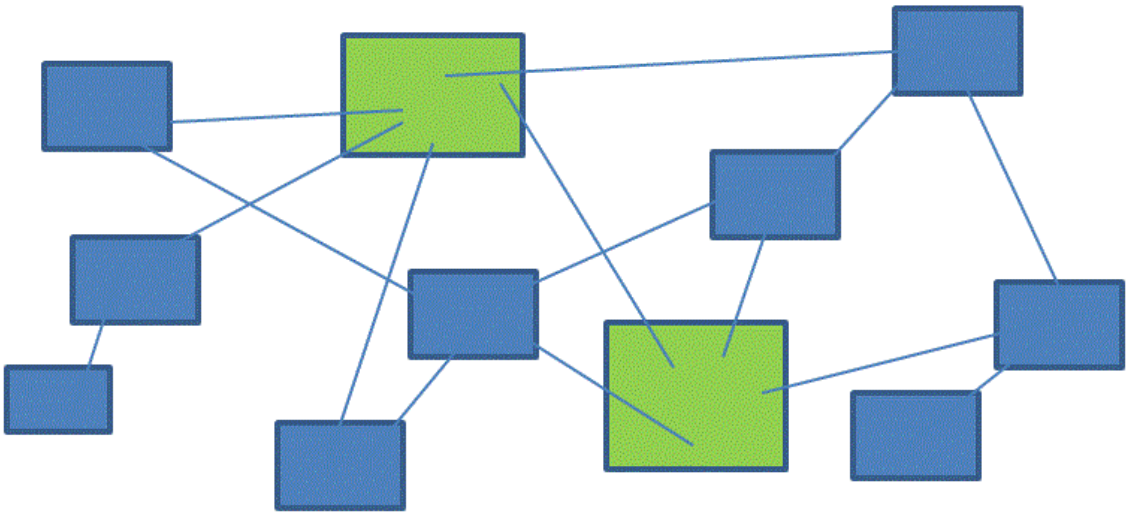
Blockchain Voting System

Vorschlag für ein

System zur Durchführung allgemeiner Wahlen über das Internet

Louis Göttertz

Version 1.3



1. EINLEITUNG **3**

2. ANFORDERUNGEN UND PROBLEME EINES BLOCKCHAIN-BASIERTEN WAHLSYSTEMS **8**

Sicherheit **9**
Integrität 9
Authentifizierung und Anonymität 11
Geheimhaltung 11

3. VORSCHLAG ZUR UMSETZUNG DER ANFORDERUNGEN **13**

4. ANHANG **16**

Verzeichnis der Methoden **17**
Wahlclient 17
Evaluation Client 17
Client für Election Office 18

Literaturverzeichnis **19**

1. Einleitung

Die größte Herausforderung ist es, das Vertrauen der Bürger zu erwerben. Die Auszählung der Stimmen in einem Wahllokal ist für jeden nachvollziehbar, die Speicherung der Stimme in einem Zentralcomputer nicht. (Johann Hahlen, Bundeswahlleiter und Präsident des Statistischen Bundesamtes, am 18. September 2001 auf dem Deutschen Internet-Kongress in Karlsruhe.)

In vielen westlichen Demokratien sinkt das Vertrauen großer Teile der Bevölkerung in das demokratische System. Die Gründe sind meist vielfältig und in den ökonomischen und sozialen Folgen der Globalisierung zu suchen. Eine Quelle des Misstrauens ist aber auch dort zu suchen, wo für den Bürger undurchschaubare komplexe digitale Prozesse die althergebrachten z.B. bürokratischen Verfahren ersetzen. Dort wo elektronische Wahlverfahren eingesetzt werden sind das Misstrauen der Bevölkerung und der Widerstand gegen die Einführung elektronischer Wahlverfahren meist weit verbreitet (Beispiele siehe https://papierwahl.at/).

Internetwahl-Systeme unterliegen von Gesetzes wegen besonderen hohen Anforderungen. Sie müssen zunächst den allgemeinen Grundsätzen einer demokratischen Wahl genügen und sie müssen vertrauenswürdig sein, sowie technisch zuverlässig funktionieren.

Das Bundesverfassungsgericht urteilte 2009:

„dass der Einsatz elektronischer Wahlgeräte voraussetzt, dass die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können." (Pressestelle Bundesverfassungsgericht, 2009)

Die Tatsache, dass schon die einfachen Wahlcomputer, die – wie man meint – unter kontrollierten Bedingungen hergestellt und betrieben wurden, vom Bundesverfassungsgericht als nicht zulässig gewertet worden sind, betont die hohen Sicherheitsanforderungen, die an Internetwahl-Systeme zu stellen sind, wollen sie ernsthaft bei demokratischen Wahlen eine Alternative zur Briefwahl darstellen.

