

Stefan Huber, Gemeinderat glp
für die Fraktion grünliberale
Grosser Gemeinderat Stadt Zug
stefan@leerzeit.ch

Parlamentarischer Vorstoss GGR
Eingang : 18.01.2022
Bekanntgabe im GGR : 22.02.2022

Tabea Zimmermann Gibson
Präsidentin GGR
Stadtkanzlei
Gubelstrasse 22
Postfach
6301 Zug

Zug 18.01.2022 – eingereicht per E-Mail

Interpellation

Fragen zum Einsatz von Blockchain-Technologie für städtische Dienstleistungen

Als «Crypto Valley» hat die Stadt Zug national und international für Schlagzeilen gesorgt. Der Stadtrat hat durch geschicktes Standortmarketing nicht nur zahlreiche Start-Ups und Unternehmen aus der Fintech-Branche angezogen, sondern sich auch selbst für den Einsatz von Distributed Ledger basierten Technologien offengezeigt, diese genutzt und ausprobiert. Neben einem E-Voting Experiment¹ bietet die Stadt auch eine blockchainbasierte digitale ID an und akzeptiert verschiedene Kryptowährungen zur Zahlung von Gebühren und Dienstleistungen. Für diese Offenheit und den gezeigten Innovationswillen darf man dem Stadtrat gratulieren.

Aufgrund neuer Entwicklungen und Erkenntnisse im Bereich der Distributed Ledger Technologien (kurz DLT) und aufgrund der immer grösseren Rolle, welche diese Technologien zunehmend auch in sensiblen staatlichen Dienstleistungen spielt, ist ein grundlegendes Verständnis der Technologie und eine aufmerksame Beobachtung ihres Einsatzes durch die Staat von zunehmender Bedeutung für unsere Stadt. Genauere Erläuterungen zu den technischen Grundlagen und dem aktuellen Kontext sind unter dem Punkt «Technische Grundlagen» aufgelistet.

1. Bei welchen Dienstleistungen setzt die Stadt aktuell auf Distributed Ledger Technology und bei welchen Dienstleistungen könnte sie sich einen Einsatz in der Zukunft vorstellen? Verfügt der Stadt dabei über eine Roadmap?
 - a. Bei welchen Projekten setzt die Stadt auf die Ethereum Blockchain?
 - b. Bei welchen Projekten setzt die Stadt auf andere DLT Technologien?
 - c. Wie prüft und stellt die Stadt einen ausreichenden Grad an Dezentralisierung einer von ihr genutzten DLT Technologie sicher?
2. Nutzt die Stadt bei ihren Projekten ausschliesslich «permissioned blockchains»?
 - a. Welche Rolle spielen die «public ledgers» bei den städtischen Projekten?
 - b. Welche Rolle spielen ihre nativen Token dabei? Z.B. Ether² für Netzwerknutzung («Gas»)
3. Nützen die sich innerhalb der «permissioned blockchain» befindlichen Nodes welche für blockchainbasierte städtische Dienstleistungen genutzt werden den Konsens-Algorithmus des

¹["E-Voting erfolgreich getestet" Webseite der Stadt Zug vom 30.11.2018](#)

² «Ether» ist das native Token des Ethereum Netzwerkes

«public ledgers» oder einen eigenen, selbstentwickelten Konsens Algorithmus?

4. Eine Audioaufnahme des Ethereum Presales hinterlässt den Eindruck, dass gezielt zur Verschleierung³ der grössten Halter von Ethereum aufgerufen wurde. Mit dem kommenden Wechsel zu Proof of Stake⁴ besteht für den «public ledger» eine grosse Manipulationsgefahr, da der Konsensmechanismus durch eine Handvoll verschleierter damaliger Grossinvestoren zum eigenen Vorteil verändert werden könnte. Inwiefern betrifft der Wechsel zu Proof of Stake die «permissioned blockchains» welche die Stadt auf Basis der Ethereum -Technologie nutzt?
5. Wer sind die Betreiber der von der Stadt für die digitale ID genutzten Nodes und wo befinden sich diese? Betreibt die Stadt alle Nodes die sie innerhalb der «permissioned Blockchain» ihrer Unique Node Lists (UNL) hinzufügt selber?
6. Wer berät die Stadt bei Projekten zu Distributed Ledger Technologien und ist für die technische Umsetzung zuständig?
7. Das grundlegende Motto hinter DLT Technologien ist «In code we trust.» und meint, dass überprüfbarer, verbindlicher Code menschliches Vertrauen ersetzen soll. Verfügt die Stadt über ausreichende Ressourcen und Kompetenzen, den einer DLT Technologie zugrunde liegenden Code zu verstehen und beurteilen zu können, ohne auf das Vertrauen in Drittparteien angewiesen zu sein?
8. Wie schätzt der Stadtrat die Seriosität des Technologiepartners der Stadt «ConsenSys»^{5 67} ein?

Technische Grundlagen zum besseren Verständnis der Interpellationsfragen

Gemäss Newsarchiv⁸ setzt die Stadt bei beiden Versuchen auf die Ethereum Blockchain. Eine Blockchain deren Ursprung stark mit der Stadt Zug verbunden ist. So hat nicht nur die Ethereum Stiftung bis heute ihren Sitz in der Zuger Altstadt, sondern auch zahlreiche mit ihr verbundene Unternehmen wie z.B. die ConsenSys AG, die Datenplattform U-Port entwickelt hat, welche die Stadt für ihre digitale Identität und ihr E-Voting Projekt nutzt.⁹

Die Stadt hebt dabei vor allem die dezentrale Natur des Ethereum-Netzwerkes vor. Die so gespeicherten Daten seien dadurch mit absoluter Sicherheit vor Manipulation, Datenverlust und Fälschung geschützt. Das Prinzip hinter den sogenannten „Distributed Ledger“-Technologien besteht darin, dass ein Datensatz nicht zentral auf einem einzigen System, sondern Kopien davon auf möglichst vielen, auf der ganzen Welt dezentralisierten Systemen gespeichert werden.

