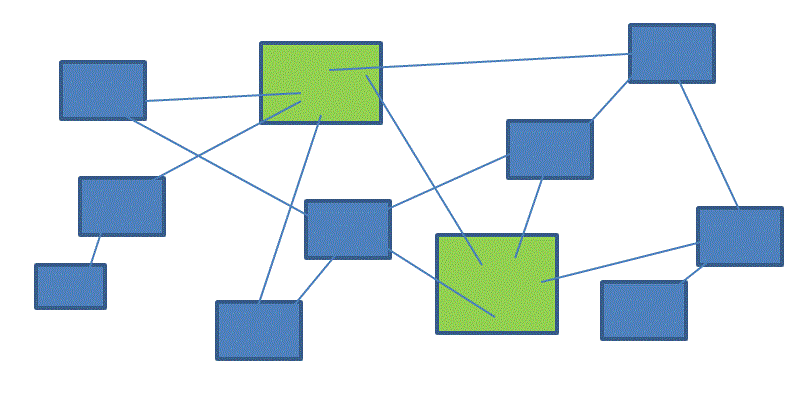
Blockchain Voting System

Whitepaper

Projektentwurf eines Systems zur Durchführung allgemeiner Wahlen über das Internet

Louis Göttertz

Version 1.0



[1. Abstract 4](#_Toc467153085)

[2. Einleitung 4](#_Toc467153086)

[3. Probleme der Sicherheit bei Online-Wahlsystemen 9](#_Toc467153087)

[Geheimhaltung 11](#_Toc467153088)

[Coercion resistance 11](#_Toc467153089)

[Anonymität 12](#_Toc467153090)

[Authentifizierung 12](#_Toc467153091)

[Verfügbarkeit Fehler! Textmarke nicht definiert.](#_Toc467153092)

[4. Bestandteile und Funktionen eines Wahlsystems zur Durchführung von Online-Wahlen 13](#_Toc467153093)

[Erweiterte Anforderungen 13](#_Toc467153094)

[Umsetzung 13](#_Toc467153095)

[Das Blockchain-Protokoll für eine Online-Wahl 13](#_Toc467153096)

[Notwendige funktionelle Abweichungen/Eigenschaften des Wahlsystems gegenüber dem Bitcoin-Protokoll: 15](#_Toc467153097)

[Netzwerk 16](#_Toc467153098)

[Daten-Model 16](#_Toc467153099)

[Wählerlisten 17](#_Toc467153100)

[Controller 18](#_Toc467153101)

[Project Controller 18](#_Toc467153102)

[Ballot Controller 18](#_Toc467153103)

[5. Entwicklung des Prototyps für ein blockchain-basiertes System zur Durchführung von Online-Wahlen 20](#_Toc467153104)

[Clients 23](#_Toc467153105)

[Multichain 24](#_Toc467153106)

[Hyperledger 25](#_Toc467153107)

[Vorläufige Architektur des Prototypen (Synthese, Fazit) 25](#_Toc467153108)

[Versiegelung der Wahl 25](#_Toc467153109)

[Versiegelung der Wahlentscheidungen beim Wahlclient 25](#_Toc467153110)

[Auswertung und Überprüfung der Wahl 26](#_Toc467153111)

[6. Ablauf einer Online-Wahl mit dem Prototypen 27](#_Toc467153112)

[7. Bisheriges Fazit 28](#_Toc467153113)

[8. Aussichten 28](#_Toc467153114)

[9. Anhang: 28](#_Toc467153115)

[Definitionen 28](#_Toc467153116)

[Verschlüsselung: 28](#_Toc467153117)

[Hash-Verfahren: 28](#_Toc467153118)

[(Schweisgut, 2007 S. 9) 28](#_Toc467153119)

[Glossar 28](#_Toc467153120)

[Übersicht von Online-Wahlsystemen 29](#_Toc467153121)

[Kommerzielle Anbieter (konventionelles Online-Voting) 29](#_Toc467153122)

[Öffentliche (staatliche) Anbieter 29](#_Toc467153123)

[Non-Profit / Open Source / andere 29](#_Toc467153124)

[Übersicht der Angriffsszenarien bei Online-Wahl-Systemen 30](#_Toc467153125)

[Fallstudien 30](#_Toc467153126)

[10. Literaturverzeichnis 31](#_Toc467153127)

# Abstract

# 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]](#footnote-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]](#footnote-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:

1. Server können sehr leicht fehlerhaft implementiert werden,
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]](#footnote-3), Estland[[4]](#footnote-4) und Australien[[5]](#footnote-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]](#footnote-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 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]](#footnote-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 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 Stimme wie beabsichtigt zugeordnet? Wurde meine Stimme gezählt wie zugeordnet und werden alle Stimmen gezählt?[[8]](#footnote-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]](#footnote-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 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.