Die Infrastruktur, um demokratische Regierungswahlen in einem Land abzuhalten, gehört ohne Frage zu den kritischen Infrastrukturen eines Landes, wenn Onlinewahlen

erst einmal etabliert sind. Die Frage, „Wer regiert in welchem Interesse?“ ist eine der wichtigsten Fragen in einer Demokratie. Daher ist das Interesse z.B. an Manipulation einer Parlamentswahl auf Staatsebene möglicherweise groß. Nicht erst das Bekanntwerden des Ausmaßes der Geheimdienstaktivitäten verschiedener Länder[1] beweist, dass mögliche Versuche der Einflussnahme auf Regierungsbildungen durch Wahlmanipulation bei Online-Wahlen längst im Bereich realistischer Bedrohungen liegen. Auch die Berichte über möglicherweise staatlich gelenkte Hackerangriffe gegen ausländische Infrastruktur (meist werden Russland oder China als potentielle Urheber genannt) geben Anlass zur Besorgnis.[2] So gilt es bei einem neuen System für Online-Wahlen nicht nur die bekannten Fehler bisheriger Systeme zu vermeiden, sondern auch ein System zu schaffen, welches für zukünftige, noch unbekannte Bedrohungen gewappnet ist und sie möglichst systematisch vollständig ausschließen kann (Systembedingte Robustheit gegenüber Angriffen).

Während bei einer Wahl mit Stimmzetteln Manipulationen oder Wahlfälschungen unter den Rahmenbedingungen der geltenden Vorschriften jedenfalls nur mit erheblichem Einsatz und einem hohen Entdeckungsrisiko möglich sind, sind Programmierfehler in der Serversoftware, fehlerhafte Implementation oder zielgerichtete Wahlfälschungen durch Manipulation der Software oder der Datenbanken bei Server-Client-Systemen nur schwer erkennbar.

Die bisherigen Internetwahl-Systeme beruhten auf Server-Client Architekturen, die systembedingte Schwachstellen haben:

- Server können sehr leicht fehlerhaft implementiert werden,
- Das Fehlen von angemessenen, sicheren Prozeduren für die alltägliche Wartung/Sicherung der Wahlserver oder das Fehlen von Prozeduren zum Umgang mit Anomalien oder deren Nichtbeachtung z.B. aus Zeit- oder Kostengründen.
- zentrale Server können außerdem von außen z.B. mittels Bot-Netzen angegriffen werden oder
- mittels Schadsoftware kompromittiert werden.

---

[1] Siehe Tagesanzeiger (Schweiz): NSA-Affäre verstärkt Misstrauen in E-Voting, http://www.tagesanzeiger.ch/schweiz/standard/NSAAffaere-verstaerkt-Misstrauen-in-EVoting/story/20525542, 4.1.2013, zuletzt abgerufen 11.06.2016

[2] Siehe den Angriff auf die Bundestags-IT im Mai 2015, der bis heute (Anfang September) nicht abgewehrt werden konnte.

Die Situation für die Clients sieht bisher nicht besser aus: Die Clients könnten auf unsicheren Endgeräten installiert sein oder auch per Schadsoftware kompromittiert werden. Man-in-the Middle-Angriffe können für eine Übermittlung falscher Stimmabgaben verantwortlich sein, oder Wahlentscheidungen ausspionieren. Die Beispiele für Sicherheitslücken der Internetwahl-Systeme bei den Wahlen in Norwegen[3], Norwegen[3], Estland[4] und Australien[5] zeigen, dass es trotz aller Bemühungen, diesen systematischen Problemen Rechnung zu tragen, immer wieder Sicherheitslücken bei Online-Wahlen aufgetreten sind, die die Legitimation dieser Art von Wahlen ernsthaft in Frage stellen. Problematisch ist bei den erwähnten Wahlen außerdem, dass ausschließlich proprietäre Software privater Firmen verwendet wurde, was nicht nur die Überprüfung der Software durch externe, unabhängige Experten erschwert, sondern vor allem auch das Vertrauen der Wähler in das System verhindert.

Nicht nur Verschwörungstheoretikern fehlt das Vertrauen in die Produkte gewinnorientierter oder staatlicher Firmen in diesem höchst sensiblen Bereich: Die Gewährleistung von Anonymität bei gleichzeitiger eindeutiger Identifizierung und Authentifizierung ist daher nicht nur eine starke technische sondern auch eine ebenso starke organisatorische Herausforderung. Die meisten Staaten haben deshalb bisher auf flächendeckenden Einsatz von Online-Wahlsystemen verzichtet: Norwegen hat ein schon gestartetes Projekt zur Onlinewahl mitten in den Vorbereitungen abgebrochen. In den Ländern, in denen über die Einführung von Online-Wahlsystemen nachgedacht wurde, formierte sich oft schon bei Bekanntwerden der Pläne Widerspruch in der Bevölkerung -besonders bei den sonst so internetaffinen sogenannten Netz- und Digital-Rights-Aktivisten.[6]

Neben dem Vertrauen in die Sicherheit und Integrität von Online-Wahlsystemen werden als Nachteile benannt, dass Menschen mit geringen Computerkenntnissen, oder

---

3 Siehe: The rise and fall of Internet voting in Norway, Vortrag auf dem 31. Chaos Computer Congress, URL: https://events.ccc.de/congress/2014/Fahrplan/events/6213.html, zuletzt abgerufen am 11.06.2016.