Jede Änderung dieser Daten auf einem einzelnen System wird durch einen im Netzwerk verankerten Konsens-Algorithmus auf seine Authentizität überprüft (validiert). Kann die Authentizität einer Änderung nicht von einer Mehrheit der dezentralen Systeme validiert werden, weil z.B. eine Information im Widerspruch zum bisherigen Konsensverlauf steht, kann diese Änderung je nach Protokoll als ungültig erkannt, ignoriert, zurückgesetzt, oder abgespalten werden.

³ [Ethereum: Some Economic Considerations - YouTube](#) ab 51:30 – Audio-Aufnahme 21.03.2014

⁴ Konsens-Mechanismus der Transaktionen durch das Eigentum von möglichst vielen Token validiert.

⁵ [ConsenSys AG Shareholders Readying Legal Action Over Share Valuation \(yahoo.com\)](#)

⁶ [Founder of Former ConsenSys-Backed Startup Sues Joseph Lubin for \\$13M \(cointelegraph.com\)](#)

⁷ [Vermeintliches Zuger Unternehmen entwickelte E-Voting mit zentralplus](#)

⁸ [Stadt Zug - Blockchain-basierte digitale ID für alle Einwohner jetzt erhältlich](#)

⁹ [Government Issued Blockchain Identity: Zug Case Study | ConsenSys](#)

Distributed Ledger Technologien sind deshalb prinzipiell sicherer als nicht DLT basierte Technologien, weil keine zentrale Autorität die Werte und Daten im Alleingang manipulieren kann. Die fehlende zentrale Kontrolle hat jedoch auch Nachteile, so können Fehler oder unentdeckte, übersehene, unterschätzte Eigenschaften des Protokolls nicht, oder nur sehr schwer und unter grossem Zeit und Ressourcen-Aufwand behoben werden. Deshalb verwendet die Stadt eine sogenannte „permissioned Blockchain“. Bei dieser können die Nutzer selber bestimmen, welchen Systemen sie auf der Blockchain trauen wollen.

Die Stadt setzt bei ihren „distributed Ledger“-Projekten auf die Ethereum Blockchain, deren Konsens-Algorithmus noch auf dem sogenannten „Proof of Work“ basiert. Noch für dieses Jahr planen die Ethereum-Entwickler unter Führung der Firma ConsenSys einen Wechsel auf „Proof of Stake“. Bei Proof of Stake werden Transaktionen durch das zur Verfügung stellen von Ether, dem Token der Ethereum Blockchain validiert. Je mehr Token jemand besitzt bzw. «staked»¹⁰ umso mehr Transaktionen werden durch diese Token validiert. Wenn eine Handvoll Personen mehr als 50% aller Token halten, dann können diese wenigen Personen den Konsens-Algorithmus zentral steuern und somit die Regeln des vermeintlich «dezentralen» Netzwerks bestimmen.

Eine kürzlich aufgetauchte Audioaufnahme¹¹ aus dem Jahr 2014 lässt den Eindruck nicht vermeiden, dass beim Vorverkauf der Ethereum Token gezielt dazu aufgerufen wurde die grössten Investoren in Ethereum durch das Schaffen von mehreren Identitäten anhand von Pseudonymen zu verschleiern. Gemäss Audioaufnahme wurde dies gemacht, damit «die Leute nicht Angst vor grossen Käufen» haben, bzw. dass einige wenige Personen oder Institutionen die Mehrheit aller Token halten könnten.

Transkript des Videoausschnittes Ethereum: «Some Economic Considerations» 21.03.2014

Person A: *“Will there be a limit on the amount that a person could invest in Ethereum?”*

Person B: *“A person can buy from any number of different identities. We may limit the size, that the unit size of a sale, just to make it easier to disguise. Let’s say if you are a whale and you want some privacy, you can buy 50,000 Units, just to so nobody scares people with an enormous initial purchase. So if you are a whale and you’re planning on investing several millions US Dollars’ worth, then you can do that through multiple identities. We will ask for a real-world identity in form of an email address so we can make sure that everything works smoothly through the whole process, but we won’t require it. We can create pseudonymous email and identity.”*

Die Ethereum Stiftung und die Entwickler des Ethereum-Netzwerkes und der auf der Blockchain aufbauenden Produkte, welche die Stadt für ihre E-Identität und das E-Voting nutzen haben ihr Produkt als dezentrale Plattform vermarktet. Angesichts des Wechsels auf Proof of Stake könnte eine Verschleierung der Identitäten und somit eine Zentralisierung der grössten Token-Halter eine ernstzunehmende Gefahr für die Dienstleistungen, welche die Stadt auf der Ethereum Blockchain aufbaut, darstellen.

Besten Dank für die schriftliche Beantwortung unserer Fragen

Stefan Huber
Gemeinderat glp

Daniel Marti
Gemeinderat glp

David Meyer
Gemeinderat glp

¹⁰ Mit „staking“ ist das zur Verfügung stellen von Token zur Validierung von Netzwerkaktivitäten gemeint.

¹¹ [Ethereum: Some Economic Considerations - YouTube](#) ab 51:30