

Andreas Meier

Zusammenfassung

E-Voting kann mit Blockchain-Technologien realisiert werden. Im Kapitel werden zuerst Anforderungen an ein elektronisches Wahlsystem erläutert, nämlich Gleichheit, Berechtigung, One Man One Vote, Authentifikation, Schutz der Privatsphäre, Gerechtigkeit sowie Verifizierbarkeit und Vollständigkeit. Nach der Diskussion von Sicherheitsaspekten wird eine Klassifikation der auf Blockchain-Technologie basierenden eVoting-Systeme vorgenommen, wie die Nutzung von Kryptowährungen, Smart Contracts oder die Blockchain als Ballot Box. Das Fallbeispiel BroncoVote und ein Protokoll für die Verwendung von blinden Signaturen zeigen im Detail, wie E-Voting-Systeme auf Blockchain-Basis realisiert werden. Ein Vorschlag zum Fuzzy Voting und zur Spannungsbreite zwischen anonymem Wahlverhalten (MyVote) und öffentlichem Abstimmungsverhalten (OurVote) erläutern Entwicklungsoptionen einer digitalen Gesellschaft für die Zukunft. Eine Diskussion von Chancen und Risiken rundet das Kapitel ab.

Schlüsselwörter

E-Voting · Blockchain · Privatsphäre · Blinde Signatur · BroncoVote · Fuzzy Voting · eDemocracy · Sicherheit

Vollständig neuer Original-Beitrag.

A. Meier (✉)
University of Fribourg, Fribourg, Schweiz
E-Mail: andreas.meier@unifr.ch

16.1 Anforderung an ein elektronisches Wahlsystem

Unter dem Begriff der politischen Partizipation werden verschiedene Formen der einflussnehmenden Beteiligung von Bürgerinnen und Bürgern verstanden (Meier und Teran 2019). Dazu zählen Informationsaustausch und Kommunikation über Sachthemen und Programme, Gestaltung politischer Inhalte und Entscheidungsprozesse oder Beteiligung an Abstimmungen über Sachthemen sowie Mitwirkung an Wahlen für politische Mandatsträger.

Für die Nutzung eines elektronischen Wahlsystems resp. für E-Voting werden die folgenden Grundsätze immer wieder hervorgehoben (siehe Schweizerische Verordnung der Bundeskanzlei über die elektronische Stimmabgabe vom 13. Dezember 2013 unter VELeS 2018; Hardwick et al. 2018; Delaune et al. 2010):

- Gleichheit (Equality): Eine Gewichtung der Stimmen ist nicht zulässig, d. h., es gilt Wahlgleichheit für Alle.
- Berechtigung (Eligibility): Nur stimmberechtige Personen können an elektronischen Wahlen teilnehmen.
- Keine Wiederverwertung (No Reusability): Wähler können nicht mehrfach ihre Stimme abgeben. Jeder berechtigte Wähler hat genau eine Stimme (One Man One Vote).
- Echtheit (Authentifikation): Die Identität des Wählers lässt sich eindeutig überprüfen.
- Schutz der Privatsphäre (Privacy): Die Privatsphäre und damit auch das Stimmgeheimnis bleiben geschützt.
- Gerechtigkeit (Fairness): Es dürfen keine vorzeitigen Teilergebnisse publiziert werden, um weitere Stimmabgaben nicht zu beeinflussen.
- Verifizierbarkeit (Verifiability) und Vollständigkeit (Completeness): Die Korrektheit des Stimmergebnisses kann individuell wie universell überprüft werden. Durch individuelle Überprüfbarkeit kann ein Bürger verifizieren, dass seine Stimme gezählt wurde. Universelle Verifizierbarkeit bedeutet das Kontrollverfahren und die Bestätigung, dass der Ausgang der Abstimmung der Summe aller gültigen Stimmen entspricht.

Neben diesen Grundsätzen werden weitere Forderungen gestellt, so z. B. den Schutz der Informationen für die Stimmberrechtigten vor Manipulationen oder den Schutz der persönlichen Informationen über die Stimmberrechtigten.

Eine oft gestellte Forderung betrifft die Option der Verzeihung (Forgiveness) resp. die Möglichkeit, seine Stimmabgabe korrigieren zu können. Damit möchte man ermöglichen, dass bei Zwang oder Nötigung ein Stimmberrechtigter seine unter Druck entstandene Stimmabgabe korrigieren kann.

16.2 Sicherheit elektronischer Wahlen

Neben rechtlichen Grundlagen kommt der technischen Sicherheit bei elektronischen Wahlen und Abstimmungen große Bedeutung zu. Ein korrektes Wahlergebnis kann nur dann erzielt werden, wenn die E-Voting-Systeme sauber entworfen, implementiert und gegen Attacken unterschiedlicher Art abgesichert sind und laufend überwacht werden. Dabei ist wichtig, sowohl den Datenschutz wie die Datensicherheit zu gewähren.

Unter Datenschutz (engl. data protection) versteht man den Schutz der Daten vor unbefugtem Zugriff und Gebrauch. Schutzmaßnahmen sind Verfahren zur eindeutigen Identifizierung und Authentifikation von Personen, zum Erteilen von Benutzerberechtigungen für bestimmte Datenzugriffe, aber auch kryptografische Methoden zur diskreten Speicherung oder Weitergabe von Informationen.

Im Gegensatz zum Datenschutz fallen unter den Begriff Datensicherung oder Datensicherheit (engl. data security) technische und softwaregestützte Maßnahmen zum Schutz der Daten vor Verfälschung, Zerstörung oder Verlust. Differenzierte Datensicherungsverfahren sind für die Speicherung und Nutzung von Datenbeständen entwickelt worden; insbesondere existieren Verfahren für die Wiederherstellung von Datenbanken nach einem Fehlerfall (sog. Recovery und Restart; z. B. in Meier und Kaufmann 2019).

Im Folgenden beschränken wir uns auf einen kurzen Überblick über die wichtigsten kryptografischen Verfahren klassischer und/oder Blockchain-basierter E-Voting-Systeme, die primär dem Schutz der Privatsphäre, der Authentifikation der Wähler sowie der Verifizierbarkeit und Vollständigkeit dienen (vgl. Anforderungen an elektronische Wahlsysteme in Abschn. 16.1):

- Homomorphe Kryptografie
- Zero-Knowledge Proof
- Mix-Net
- Blinde Signaturen oder
- Blockchain

Homomorphe Verschlüsselungsverfahren erlauben die Verarbeitung von verschlüsselten Daten (hier Stimmabgaben), ohne den Inhalt der Daten im Klartext zu kennen (vgl. additive resp. multiplikative homomorphe Kryptografie in Craig 2009). Sie liefern dasselbe Ergebnis, wie wenn die dazu notwendigen Additionen zur Summe der gültigen Stimmen im Klartext ausgeführt worden wären. Homomorphe Verfahren sind beispielsweise wichtig bei der Nutzung von Cloud-Technologien. Werden verschlüsselte Daten in einer Cloud abgelegt, so können sie jederzeit analysiert oder verarbeitet werden, ohne sie zu entschlüsseln.