4 Siehe: Independent Report on E-voting in Estonia: https://estoniaevoting.org/, zuletzt abgerufen am 11.06.2016.

5 Siehe: New South Wales Attacks Researchers Who Found Internet Voting Vulnerabilities, URL: https://www.eff.org/deeplinks/2015/04/new-south-wales-attacks-researchers-who-warned-internet-voting-vulnerabilities, zuletzt abgerufen am 11.06.2016

6 Eine reichhaltige Linksammlung zur Kritik an Online-Wahlen findet man unter: http://papierwahl.at.

ohne Zugang zum Internet benachteiligt würden. Der Kritikpunkt ist zwar nicht ganz unberechtigt, vor allem dort, wo Abstimmungen und Wahlen *ausschließlich* als Wahlen stattfinden sollen. Wenn aber die Onlinewahl zusätzlich zu den bisherigen Wahlmöglichkeiten angeboten wird, sticht dieses Argument weniger.

Die Motivation für die Entwicklung eines neuen Systems für die Durchführung von Online-Wahlen, liegt in den Vorteilen, die ein solches System bietet, sofern Transparenz-, Sicherheits- und organisatorische Probleme zufriedenstellend gelöst sind:

1. Neue Möglichkeiten demokratischer Partizipation, und dadurch Steigerung der politischen Einflussnahme
2. Zeit- und Ortsunabhängigkeit für Wähler bei Stimmabgabe -> Steigerung der Wahlbeteiligung
3. Langfristig Senkung der Kosten für Wahlen

Vor allem der zweite Punkt (Zeit- und Ortsunabhängigkeit der Wähler) erscheint mir sehr entscheidend; diese Funktion wird bei konventionellen Wahlen bisher vor allem durch die Möglichkeit der Briefwahl dargestellt. Bei Verwendung eines Onlinewahlsystems könnten Wahlen auch dort ermöglicht werden, wo konventionelle Wahlen nur unter sehr erschwerten Bedingungen durchgeführt werden können. Die Vorteile der Orts- und Zeitunabhängigkeit würde in Ländern mit schwacher Infrastruktur oder in Ländern, die unter Bürgerkrieg oder Terrorismus leiden, besonders zum Tragen kommen, da gerade dort wo es eine schwache oder zerstörte Infrastruktur gibt, die Nutzung des mobilen Internets in allen Bevölkerungsschichten schon sehr verbreitet ist und schneller zunimmt als in den entwickelten Industrieländern.[7]

Die Blockchain-Technologie, die mit der Erfindung der digitalen Kryptowährung Bitcoin, bekannt wurde, könnte das zentrale Problem der Transparenz und des Vertrauens bei Online-Wahlen lösen und andere Sicherheitsprobleme entschärfen. Im Gegensatz zu den bisher verwendeten Server-Client-Architekturen besteht der Kern der Blockchain-Technologie aus einer mittels Peer-To-Peer-Protokoll verteilten Datenbank, deren Integrität durch einen kryptografischen Hash-Algorithmus sichergestellt wird. Dadurch sind alle Vorgänge in dieser Datenbank für alle

[7] (International Telecommunication Union (ITU), 2015)

Teilnehmer zugänglich und transparent. Bezogen auf ein Wahlsystem hieße das, dass alle Stimmzuweisungen und Stimmabgaben sicher aufgezeichnet würden und jeder Zugriff auf diese Informationen hätte und darüber hinaus die Gültigkeit dieser Informationen gesichert sei. Jeder Wähler kann zum Schluss überprüfen: Wurde meine meine Stimme wie beabsichtigt zugeordnet? Wurde meine Stimme gezählt wie zugeordnet und werden alle Stimmen gezählt?[8]

Die Transparenz, die die Verwendung der Blockchaintechnologie bietet, ist ein Vorteil bezogen auf das Vertrauensproblem, jedoch auch ein Problem für die Durchführung von politischen Wahlen, bei denen u.a. die Anonymität und Geheimhaltung der Wahlergebnisse bis zum Ende der Wahl gewährleistet sein muss. Trotzdem erscheint mir die Blockchain-Technologie aufgrund der Robustheit einer verteilten Anwendung[9] und des enormen Vorteils des Vertrauens in dessen Korrektheit geeignet, als Basistechnologie für ein System zur Durchführung von Wahlen über das Internet vielversprechend, wenn es gelingt die Probleme, die sich z.B. aus der Transparenz der Blockchain ergeben, zu lösen.