# 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 schreiben 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 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, Smartphones und andere Geräte, die als Endgeräte für Internetwahlen infrage kommen, anfällig für allerlei Gefahren: Viren, Trojaner etc. sind, was dazu 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 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]](#footnote-10): Die Gefahr, dass Stimmen gekauft oder erpresst werden, lässt sich nur verhindern, wenn eine Wählerin nicht die 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, 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.

## 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 möglich, anhand eines Zeitabgleiches und der IP-Nummer des Wählers eine Zuordnung zwischen Wahlentscheidung und Wähler herzustellen[[11]](#footnote-11), wenn keine zusätzlichen Tools zur Anonymisierung entwickelt werden (Proxy-Server, 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.

# 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 Apps auf Android oder iOS) und zu bedienen sein und möglichst auf vielen Endgeräten (Smartphone, PC, TV etc.) funktionieren. Die Ergebnisse müssen transparent errechnet und einfach mit unabhängiger Software überprüfbar sein. Das System muss außerdem flexible Wahlmöglichkeiten und Layouts für Stimmzettel ermöglichen. Darüber hinaus sollten verschiedene Scoring-Protokolle[[12]](#footnote-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?

### 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]](#footnote-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?!

[Skizze]

Möglichkeit „Assets“ zu erzeugen statt nur Coins zu minen.

Kontrolle über die Blockchain: Rechteverwaltung: Zugang, Issue, Senden, Empfangen

Steigerung der Performance für heiße Wahlperiode

Bei einem Peer-to-Peer-System (P2P) sind alle Clients theoretisch gleichberechtigt und stellen Dienste zur Verfügung, bzw. nehmen diese in Anspruch (Client-Server-Funktionalität). Ein P2P-System ist selbstorganisierend, d.h. niemand hat als zentrale Instanz die Kontrolle über die Clients. Als Overlay-Netzwerk über dem Internet ist es einerseits billig zu implementieren, andererseits können –wenn gewünscht– eigene Formen der Kontrolle (Routing, Zugang etc.) verwirklicht werden. Da es keine zentrale Instanz gibt, gibt es auch keinen zentralen Angriffspunkt, um Manipulationen an einem Server vorzunehmen (das heißt aber nicht, dass Angriffe auf das Gesamtsystem nicht möglich sind).

Das Peer-To-Peer-Netzwerk deshalb ist die entscheidende Voraussetzung für den Betrieb der Wahlclients. Der Stabilität und Sicherheit des Protokolls für das Overlay-Netzwerk wird daher im Verlaufe dieses Dokuments besondere Aufmerksamkeit gewidmet sein.

## Daten-Model

### Wählerlisten

Das besondere Problem ist die Anonymisierung des Wahlvorganges bei gleichzeitig sicherer Authentifizierung der Wähler, d.h. Prüfung der Wahlberechtigung. Aus der Wählerliste mit den Klardaten muss eine Liste anonymer Wähleradressen werden, die garantiert, dass zwar nur die Berechtigten ihre Stimme abgeben können, aber ohne dass die Wahlentscheidung auf die konkrete Person zurückgeführt werden kann.

Assets

BVS-Adressen

Wählerliste

Die Erzeugung und Verwaltung der Wählerlisten ist unabhängig von dem eigentlichen BV-System.

Dem Wähler muss dazu zur Authentifizierung bei der Stimmabgabe ein geheimes „Token“ zur Verfügung gestellt werden, welches nur er kennt. Dazu könnte ein Hash-Verfahren genutzt werden, bei dem aus der Wählerliste zuerst individuelle und geheime [Schlüssel] generiert werden, aus denen Hashes erstellt werden, die auf einem Autorisierungsserver gespeichert werden, der letztendlich für die späteren Authentifizierungszwecke genutzt werden kann. Die Schlüssel werden den Wählern wie PINs bei einer Bankkarte verdeckt übermittelt und nicht gespeichert, sondern nach Druck sofort aus dem Speicher gelöscht.

