Anwendungsmöglichkeit der Blockchain-Technologie für Bundestagswahlen

Tobias Perenthaler, Arne Schloßmacher und Sebastian Windeck

Technische Universität Dresden, Fakultät Wirtschaftswissenschaften, Lehrstuhl für Wirtschaftsinformatik insbes. Informationsmanagement, Dresden, Deutschland
{tobias_horst_amadeus.perenthaler, arne.schlossmacher, sebastian.windeck}@mailbox.tu-dresden.de

Abstract. Geringe Wahlbeteiligung von jungen Wählenden und Beeinflussbarkeit der Ergebnisse sind aktuelle Herausforderungen, die über die Politik eines Landes entscheiden. Hierfür wird die Implementierung von Blockchain-Technologien als einen netzwerkbasierten, demokratischen Ansatz für eine elektronische Bundestagswahl diskutiert. Anhand eines Design-Science-Ansatzes wurden in mehreren Literaturrecherchezyklen ein Kriterienkatalog mit rechtlichen, fachspezifischen und akzeptanzrelevanten Anforderungen erstellt sowie technische Systemarchitekturen analysiert. Das Ergebnis dient als Basis eines prozeduralen und strukturellen *Votechain*-Modells für die Bundestagswahlen. Dieses Artefakt wurde anhand des Kriterienkataloges evaluiert und zeigt Handlungsempfehlungen auf. Diese Studie kommt zu dem Ergebnis, dass die Blockchain-Technologie als Grundlage für ein dezentrales elektronisches Wahlsystem erhebliches Potential für eine demokratische Wahl bietet.

Keywords: Blockchain, Bundestagswahl, Design Science, verteilte Systeme, internetbasierte Wahlen

1 Einleitung

Trotz Digitalisierung wurde bei der Bundestagswahl 2017 mit Wahlzetteln aus Papier gewählt (Urnenwahl). Es herrscht ein latentes Unsicherheitsgefühl sowie geringes Vertrauen in IT-Systeme, die ein Szenario der elektronischen Stimmabgabe unwahrscheinlicher machen. Laut Forsa-Umfrage hätten bei der Wahl 2013 51% der Befragten ihre Stimme per Internet abgegeben [1]. Hieraus leitet sich die Bedeutung der näheren Betrachtung elektronischer Wahlsysteme ab.

Die Blockchain-Technologie (kurz: Blockchain), eine dezentrale Systemarchitektur und deren mögliche Anwendungsbereiche in Wissenschaft und Praxis werden momentan intensiv untersucht [2, 3]. Einen möglichen Bereich stellen elektronische Wahlsysteme dar. Diese werden in der Literatur sowohl als zentrale als auch als dezentrale Systeme diskutiert. Die Schwächen zentraler Systeme fördern die Bedenken der Wählenden und können durch den Einsatz der dezentralen Blockchain überwunden werden.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Als Zielsetzung der Arbeit werden die Themengebiete Blockchain und Bundestagswahl nach dem Modell der Design Science untersucht. Abbildung 1 stellt die Forschungsfragen im Kontext der Anwendung der Blockchain in Wahlsystemen dar. Basierend auf der Literaturrecherche, werden Potentiale und Risiken elektronischer Wahlsysteme zusammengefasst und die Forschungsfragen in deren Mittelpunkt gesetzt.

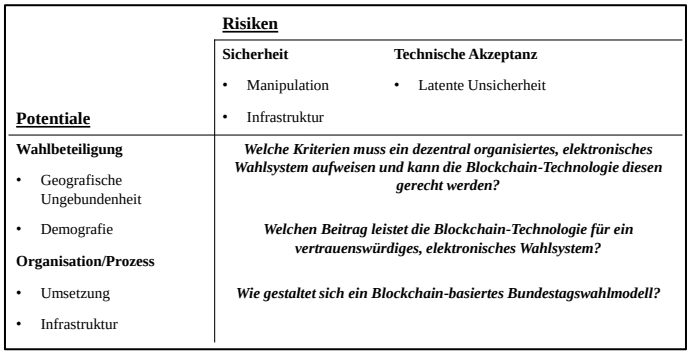

Abbildung 1. Motivation und Forschungsfragen [4–8]

Als Ergebnis der Forschung stellte sich das Potential der Blockchain für die Anwendung bei demokratischen Wahlen heraus. Die Anforderungen des Kriterienkatalogs an das entwickelte Artefakt sind nahezu vollständig erfüllt. Zusätzlich ergeben sich neue Forschungsfelder im Bereich der technischen Umsetzung und Akzeptanz.

2 Methodik

Methodische Grundlage des Forschungsvorhabens war Design Science. Als konstruktionswissenschaftliches Forschungsparadigma eignet sich diese Forschungsmethode zur Entwicklung von Modellen mit praktischem Fokus [9]. Mit Hilfe einer systematischen Literaturanalyse wurden Rigorosität und Relevanz untersucht. Ergebnis der Arbeit ist das *Votechain* Artefakt, das mit dem Kriterienkatalog evaluiert wird [10]. Dieser bezieht sich dabei auf die erste Forschungsfrage.