Es gibt bereits zahlreiche Weiterentwicklungen von Bitcoin und anderen digitalen Währungen auf Blockchain-Basis, die viel weitergehende Funktionen auch abseits von digitalen Währungen haben und z.B. Intelligente (automatische) Verträge ermöglichen (Smart Contracts), sowie Werkzeuge für Voting, virtuelle Gesellschaften aller Art u.v.m. ermöglichen, deshalb bin ich überzeugt, dass die Blockchain-Technologie auch als Basis für ein „richtiges“ Online-Wahlsystem taugt – ein Wahlsystem, welches politische Wahlen nach demokratischen Standards ermöglicht und damit auch hierzulande – wenn gewollt - umsetzbar wäre.

[8] Vergl.: End-to-End (E2E) Voter-Verifiability (Halderman, 2015)., (Clark, 2011)
[9] Das Bitcoin-Netzwerk funktioniert seit 2009 ohne größere Probleme und Sicherheitslücken.

2. Anforderungen und Probleme eines Blockchain-basierten Wahlsystems

Sicherheit

Integrität

Der Vorteil der jederzeit überprüfbaren Integrität der Informationen in einer Blockchain soll in dem hier vorgeschlagenem Blockchain Voting System (BVS) genutzt werden, um alle relevanten Informationen und Variablen zu speichern, damit kein zusätzlicher Server notwendig ist der z.B. die Stimmzettel für die Clients bereit stellt, oder die Stimmzettel mitsamt der Wahloptionen und Ihrer Codierung auf den unsicheren Clients gespeichert werden müssen. Im BVS sollen sowohl die Daten für die Stimmzettel und Wahloptionen als auch die Stimmen der Wähler (Wahlentscheidungen) in Form von Transaktionen in der Blockchain gespeichert werden.

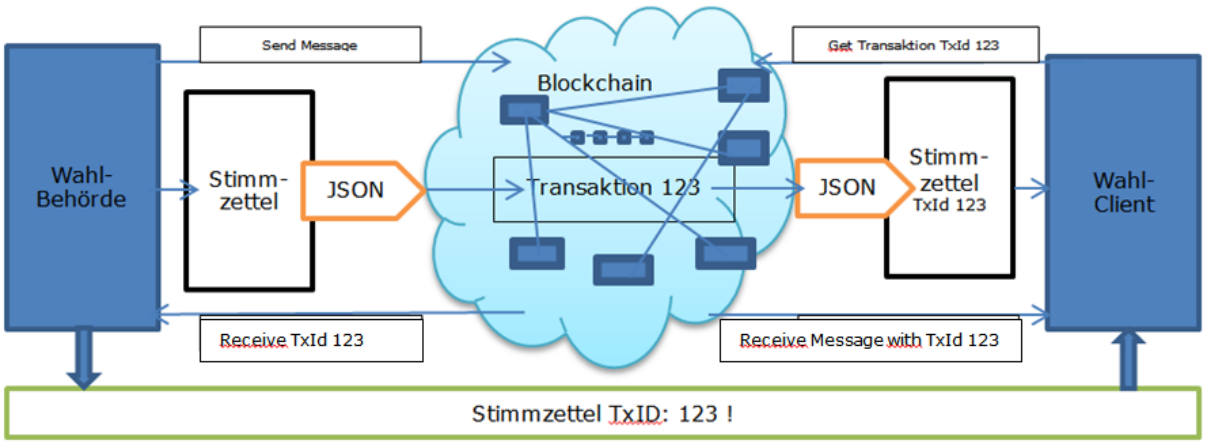


Abbildung 1: Speichern und Lesen der Stimmzettel in bzw. aus der Blockchain.

Im Fall der Stimmzettel, werden diese Daten einfach von den Clients aus der Blockchain geladen. Dazu muss lediglich den Clients die Transaktions-ID (TxId) bekannt sein, die den Stimmzettel enthält. Diese wird vor Beginn der Wahl von den Wahlbehörden bekannt gegeben. Die Gefahr, dass falsche Stimmzettel von einem manipulierten Server geladen werden, ist durch die Blockchain gebannt.[10]

Eine andere Anforderung in Bezug auf die Integrität einer Online-Wahl ist, dass zum Schluss das Wahlergebnis überprüfbar sein muss. Die notwendige Geheimhaltung bei

[10] Vergl.: Decker, et al., 2013

einer Wahl macht es jedoch schwer, ein Verfahren zu entwickeln, welches einerseits einfach für Wählerinnen und Wahlbeobachter zu handhaben ist und andererseits gewährleistet, dass einzelne Stimmen und das Wahlergebnis insgesamt überprüfbar sind. Diese Anforderung wird in der Fachliteratur als End-To-End Verifiability, abgekürzt E2E-V bezeichnet. End-To-End Verifiability wird in der englischen Fachliteratur auf eine kurze Formel gebracht:

The verification objectives can be summarized with the catchphrase, "Cast as intended; recorded as cast; and counted as recorded."[11]

Das bedeutet, dass überprüfbar sein muss:

1. Wurde der beabsichtigte Kandidat gewählt. Wenn beispielsweise die Kandidaten auf den Listen vertauscht würden, könnte ein Wähler unbeabsichtigt die falsche Wahl treffen.
2. Wurde die Stimme so übermittelt und gespeichert, wie gewählt. Durch Manipulationen bei der Übermittlung oder Speicherung können bei einem Online-Wahlsystem
3. wurde die Stimme auch so gewertet wie gespeichert.

