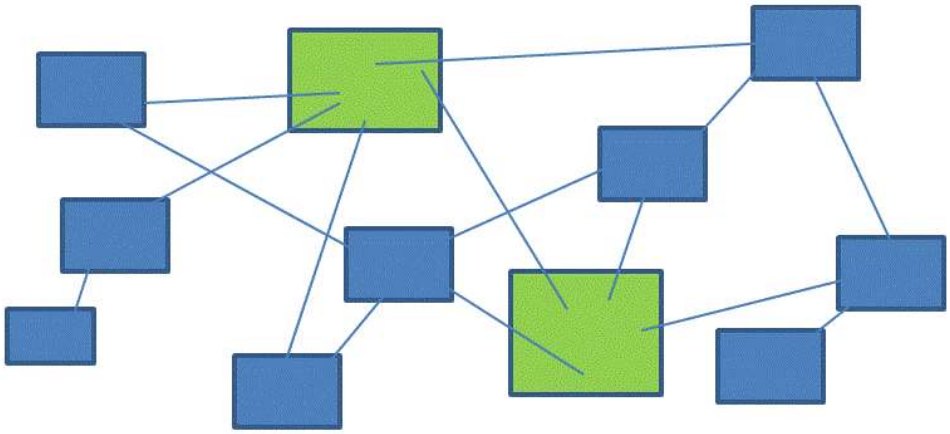
Blockchain Voting System

Whitepaper

Projektentwurf eines Systems zur Durchführung allgemeiner Wahlen über das Internet

Louis Göttertz

Version 1.0



9. ANHANG:

FEHLER! TEXTMARKE NICHT DEFINIERT.

Definitionen

Fehler! Textmarke nicht definiert.

Verschlüsselung:

Fehler! Textmarke nicht definiert.

Hash-Verfahren:

Fehler! Textmarke nicht definiert.

(Schweisgut, 2007 S. 9)

Fehler! Textmarke nicht definiert.

Glossar

Fehler! Textmarke nicht definiert.

1. Abstract

2. 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 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 ausländische Infrastruktur (meist werden Russland oder China als potentielle 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 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:

1. Server können sehr leicht fehlerhaft implementiert 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.

2. 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.
3. zentrale Server können außerdem von außen z.B. mittels Bot-Netzen angegriffen werden oder
4. mittels Schadsoftware kompromittiert werden.

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 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 sondern vor allem auch das Vertrauen der Wähler in das System verhindert.

---

[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

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 ohne Zugang zum Internet benachteiligt würden. Der Kritikpunkt ist zwar nicht ganz unberechtigt, vor allem dort, wo Abstimmungen und Wahlen *ausschließlich* als Online-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

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

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 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 Teilnehmer 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 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 Korrektheit geeignet, als Basistechnologie für ein System zur Durchführung von Wahlen Wahlen über das Internet vielversprechend, wenn es gelingt die Probleme, die sich z.B. z.B. aus der Transparenz der Blockchain ergeben, zu lösen.

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

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 höchsten demokratischen Standards ermöglicht und damit auch hierzulande – wenn gewollt - umsetzbar wäre.

Das ist das Hauptziel dieses Projekts: ein Wahlsystem welches politische Wahlen nach höchsten demokratischen Standards ermöglicht.

Dazu soll eine Reihe von Wahlclients sowie eine Web-basierte Plattform für die Organisation von Wahlen und Abstimmungen über das Internet entwickelt werden, die es Organisatoren von Wahlen erleichtert, die nötigen Wahlvorbereitungen zu treffen und die Wahl für die Öffentlichkeit zu organisieren unter *Einhaltung verbindlicher Standards*: Dazu gehört die Verteilung von Informationen zur Wahl, die Erzeugung von Stimmzetteln und deren Bereitstellung in der Clientsoftware - genügend den Anforderungen im Bundeswahlgesetz § 30 ff., die Bereitstellung von Templates für die notwendigen Blockchain-Parameter uvm., welches Thema des nächsten Kapitels „Bestandteile und Funktionen eines Online-Wahlsystems“ ist.

3. Probleme der Sicherheit bei Online-Wahlsystemen

Die wichtigsten Voraussetzungen für den Betrieb eines Online-Wahlsystems bestehen jedoch in der Gewährleistung der gesetzlichen Anforderungen vor allem in Bezug auf die Sicherheit des Systems. Da die bisher bei Wahlen eingesetzten Online-Wahlsysteme den Anforderungen an Sicherheit, Transparenz und Verfügbarkeit bisher nicht genügen, sollte ein neuer Entwurf, die bisherigen Probleme systematisch ausschließen können.