Die Analyse des Anwendungsszenarios Bundestagswahl orientiert sich am Bundeswahlgesetz [11] und der Bundeswahlordnung [12]. Die folgende Abbildung gibt eine Übersicht der nach den Regularien unterteilten Schritte.

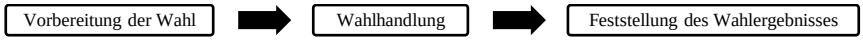

Abbildung 2. Ausschnitt des Prozessablaufs der Bundestagswahl

Jeweilige Akteure dieser Prozessschritte sind Bundes-, Landes- sowie Kreiswahlleiter und Kreisausschuss, amtliche Druckerei, Wahlvorstand und Gemeindebehörden. Aktuell ist der Prozess Feststellung des Wahlergebnisses Software-unterstützt. Mit Hilfe einer Modelliersprache wurden die Prozesse formalsprachlich dargestellt (BPMN 2.0 Modell der Bundestagswahl). Die Kreiswahlleiter melden mit Hilfe der Software

PC-Wahl, die ein erhebliches Risiko durch Hackerangriffe birgt, die Ergebnisse an die Landeswahlleiter [4].

Neben den gesetzlichen Bestimmungen liegt ein zweiter Fokus auf E-Wahlsystemen, die mittels elektronischer Hilfsmittel eine Stimmabgabe und deren Übertragung per Internet ermöglichen. Dadurch ist der Wählende weder zeitlich noch lokal an die Beschränkung der Urnenwahl gebunden und benötigt lediglich eine Internetverbindung und seine persönliche Authentifikation [13].

In Form eines Kriterienkataloges werden Eigenschaften, die ein E-Wahlsystem erfüllen muss, aggregiert dargestellt. Ein Änderungsvorschlag muss den Status Quo des bestehenden Systems beibehalten und mindestens einen Aspekt verbessern. Dementsprechend werden neben den Grundsätzen im Bundeswahlgesetz weitere Aspekte als Kriterien einbezogen. Tabelle 1 fasst die Kriterien zur Bewertung von E-Wahlsystemen, ihre Bedeutung und Quellen zusammen.

Insbesondere Sicherheitsaspekte werden berücksichtigt, um dem latenten Unsicherheitsgefühl der Nutzer eines solchen Systems entgegenzuwirken. Zusätzlich werden Standards zur Evaluierung der technischen Akzeptanz (TAM-Modell) hinzugezogen [14]. Hierbei ist das Input-Modell nach Huijts et. al [15] am besten geeignet, da die Veränderung einseitig und die Größe der Auswirkungen ähnlich eines grundlegenden Technologiewandels ist. Abschließend wird der entstandene Kriterienkatalog mit bestehenden Kriterienkatalogen zu IT-Sicherheit oder Wahlen verglichen. Dieser Kriterienkatalog soll im weiteren Verlauf der Arbeit dazu dienen, das entwickelte Wahlsystem zu evaluieren.

3 Systemarchitekturen für E-Wahlsysteme

Die Topologie von Rechnernetzen lässt sich grundsätzlich in zentrale (sternförmige) und dezentrale bzw. verteilte (vermaschte) Strukturen (hier Blockchain) untergliedern. Die verschiedenen Systeme haben aufgrund ihrer Datenhaltung und Transaktionsabwicklung Vor- und Nachteile und werden häufig verglichen [16, 17]. Die wesentlichen funktionalen Merkmale lassen sich in vier Kategorien unterteilen: *Vertraulichkeit, Robustheit, Leistungsgeschwindigkeit* und *Sicherheit* [18]. Technische Unterschiede der Netzwerkprotokolle und Architekturen werden hierbei nicht betrachtet.

Zentrale Systeme bieten eine *vertrauliche* digitale Architektur, weil jede Transaktion zwischen einem Client und dem Server stattfindet. Probleme der Server können wiederum zum Gesamtausfall führen. Die Leistungsgeschwindigkeit dieser Transaktionen bietet einen Effizienzvorteil. Hier ist nur die Authentifizierung des Clients zum Server notwendig. Kein weiterer Client erhält Einblick in die Transaktion [19]. In Bezug auf die Sicherheit, ist nur ein Zugriff auf die zentrale Administration notwendig, um die Daten zu fälschen.

Bei einer *dezentralen* Authentifizierung mit Blockchain ist jegliche Transaktion in allen Knoten zugänglich. Des Weiteren müssen Transaktionen von Prüfern authentifiziert, geprüft und der Blockchain angehangen werden. Dieser Prozess ist wesentlich aufwendiger und erfordert mehr Rechenkapazität und Zeit. Die Leistung eines