Es wäre einfach, diese Anforderungen in einem blockchain-basiertem System zu erfüllen, gäbe es nicht das Wahlgeheimnis, wodurch eine offene Stimmabgabe durch Versenden von Coins oder Assets an Adressen von Kandidaten nicht möglich ist, wenn es um politische Wahlen geht.

Ein Problem dabei ist, dass eine offene Stimmabgabe dazu führt, dass diejenigen, die später wählen, durch Informationen über die bereits abgegebenen Stimmen einen Vorteil haben gegenüber denjenigen, die früher gewählt haben. Die späten Wähler könnten bei ihrer Wahlentscheidung durch diese Informationen beeinflusst werden, um z.B. taktisch zu wählen. Außerdem wäre es den Wählern, die ihre eigenen Adressen ja kennen, zu beweisen, was sie gewählt haben, was mit der Gefahr des Stimmenkaufs verbunden ist (siehe Abschnitt „Geheimhaltung").

Um diesem Problem zu begegnen ist es notwendig, die Stimmabgabe geheim zu halten. Dazu muss die einfachste Möglichkeit für Transaktionen, Stimmen als Assets oder Coins direkt an Adressen von Kandidaten oder Wahloptionen zu senden, ersetzt

[11] Kiniry, et al., 2015 S. 20

werden durch ein Verfahren, das Transaktionen, die die Wahlentscheidungen enthalten diese geheim, das heißt in verschlüsselter Form speichern und an eine „neutrale“ Adresse senden.

[Skizze]

Authentifizierung und Anonymität

Für eine demokratische Wahl muss gewährleistet werden, dass nur berechtigte Wählerinnen ihre Stimme abgeben können und dass jeder die gleiche Anzahl von Stimmen hat. Gleichzeitig muss die Anonymität der abgegebenen Stimmen gewahrt bleiben. Bei einem Peer-To-Peer-Netzwerk auf Basis des Bitcoin-Protokolls ist eine Authentifizierung nicht vorgesehen, jeder kann Teilnehmer in dem Netzwerk werden und alle Transaktionen beobachten. Das sollte sich auch möglichst nicht ändern, da so theoretisch jeder Internetnutzer auch als Wahlbeobachter teilnehmen kann. Stattdessen kann die Eigenschaft eines Blockchain-basierten Netzwerks, über eine native Währung zu verfügen oder auch „Assets“[12] erzeugen zu können, für ein Online-Wahlsystem ausgenutzt werden, um den Wählern ihre Stimmrechte zuzuteilen. Anstatt Stimmzettel auszuhändigen, werden Stimmrechte in Form von digitalen Assets anonymisiert z.B. per Paper Wallet an die Clients der Wähler gesendet, deren Besitz einen Wähler als wahlberechtigt identifiziert.

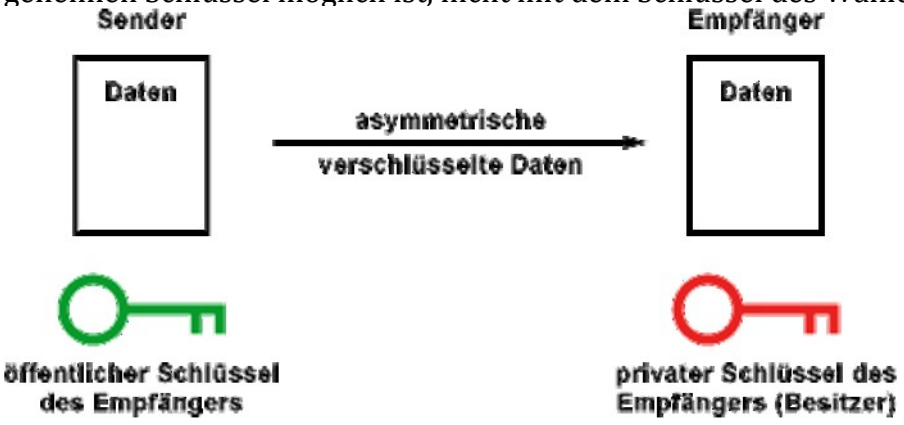
Geheimhaltung

Ein Online-Wahlsystem muss eine geheime Wahl garantieren. Da eine Online-Wahl unter „unkontrollierten“ Bedingungen stattfindet (nicht im Wahllokal sondern zuhause auf unsicheren Endgeräten), muss außerdem sichergestellt werden, dass kein massenhafter Stimmenkauf, Erpressung etc. technisch ermöglicht wird, ohne dass dies entdeckt wird. Das bedeutet, dass das System beispielsweise nicht offenbaren darf, wie ein bestimmter Wähler gewählt hat.