Ein Zero-Knowledge Proof ist ein Verfahren, mit dem die beweisführende Partei (Prover) einer anderen Partei (Verifizierer) nachweisen kann, dass eine bestimmte Aussage wahr ist, ohne weitere Informationen zu übermitteln, ausser dass die Aussage tatsächlich wahr ist (Beutelspacher et al. 2015). Beim E-Voting bedeutet dies, dass das Beweisverfahren dem Verifizierer erlaubt, den Wahrheitsgehalt der

Stimmabgabe zu überprüfen, ohne den Inhalt zu kennen (vgl. Abschn. 16.3 über E-Voting-Systeme). Damit kann das Stimmgeheimnis (Forderung der Privacy) bei elektronischen Wahlen und Abstimmungen jederzeit gewahrt bleiben.

David Chaum hat für E-Mail-Systeme 1981 eine Technik vorgeschlagen, die auf der Public-Key-Infrastruktur basiert und verbirgt, mit wem ein Netzteilnehmer kommuniziert und wie der Inhalt der Kommunikation lautet (Chaum 1981). Trotz ungesicherter Kommunikationsnetze erfordert diese Technik kein Trust Center als vertrauenswürdige Autorität. Die Technik ist unter dem Begriff Mix-Netze bekannt geworden und findet bei E-Voting-Systemen mit Mix-Servern Verwendung, um die Verbindungen zum Wähler zu kappen. Mix-Netze mischen und verschlüsseln die Stimmzettel, damit sie anders aussehen als zuvor. Die Richtigkeit des Ergebnisses kann anhand von Zero-Knowledge Proofs verifiziert werden, bei denen jede Autorität das Ergebnis nach dem Mischen veröffentlicht. Solange es mindestens einen ehrlichen Mix-Server gibt, ist die Anonymität des Wählers gewährleistet.

David Chaum entwickelte die blinden Signaturen, um elektronisches Geld zu realisieren (Chaum 1982). Blinde Signaturen können aber auch bei elektronischen Abstimmungen und Wahlen Anwendung finden. Eine Signatur nennt man blind, wenn der Unterzeichner eines Stimmzettels den Inhalt des Stimmzettels nicht sieht, diesen aber mit seiner digitalen Signatur versieht und demnach blind signiert. In Abschn. 16.5 wird ein E-Voting-System mit blinden Signaturen im Detail vorgestellt und diskutiert, basierend auf der Forschungsarbeit von Liu und Wang (2017).

Die Blockchain ist ein verteiltes Peer-to-Peer-Netzwerk von Hauptbüchern, wobei die einzelnen Datenblöcke miteinander verkettet sind (Bashir 2017; Berentsen und Schär 2017; Meier und Stormer 2018). Um die Integrität und Sicherheit in der Blockchain zu gewährleisten, werden Schlüsselpaare bestehend aus einem privaten und einem öffentlichen Schlüssel der Public-Key-Infrastruktur verwendet. Im verteilten Netz kann jeder Rechnerknoten nicht nur einzelne Blöcke samt Block Header, Hashbaum und Transaktionsdaten durchforsten, sondern in der ganzen Blockkette rückwärts blättern und zum Beispiel alle an das System übertragenen Transaktionsdaten (Inhalte) konsultieren. Wird ein E-Voting-System also mit der Blockchain-Technologie realisiert, können sowohl die Wähler wie ihre Stimmabgaben eingesehen werden (vgl. Forderung der Verifizierbarkeit und Vollständigkeit). Allerdings sind Blockchain-basierte E-Voting-Systeme entwickelt worden, die auch die Forderung der Anonymität und den Schutz der Privatsphäre respektieren (siehe Abschn. 16.3 über Klassifikation Blockchain-basierter E-Voting-Systeme).

Nach unserer Auffassung wird die Diskussion in der Öffentlichkeit zu wenig geführt, ob ein elektronisches Wahlsystem geheim oder offen realisiert werden soll. In Abschn. 16.7 plädieren wir, sowohl Optionen der Urnendemokratie (unter MyPolitics) wie der Versammlungsdemokratie (OurPolitics) oder gar Abstufungen zwischen beiden Ansätzen zu prüfen und der Öffentlichkeit zur Verfügung zu stellen (Meier et al. 2018; Kaskina 2018).

16.3 Klassifikation Blockchain-basierter E-Voting-Systeme

In ihrem Forschungspapier ‚Platform-independent Secure Blockchain-Based Voting System‘ (Yu et al. 2018) klassifizieren die Autoren E-Voting-Systeme aufgrund eines hervorstechenden Merkmals in drei Kategorien:

- Kryptowährung: Ein E-Voting-System kann mit der Hilfe einer auf Blockchain-basierten Kryptowährung vorangetrieben werden. Zhao und Chan (2015) schlagen das System Bitcoin vor, wobei Zufallszahlen für das Unkenntlichmachen der Stimmabgaben verwendet und mit Zero-Knowledge-Proof-Verfahren (Beutelspacher et al. 2015) verteilt werden. Dabei wird zwischen den beiden Parteien einer Transaktion (hier Wahl oder Stimmabgabe), d. h. zwischen dem Prüfer (Prover) und dem Verifizierer (Verifier), ein Beweisverfahren angewendet, das dem Verifizierer erlaubt, den Wahrheitsgehalt der Stimmabgabe zu überprüfen, ohne den Inhalt der Stimmabgabe zu kennen. Der Verifizierer hat also ‚Zero Knowledge‘ über die konkrete Stimmabgabe, der Prüfer kann jedoch beweisen, dass er über einen korrekt ausgefüllten Stimmzettel verfügt, den Inhalt seiner Stimmabgabe jedoch nicht preisgeben wird. Mit dem Zero-Knowledge-Proof-Verfahren wird demnach das Stimmgeheimnis geschützt (siehe Forderung Privacy). Tarasov und Tewari (2017) gehen einen Schritt weiter und verwenden anstelle von Bitcoins die Erweiterung Zcash. Zcash ist ein dezentrales E-Payment-System basierend auf Blockchain, das Anonymität bei Zahlungstransaktionen unterstützt. Im Gegensatz zu Bitcoin verwendet Zcash als Konsensalgorithmus nicht den Proof-of-Work-Ansatz, sondern das Zero-Knowledge-Proof-Verfahren.
- Smart Contracts: Für die Realisierung eines E-Voting-Systems können Smart Contracts verwendet werden. Smart Contracts sind Protokolle basierend auf der Blockchain, die schriftliche Vereinbarungen (Verträge) abbilden und die Abwicklung und Überprüfung der Vertragsklauseln vornehmen. McCorry et al. (2017) schlagen ein E-Voting-System für Boardroom Voting vor, basierend auf Blockchain-basierten Smart Contracts. Das System ist allerdings beschränkt auf Ja-/Nein-Antworten, und die Menge der Wähler ist aufgrund des Leistungsvermögens dieser Lösung eingeschränkt.
- Ballot Box: Hier wird die Blockchain als Wahlurne, d. h. verteiltes Buchhaltungssystem für Wahlen, verwendet. Erste produktive Systeme wie TIVI.io oder FollowMyVote.com sind mit diesem Ansatz entstanden. Das System TIVI aus Tallin, Estland verwendet zur Verifikation der Wählerschaft Selfies, wobei ein hinterlegtes Bild mit dem Selfie durch ein biometrisches Verfahren abgeglichen wird. Erste praktische Wahlen sind mit TIVI erfolgreich durchgeführt worden. FollowMyVote verlangt vom Wähler eine Webcam und eine vom eGovernment ausgestellte Identifikation, um an einer elektronischen Wahl teilhaben zu können. Mit einer Blockchain lässt sich nach der Registrierung eine elektronische Wahl durchführen. Eine weitere Option besteht darin, blinde Signaturen für eine elektronische Wahl zu verwenden, wie sie von Liu und Wang (2017) vorgeschlagen wird.

Um E-Voting-Varianten mit Blockchain-Technologie im Detail zu illustrieren, wird im nächsten Abschn. 16.4 das Wahlsystem BroncoVote und im übernächsten Abschn. 16.5 ein Protokoll mit blinden Signaturen vorgestellt.

16.4 Fallbeispiel BroncoVote

Das E-Voting-System BroncoVote ist ein universitäres Abstimmungssystem, das auf Smart Contracts einer privaten Blockchain basiert (Dagher et al. 2018). Im Gegensatz zu einer öffentlichen Blockchain können bei BroncoVote demnach nur Teilnehmer einer Universität dieses E-Voting-System nutzen. Smart Contracts erzeugen Ereignisse, die es den Verträgen ermöglichen, untereinander und mit den Universitätsangehörigen zu interagieren. Als Smart-Contracts-Umgebung wurde Ethereum gewählt, ein bekanntes Open-Source-System mit der internen Kryptowährung Ether als Zahlungsmittel für die Abwicklung der Transaktionen (Buterin 2013).

Die Anwender von BroncoVote können Umfragen oder Wahlen durchführen und bestimmen, wer daran teilnehmen darf. Der Schutz der Privatsphäre ist gewährleistet, da die gültigen Stimmen mit einem homomorphen Kryptosystem (Paillier 1999) verwaltet werden.

Die folgenden Rollen werden für BroncoVote vergeben:

- Administrator: Er ist verantwortlich für das Aufsetzen der beiden Smart Contracts ‚Registrar Contract‘ und ‚Creator Contract‘ (vgl. Abb. 16.1).
- Creator: Der Creator ist ein Student oder Universitätsangehöriger, der die Erlaubnis zur Erstellung eines Voting Contracts besitzt (Ballot Creation).
- Voter: Die Wähler können sich mit ihrer gültigen Studenten-ID resp. ihrer gültigen Universitätsangehörigen-ID samt E-Mail-Adresse registrieren, um an einer bestimmten Wahl (Ballot ID) teilzunehmen.

In Abb. 16.1 ist der Vorgang zur Erstellung eines Wahlzettels durch den Creator aufgezeigt:

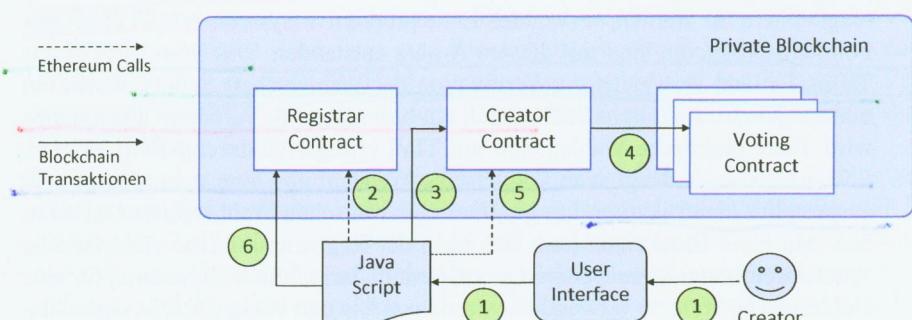


Abb. 16.1 Erstellen eines Wahlzettels in BroncoVote, angelehnt an Dagher et al. (2018)

- (1) Der Creator eines Stimmzettels gibt seine Wahlinformation in der Benutzeroberfläche ein und diese Information wird an JavaScript weitergeleitet.
- (2) JavaScript sendet einen Ethereum Call an den Registrierungsvertrag (Registrar Contract), um die Information des Creators zu überprüfen.
- (3) Wenn der Creator die Überprüfung besteht, wird eine Transaktion an den Creator Contract gesendet, um einen Abstimmungsvertrag zu beantragen.
- (4) Der Creator Contract sendet eine Transaktion zur Erstellung eines neuen Wahlvertrags (Voting Contract).
- (5) JavaScript sendet einen Ethereum Call an den Creator Contract, um die neue Adresse des Wahlvertrags abzurufen.
- (6) JavaScript sendet eine Transaktion an den Registrar Contract mit der ID des Stimmzettels und der Vertragsadresse, um die Wahl zu registrieren.