Tabelle 1. Kriterienkatalog zur Evaluierung des Artefakts

Kriterium	**Bedeutung**
Rechtliche Aspekte	
Allgemein [22]	Niemand darf aus politischen, wirtschaftlichen oder sozialen Gründen von der Wahl ausgeschlossen werden.
Unmittelbar [22]	Stimmen werden direkt auf die Abgeordnetensitze ohne Wahlmänner oder Ähnliches zugeteilt.
Frei [22]	Stimmabgabe erfolgt unbeeinflusst und darf zu keiner Benachteiligung führen.
Gleich [22]	Alle Wahlberechtigten haben dieselbe Stimmanzahl, die wiederum das gleiche Gewicht haben. Die Fünf-Prozent-Klausel ist hierbei eine Ausnahme.
Geheim [22]	Es darf nicht feststellbar sein, wie eine Person gewählt hat.
Wahlpropaganda [11]	§32 beinhaltet unzulässige Wahlpropaganda und Unterschriften sowie die unzulässige Veröffentlichung von Wählerbefragungen bzw. Wahlergebnissen.
Veröffentlichung von Wählerbefragungen [11]	Wählerbefragungen bzw. Wahlergebnissen beinhaltende Veröffentlichungen sind unzulässig.
Authentizität (ISO 15489)	Die Klassifikation der abgegebenen Stimme als Original ist essentiell für den gesamten Wahlprozess und bildet die technische Grundlage der Demokratie.
Fachspezifische Aspekte	
Verfügbarkeit [23]	Die Verfügbarkeit des Wahlsystems muss über die gesamte Wahlperiode gewährleistet sein.
Integrität [23]	Das Gesamtsystem muss integer sein, so dass die Manipulation von Stimmen während des Wahlvorgangs unmöglich ist.
Individuelle Nachprüfbarkeit [23]	Der Wählende muss nach Abschluss der Wahl die Möglichkeit haben zu prüfen, ob seine individuelle Stimme mitgezählt wurde. Zusätzlich soll jeder in der Lage sein, universell nachzuprüfen, ob alle Stimmen mitgezählt wurden.
Universelle Nachprüfbarkeit [23]	
Legitimation [24]	Nur rechtlich legitime Wählende dürfen eine genau definierte Anzahl an Stimmen abgeben.
Belegfrei [24]	Nach Abgabe der Stimme darf keine Quittung, die Auskunft über die Stimmabgabe gibt, erstellt werden, da diese möglichen Beeinflussern Informationen über die Wahl der jeweiligen Person geben würde.
Beeinflussungsresistent [25]	Das Wählen muss trotz Beeinflussung frei möglich sein. Selbst wenn ein Wählender beeinflusst wird, muss er dazu in der Lage sein, seine Stimme frei abzugeben
Vertraulichkeit [26]	Informationen sind vor unautorisierten Zugriffen zu schützen.
Anwenderbezogene Aspekte	
Benutzerfreundlichkeit[27, 28]	Anhand externer Variablen und dem Einfluss der Benutzerfreundlichkeit und dem direkten Nutzen eines Systems entsteht die Haltung und Absicht des Nutzers zu einem System.
Direkter Nutzen [27, 28]	
Haltung [29]	Vier Hauptkriterien zur technologischen Akzeptanz mit den jeweils „subjektiven“ Konstrukten zur Wahrnehmung des Akzeptanzobjektes.
Wahrgenommene, individuelle Verhaltenskontrolle [29]	
Persönliche Normen [29]	
Soziale Normen [29]	

Blockchain-Systems ist geringer und erzeugt eine Pseudoanonymität, die nur bedingt vertraulich ist [20]. Dezentrale Systeme mit verteilter Datenhaltung und Transaktionskontrolle wie bei Blockchain erzeugen eine sicherere und robuste digitale Umgebung, weil kein isolierter Angriffspunkt existiert [21]. Hierfür sichern die Knoten des Netzwerks das Protokoll der Blockchain, in dem alle Blöcke miteinander verbunden sind. Die Analogie dazu ist ein digitales Logbuch, das als identische Kopie auf Knoten dezentral gespeichert wird. Daher ist es nicht möglich, Transaktionen nachträglich zu manipulieren. Für die Validierung eines Blockes wird eine Gültig-keitsprüfung von Inhalt, Form und Struktur sowie einen Zeitstempel genutzt und dieser mit allen vorigen Blöcken verknüpft [30]. Diese Validierung ist sicher, weil sie im Peer-to-peer-Verfahren ohne dritte Partei funktioniert [31]. Prüfer prüfen einen Block, Validierer verteilen und sichern diesen nach dem Konsensprinzip im System. Für ein System ohne Vertrauen in alle Parteien ist Blockchain eine Lösung, weil ein digitaler Konsens des gesamten Netzwerkes durch übereinstimmende Blöcke getroffen wird und einzelnen Server- bzw. Knotenausfällen standhalten kann. Für den weiteren Aufbau der Arbeit ist die Unterscheidung der Akteure und deren Aufgaben für eine Blockchain relevant, um die Analogie für das Wahlmodell aufzubauen.