Widerstandsfähigkeit gegen Erpressung - Coercion resistance und Quittungsfreiheit

[12] Asset (englisch) zu Deutsch „Wert“ als allgemeiner Begriff, bezeichnet in den Blockchain-Protokollen eine Werteinheit, die für beliebige Werte z.B. Aktienanteile, Geld, oder auch Stimmrechte stehen kann. Assets können genau wie die „native Währung“ (z.B. BTC) im Netzwerk transferiert bzw. gehandelt werden.

Das Problem der potentiellen Erpressbarkeit erweitert die Anforderung der bloßen Geheimhaltung: Die Gefahr, dass Stimmen gekauft oder erpresst werden, lässt sich nur verhindern, wenn eine Wählerin keine Möglichkeit hat, zu beweisen, wie sie gewählt hat. Wäre sie dazu in der Lage, könnte ein Erpresser diesen Beleg fordern und sie wäre erpressbar. Eine Anforderung, die deswegen an elektronische Wahlsysteme gestellt wird, wird in der Literatur als „Coercion resistance" - zu Deutsch etwa „Widerstandsfähigkeit gegen Erpressung" bezeichnet.[13] Etwas schwächer formuliert ist in der Literatur die Anforderung der Quittungsfreiheit. Die Quittungsfreiheit besagt einfach, dass ein Wähler keine Information (=Quittung) vom System erhalten darf, wie er gewählt hat, also nicht in der Lage sein darf, die eigene Wahlentscheidung zu überprüfen. Ein möglicher Erpresser darf außerdem auch **ohne Kooperation** der Wählerin keine Möglichkeit haben, eine Verbindung zwischen der Wählerin und ihrer Wahlentscheidung herstellen können dürfen. Um die Anforderungen betreffs der Geheimhaltung und Widerstandsfähigkeit zu erfüllen, ist es notwendig, die Wahlentscheidungen bei der Übertragung in die Blockchain so zu verschlüsseln, dass ein Erpresser keine Möglichkeit hat, vom Opfer oder dem Computer des Opfers einen Schlüssel zur Entschlüsselung der Daten zu bekommen, um Kenntnis über die tatsächliche Wahlentscheidung der Wählerin zu erlangen – sei es mit oder ohne Kooperation der Wählerin. Ein asymmetrisches Verschlüsselungsverfahren stellt sicher, dass eine Entschlüsselung nur mit dem geheimen Schlüssel möglich ist, nicht mit dem Schlüssel des Wahlclients.



[13] Siehe: Bundeamt für Sicherheit in der Informationstechnik, 2008; Delaune, et al., 2006; Juels, et al., 2005; Ryan, et al., 2009

3. Vorschlag zur Umsetzung der Anforderungen

In einem konventionellen Blockchain-basierten Netzwerk ist die Geheimhaltung der Informationen nicht vorgesehen. Die einfache Methode, Coins oder Assets direkt an Kandidatenadressen zu senden, fällt aus, weil jeder der Transaktionen auf die Adressen der Wählerinnen zurückverfolgt werden könnte.

Ich schlage daher ein zweistufiges Verfahren vor, bei dem im ersten Schritt die Stimmabgabe verschlüsselt erfolgt und Transaktion in der Blockchain dokumentiert wird und im zweiten Schritt die Entschlüsselung auf mehreren unabhängigen und vertrauenswürdigen Nodes des Blockchain-Netzwerkes erfolgt. Die Wahlentscheidungen könnten direkt als Rohdaten zur Weiterverarbeitung über eine API publiziert werden, um sie schnell verfügbar zu haben; eine bessere Option könnte aber sein, aus für jeden entstandenen Rohdatensätzen wiederum eine Transaktion zu generieren, die diesmal ein Asset gesendet an die entschlüsselte Kandidatenadresse enthält, um eine öffentliche Überprüfbarkeit der Einzelergebnisse zu erleichtern.

Genauer:

Im ersten Schritt sendet der Client eine Transaktion, die sein Asset für die Berechtigung zur Stimmabgabe erhält sowie einen Text in den Metadaten, der die **verschlüsselte Wahlentscheidung (Kandidatenadresse)** und eine Prüfziffer enthält. Damit ein Wähler trotz Verschlüsselung die Möglichkeit hat, die E2E-V zu prüfen, schlage ich vor, dass der Wahlclient für jede Wahloption im Client Stimmzettel einen individuellen Code generiert, der neben der verschlüsselten Kandidatenadresse und einer Prüfsumme für beide Angaben zusammen bei der Stimmabgabe übermittelt und auch angezeigt wird. Dieser Code kann nach der Stimmabgabe in den Transaktionen zur Überprüfung der E2E-V abgefragt werden. Ist der Code korrekt, bedeutet das, dass die richtige Wahloption übermittelt wurde.

