeit sicher nutzen können. Wie steht der Stadtrat zu dieser Problematik?

Antwort

Zunächst sei der Hinweis erlaubt, dass es durchaus asymmetrische Verschlüsselungsverfahren gibt, welche mutmasslich nicht mittels eines Quantencomputers geknackt werden können. Diese fallen unter den Begriff der Post-Quanten-Kryptografie. Ein Beispiel hierfür wären hashbasierte Signaturverfahren. Es ist indes richtig, dass das sogenannte "Paillier-Kryptosystem" durch einen Quantencomputer geknackt werden kann. Allerdings trifft das für die meisten asymmetrischen Verschlüsselungsverfahren zu und somit auch für die meisten Anwendungen, die heutzutage genutzt werden, wie z.B. e-Banking, Online-Shopping etc. Eine Blockchain ist kein starres System, sondern kann beliebig angepasst werden. Im Falle der getesteten E-Votin-Lösung (Hyperledger Fabric) sogar einfacher als zum Beispiel bei der Bitcoin-Blockchain, da ein sogenannter "Hard Fork" einfacher umzusetzen ist. Die Verschlüsselungsalgorithmen können also auch beim getesteten E-Voting System, bzw. bei einer Blockchaintechnologie, durch quantencomputer-resistente Algorithmen ersetzt werden.

Frage 11

Verfügt die Stadt über das nötige Knowhow für den staatlichen Betrieb eines solchen E-Voting Systems? Wäre sie bereit die dafür nötigen Investitionen zu tätigen? Welche Rolle würden private Konzerne wie bspw. Luxsoft bei einem solchen E-Voting-System einnehmen? Würden Unterhalt, Support und Weiterentwicklung des Systems, Vorbereitung, Durchführung und Nachbearbeitung der Wahlen durch die Stadt erfolgen, oder ganz oder teilweise an private Unternehmen ausgelagert? Wie schätzt der Stadtrat die Gefahrenpotentiale dieses möglichen Outsourcings ein?

Antwort

Wie bereits erwähnt, sind Abstimmungen und Wahlen Sache des Bundes und der Kantone. Die Stadt Zug sieht sich damit nicht in der Rolle, ein solches E-Voting-System zu betreiben. Vielmehr war es Ziel des Pilotversuches, das Thema Blockchain beim Thema E-Voting auch auf Bundes- und Kantonsebene einzubringen. Es kann an dieser Stelle jedoch auch die Haltung der Stadt Zug aufgeführt werden, dass es nach Ansicht der Stadt Zug klare Staatsaufgabe ist, sowohl im Bereich der digitalen Identitäten als auch im Bereich des E-Votings als Staat die Grundlagen zur Verfügung zu stellen. Es kann nicht sein, dass derart zentrale Bereiche unseres Demokratiesystems an private ausgegliedert werden. Insofern steht die Stadt Zug den aktuellen Bestrebungen, die digitale Identität durch Privatanbieter herauszugeben, äusserst kritisch gegenüber.

Frage 12

Wie hoch schätzt der Stadtrat die möglichen Gesamtkosten für den Betrieb eines solchen E-Voting Systems ein?

Antwort

Dies kann aus heutiger Sicht nicht ausgeführt werden. Wie schon erwähnt, sieht sich die Stadt Zug auch nicht in der Rolle als Betreiber einer E-Voting-Lösung. Der Vollständigkeit halber kann ausgeführt werden, dass der vorliegende Pilotversuch nur geringe interne Kosten auslöste. CHF 3'000.00 wurden für die Übersetzungsarbeit des Berichtes aufgeworfen, die restlichen Kosten ergeben sich aus Arbeitsleistungen von städtischen Mitarbeitenden (ca. acht volle Arbeitstage von Jan Gerlach/Team Informatik, ein Arbeitstag vom Stadtpräsidenten und Stadtschreiber).

Frage 13

Heute werden die abgegebenen Stimmzettel unter den Augen des Stimmbüros gezählt. Die Mitglieder des Stimmbüros gehören unterschiedlichen Parteien an. Das Stimmbüro übernimmt so die Funktion einer objektiven Kontrollinstanz. Wie können die digital abgegebenen Stimmen durch das Stimmbüro auf ihre Gültigkeit kontrolliert werden? Ist ein solcher Prozess auch für Laien nachvollziehbar?

Antwort

In der getesteten Lösung ist das Stimmbüro in der Rolle des Wahlkomitees abgebildet, welches am Schluss einer Abstimmung die elektronischen Stimmen prüft und deren Echtheit bestätigt. Dies geschieht mittels kryptografischer und mathematischer Funktionen. Das Wahlkomitee kann wie bis anhin aus verschiedenen Personen aus unterschiedlichen Parteien bestehen. Ob der gesamte Prozess auch für Laien nachvollziehbar ist, bleibt fraglich, gerade was die mathematischen und kryptografischen Prüfungen angeht. Durch den offenen Quellcode besteht jedoch die Möglichkeit, dass sich Fachleute mit den mathematischen und kryptografischen Grundlagen auseinandersetzen und diese einem Test unterziehen können.

Frage 14

Wie würden Stimmen aus dem E-Voting mit Stimmen aus der Brief-, oder Urnenabstimmung verrechnet? Welche Rolle würde das Stimmbüro in Zukunft übernehmen?