- **Prüfer:** Validieren und authentifizieren Transaktionen und ketten diese in Blöcken an die Blockchain.
- **Validierer:** Validieren Transaktionen der Benutzer und verteilen diese im Netzwerk
- **Benutzer:** Senden und empfangen von Transaktionen
- **Wallet:** Repräsentieren digitale Identität des Benutzers [32, 33]

4 Votechain: Blockchain-basiertes Bundestagswahlmodell

Die Blockchain mit dezentraler Verifizierung und Authentifizierung der Transaktionen bietet unter der Annahme eines Systems ohne vollständiges Vertrauen die Grundlage für ein digitales Wahlsystem. Zur formalsprachlichen Darstellung des Artefakts wurde ein BPMN 2.0 Modell genutzt. Entgegen eines zentralen Systems wird dieses nicht vom Staat zentral geführt, sondern von den Bürgern, die sich digital an der Wahl beteiligen. Hierfür wurde von einer geschlossenen, öffentlichen Blockchain ausgegangen, in der nur autorisierte Wahlbeteiligte WALLETs nutzen dürfen. Durch die Offenlegung des Quellcodes und dem Einblick in die *Votechain* kann jeder Bürger an der digitalen Wahl teilhaben. Dies unterbindet die Manipulation durch Individuen oder Organisationen. Die Autoren gingen hierfür von einer etablierten Nutzung der Online-Funktionen des Personalausweises und von einer Verknüpfung der Identität an die Wahl aus, damit der Stimmverkauf ein hohes persönliches Risiko erzeugt. Des Weiteren liegt die Aufgabe der Entwicklung des Systems beim Staat.

4.1 Akteure

Das Blockchain-basierte Wahlmodell benötigt *Prüfer, Validierer* und *Benutzer*. Die *Prüfer* sind im Szenario die Wahlhelfer. Diese unterstützen die Wahl mittels Rechenkapazität über internetfähige Endgeräte, um die Stimmen in fälschungssichere Blöcke umzuwandeln. Die Wahlbeobachter sind *Validierer* und repräsentieren den dezentralen Sicherungsmechanismus, in dem jeder das gesamte System ständig synchronisiert und validiert. Die Klasse der *Benutzer* unterteilt sich in Wählbare, Wahlberechtigten und Wahlkreise. Die Wählbaren sind entweder Personen (Erststimme) oder Parteien (Zweitstimme) und haben jeweils eine Wahl-WALLET. Diese kann per Protokoll nur Transaktionen empfangen. Die Wahlberechtigten erhalten nach der Authentifizierung für die elektronische Wahl eine randomisierte Wähler-WALLET. Diese enthält bei der Initiierung der Wallet zwei TOKENs, um die lokale Erststimme und die Zweitstimme zu wählen. Die Wähler-WALLET kann TOKENs ausschließlich senden. Wählende, die sich für eine andere Wahlmöglichkeit entscheiden, können weiterhin analog wählen. Um die Brief- und Urnenwahl nach der Wahlhandlung einzubinden, haben Wahlkreise Kreis-WALLETs.

4.2 Wahlprozess

Der rechtliche Wahlprozess wurde für das Blockchain-basierte Wahlsystem übernommen. Die Struktur der Wahl wurde modifiziert, indem die Internetwahl als zusätzliche Wahlmöglichkeit hinzugefügt wurde und die Speicherung und Validierung der Transaktionen in einem dezentralen System erfolgen. Im Folgenden werden Verantwortungen und Rollen beschrieben.

Nachdem die Landeslisten und Kreislisten von den Wahlleitungen erstellt wurden, senden diese die Listen zur Bundeswahlleitung. Die Bundeswahlleitung initiiert zentral die *Votechain* und entwickelt das Protokoll, das die technischen Spezifikationen der Transaktionen und WALLETs beschreibt. Die Wählbaren (Kandidaten und Parteien) senden nach der Abstimmung auf Kreis- oder Landeswahlleitung eine Anmeldung an die Bundeswahlleitung, um eine Wahl-WALLET zu beantragen. Für diese erhalten sie den Public KEY, um damit zu werben (beispielsweise als QR-Code oder ASCII-Code auf Wahlplakaten). Das System wird über einen Client für Wahlbeobachter (*Validierer*) und Wahlhelfer (*Prüfer*) geöffnet. Diese können sich vor Wahlbeginn anmelden und erhalten so einen persönlich authentifizierten, ortsabhängigen Zugang.

Die Gemeindebehörden erzeugen bei der Erstellung des Wählerverzeichnisses für den Wahlkreis spezifische Access-KEYs und individuelle Access-KEYs für die Wählenden. In Kombination mit dem Personalausweis und dem Wahlkreis-KEY schalten die Wählenden einen Login zu einer randomisierten anonymen Wähler-WALLET frei. Mit der Benachrichtigung erhalten die Wählenden die notwendigen KEYs. Die Wählenden können entscheiden, ob sie per Internet-, Brief- oder Urnenwahl wählen. Wenn sie per Brief- oder Urnenwahl wählen, bleibt der vorherige Wahlprozess erhalten. Per Internetwahl rufen die Wählenden über ein internetfähiges Endgerät eine Applikation auf und benutzen die Multifaktor-Authentifizierung (Wahlkreis-Key, Access-Key und Personalausweis) zum Registrieren. Danach wird der Access-Key deaktiviert, damit ein