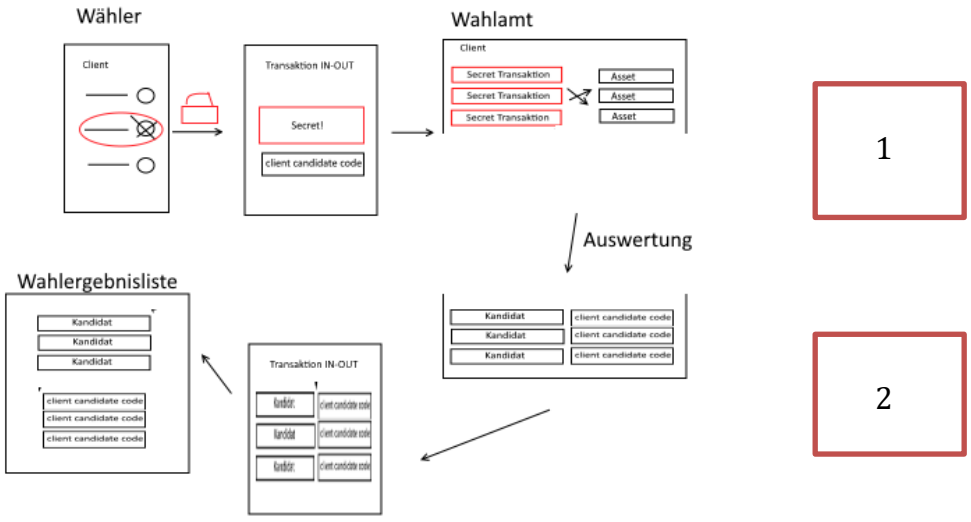
[Skizze]

Die Zieladresse der Transaktion ist dabei eine **neutrale** Adresse, die an den Stimmzettel gebunden ist. Wenn alle Stimmen abgegeben wurden, enthält diese neutrale Adresse 100% der Stimmberechtigungen (Assets).

[Skizze]

Im zweiten Schritt nach Ende der Stimmabgabe werden diese Transaktionen, die leicht anhand der neutralen Zieladresse und anhand der Assets zu identifizieren sind, von **besonderen** Nodes aus der Blockchain gelesen und entschlüsselt. Damit stünde schon sehr schnell ein Ergebnis zur Verfügung. Damit die Auswertung jedoch dokumentiert wird und der dritte Punkt der E2E-V erfüllt ist, wird für jede Transaktion ein zufälliges Asset mit dem individuellen Code aus der Stimmabgabe von der neutralen Adresse an die nun entschlüsselte Adresse des jeweiligen Kandidaten gesendet. Nach der Auswertung enthält die neutrale Adresse keine Assets mehr, da diese entsprechend den Wahlentscheidungen auf die Kandidatenadressen verteilt sind, wenn die Auswertung vollständig und korrekt erfolgt.

Die Prüfsummen aus dem ersten und zweiten Schritt jeweils addiert müssen die gleiche Gesamtsumme ergeben, dann ist die Wahl erfolgreich überprüft.



Durch dieses zweistufige Verfahren ist die ursprüngliche Wahlentscheidung für jeden überprüfbar: Jeder kann die Prüfsumme der verschlüsselten Wahlentscheidung aus der Blockchain vergleichen mit der, die bei Stimmabgabe angezeigt wurde und prüfen ob diese bei der Auswertung auch enthalten sind. Kein Wähler ist jedoch dadurch in der Lage zu beweisen, welchen Kandidaten er gewählt hat, da sowohl die verschlüsselte Adresse als auch der individuelle Code nicht einem Kandidaten zugeordnet werden kann, ohne den geheimen Schlüssel zu kennen.

Die Anforderungen der Geheimhaltung werden ebenfalls gewahrt: In der Blockchain ist der Weg der Transaktionen unterbrochen, da im zweiten Schritt der Auswertung ein zufälliges Asset übermittelt wird und dadurch nicht die Adresse eines Wählers in den Inputs der Kandidatenstimmen enthalten sind.

Die Anonymität der Stimmabgabe kann durch eine Kombination von Maßnahmen erreicht werden:

Die Assets als Stimmberechtigungen werden anonymisiert, in dem zufällige Adressen erzeugt werden, die diese vor Beginn der Wahl enthalten. Diese werden z.B. als „Paper-Wallets“ oder in anderer Form gespeichert und versiegelt. Wählerinnen importieren immer eine **zufällige** Paper Wallet mit den darin enthaltenen Assets für eine bestimmte Wahl. Durch dieses Verfahren bleiben die Adressen anonym und das Wahlgeheimnis in dieser Hinsicht gewahrt.

Anders als bei Bitcoin werden die Adressen nur einmal bei der Stimmabgabe verwendet, so dass eine Zuordnung zwischen bestimmten Clients oder IP-Adressen und den Bitcoin-Transaktionen unwahrscheinlich ist, wenn ein Proxy-Netzwerk ähnlich Tor bei der Stimmabgabe genutzt wird.