Die Anwendung für die Wahlvorbereitungsphase muss daher zumindest aus drei unabhängigen Serversystemen bestehen: eines für die Wählerlisten der Onlinewähler, ein zweites hochgesichertes System für die Erzeugung der Schlüssel und Hashes und ein drittes System in dem die Hashes für die Online-Authentifizierungszwecke gespeichert werden. Die ersten beiden Systeme müssen unbedingt unabhängig voneinander (technisch und organisatorisch) betrieben werden.

Das zweite System, welches für die Generierung der Hashes zuständig ist, sollte aus Sicherheitsgründen nicht vernetzt sein, sondern nur einmal eine verschlüsselte Wählerliste über einen Datenträger erhalten. Für alle Systeme gilt: Es sollte sich um geprüfte OpenSource-Software handeln, um ein größtmögliches Vertrauen in die Vorgänge zu ermöglichen. Betriebssysteme und Software sollten möglichst als unveränderliche Live-Betriebssysteme betrieben werden, um nachträgliche Manipulationen auszuschließen. Alle Installations- und Wartungsvorgänge sollten unter öffentlicher Kontrolle (Anwesenheit unabhängiger Experten, Kameraaufzeichnung etc.) stattfinden.

Projekt

Ballot

Option

## Controller

### Project Controller

Bei der *Wahlvorbereitung* stehen das Wahlprojekt, Wählerlisten und Kandidaten oder Gesetzentwürfe im Mittelpunkt.

Entschlüsseln der Wählertransaktionen

Ergebnis der Verschlüsselung in Blockchain eintragen (Re-broadcast a transaction).

### Ballot Controller

Bei der *Wahldurchführung* steht die **Stimmabgabe** als zentrale Funktion im Mittelpunkt. „Sie erfolgt aus der Ferne, über ein offenes Netzwerk und von einem Endgerät, das in der Lage ist, den gesamten Inhalt des Stimmzettels darzustellen und die Vorgaben des Wahlveranstalters für die Art der Darstellung, insb. die Reihenfolge der Wahlvorschläge, umzusetzen.“ [[14]](#footnote-14) Als Komponenten werden ein sicheres **Netzwerk-Protokoll** und **Wahlclients** benötigt. Da eine Bedingung für ordnungsgemäße politische Wahlen darin besteht, dass keine Zwischenergebnisse publik werden dürfen, muss die Wahlentscheidung zunächst in irgendeiner Form zurückgehalten werden. Die vorläufige Lösung dieses Problems besteht darin, dass die Stimmabgabe zunächst **verschlüsselt** (Öffentlicher Schlüssel des Wahlamtes) dokumentiert wird und dies als Message in einer Transaktion in die Blockchain übernommen wird. Erst nach Ende der Stimmabgabeperiode, werden schließlich diese Skripte mit dem privaten Schlüssel entschlüsselt und in Form von Transaktionen den jeweiligen Wahloptionen, d.h. Kandidaten oder Listen zugeordnet.

Schließlich stehen die Stimmenauszählung und die Veröffentlichung der Wahlergebnisse als letzte Phase einer Wahl im Mittelpunkt. Als weitere Komponenten werden also eine **Software zur Auszählung** der Stimmen und ein **System zur Veröffentlichung** der Wahlergebnisse gebraucht.

# Entwicklung des Prototyps für ein blockchain-basiertes System zur Durchführung von Online-Wahlen

Aus der im vorigen Kapitel erfolgten Beschreibung der notwendigen Komponenten und Funktionen ergibt sich der Ansatz für die weitere Softwareentwicklung gemäß dem Paradigma des „Domain-Driven-Designs“[[15]](#footnote-15), welches im Folgenden zur Modellierung herangezogen wird. Die Skizze auf der folgenden Seite zeigt die eben erwähnten Komponenten in einer schematischen Darstellung.

Stimmen/Assets

Online-Wähler

Cold-Wallet

Wallet-Knoten mit Stimmen (Assets)

Online-Wähler

Wähler | Anon. Accounts

Anon. Accounts

Wähler / Wallet / Client

Entschlüsselung der Wahlentscheidung;   
Ausführung der Skripte:   
Transaktion von Cold Wallet zu Kandidaten/Listen-Wallets

Zählen der Inputs in der Blockchain

Figure 1: Erstes Arbeitsmodell

Anon. Zugangsdaten  
per Post (verdeckt)  
Per Email  
(verschlüsselt)