Nachdem der Wähler einen Stimmzettel (Ballot ID) angefordert hat, basierend auf dem entsprechenden Voting Contract, kann er abstimmen (siehe Abb. 16.2):

- (1) Der Voter gibt seine Stimme im User Interface basierend auf seiner E-Mail-Adresse ab; diese wird zum JavaScript weitergeleitet.
- (2) JavaScript sendet einen Ethereum Call an den Registrar Contract, um den Wähler zu verifizieren.
- (3) Falls der Wähler die Überprüfung des Registrar Contracts erfolgreich übersteht, schickt JavaScript einen Ethereum Call zum Voting Contract, um den Status des Wählers im Voting Contract sowie die Abstimmungszeitlimite zu prüfen.
- (4) Übersteht der Wähler die Prüfung des Voting Contracts, wird seine Stimme via Encryption Call auf dem Server verschlüsselt.
- (5) JavaScript sendet einen weiteren Ethereum Call an den Voting Contract, um den aktuellen verschlüsselten Abstimmungszähler zu erhalten.
- (6) JavaScript schickt den verschlüsselten Abstimmungszähler zusammen mit der verschlüsselten Stimmabgabe zum Server mit der Hilfe eines Encryption Calls.
- (7) Zudem schickt JavaScript eine Transaktion an den VotingContract, um den neuen Abstimmungszähler zu registrieren.

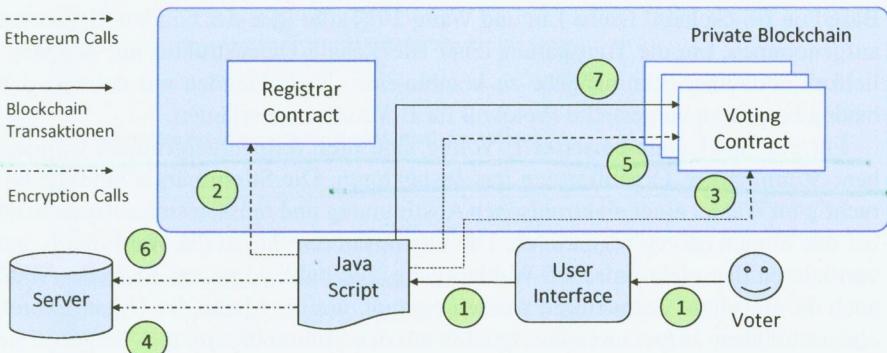


Abb. 16.2 Abgabe einer Stimme eines Wählers im BroncoVote-System, angelehnt an Dagher et al. (2018)

Das Wahlsystem BroncoVote, basierend auf der Blockchain-Technologie, erfüllt dank der Nutzung von Smart Contracts und der homomorphen Kryptografie die oft gestellte Forderung nach geheimer Abstimmung (Privacy). Eine weitere Option zur Geheimhaltung der Wähler und Stimmabgaben besteht beim Verwenden blinder Signaturen.

16.5 E-Voting-Protokoll mit blinden Signaturen

Die Blockchain ist ein verteiltes Buchhaltungssystem, bei dem jederzeit der Inhalt der einzelnen Blöcke konsultiert werden kann. Soll dieses System nun für elektronische Wahlen genutzt werden, stellt sich die Frage, wie Stimmabgaben geheim gehalten werden. Eine Möglichkeit besteht darin, blinde Signaturen zu verwenden.

Blinde Signaturen wurden 1982 von David Chaum an der International Cryptology Conference in Santa Barbara, CA vorgestellt (Chaum 1982), um elektronische Münzen anonym verwenden zu können. Die Echtheit solcher Münzen wird durch blinde Signaturen des dahinterstehenden Bankinstituts garantiert, wobei die Bank auch die Umwandlung von echten Münzen in elektronische und umgekehrt vornimmt. Damit können Kunden ihre elektronischen Münzen anonym verwenden (vgl. das elektronische Zahlungssystem eCash, das in der Zwischenzeit stillgelegt wurde).

David Chaum hat für die Verwendung blinder Signaturen allerdings auch das E-Voting als sinnvoll erachtet, um die Echtheit der Wähler (Authentizität) wie deren Anonymität bei der Stimmabgabe zu garantieren. Allgemein können blinde Signaturen dazu benutzt werden, um digitale Unterschriften für Daten (Dokumente, Stimmzettel, Zahlungen etc.) zu erzeugen, ohne dass der Lieferant digitaler Signaturen diese Daten einsehen kann.

David Chaum erläutert das Verfahren der blinden Signaturen durch folgende Analogie: Der zu signierende Wahlzettel wird in ein Couvert mit Blaupause gesteckt und der Wahlorganisator unterschreibt dieses Couvert blind, d. h. ohne dessen Inhalt zu kennen. Die Signatur drückt sich dank der Blaupause auf den Wahlzettel durch und der Wähler kann den blind signierten Wahlzettel anonym in die Urne werfen.

Yi Liu und Qi Wang haben in ihrem Forschungspapier ‚An E-Voting Protocol Based on Blockchain‘ (siehe Liu und Wang 2017) die Idee der blinden Signaturen aufgenommen, um die Transparenz einer Blockchain-Datenstruktur mit der Möglichkeit anonymer Stimmabgabe zu kombinieren. Im Folgenden wird das von den beiden Forschern vorgestellte Protokoll für E-Voting kurz erläutert.

Für ein Blockchain-basiertes E-Voting sind drei Teilnehmergruppen vorgesehen: Stimmbürger, Organisatoren und Inspektoren. Die Stimmbürger sind die berechtigten Wähler einer elektronischen Abstimmung und müssen sich entsprechend bei den Organisatoren registrieren. Die Organisatoren führen die Wahl durch und verifizieren den elektronischen Wahlvorgang. Sie publizieren am Ende der Wahl auch die Resultate. Inspektoren werden ernannt, um die Macht der Organisatoren einzuschränken. Inspektoren interagieren mit den Stimmbürgern; u. a. vergeben sie blinde Signaturen. Zudem haben sie Zugriff auf die Blockchain und können unterschiedliche Audits durchführen.

Betrachten wir ein kleines Beispiel in Abb. 16.3: Der Einfachheit halber beschränken wir uns auf eine Wählerin Alice und nehmen an, dass nur ein Organisator (Bob) und nur eine Inspektorin (Carol) beteiligt sind. Nach einer erfolgreichen Registrierung von Alice beim Organisator Bob kann Alice ihre digitale Stimme in zwei Phasen abgeben: In der ersten Phase holt sie zwei blinde Signaturen ein, je eine vom Organisator Bob (Fall 1a in Abb. 16.3) und je eine von der Inspektorin Carol (Fall 1b).