Wählender nur einmal abstimmen kann. Nun wählt der Wählende den Public KEY des gewünschten Empfängers und kann seine Stimme abgeben bzw. den Wahl-TOKEN bis spätestens 18 Uhr am Wahltag senden. Diese Transaktion wird von Wahlbeobachtern erkannt und validiert. Sie kontrollieren dabei, ob der Wählende nicht bereits gewählt hat und ob dieser den Kandidaten als Erststimme wählen darf. Wahlhelfer prüfen die Transaktionen und verketten sie im Anschluss zu einem Block der *Votechain* [34]. Der Proof-of-work wird durch den Proof-of-stake ersetzt. Da das erstgenannte Konzept aufgrund der benötigten Rechenleistung energie- und kostenintensiv ist, eignet es sich für das Anwendungsszenario dieser Arbeit nicht. Bei dem Proof-of-stake-Konzept ist im *Votechain*-Protokoll definiert, dass beispielsweise minütlich aus der Menge authentifizierter Wahlbeobachter zufällig einer ausgewählt wird. Dieser verifiziert die Transaktionen des nächsten Blocks und fügt diese der *Votechain* hinzu.

Das Vergütungssystem für Wahlhelfer und -beobachter kann aus Anerkennung des Beitrages zu transparenten und fairen Wahlen bestehen. Bei der Validierung der noch offenen Transaktionen werden die geprüften Blöcke erneut verifiziert. Wenn es zu Diskrepanzen durch einen korrupten Helfer kommt, kann dieser leicht identifiziert und vom weiteren Verlauf der Wahl ausgeschlossen werden [35]. Der Wählende bekommt hiervon nichts mit. Dennoch kann er im Anschluss kontrollieren, ob die eigene Stimme in einem bestimmten Block enthalten ist und erhält eine anonyme Bestätigung.

Für die analoge Wahl (Urnen- und Briefwahl) werden während der Wahlhandlung für jeden analogen Wählenden eines Wahlkreises zwei TOKENs auf eine Kreis-WALLET gebucht. Diese Kreis-WALLET wird ab 18 Uhr am Wahltag freigeschaltet. Danach werden die Urnen von den analogen Wahlhelfern geöffnet und die analogen Wahlscheine im 4-Augenprinzip und unter Kontrolle einer elektronischen Auszählung in Transaktionen umgewandelt und den Wahl-WALLETs zugeschrieben. Diese Transaktionen werden ebenso von Wahlhelfern und -beobachtern validiert und geprüft.

Nachdem die Mehrheit der Transaktionen in der *Votechain* verkettet wurde, werden um 21 Uhr die Wahl-WALLETs von der Bundeswahlleitung mit dem jeweiligen PRIVATE KEY transparent geöffnet und die prozentuale Verteilung der TOKENs errechnet. Nachträgliche Manipulationen sind ausgeschlossen, weil diese nur durch angefügte Blöcke mit falschem Zeitstempel möglich sind [34].

4.3 Potentiale und Risiken

Die elektronische Wahl bietet organisatorische Vorteile in der Wahlhandlung und Feststellung des Wahlergebnisses. Überfüllte Wahlbüros in Großstädten werden entlastet und Wählende können mithilfe ihrer Wahlunterlagen, dem Personalausweis und einer Internetverbindung elektronisch wählen. Dies hilft insbesondere im Ausland lebenden deutschen Bürgern mit erschwertem Zugang zu Brief- und Urnenwahl. Die Repräsentanz der Wahl steigt mit Hilfe von *Votechain* durch eine demografisch gleichmäßiger verteilte Wahlbeteiligung, da die junge Altersgruppe aktuell prozentual unterdurchschnittlich wählt [6]. Kritische Bürger können sich leicht als Wahlbeobachter digital einschalten, den Quellcode kontrollieren und den Wahlprozess überwachen. Technisch bietet die *Votechain* in einer vermaschten Topologie einen Sicherheitsvorteil gegenüber einer zentralen sternförmigen.

Das dezentrale, elektronische Wahlsystem ist bei einer zu geringen Beteiligung an Wahlhelfern und -beobachtern ein Sicherheitsrisiko. Dementsprechend setzt die *Votechain* eine Mindestanzahl an Validierern und Prüfern voraus. Zum einen erhöht sie durch höhere Transparenz die individuelle und universelle Nachvollziehbarkeit, zum anderen reduziert sie die Anonymität und Geheimhaltung der Wählenden und ermöglicht die Einsicht in vorläufige Wahlergebnisse, die bis zum Ende der Wahlhandlung geheim bleiben müssen. Die Funktionsweise der *Votechain* ist komplexer als die bisherigen Wahlmodelle. Deshalb ist eine ablehnende Haltung der Wählenden aufgrund einer geringeren technischen Akzeptanz möglich. Das Bundesverfassungsgericht muss einer Veränderung des Wahlgesetzes zustimmen, um elektronische Wahlen zu realisieren.

5 Diskussion

Im Folgenden wird die *Votechain* anhand des Kriterienkatalogs bewertet, damit die Anforderungen eines E-Wahlsystems erfüllt werden. Einen Überblick des Evaluationsergebnisses gibt *Abbildung 3*.