VergleichHashes

Wahlentscheidung   
Skript mit Endadresse verschlüsselt1

**Auszählung**

**Stimmabgabe**

**Stimmrechte**

User Hash

PIN/Passwort

+ Adresse

**Modell-Entwurf**

**Auszählung**

Wie schon erwähnt, löst die Adaption der Bitcoin-Technologie das Problem der Sicherstellung von Anonymität bei gleichzeitiger sicherer Authentifizierung nicht ausreichend, da a) die Technologie nicht ausreicht, um alle Vorgänge abzubilden, die für die Organisation und Durchführung einer Wahl notwendig sind (Online-Wahl-Registrierung, Führung von Wählerlisten, damit die Wähler aus den Verzeichnissen für die Wahllokalen gestrichen werden, Autorisierung etc.); und b) gibt es Probleme, die die Transparenz und Kapazität eines blockchain-basierten Systems betreffen, wie am Beispiel Bitcoin deutlich geworden ist.[[16]](#footnote-16)

Nachdem trotz dieser Herausforderungen die Entscheidung gefallen ist, ein neues Online-Voting-System auf der Basis der Blockchain-Technologie zu entwickeln, müssen die spezifischen Eigenschaften verschiedener bis jetzt vorhandener Blockchain-Implementationen miteinander verglichen, um hinsichtlich ihrer Eignung für ein Online-Wahl-System beurteilt zu werden. Zunächst werden die *allgemeinen* Eigenschaften und Probleme einer Blockchain-Anwendung anhand der digitalen Währung „Bitcoin“ untersucht. Danach werden verschiedene Weiterentwicklungen der Blockchain bzw. Bitcoin-Forks auf ihre Eignung für ein Online-Wahlsystem in ihrem Anpassungsbedarf bzw. –aufwand analysiert. Die Kandidaten sind

1. Etherium[[17]](#footnote-17),
2. Multichain i.V.m. Open Assets (Bitcoin-Fork)[[18]](#footnote-18) und
3. Hyperledger[[19]](#footnote-19) –Fabric (Hyperledger ist eine Open Source Initiative unter Führung von IBM, die das Ziel hat, die Standardisierung im Bereich Blockchain-Technologie (Protokolle, APIs) voranzutreiben mit verschiedenen Projekten zur Implementation.

## Clients

Bei der Entwicklung von Clients für den eigentlichen Wahlvorgang gibt es theoretisch viele Möglichkeiten. Ein Teil der bisherigen Systeme setzt auf eine Browser-basierte Lösung, bei der die Wähler keine zusätzliche Software auf ihren Computern oder mobilen Endgeräten installieren müssen. Der große Vorteil dabei ist, die geringe Einstiegshürde: Ein Browser ist auf nahezu jedem internetfähigen Endgerät schon installiert und nahe jeder Internetnutzer kennt sich mir der Bedienung ausreichend aus. Bei der Verwendung einer Blockchain ist es zwar auch möglich eine browserbasierte Anwendung bereitzustellen, die die Aufgabe der Generierung der Transaktionen über einen rpc-Server an den eigentlichen Blockchain-Node weiterreicht (analog zu Online-Wallets), der große Vorteil der Blockchain als dezentrale, verteilte Anwendung, die eine gewisse Robustheit gegen Angriffe besitzt, würde dadurch jedoch konterkariert. Eine browser-basierte Anwendung wäre auf jeden Fall nur eine Notlösung.

Eine browser-unabhängige Lösung, bedingt eine eigene Applikation, die jedoch den Nachteil hat, dass sie verteilt und auf einem Endgerät eines jeden Wählers installiert werden muss (Deployment). Außerdem erfordert die Vielfalt an unterschiedlichen Endgeräten, dass wahrscheinlich mehrere Versionen für verschiedene Endgeräteklassen erstellt und anschließend gepflegt werden müssen. Auch wenn es Möglichkeiten gibt, den Kern der Software betriebssystemübergreifend zu programmieren, ist das ein hoher zusätzlicher Aufwand gegenüber einer browser-basierten Lösung.

Die Hauptfunktion einer solchen Anwendung ist die Stimmvergabe. Dabei muss die Benutzeroberfläche zum Wählen dem offiziellen Wahlzettel entsprechen und einfachen Zugang zu allen nötigen Informationen bieten. Eine GUI-Anwendung ist also Pflicht.

Der Client muss mindestens die Fähigkeiten haben

1. zur funktionelle Darstellung des Stimmzettels;
2. zur Registrierung einer Adresse, um Stimmen bzw. Assets zu empfangen;
3. zum Versenden von Wahlentscheidungen bzw. Assets verschlüsselt als TX-Message,

um die nötige Funktionalität, Sicherheit und Vertraulichkeit für die Stimmabgabe zu gewährleisten.