Konkret sieht die digitale Stimmabgabe für Alice wie folgt aus: Alice füllt den Stimmzettel aus, indem sie den gewünschten Wahlcode drückt und damit den VoteString V generiert. Ein VoteString V besteht aus den drei Teilen Wahlcode (ChoiceCode: x Bits), Nullerkette (ZeroString: y Bits, wobei alle Bits = 0) und Zufallskette (RandomString: z Bits). Die Nullerkette wird zur Wohlgeformtheit des Wahlzettels gebraucht (well-formed VoteString); die Zufallskette wird benötigt, um die unterschiedlichen Stimmabgaben aller Wähler mit demselben Wahlcode zu unterscheiden.

Nehmen wir als kleines Beispiel eine Stimmabgabe für ein politisches Programm, bei dem der Wähler Ja (ChoiceCode = ,10⁴), Nein (ChoiceCode = ,01⁴) oder Enthaltung (ChoiceCode = ,00⁴) eingeben kann. Bei der Wahl von mehreren politischen Mandatsträgern müsste ein entsprechender ChoiceCode für alle Wahloptionen vorgesehen werden.

Nachdem Alice den VoteString V erstellt hat, generiert der Computer von Alice einen Hash-Wert für V, d. h. hash(V). Zudem wird die Berechnungsfunktion C (calculation function) für die Erstellung blinder Signaturen durchgeführt und Alice schickt $C_{Alice}(\text{hash}(V))$ verschlüsselt zu Bob, indem sie den öffentlichen Schlüssel von Bob verwendet (siehe asymmetrische Kryptografie in Meier und Stormer 2012).

Der Organisator Bob prüft die Nachricht von Alice mit verifyVoter(Alice) und signiert $C_{Alice}(\text{hash}(V))$ mit seiner Unterzeichnungsfunktion S (signing function),

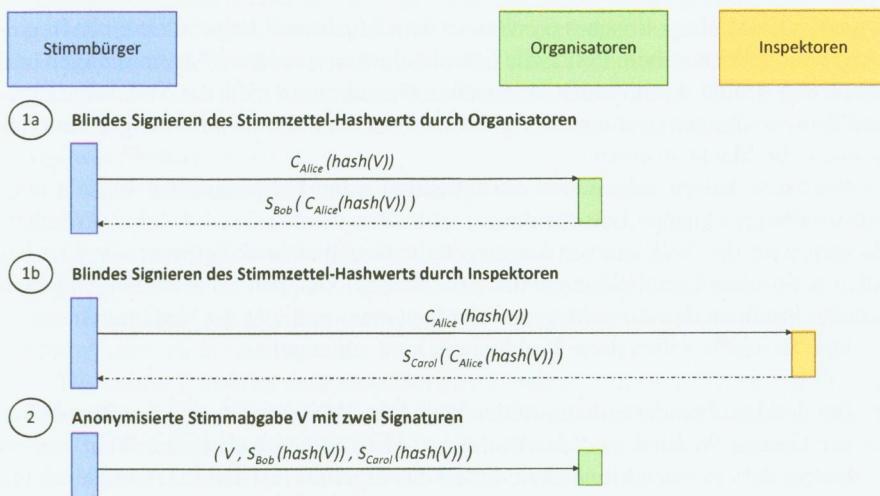


Abb. 16.3 E-Voting-Protokoll mit blinden Signaturen, angelehnt an Liu und Wang (2017)

falls Alice als Wählerin registriert ist. Danach schickt er $S_{Bob}(C_{Alice}(\text{hash}(V)))$ an Alice zurück, natürlich verschlüsselt mit dem öffentlichen Schlüssel von Alice.

Alice holt nun die blinde Unterschrift von der Inspektorin Carol auf analoge Art und Weise ein (siehe Fall 1b in Abb. 16.3). Sie verfügt danach über die beiden blinden Unterschriften, je eine vom Organisator Bob und je eine von der Inspektorin Carol.

Die Stimmabgabe von Alice kann anonym erfolgen, indem Alice die beiden Signaturen $S_{Bob}(\text{hash}(V))$ und $S_{Carol}(\text{hash}(V))$ extrahiert und die beiden Signaturen zusammen mit dem Original ihres Stimmzettels einreicht. Für die Extraktion muss sie lediglich die inverse Berechnungsfunktion für blinde Signaturen C^{-1} anwenden, d. h. $S_{Bob}(\text{hash}(V)) = C^{-1}_{Alice}(S_{Bob}(C_{Alice}(\text{hash}(V))))$ resp. $S_{Carol}(\text{hash}(V)) = C^{-1}_{Alice}(S_{Carol}(C_{Alice}(\text{hash}(V))))$.

Die hier aufgeführten Schritte wie das Einholen von Signaturen oder das anonyme Abstimmen werden in der Blockchain abgelegt. Manipulationen an digitalen Stimmzetteln werden damit verhindert. Die Stärke des vorgestellten Protokolls von Liu und Wang (2017) liegt darin, dass die Verwaltung der digitalen Stimmzettel mit der Blockchain-Technologie für Transparenz sorgt. Mit anderen Worten können jederzeit die Wähler verifizieren, ob ihre Stimmen gezählt wurden (individuelle Verifizierbarkeit). Zudem kann das endgültige Stimmresultat, das vom Organisator berechnet und publiziert wurde, z. B. von der Inspektorin Carol überprüft werden (universelle Verifizierbarkeit). Weitere Audits lassen sich bei Bedarf durchführen.

Neben der Offenheit einer Blockchain ermöglichen die blinden Signaturen, dass die Wähler ihre Stimmen anonym abgeben können (siehe Forderung der Privacy). Mit anderen Worten kann niemand eine Verbindung zwischen einem Stimmzettel und einem Wähler rekonstruieren und die Wählerschaft bleibt geschützt.

16.6 Überwindung politischer Krisen durch Fuzzy Voting

Demokratie ist ein politisches System, in dem Macht und Legitimität einer Regierung vom Volk ausgehen. Politische Entscheidungen werden in Abstimmungen und Wahlen getroffen. In direktdemokratischen Demokratien trifft das Volk seine eigenen Entscheidungen, während in repräsentativen Demokratien die Bürger Vertreter wählen, die Macht ausüben.

Politische Krisen zeigen sich am stärksten, wenn bei politischen Wahlen oder Abstimmungen knappe Entscheidungen getroffen werden. Nach solchen Entscheidungen wird das Volk in zwei Lager geteilt: Gewinner und Verlierer. Dies ist bei allen politischen Entscheidungen der Fall, aber bei knappen Entscheidungen geben wenige Stimmen den Ausschlag, wer der Gewinner und wer der Verlierer ist.