Bei der Betrachtung der traditioneller Wahlverfahren werden schon die grundsätzlichen Sicherheitsprobleme und Anforderungen deutlich: 1. Wähler ihre Wahlentscheidung in eine öffentliche Liste: Wähler und Wahlbeobachter können die Integrität der Aufzeichnung gleichermaßen verifizieren. Jedoch kann auch jeder

beobachten, wer welche Wahlentscheidung getroffen hat. 2. Urnenwahl: Die abgegebenen Stimmen können nicht auf die einzelnen Wähler zurückverfolgt werden: was eine geheime Wahl ermöglicht. Der Wähler hat jedoch keine absolute Sicherheit, was nach Einwurf des Stimmzettels in die Urne geschieht, ob seine Stimme korrekt gezählt wird, ist nicht garantiert. 3. Briefwahl: Bei einer traditionellen Briefwahl ist es theoretisch möglich, dass Stimmen gefälscht werden. Da außerdem der Wahlvorgang nicht mehr in einer geschützten Umgebung stattfindet, sondern „unkontrolliert" zuhause, ist es außerdem theoretisch möglich, dass der Wähler zuhause in seiner Entscheidung unzulässig beeinflusst oder gar erpresst wird. Mit der Briefwahl muss außerdem ein Identifizierungsmerkmal mitgesendet werden, dass den Wähler identifiziert, um unberechtigte Stimmen auszuschließen und so eine Stimmzuordnung Stimmzuordnung theoretisch möglich macht, wenn z.B. den hierzulande gesetzlich festgelegten Prozeduren der Trennung von Stimmzettel und Briefumschlägen nicht entsprochen wird.

Den bei traditionellen Wahlverfahren auftretenden Gefahren für die Sicherheit wird mit erheblichen *organisatorischem* Aufwand entgegen gewirkt, so dass der Aufwand für Wahlmanipulationen so erheblich und das Entdeckungsrisiko so groß ist, dass sich eine größer angelegte Manipulation nicht lohnt. Bei elektronischen Wahlverfahren ist das jedoch – wie in der Einleitung erwähnt – ganz anders. Zunächst werden die Probleme der traditionellen Wahlsysteme quasi vererbt und es ergeben sich erhebliche neue Probleme, weil sich Fehler in der Sicherheitsarchitektur gleich massenhaft auswirken und nicht nur auf einen kleinen Teil der Stimmen beschränkt sind, wie das in der Regel bei traditionellen Wahlverfahren der Fall ist.

In der Literatur wird bei den Gefahren einer Online-Wahl über das Internet meist zuallererst das Endgerät des Wählers genannt. Es ist allgemein bekannt, dass Computer, Computer, Smartphones und andere Geräte, die als Endgeräte für Internetwahlen infrage kommen, anfällig für allerlei Gefahren: Viren, Trojaner etc. sind, was dazu führen führen kann, dass die Wahlentscheidungen auf einem Client-Endgerät gefälscht oder ausspioniert werden können. Da diese Art von Angriff nicht ausgeschlossen werden kann, sind außer den organisatorischen Maßnahmen für die Verteilung der Software (Zertifizierung von Server und Software, Linux-Live-Systeme u.a.), *Maßnahmen in der Software selbst* zu treffen, die die Integrität der Stimmenübermittlung sicherstellen und

und die Geheimhaltung bzw. Anonymität der Stimmabgabe so weit wie möglich schützen.

Geheimhaltung

Zu lösen ist zuerst das Problem der Geheimhaltung. In einem Blockchain-basierten Peer-to-Peer-Netzwerk - wie geplant - sind alle gespeicherten Informationen für alle Teilnehmer sichtbar. Das heißt natürlich auch, dass ohne weitere Maßnahmen (Verschlüsselung etc.) Wahlentscheidungen unmittelbar sichtbar sein würden. Für politische Wahlen ist das ein Problem, denn damit diese allgemein und für jeden gleich sind, dürfen die Wahlergebnisse von Wählern, die zu einem früheren Zeitpunkt gewählt haben, nicht vorab bekannt werden, so dass keine strategische Beeinflussung geschieht. Die einzige Lösung besteht bisher in der Verschlüsselung der Wahlentscheidungen.

Coercion resistance

Zusammenhängend mit der Geheimhaltung ist auch das Problem der potentiellen Erpressbarkeit[10]: Die Gefahr, dass Stimmen gekauft oder erpresst werden, lässt sich verhindern, wenn eine Wählerin nicht die Möglichkeit hat, zu beweisen, wie sie hat. Wäre sie dazu in der Lage, könnte ein Erpresser diesen Beleg fordern und sie erpressbar. Eine Anforderung, die deswegen an elektronische Wahlsysteme gestellt wird, ist die Erpressungs-Widerstandsfähigkeit.