## Multichain

(http://www.multichain.com/developers/)

Multichain ist ein Fork des originalen Bitcoin-Clients. Multichain ist ein Ableger von Bitcoin, das durch die zusätzlichen Möglichkeiten der Rechtevergabe und von sogenannten „Assets“ zunächst als Basis für das Blockchain-Voting-System ausgewählt wurde. Native asset transactions (use OP\_DROP and OP\_RETURN metadata).

Die Möglichkeit der Rechtevergabe für die Blockchain besteht in der Kontrolle darüber, welche Teilnehmer sich verbinden, „minen“, Coins und Assets senden und/oder empfangen dürfen. Für Wahlprojekte z.B. erscheint es sinnvoll, das minen derart zu beschränken, dass niemand plötzlich aufgrund seiner Rechenleistung, das Netzwerk dominieren kann, oder Clients, die das Netzwerk mit unsinnigen Requests stören, auszuschließen. Permissions management transactions (use OP\_DROP metadata in transaction outputs). Extensions to the raw transactions APIs to support MultiChain-specific metadata and more.

The format of addresses which differs slightly from bitcoin’s scheme. Mining and block signatures (use OP\_RETURN in coinbase transaction).

Additional runtime parameters that can be used on the command line or in a node’s per-chain config file.

Das Multichain-Projekt befindet sich zurzeit noch in einer frühen Entwicklungsphase, so dass es bisher nur Clients für Linux-Systeme gibt. Der Client braucht keine aufwendige Konfiguration und Installation. Eine neue Blockchain für ein neues Projekt wird eingerichtet und gestartet mit:

Extended peer-to-peer handshaking to include node identification.

multichain-util create Beispielwahl

multichaind Beispielwahl -daemon

Andere Knoten (d.h. Clients) können sich dann mit dem Blockchain@Knoten verbinden und so zum Teilnehmer (Node) des Netzwerks werden:

multichaind Beispielwahl@[ip-address]:[port]

Eine zweite Möglichkeit bestünde darin, dass die Wähler anonym eine Wallet-Adresse registrieren, so dass die Stimm-Assets an die Wähler transferiert werden können. Dies würde aber einen weiter erhöhten Aufwand bedeuten, um die Identität der Wähler zu schützen.

## Hyperledger

## Vorläufige Architektur des Prototypen (Synthese, Fazit)

Konzentration auf die neu zu entwickelnden Komponenten …

### Versiegelung der Wahl

(Kandidatenliste, Wahlgesetz etc)

### Versiegelung der Wahlentscheidungen beim Wahlclient

Normale OP-Return-Messages im Bitcoin-Protokoll

Beim Versiegeln des Stimmzettels werden alle relevanten Daten aus der Datenbank in ein JSON-Dokument geschrieben. Die Signatur dieses Dokumentes wird in der Blockchain gespeichert. Wahlclients können später überprüfen, ob der Stimmzettel echt ist.

### Auswertung und Überprüfung der Wahl

# Ablauf einer Online-Wahl mit dem Prototypen

Wahl Vorbereitungen

1. Sichere BVS-Clients sind in den offiziellen App-Shops (Google Play, Apple und Windows, sowie Linux-Repositories) verfügbar.
2. Öffentlichkeitsarbeit für Online-Wahl beginnt.
3. BVS-Netz und Blockchain wird gestartet: Client-Adressen für Kandidaten und Parteilisten werden erstellt und in die Online-Stimmzettel etc. eingepflegt.
4. Online-Stimmzettel wird versiegelt
5. Wahlbenachrichtigungen werden verschickt: Antrag auf Online-Wahl zusätzliche Alternative zur Briefwahl: Zur Verhinderungserklärung muss nur eine Wallet-Adresse, die vom BVS-Client generiert wird, zurückgeschickt werden. Das könnte auch auf alternativem Weg geschehen, das einfachste wäre aber auf der Rückseite der Wahlbenachrichtigung.
6. Stimmzettel mit QR-Code werden an die Online-Wähler verschickt. Die anderen bekommen normale Briefwahlunterlagen.
7. Die „Stimmen“ (bzw. digitalen Stimmrechte) werden kurz vor Beginn des Wahlzeitraums an die Online-Wähler „verschickt“, so dass sie in den BVS-Clients zur Stimmabgabe nutzbar sind.
8. Die Online-Wähler können dann mit diesen digitalen Stimmrechten wählen, in dem die QR-Codes mit dem BVS-Client gescannt werden (vom Stimmzettel oder einer sicheren Online-Quelle).