Drei Beispiele sollen diese Problematik kurz aufzeigen:

- Bei den US-Präsidentswahlen vom Jahr 2000 standen sich der Republikaner George W. Bush und der Demokrat Al Gore gegenüber. Die Wahl war so knapp, dass es einen Monat dauerte, bis das Ergebnis feststand. Al Gore erreichte mehr Volksstimmen (50.999.897 insgesamt) als Bush (50.456.002 Stimmen), aber George W. Bush gewann mehr Wahlmännerstimmen und wurde zum Präsidenten gewählt.

- In der Schweiz wurde 2014 die Volksinitiative ‚Gegen Masseneinwanderung‘ zur Abstimmung gebracht. Diese Initiative weist den Gesetzgeber an, die Einwanderung von Ausländern in die Schweiz durch jährliche Quoten zu begrenzen. Mit einer Beteiligung von 56,57 % erreichte die Initiative eine Volksmehrheit von 50,3 % und eine Mehrheit der Kantone (eine Volksinitiative wird angenommen, wenn die Mehrheit der Stimmberchtigten wie die Mehrheit der Kantone sie genehmigt). Bei dieser Abstimmung gaben 19.302 Stimmen (0,6 %) den Ausschlag zur Annahme der Initiative, davon 1.463.854 Stimmen für Ja und 1.444.552 für Nein.
- Bei der Brexit-Abstimmung von 2016 haben die Bürger Großbritanniens darüber abgestimmt, ob ihr Land in der Europäischen Union bleiben soll oder nicht. Die Beteiligung betrug 72,2 %. Der Rückzug des Vereinigten Königreichs aus der EU wurde von 51,9 % der Wähler unterstützt, d. h. von etwa 17,4 Millionen oder 37,4 % der wahlberechtigten Wähler. 48,1 % stimmten für den Verbleib in der EU. Interessant sind auch die Ergebnisse in den jeweiligen Regionen: Unter den Brexit-Anhängern stimmte England mit 53,3 % für den Rücktritt und 46,7 % für den Verbleib, während Wales mit 52,5 % für den Rücktritt und 47,5 % für den Verbleib stimmte. Unter den EU-Befürwortern stimmte Nordirland mit 44,2 % für den Brexit und 55,8 % dagegen, während Schottland mit 38 % für den Brexit und 62 % dagegen stimmte.

Was sagen uns diese drei Beispiele? Bei politischen Wahlen oder Abstimmungen ist es oft so, dass die Wahl der politischen Vertreter knapp ausfallen kann oder dass die Befürworter und Gegner eines politischen Programms beinahe im Gleichgewicht sind. In diesen Fällen gibt es einen Graben in der Bevölkerung und das Vertrauen in demokratische Prozesse kann darunter leiden.

Was könnte man besser machen? Enge Entscheidungen führen zu einer polarisierenden Gesellschaft, die sich in gegensätzliche Lager mit gegensätzlichen Ansichten teilt. Die Ursachen für eine solche Entwicklung liegen unserer Meinung nach im demokratischen Wahlsystem selbst, da es auf einer Dichotomie basiert. Als Wahloption gibt es nur Ja oder Nein, Dafür oder Dagegen, Richtig oder Falsch. Mit anderen Worten: eine komplexe Welt voller Differenzierungen wird in Schwarzweißbilder gepresst. Wozu?

Unserer Meinung nach sollte das dichotome Wahlsystem durch ein differenzierteres Wahlsystem ersetzt werden. Eine Option ist die Fuzzy-Logik von Lotfi Zadeh (1965), die unendlich viele Wahrheitswerte zwischen wahr und falsch erlaubt. Mit anderen Worten, die Fuzzy-Logik erlaubt Grautöne und überwindet die Dichotomie. Zusätzlich zur Option ‚entweder oder‘ ermöglicht die Fuzzy-Logik auch die Option ‚sowohl als auch‘.

Die Fuzzy-Logik ist dem menschlichen Denken, Sprechen, Verhalten und Handeln näher als die klassische Logik, die nur zwischen richtig und falsch unterscheidet. Der Forscher Paulo Côrte-Real brachte diesen Konflikt 2007 in einem wissenschaftlichen Papier mit dem Titel ‚Fuzzy voters, crisp votes‘ zum Ausdruck (Côrte-Real 2007). Damit meinte er, dass Menschen mit differenzierten Bewertungen zu einer scharfen Wahl oder zu einer scharfen Abstimmung verdammt sind. Er

nannte die jeweiligen Abstimmungssysteme Binary Choice Voting Systems und plädierte für Fuzzy Voting.

Ein fiktives und einfaches Beispiel ist in Abb. 16.4 dargestellt. Insgesamt 21 Bürger stimmen über ein politisches Projekt ab. Im ersten Fall von Crisp Voting zählen wir 11 Stimmen für Black und 10 Stimmen für White; das Projekt wird mit 52,4 % abgelehnt. Im zweiten Fall einer unscharfen Abstimmung (Fuzzy Voting) sind 4 Bürger für Black, 7 für White und 6 für Fifty-Fifty, d. h. zur Hälfte für White und zur Hälfte für Black. Zudem sind 4 Wähler für White mit 75 % und für Black mit 25 % (0,75 für White und 0,25 für Black). Als Endergebnis erhalten wir für White eine Zustimmung von 61,9 %.

Warum ändert sich das Abstimmungsverhalten von der Ablehnung (Crisp Voting mit 52,4 % für Black) zur Zustimmung (Fuzzy Voting mit 61,9 % für White)? Eine mögliche Erklärung liegt darin, dass viele Bürger grundsätzlich für ein Projekt sind („Etwas sollte verbessert werden!“), wenn auch mit Vorbehalten. Daher befürwortet die Mehrheit der Wähler, die Schwarz-Weiß-Klischees vermeiden wollen, zur teilweisen Annahme der politischen Initiative, obwohl sie gleichzeitig auch Verbesserungen anstreben. Wenn es sich bei einer Abstimmung um eine Konsultativabstimmung handelt, könnten im Nachgang eine Reihe von Mängeln behoben werden, falls die Kommentare von Befürwortern (100 % für White), Gegnern (100 % für Black) und Grautonwählern (zu einem bestimmten Grad für White, zu einem bestimmten Grad für Black) analysiert würden.