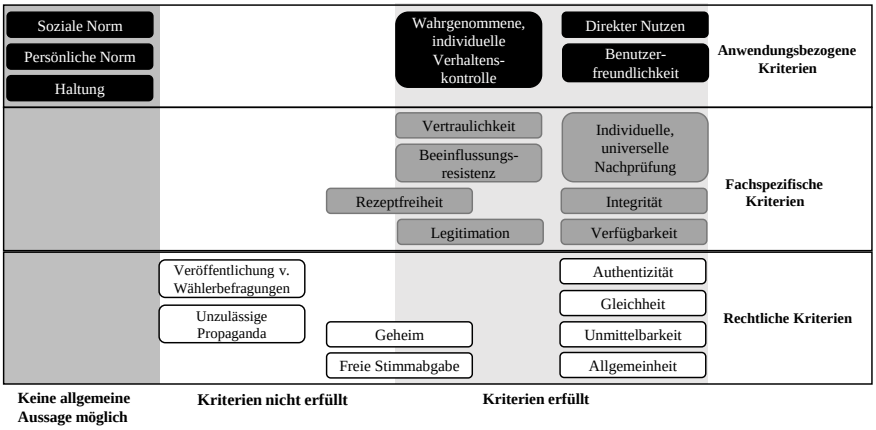

Abbildung 3. Erfüllung des Kriterienkatalogs

5.1 Rechtliche Kriterien

Das Kriterium der *Allgemeinheit* ist durch die *Votechain* erfüllt. Niemand wird aus politischen, wirtschaftlichen oder sozialen Gründen von der Wahl ausgeschlossen. Zur Nutzung der *Votechain* ist ein internetfähiges Endgerät notwendig, das auch ein öffentlicher Computer sein kann. Zusätzlich nimmt frei verfügbares Internet in Großstädten immer weiter zu und ist in Gesetzestexten verankert [36]. Die eingeführten Akteure erfüllen das Kriterium der *unmittelbaren Zuordnung*, die durch die WALLETs der Erst- und Zweitstimmen erfolgt und der *Gleichheit*, da jeder Wählende über genau zwei TOKENs verfügt. Auch die *Authentizität* der Stimmen ist durch die dezentrale und vielfach verifizierte Struktur der Blockchain erfüllt. Wie im vorherigen Kapitel aufgezeigt, wird

in der *Votechain* auf der einen Seite die Nachvollziehbarkeit der eigenen Stimme erreicht, auf der anderen Seite ist aber auch die *freie Stimmabgabe* durch eine Anonymisierung und kryptografische Verschlüsselung der Stimmen möglich. Dadurch ist das nächste rechtliche Kriterium der *geheimen* Wahl zwar nur teilweise erfüllt, die Autoren sind jedoch der Meinung, dass die Zuordnung der Stimmen aufgrund der Pseudonymität möglich, aber nicht wahrscheinlicher als bei einer Urnen- oder Briefwahl ist. Die Vorgaben zur *unzulässigen Propaganda* und *Veröffentlichung von Wählerbefragungen* sind nicht erfüllt. Denn die Basis der Blockchain ist die absolute Transparenz der Transaktionen. Diese ermöglicht es beispielsweise Wahlbeobachtern, die *Votechain* lokal zu speichern und so die bis zum Abruf der Daten erfolgten Transaktionen auszulesen. Dadurch ist es theoretisch möglich, Rückschlüsse auf die Anzahl der erfolgten Stimmen pro Partei bzw. Direktkandidaten zu ziehen. So könnte unzulässige Wahlpropaganda durch die Möglichkeit der verfrühten Veröffentlichung der Stimmverteilung erfolgen.

5.2 Fachspezifische Kriterien

Die Wahlhelfer und –beobachter gewährleisten durch ihre ständige Anwesenheit im P2P-Netzwerk die *Verfügbarkeit* der *Votechain*. Der Merkle-Tree in den Blöcken sorgt per Definition für ein integres System, wodurch das Kriterium der *Integrität* erfüllt ist [32]. Aufgrund der Transparenz der *Votechain* ist sowohl die *individuelle Nachprüfung* der Erst- und Zweitstimme, als auch eine *universelle Nachprüfung* gegeben. Denn die *Votechain* bietet neben der Sicherstellung der korrekten Verrechnung der eigenen Stimme zusätzlich die Transparenz zur Nachvollziehbarkeit der ordnungsgemäßen Durchführung aller Transaktionen. Dies ist gegeben, wenn der letzte Block der Kette, der per Definition auch alle anderen Transaktionen konsolidiert beinhaltet, vollständig verifiziert ist. Damit ist die Gesamtmenge der Stimmen korrekt und unverfälscht abgegeben. Der Prozess der *Votechain* beinhaltet die 2-Faktor-Authentifizierung des berechtigten Wählenden in Form des Wahlkreis-KEYs und der Identifikation mit dem elektronischen Personalausweis. Dadurch ist sichergestellt, dass sich nur legitimierte Personen für die Onlinewahl freischalten können und das Kriterium der *Legitimation* erfüllt. Unter der Annahme einer hinreichenden Auslastung und der damit einhergehenden hohen Transaktionsfrequenz ist es für Dritte nicht möglich, einen konkreten Wählenden zu verfolgen. Dementsprechend ist das Kriterium der *Beeinflussungsresistenz* erfüllt. Die *Votechain* stellt durch ihre kryptografische Verschlüsselung den Schutz persönlicher Daten vor dem Zugriff Dritter sicher. Das Kriterium der *Vertraulichkeit* ist dadurch erfüllt. Ein Aspekt, der nicht vollständig durch das Blockchain-basierte Wahlsystem abgedeckt wird, ist die *Receipt Freeness*. So schreibt das Protokoll vor, dass dem Wählenden nach erfolgreicher Stimmabgabe eine Bestätigung zugesandt wird. Diese ist jedoch standardisiert und enthält keine Information darüber, welche Partei gewählt wurde. Demnach ist das Kriterium nicht vollständig erfüllt. Dennoch wird eine Belegbarkeit durch Dritte ausgeschlossen.