# Bisheriges Fazit

# Aussichten

# Anhang:

## Definitionen

## Verschlüsselung:

## Hash-Verfahren:

## (Schweisgut, 2007 S. 9)

## Glossar

coercion-resistance - erpressungsresistent

End-to-End (E2E) Voter-Verifiability

mix networks

receipt-freeness

Roster - Dienstplan

Secure Printing: In paper-based E2E elections, ballots are printed by a trusted entity. We consider the problem of how to print a human-readable message or image on a piece of paper, without the printing agents or devices learning its contents. We examine the problem in two settings: with a trusted dealer who knows the secret and with a two- party protocol that allows two non-colluding printers to obliviously generate the secret and print it while never learning it. The protocols allow the printers to print a randomly selected element from a set or a random permutation of elements in a set. When the elements are alphanumeric strings, we oﬀer an optimization for representing them. By obliviously printing codes or shuﬄed lists of candidates, these protocols could form the basis for eliminating the trusted printer in paper-based E2E election systems like Prêt à Voter, Punchscan, and Scantegrity. (Clark, 2011 S. 5)

## 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

## Übersicht der Angriffsszenarien bei Online-Wahl-Systemen

1. Manipulation der Voting-DB (tally)

## Fallstudien

# Literaturverzeichnis

**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.

**Decker, Christian und Wattenhofer, Roger. 2013.** *Information Propagation in the 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 vom: 2. September 2015.] http://www.heise.de/tp/artikel/8/8328/1.html.

**Greenspan, Gideon. 2015.** MultiChain Whitepaper. *MultiChain.* [Online] 23. August 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 2016.] http://www.arijuels.com/wp-content/uploads/2013/09/JCJ10.pdf.

**Mattke, Sascha. 2016.** http://www.heise.de/newsticker. *Kapazitätsgrenze erreicht: Bitcoin-Transaktionen in der Warteschlange.* [Online] 15. März 2016. [Zitat 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 Observer. *Dissertation.* [Dokument]. Gießen, Deutschland : Fachbereich Mathematik und Informatik, Physik, Geographie. Justus-Liebig-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, 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. S. 13.

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 [↑](#footnote-ref-1)
2. Siehe den Angriff auf die Bundestags-IT im Mai 2015, der bis heute (Anfang September) nicht abgewehrt werden konnte. [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)
4. Siehe: Independent Report on E-voting in Estonia: <https://estoniaevoting.org/>, zuletzt abgerufen am 11.06.2016. [↑](#footnote-ref-4)
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 [↑](#footnote-ref-5)
6. Eine reichhaltige Linksammlung zur Kritik an Online-Wahlen findet man unter: <http://papierwahl.at>. [↑](#footnote-ref-6)
7. (International Telecommunication Union (ITU), 2015) [↑](#footnote-ref-7)
8. Vergl.: End-to-End (E2E) Voter-Verifiability (Halderman, 2015)., (Clark, 2011) [↑](#footnote-ref-8)
9. Das Bitcoin-Netzwerk funktioniert seit 2009 ohne größere Probleme und Sicherheitslücken. [↑](#footnote-ref-9)
10. (Bundeamt für Sicherheit in der Informationstechnik (BSI), 2008 S. 26) [↑](#footnote-ref-10)
11. (Biryuk, et al., 2014) [↑](#footnote-ref-11)
12. Verschiedene Wahlsysteme gestatten es z.B. eine Rangfolge zwischen Kandidaten festzulegen oder mehrere Stimmen zu verteilen. [↑](#footnote-ref-12)
13. Bei der Verwendung von Assets z.b. könnten [↑](#footnote-ref-13)
14. Bundeamt für Sicherheit in der Informationstechnik (BSI), 2008 [↑](#footnote-ref-14)
15. Domain-driven Design (DDD) ist eine Herangehensweise an die Modellierung komplexer objektorientierter Software. (Quelle Wikipedia: Domain-Driven-Design, URL: <https://de.wikipedia.org/wiki/Domain-driven_Design>, zuletzt abgerufen am 10.06.2016 [↑](#footnote-ref-15)
16. Z.Z beträgt die Kapazitätsgrenze etwa 7 Transaktionen pro Sekunde, vgl.: Mattke, 2016 [↑](#footnote-ref-16)
17. Siehe: <https://www.ethereum.org/> [↑](#footnote-ref-17)
18. Siehe: <http://www.multichain.com> [↑](#footnote-ref-18)
19. Siehe: <http://www.hyperledger.org> [↑](#footnote-ref-19)