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 Client des Opfers?!) einen Schlüssel zur Entschlüsselung der Daten zu bekommen und so auch nicht wissen kann, wie der Wähler gewählt hat. Um dennoch die Überprüfbarkeit durch den Wähler zu gewährleisten, könnte ein Hash der Wahlentscheidung beim Client angezeigt und in der BC gespeichert und nach Entschlüsselung und Auszählung der Stimmen wieder der Wählerin zur Verfügung gestellt werden, wenn sie die entsprechende TransaktionsID ihres Wahlvorganges eingibt.

[10] (Bundeamt für Sicherheit in der Informationstechnik (BSI), 2008 S. 26)

Anonymität

Auch wenn Bitcoin in der Öffentlichkeit mit anonymen Geldtransfers zur Geldwäsche und illegalen Geschäften im Darknet in Verbindung gebracht wird, so garantiert ein Netzwerk wie Bitcoin keineswegs die Anonymität der Netzteilnehmer. Es ist theoretisch theoretisch möglich, anhand eines Zeitabgleiches und der IP-Nummer des Wählers eine eine Zuordnung zwischen Wahlentscheidung und Wähler herzustellen[11], wenn keine zusätzlichen Tools zur Anonymisierung entwickelt werden (Proxy-Server, verbesserte verbesserte Tor-Integration o.ä.), die als ein fester Bestandteil eines Online-Wahlsystems zu gelten haben.

Authentifizierung

Es muss sichergestellt werden, dass nur berechtigte Wählerinnen ihre Stimme abgeben können und dass jeder die gleiche Anzahl von Stimmen hat.

Bei den traditionellen Wahlverfahren geschieht die Authentifizierung mittels physischer Zugangskontrolle und Abgleich mit Wählerlisten oder bei der Briefwahl mittels eines Identifizierungsmerkmals in dem Brief. Die Zuweisung der Stimmrechte geschieht durch Übergabe der Stimmzettel.

Bei einem Peer-to-Peer-Netzwerk auf Basis z.B. des Bitcoin-Protokolls ist eine Authentifizierung nicht vorgesehen. Den Zugang zum Netzwerk selbst mit einer Authentifizierung abzusichern, wäre eine Möglichkeit, um unautorisierte Wähler an der Wahl zu hindern. Das Problem der Zuweisung von Stimmrechten wäre damit noch nicht gelöst.

Eine Möglichkeit der Zuweisung von Stimmrechten für die jeweiligen Wahlen würde gleichzeitig das Problem der Authentifizierung lösen, da nur stimmberechtigte Ihre Stimme abgeben könnten. Gleichzeitig würde das Netzwerk für beobachtende Teilnehmer offen bleiben können, wenn gewünscht.

[11] (Biryuk, et al., 2014)

4. Bestandteile und Funktionen eines Wahlsystems zur Durchführung von Online-Wahlen

Transparenz, Robustheit und Sicherheit -> Blockchain-System

Erweiterte Anforderungen

Um als Alternative zur bisherigen Praxis von Politik und Wählern akzeptiert zu werden, muss ein Online-Wahlsystem organisatorisch leicht implementierbar, billig, effizient und anwenderfreundlich sein. Das heißt: das System müsste möglichst ohne Änderung oder Neuanschaffung von aufwendiger Infrastruktur auf zumindest auf Wählerseite funktionieren. Die Wahlclients sollten einfach zu installieren (z.B. wie auf Android oder iOS) und zu bedienen sein und möglichst auf vielen Endgeräten (Smartphone, PC, TV etc.) funktionieren. Die Ergebnisse müssen transparent und einfach mit unabhängiger Software überprüfbar sein. Das System muss flexible Wahlmöglichkeiten und Layouts für Stimmzettel ermöglichen. Darüber sollten verschiedene Scoring-Protokolle[12] möglich sein.

Umsetzung

Für die Umsetzung der genannten Anforderungen ist eine Reihe von Entscheidungen nötig.

Grundentscheidungen:

1. Wie soll eine Wahlentscheidung technisch in der verteilten Blockchain-Datenbank gespeichert werden?
2. Wie soll die Verschlüsselung erfolgen, ohne dass ein Schlüssel auf dem Client-Computer existiert, mit dem die Wahlentscheidung entschlüsselt werden kann?
3. Authentifizierung: Wählerlisten und Zuweisung von Assets?
4. Verfügbarkeit: Welche Änderungen sind gegenüber z.B. dem Bitcoin-Protokoll nötig?
5. Speicherung der Stimmzettel und Wahloptionen in der Blockchain?

[12] Verschiedene Wahlsysteme gestatten es z.B. eine Rangfolge zwischen Kandidaten festzulegen oder mehrere Stimmen zu verteilen.