5.3 Anwenderbezogene Kriterien

Im Gegenteil zu den zuvor evaluierten rechtlichen und fachspezifischen Kriterien müssen die anwenderbezogenen Aspekte ganzheitlich betrachtet werden. Sie unterliegen der Subjektivität der Autoren. Die technische Akzeptanz hängt von einer transparenten und verständlichen Einführung des neuen Wahlsystems ab. Durch Interaktion mit den Bürgern beispielsweise anhand von Umfragen oder mittels einer digitalen staatlichen Plattform können negativen Entwicklungen frühestmöglich vorgebeugt werden.

Die Kategorien *Benutzerfreundlichkeit* und *direkter Nutzen* sind für die Wahlberechtigten und insbesondere für junge Wählende erfüllt. Die anderen Kriterien können aufgrund der persönlichen Individualität nicht kategorisch, sondern eher tendenziell beantwortet werden. Die *wahrgenommene individuelle Verhaltenskontrolle* ist analog zum Kriterium der individuellen Nachprüfbarkeit. Entsprechend ist durch eine mögliche Partizipation an der Wahl als Wahlbeobachter die Nachvollziehbarkeit des korrekten Ablaufs gegeben. Die *Haltung* und *persönliche Norm* eines Individuums zu dem neuen Wahlsystem ist stark von der Kommunikation bei der Einführung und der persönlichen Erfahrung mit Technologie abhängig. Dementsprechend können Präventivmaßnahmen eine positive Haltung unterstützen. Die *soziale Norm* bietet durch die steigende Quote der *Digital Natives*, Personen, die mit der digitalen Welt aufgewachsen sind, eine positive Tendenz für E-Wahlen. Zusammenfassend sind die Kriterien des TAM-Modells nach Auffassung der Autoren langfristig für die Gesamtbevölkerung erfüllt.

6 Fazit

Die Blockchain-Technologie ermöglicht es, Systeme in die digitale Welt zu überführen und ihre Sicherheit zu erhöhen. Die Anwendung auf elektronische Wahlen erhöht die Zugänglichkeit und bietet organisatorische und finanzielle Vorteile gegenüber analogen Wahlen. Für E-Wahlsysteme müssen dazu rechtliche, fachspezifische und anwenderbezogene Kriterien erfüllt werden, die in einem Kriterienkatalog zusammengefasst wurden. Hierbei kann ein Blockchain-basiertes Wahlsystem lediglich §32 Abs. 2 des Bundeswahlgesetzes nicht vollkommen genügen. Die Transparenz durch die Offenlegung der Blockchain steht im Konflikt zwischen Nachvollziehbarkeit und Anonymität der Wahlen. Die *Votechain* wurde anhand des Wahlprozesses der Bundestagswahl modelliert und diskutiert. Sie kann als Referenz für Blockchain-Anwendungen auf andere Wahlen in Deutschland genutzt werden.

Bei einer konkreten Implementierung müssen folgende Aspekte der *Votechain* näher untersucht werden: Transaktionsgeschwindigkeit bei hoher Skalierung, mögliche Nutzung des elektronischen Personalausweises für die persönliche Authentifizierung und detaillierte Anforderungen an Oberfläche und Logik des technischen Systems, sowie die Identifizierung der sicherheitsrelevanten Schwachstellen.

Um eine möglichst objektive Evaluierung der anwenderbezogenen Kriterien zu erreichen, bietet sich eine repräsentative Umfrage an. Ebenso müssen nach der technischen Klärung Test-Wahlen stattfinden, um das entwickelte System zu simulieren und Verbesserungspotenziale zu identifizieren.