Antwort

Die Frage führt sehr weit, zumal nicht angedacht ist, die Lösung auch tatsächlich umgesetzt wird. Bei einem gemischten Einsatz von elektronischer und brieflicher-, bzw. Urnenabstimmung müsste ein Prozess ausgearbeitet werden, der eine sichere und überprüfbare Gesamtauszählung der Stimmen garantiert. Für das Stimmbüro würde sich dabei vermutlich wenig ändern.

Fragen zum E-Voting allgemein

1. Welche Nachteile und Gefahren sieht der Stadtrat durch die mögliche Einführung von E-Voting in der Stadt Zug und allgemein?

Die grösste Gefahr liegt beim Einsatz eines E-Voting Systems, das nicht genügend Sicherheit und Schutz gegenüber Angriffen und Manipulationen bietet. Letztlich kann und will die Stadt Zug jedoch nicht unabhängig von Bund und Kanton eine E-Voting-Lösung implementieren. Bei einer Bundes- bzw. Kantonslösung wird das Thema Sicherheit eines der zentralen Evaluationskriterien sein.

- 2. Ist der Stadtrat ebenfalls der Überzeugung, dass bei einer zukünftigen Einführung von E-Voting, auch langfristig noch eine Wahl/Abstimmung per Brief/Zettel möglich sein muss?*

Heute gibt es zwei Möglichkeiten, an einer Urnenabstimmung teilzunehmen: entweder schriftlich oder durch Abgabe der Stimme an der Urne. Es macht sicher Sinn, dass es bei einer allfälligen Einführung von E-Voting möglich bliebe, unabhängig von technischen Hilfsmitteln an einem Urnengang teilzunehmen. Jedoch könnte man sich dannzumal ebenfalls auf zwei Möglichkeiten beschränken, nämlich auf E-Voting und die briefliche Stimmabgabe. Dies würde insofern auch dem Trend entsprechen, als die persönliche Stimmabgabe an der Urne stetig an Bedeutung verliert.

- 3. Ist der Stadtrat ebenfalls der Überzeugung, dass durch den Unterhalt und die nötige, ständige Weiterentwicklung eines sicheren E-Voting-Systems sowohl Aufwand und Kosten für die Durchführung von sicheren Abstimmungen steigen würden? Insbesondere bei einer Fortführung der Brief- und Urnenabstimmungen?*

Eine definitive Aussage kann dazu nicht gemacht werden. Vermutungsweise dürfte es jedoch so ein, dass die Kosten für die regelmässige Wartung eines elektronischen Systems eher hoch sind, zumal allfällige Sicherheitsanforderungen zu erfüllen sind.

- 4. E-Voting kann den Abstimmungsvorgang bequemer machen, da sich der Gang zum Briefkasten erübrigt. Neben der Bequemlichkeit, welche anderen Vorteile sieht der Stadtrat im E-Voting im Vergleich mit der Brief-, Urnenabstimmung in der Stadt Zug?*

Dies kommt auf die verwendete Lösung an. Bei der getesteten Lösung kann der Stimmende jederzeit die abgegebene Stimme verifizieren. Er kann verifizieren, ob seine Stimme auf dem elektronischen Kanal unterwegs nicht verändert wurde. Ein weiterer Vorteil liegt darin, dass von überall her die Stimme abgegeben werden kann, also standortunabhängig. Des Weiteren ist die Auszählung der Stimmen innert Sekunden erledigt und weniger fehleranfällig als bei der Auszählung der schriftlichen Wahlzettel.

- 5. Wie gross schätzt der Stadtrat das Potential einer möglichen, durch E-Voting bedingten, höheren Wahlbeteiligung ein?*

Dazu kann keine Aussage gemacht werden. Allenfalls wurde diese Frage im Bericht jedoch zu optimistisch verfasst. Auswertungen haben nämlich gezeigt, dass jene Kantone, die über den Kanal der elektronischen Stimmabgabe verfügen, keine höhere Stimmbeteiligung aufweisen. Dies zeigen auch Auswertungen aus dem Ausland.

- 6. Wie schätzt der Stadtrat insgesamt das Kosten / Nutzenverhältnis von E-Voting ein?*

Auf die Beantwortung dieser Frage wird verzichtet. Eine verlässliche Antwort ist auf dem aktuellen Stand der Entwicklung nicht möglich.

- 7. Welche weiteren Schritte plant die Stadt bezüglich E-Voting kurz-, mittel- und langfristig? Gibt es eine Roadmap?*

Nein, eine Roadmap gibt es nicht. Wie verschiedentlich aufgeführt sieht sich die Stadt Zug im Bereich von E-Voting nicht im Lead. Mit dem vorliegenden Versucht sollte aufgezeigt werden, dass eine blockchainbasierte Lösung für Bund und Kantone von Interesse sein könnte.

Antrag

Wir beantragen Ihnen

- die Antwort des Stadtrats zur Kenntnis zu nehmen.

Zug, 14. Mai 2019

Dr. Karl Kobelt
Stadtpräsident

Martin Würmli
Stadtschreiber

Beilage:

- Interpellation "E-Voting in der Stadt Zug – ein trügerischer Erfolg"

Die Vorlage wurde vom Präsidialdepartement verfasst. Weitere Auskünfte erteilt Ihnen gerne Stadtpräsident Karl Kobelt, Tel. 041 728 21 04.