1. Wahlentscheidungen in der Blockchain speichern

Es gibt zwei grundsätzliche Möglichkeiten, Wahlentscheidungen in der Blockchain abzubilden bzw. zu übermitteln und zu speichern:

1. Senden von Coins oder Assets [Link Erklärung]
2. Speichern der Wahloption als Text, Code, Adresse etc.

Gemeinsam ist beiden Möglichkeiten, dass in beiden Fällen eine Transaktion erzeugt wird, die in der Blockchain im nächsten Block integriert wird und als Rückgabewert eine Transaktionsnummer erzeugt wird. Der technische Unterschied besteht darin, dass

Vorteile, Nachteile und Lösungen:

Beim Senden von Coins oder Assets besteht der Vorteil in der einfachen Zuordnung zu den Wahloptionen und in der einfachen Verwaltung der Stimmrechte. Der Nachteil besteht darin, dass keine Verschlüsselung der Wahlentscheidungen möglich sind, wenn direkt Coins oder Assets an Kandidatenadressen gesendet werden o.ä.

Beim Speichern der Wahloption als Text oder Code wäre eine Verschlüsselung an sich kein Problem, jedoch würde ein Vorteil der Blockchain-Technologie, die leichte Überprüfbarkeit und Auswertbarkeit darunter leiden und die Funktion der einfachen Distribution von Stimmrechten[13] wegfallen.

Zwitter als Lösung? OP-Return

Verschlüsselung:

1. Asymmetrisches Verfahren: Wahlentscheidungen können nur mit amtlichen Secret Key entschlüsselt werden.
2. Der Client erzeugt mehrere Schlüsselpaare, um Fakes zu erzeugen?!
3. Die Fakes werden anhand des Public-Key aussortiert?!

[13] Bei der Verwendung von Assets z.b. könnten

[Skizze]

Übersicht von Online-Wahlsystemen

Kommerzielle Anbieter (konventionelles Online-Voting)

OPA-Vote: https://www.opavote.com/
(Proprietäre Software)

Polyas: http://www.polyas.de
(Proprietäre Software)

Simply Voting: http://www.simplyvoting.com/
(Proprietäre Software)

Öffentliche (staatliche) Anbieter

iVote (Australien, NSW): https://www.ivote.nsw.gov.au
(Proprietäre Software)

Non-Profit / Open Source / andere

4. Manipulation der Voting-DB (tally)

5. Literaturverzeichnis

Biryuk, Alex, Khovratovic, Dimitry und Pustogarov, Ivan. 2014.
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/portePP/pp0037b_pdf.html.

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

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

Garay, Juan A., Kiayias, Aggelos und Leonardos, Nikos. 2015. *The Bitcoin Backbone Protocol: Analysis and Applications.* 2015.

Goltzsch, Patrick. 2000. Wahlgeheimnis Software. [Online] 5. Juli 2000. [Zitat 2. September 2015.] http://www.heise.de/tp/artikel/8/8328/1.html.

Greenspan, Gideon. 2015. MultiChain Whitepaper. *MultiChain.* [Online] 23. 2015. [Zitat vom: 04. September 2015.] http://www.multichain.com/whitepaper.pdf.

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 November 2016.] http://www.arijuels.com/wp-content/uploads/2013/09/JCJ10.pdf. content/uploads/2013/09/JCJ10.pdf.

Mattke, Sascha. 2016. http://www.heise.de/newsticker. *Kapazitätsgrenze erreicht: erreicht: Bitcoin-Transaktionen in der Warteschlange.* [Online] 15. März 2016. [Zitat vom: vom: 10. Juni 2016.] http://www.heise.de/newsticker/meldung/Kapazitaetsgrenze-erreicht-Bitcoin-Transaktionen-in-der-Warteschlange-3132893.html.

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.

Ryan, Peter Y A und Teague, Vanessa. 2009. *Pretty Good Democracy.* Dept. Computer Science and Communications, University of Luxembourg; University of Melbourne. Luxembourg; Melbourne : s.n., 2009. Proposal.

Schweisgut, Jörn. 2007. Elektronische Wahlen unter dem Einsatz kryptografischer kryptografischer Observer. *Dissertation.* [Dokument]. Gießen, Deutschland : Fachbereich Fachbereich Mathematik und Informatik, Physik, Geographie. Justus-Liebig-Universität Universität Gießen, 2007.

Simmel, Georg. 1908. Das Geheimnis und die geheime Gesellschaft. *Soziologie - Untersuchungen über die Formen der Vergesellschaftung.* Berlin : Duncker & Humblot, 1908, S. 256-304.

Sriram, S. Samundeeswari and V.S. Shankar. 2013. NIZKP to Achieve Authentication in Ad-hoc Networks. *Research Journal of Information Technology.* 2013, 2013, Bd. 5, 3, S. 402-510.

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.

Volkamer, Melanie und Krimmer, Robert. 2006. *Overview Online-Wahlen.* 2006. 13.