Quellenverzeichnis

1. Pommer, K.: Forsa-Umfrage: Jeder zweite würde online wählen, https://web.archive.org/web/20130602070821/http://www.microsoft.com/de-de/news/pressemitteilung.aspx?id=533684.
2. Yermack, D.: Corporate governance and blockchains. Rev. Financ. 21, 7–31 (2017).
3. Rückeshäuser, N., Brenig, C., Müller, G.: Blockchains als Grundlage digitaler Geschäftsmodelle. Datenschutz und Datensicherheit - DuD. 41, 492–496 (2017).
4. Berninger, V.: Chaos Computer Club: Wahl-Software ist hackbar, http://www.sueddeutsche.de/digital/bundestagswahl-chaos-computer-club-wahl-software-ist-hackbar-1.3656904.
5. Buhl, H.U., Schweizer, A., Urbach, N.: Blockchain-Technologie als Schlüssel für die Zukunft ? Zeitschrift für das gesamte Kreditwes. 4801, 596–599 (2017).
6. Bundeszentrale für politische Bildung: Wahlbeteiligung nach Altersgruppen, http://www.bpb.de/nachschlagen/zahlen-und-fakten/bundestagswahlen/205686/wahlbeteiligung-nach-altersgruppen.
7. Netigate: Mehrheit der Deutschen bereit online wählen zu gehen, https://www.netigate.net/de/marktforschung/mehrheit-der-deutschen-bereit-online-waehlen-zu-gehen/.
8. Spiegel Online: Kosten für Bundestagswahl so hoch wie nie, http://www.spiegel.de/politik/deutschland/bundestagswahl-kosten-laut-innenministerium-hoch-wie-nie-a-1164713.html.
9. Wilde, T., Hess, T.: Forschungsmethoden der Wirtschaftsinformatik Eine empirische Untersuchung. Wirtschaftsinformatik. 49, 280–287 (2007).
10. Hevner, A.R.: A Three Cycle View of Design Science Research. Scand. J. Inf. Syst. 19, 87–92 (2007).
11. BWahlG: Bundeswahlgesetz (BWahlG). (1956).
12. BWO: Bundeswahlordnung (BWO). (2002).
13. Volkamer, M., Krimmer, R.: Ver-/Misstrauen Schaffende Maßnahme beim e-Voting. In: GI Jahrestagung (1). pp. 418–425 (2006).
14. Davis, F.D.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Q. 319–340 (1989).
15. Huijts, N.M.A., Molin, E.J.E., Steg, L.: Psychological Factors Influencing Sustainable Energy Technology Acceptance: A Review-Based Comprehensive Framework. Renew. Sustain. Energy Rev. 16, 525–531 (2012).
16. Tanenbaum, A.S., Van Steen, M.: Architecture. In: Distributed systems: principles and paradigms. pp. 33–58. Pearson Prentice-Hall, Amsterdam (2007).
17. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B.: Blockchain Technology Innovations. In: Technology & Engineering Management Conference (TEMSCON), 2017 IEEE. pp. 137–141. IEEE (2017).
18. Buchegger, S., Le Boudec, J.-Y.: Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile ad hoc Networks. In: Parallel, Distributed and Network-based Processing, 2002. Proceedings. 10th Euromicro Workshop on. pp. 403–410. IEEE (2002).
19. Pandya, K.: Network Structure or Topology. Int. J. Adv. Res. Comput. Sci. Manag. Stud. 1, (2013).
20. Kovic, M.: Blockchain for the people Blockchain technology as the basis for a secure and reliable e-voting system. ZIPAR Discuss. Pap. (2017).
21. Osgood, R.: The Future of Democracy: Blockchain Voting. COMP116 Inf. Secur. 1–21 (2016).
22. Korte, K.R.: Wahlen in Deutschland. Bundeszentrale für politische Bildung (2009).
23. Clarkson, M.R., Chong, S., Myers, A.C.: Civitas: Toward a secure voting system. Proc.

- IEEE Symp. Secur. Priv. 354–368 (2008).
24. Delaune, S., Kremer, S., Ryan, M.: Verifying Privacy-Type Properties of Electronic Voting Protocols: A Taster. Towar. Trust. Elections - New Dir. Electron. Voting. 6000, 260–273 (2010).
25. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. WPES '05 Proc. 2005 ACM Work. Priv. Electron. Soc. 6000 LNCS, 61–70 (2005).
26. Pfleeger, C.P., Pfleeger, S.L.: Security in Computing. Prentice Hall (2006).
27. Choi, S.O., Kim, B.C.: Voter Intention to Use E-Voting Technologies: Security, Technology Acceptance, Election Type, and Political Ideology. J. Inf. Technol. Polit. 9, 433–452 (2012).
28. Yao, Y., Murphy, L.: Remote Electronic Voting Systems: An Exploration of Voters' Perceptions and Intention to use. Eur. J. Inf. Syst. 16, 106–120 (2007).
29. Keppler, D., Schäfer, M.: Modelle der technikorientierten Akzeptanzforschung - Überblick und Reflexion am Beispiel eines Forschungsprojekts zur Implementierung innovativer technischer Energieeffizienz-Maßnahmen. Zent. Tech. und Gesellschaft. 12, (2013).
30. Merkle, R.C.: Protocols for Public Key Cryptosystems. Proc. - IEEE Symp. Secur. Priv. 122–134 (1980).
31. Grewal-Carr, V., Lewis, H., Marshall, S.: Blockchain: Enigma. Paradox. Opportunity. Deloitte LLP. 25 (2016).
32. Antonopoulos, A.M.: Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media (2014).
33. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Www.Bitcoin.Org. 9 (2008).
34. Noizat, P.: Blockchain Electronic Vote. Handb. Digit. Curr. Bitcoin, Innov. Financ. Instruments, Big Data. 453 (2015).
35. King, S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. In: self-published paper, August (2012).
36. Reents, R.R.: Ausbau und Finanzierung einer flächendeckenden Breitbandversorgung in Deutschland. Mohr Siebeck (2016).