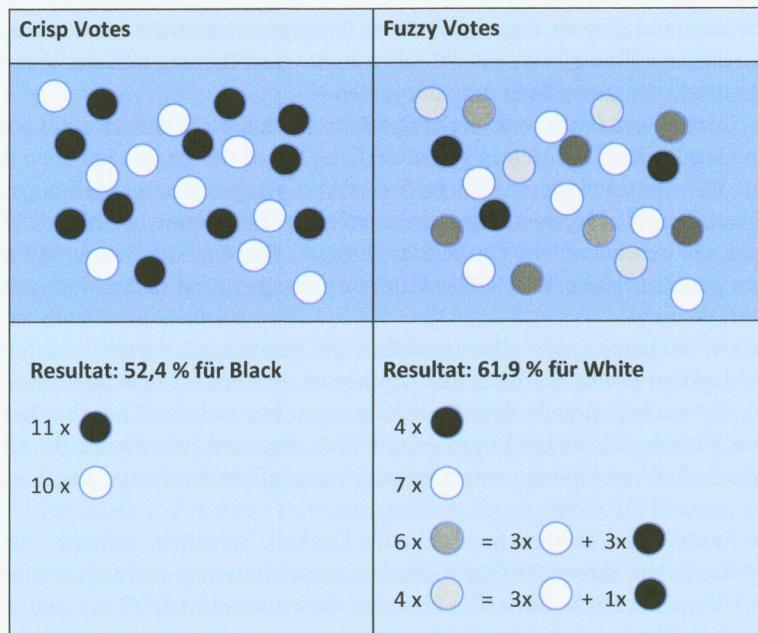


Abb. 16.4 Unterschiede zwischen scharfem und unscharfem Abstimmungsverhalten, basierend auf Ladner und Meier (2014)

Frage: Sollten wir nicht unserer Demokratie Sorge tragen und beispielsweise die Abstimmung mit Grautönen oder andere Alternativen zulassen und damit Erfahrungen sammeln?

16.7 Spannungsfeld zwischen MyPolitics und OurPolitics

Bei der Nutzung der Blockchain-Technologie für elektronische Wahlen wird immer wieder betont, wie wichtig die Anforderung des Stimmgeheimnisses für die Wähler ist. Allerdings stellt sich im Zeitalter der Digitalisierung die Frage, ob nicht differenziertere Wege bezüglich offener und geheimer Wahl beschritten werden sollten. Wichtig scheint uns jedenfalls, dass der Bürger selbst entscheiden kann, ob er geheim oder offen abstimmen möchte. Eventuell werden gar differenzierte Optionen mit der Hilfe eines Filters angeboten, um den Kreis derjenigen Nutzer zu bestimmen, die auf Teile des eigenen Profils sowie auf Teile des eigenen Stimmverhaltens zugreifen dürfen (Kaskina 2018; Meier et al. 2018).

Ladner und Meier (2014) schlagen für die digitale Gesellschaft vor, das demokratische Zusammenleben in einer Gemeinschaft neu zu erfinden. Sie plädieren für zwei sich ergänzende Optionen für die Bürgerinnen und Bürger: MyPolitics und OurPolitics. MyPolitics geht von den persönlichen und individuellen Partizipationsrechten aus, wobei OurPolitics die kollektiven und deliberativen Teilnahmemöglichkeiten betrifft (vgl. Abb. 16.5).

Bürgerinnen und Bürger, die regelmäßig elektronische Abstimmungen oder Wahlen durchführen, können auf dem eGovernment-Portal eine gesicherte Umgebung zu MyPolitics ablegen. In MyPolitics können sie ihre politischen Präferenzen resp. ihr politisches Profil aufgrund eines ausgefüllten Fragebogens deponieren. Daneben können sie eine persönliche politische Agenda aufstellen und sich festlegen, welche politischen Programme sie verfolgen und welche sie gar aktiv

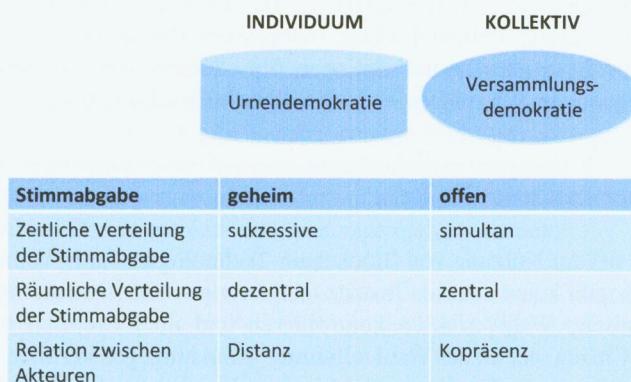


Abb. 16.5 Urnendemokratie versus Versammlungsdemokratie angelehnt an Ladner und Meier (2014)

mitgestalten möchten. Sie kommentieren aktuelle Abstimmungen und Wahlen und legen ihre Stimmabgaben in MyPolitics ab. Eventuell öffnen Sie mit der Hilfe des Privacy Setting Frameworks (Kaskina 2018) ihr politisches Tagebuch oder Teile davon gegenüber einzelnen Familienmitgliedern, Freunden oder Mitgliedern unterschiedlicher Interessensgruppen. Dadurch entstehen Political Communities of Interest.

Möchten sich eCitizens stärker für politische Anliegen engagieren, wählen Sie die Option OurPolitics. Sie hinterlegen ihr politisches Profil halb offen oder offen, wobei sie jederzeit Änderungen oder Ergänzungen vornehmen können. Dank der Offenlegung ihres politischen Profils können sich die eCitizens auf der Webplattform treffen, indem sie Empfehlungssysteme nutzen, die ähnlich gelagerte Profile aufzeigen und entsprechend interessierte Bürgerinnen und Bürger zusammenführen. Damit ergeben sich im besten Fall Political Communities of Practice. Vernetzte Bürgergruppen mit ähnlichen politischen Präferenzen entwickeln gemeinsame Initiativen, investieren Zeit und Wissen und versuchen, ihren Lebensraum aktiv zu gestalten.

Die beiden Optionen MyPolitics und OurPolitics verkörpern zwei unterschiedliche Erwartungen an das gute Funktionieren einer Demokratie (siehe Abb. 16.5). Die Option MyPolitics steht für Möglichkeiten der Urnendemokratie. Dabei entspricht die politische Partizipation einem individuellen Akt, bei dem die Stimme geheim an der Urne abgegeben wird. Die Anhänger von OurPolitics bevorzugen die Versammlungsdemokratie; hier wird der offene Stimmabgabe im kollektiven und interaktiven Prozess nachgelebt. Beide Optionen, MyPolitics wie OurPolitics, haben ihre Vor- und Nachteile (vgl. Schaub 2014). Wichtig bei der Nutzung elektronischer Plattformen ist, dass der eCitizen seine Präferenz wählen kann und nicht vom Staat aufgefordert wird, geheim oder offen abzustimmen.