4. Anhang

Verzeichnis der Methoden

Wahlclient

Konfiguration, Paper Wallet

Funktionen

1. Import Project, Import Paper Wallet als ein Prozess am besten durch QR-Code

Stimmabgabe

a) Transaktion Stimmabgabe generieren

Funktionen

1. Wahlentscheidung verschlüsseln -> Metadaten erster Abschnitt Algorithmus:
2. Client-Prüfziffer für die Kandidaten ermitteln + Individueller Code (nachvollziehbar, aber nicht vorhersehbar z.B. aus den aktuellen Börsenkurse eines Indexes -> Metadaten zweiter Abschnitt
3. Metadaten erzeugen

b) Transaktion senden

1. Asset Allocation
2. Asset und Metadaten senden

Evaluation Client

c) Transaktionen lesen

Für jeden Stimmzettel:

List Address Transaktions

d) Transaktion auswerten

Für jede Transaktion:

1. Get Metadata.
2. Decrypt Metadata 1

3. Generate Transaktion

e) Asset an Kandidatenadresse senden

Für jede neue Transaktion: Send Transaktion

f) Asset-Verteilung auswerten

Für jede Option:

getaddressbalances(Option Adresse)

Client für Election Office

Literaturverzeichnis

Ben-Sasson, Eli, et al. 2014. *Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version).* 2014.

Biryuk, Alex, Khovratovic, Dimitry und Pustogarov, Ivan. 2014. Deanonymisation of Clients in Bitcoin P2P Network. [Online] 2014. [Zitat vom: 29. 09 2015.] http://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf.

Bundeamt für Sicherheit in der Informationstechnik (BSI). 2008. Common Criteria Protection Profile BSI-CC-PP-0037. *www.bsi.de.* [Online] 1.0, 18. April 2008. [Zitat vom: 09. Juni 2016.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0037b_pdf.html.

Clark, Jeremy. 2011. Democracy Enhancing Technologies:Toward deployable and incoercible E2E elections. *Université Concordia.* [Online] 2011. [Zitat vom: 15. November 2016.] http://users.encs.concordia.ca/%7Eclark/theses/phd_electronic.pdf.

De Vries, Manon und Bokslag, Wouter. 2016. *Evaluating e-voting: theory and practice.* Department of Information Security Technology, Technical University of Eindhoven. Eindhoven : s.n., 2016. [Dokument]. arXiv:1602.02509v1 [cs.CY] 8 Feb 2016.

Decker, Christian und Wattenhofer, Roger. 2013. *Information Propagation in the Bitcoin Network.* ETH Zurich; Microsoft Research. Zürich : s.n., 2013.

Delaune, Stephanie, Kremer, Steve und Ryan, Mark. 2006. Coercion-Resistance and Receipt-Freeness in Electronic Voting. [Hrsg.] IEEE. *Computer Security Foundations Workshop.* 2006.

Hahlen, Johann. 2001. *Vortrag zum Thema Internetwahlen.* Deutscher Internet-Kongress in Karlsruhe : s.n., 18. September 2001.

Halderman, Alex. 2015. Security Analysis of Estonia's Internet Voting System. [Online] 2015. [Zitat vom: 2. September 2015.] https://estoniaevoting.org/.

International Telecommunication Union (ITU). 2015. The World in Facts and Figures. [Online] 05 2015. [Zitat vom: 09. Juni 2016.] http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

Juels, Ari, Catalano, Dario und Jakobsson, Markus. 2005. Coercion-resistant electronic elections. *http://www.arijuels.com.* [Online] 2005. [Zitat vom: 16. November 2016.] http://www.arijuels.com/wp-content/uploads/2013/09/JCJ10.pdf.

Kiniry, Joseph R, et al. 2015. *The Future of Voting.* U.S. VOTE FOUNDATION. s.l. : Galois, 2015.

Luo, Shoufu, Seideman, Jeremy D. und Tsai, Gary. 2016. THE PEOPLE'S CHOICE - A accountable distributed blockchain-based digital voting system. *economist.com.* [Online] 29. September 2016. [Zitat vom: 26. November 2016.] www.economist.com/sites/default/files/cuny.pdf.

New South Wales Electoral Commission. 2014. *iVote® Project- iVote® System Security Implementation Statement.* Sydney : s.n., 2014. Statement.

Pressestelle Bundesverfassungsgericht. 2009. *Verwendung von Wahlcomputern bei der Bundestagswahl 2005 verfassungswidrig.* Karlruhe : s.n., 3. März 2009.

Teague, Vanessa und Halderman, J. Alex. 2015. The New South Wales iVote System:. *CITP Center for Information Technology Policy.* [Online] 22. März 2015. [Zitat vom: 2. September 2015.] http://arxiv.org/pdf/1504.05646v2.pdf.