Dank elektronischer Plattformen und Partizipationsoptionen können fließende Übergänge zwischen MyPolitics und OurPolitics realisiert werden. Der eCitizen allein bestimmt, ob er seine Stimme geheim abgibt oder diese gemäß dem Privacy Setting Framework einzelnen Individuen oder Gruppen (Familie, Freunde, Partei, Arbeitskreis, Interessengruppe etc.) zur Verfügung stellt und kommentiert. Damit ergibt sich ein Spektrum von Handlungsoptionen zwischen der Urnen- und der Versammlungsdemokratie. Politbeobachter, Journalisten, Historiker oder Medienschaffende können diese Partizipationsoptionen der eSociety jederzeit auswerten und damit aufzeigen, wie differenziert sich eine digitale Gesellschaft weiterentwickelt.

16.8 Chancen und Risiken

Die Vorteile bei der Nutzung von Blockchain-Technologien für E-Voting liegen auf der Hand: Es gibt keine zentrale Instanz (Regierungs- oder Verwaltungsstelle), die das elektronische Wahlverfahren kontrollieren und im Extremfall manipulieren kann. Jeder Citizen, der an der Wahl teilnimmt, kann hingegen verifizieren, ob seine Stimme gezählt wurde (Forderung der Verifizierbarkeit). Zudem haben alle Beteiligten Zugriff auf das Stimmergebnis (Forderung der Vollständigkeit).

Der Vorteil, dass ein verteiltes Buchhaltungssystem für Wahlen mit einem entsprechenden Konsensalgorithmus Manipulationen verhindert, kann nicht hoch

genug eingeschätzt werden. Vor allem in Staaten, deren Regierungen zu Korruption tendieren, ist ein unverfälschtes Wahlergebnis ein großes Plus.

Was die Anonymität der Wähler betrifft, so kann diese entweder mit Zero-Knowledge-Proof-Verfahren oder mit blinden Signaturen gewährleistet werden. Allerdings wäre für digitale Gesellschaften das Bereitstellen von Wahlplattformen innovativ, welche das ganze Spektrum zwischen einer anonymen Urnenwahl (My-Politics) und einer offenen Versammlungswahl (OurPolitics) mit diversen Abstufungen anbieten würde. Selbstverständlich könnte jeder Citizen selbst bestimmen, wie weit und an wen er den Inhalt seines Stimmzettels offenlegen möchte.

Eine weitere Option zur Verbesserung der demokratischen Grundrechte könnte darin bestehen, den Stimmenden nicht nur Ja (Wert 1) und Nein (Wert 0) zu offerieren, sondern das ganze Wahlspektrum zwischen 0 und 1. Eine Möglichkeit dazu wäre die Einführung von Fuzzy Voting (Ladner und Meier 2014; Portmann und Meier 2019), bei dem jeder Bürger den Grad seiner Annahme oder Ablehnung eines politischen Programms oder eines Mandatsträgers selbst bestimmen kann.

Erinnern wir uns an knappe Entscheidungen, die die Bevölkerung in zwei Lager dividiert und oft für Jahre hinaus lähmt. Nach unserer Auffassung würden unscharfe Stimmoptionen diese Problematik entschärfen, da meistens nur ein Teil der Bevölkerung in schwarz-weiss denkt und handelt. Ein E-Voting-System, basierend auf Blockchain-Technologie und Fuzzy Voting, wäre prüfenswert.

Blockchain-Technologien bergen auch Risiken, gerade bei der Nutzung von E-Voting. Viele Bürgerinnen und Bürger fragen sich, ob man Datenstrukturen (Kette von Blöcken) und Algorithmen (Konsensfindung) vertrauen kann. Abhängigkeit von Technologie war immer schon eine Bedrohung, obwohl unsere Wirtschaft ohne zuverlässige Informations- und Kommunikationssysteme schon heute nicht mehr überlebensfähig ist.

Von einigen Sicherheitsspezialisten und Forschern im Kryptobereich wird hinterfragt, ob die Blockchain-Technologie das E-Voting vorwärts bringen kann, da viele Fragen der Sicherheit, Anonymität, Gleichheit, Privatsphäre etc. (siehe Anforderungen in Abschn. 16.1) oft mit herkömmlichen Methoden abgedeckt werden und die Blockchain letztlich nur als verteilter Speicher für die Stimmabgaben genutzt wird (siehe z. B. Nasser et al. 2018).

Mit E-Voting basierend auf Blockchain stehen wir jedenfalls am Anfang. Erste produktiv nutzbare Systeme sind entwickelt, erste Blockchain-basierte Wahlen durchgeführt worden und doch gibt es noch weiteres Verbesserungspotenzial. Eines bleibt jedoch unumstritten: So wie sich Gesellschaften aufgrund des technologischen Fortschritts stetig weiterentwickeln, sollten auch demokratische Verfahren hinterfragt und bei Bedarf mit Innovationen angereichert werden.

Danksagung Für die kritische Würdigung meines Kapitels möchte ich mich bei Hans-Georg Fill von der Universität Fribourg sowie bei Rolf Hänni von der Berner Fachhochschule herzlich bedanken.

Literatur

- Bashir I (2017) Mastering blockchain – deeper insights into decentralization, cryptography, bitcoin, and popular blockchain frameworks. Packt Publishing, Birmingham
- Berentsen A, Schär F (2017) Bitcoin, blockchain und kryptoassets. Books on Demand, Norderstedt
- Beutelspacher A, Schwenk J, Wolfenstetter K-D (2015) Moderne Verfahren der Kryptographie – von RSA zu Zero Knowledge. Springer, Heidelberg
- Buterin V (2013) Ethereum white paper – a next generation smart contract & decentralized application platform. [ethereum.org; http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf). Zugegriffen am 24.06.2019
- Chaum DL (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun ACM* 24(2):84–88
- Chaum DL (1982) Blind signatures for untraceable payments. In: Chaum D, Rivest RL, Sherman AT (Hrsg) *Advances in cryptology. Proceedings of the international conference. CRYPTO'82*, Santa Barbara, CA, USA, August 23–25, 1982. Plenum Press, New York, S 199–203
- Cörte-Real P (2007) Fuzzy Voters, crisp votes. *Inter Game Theor Rev* 9(1):67–86
- Craig G (2009, September) A fully homomorphic encryption scheme. PhD Thesis, Stanford University, Pao Alto
- Dagher GG, Marella PB, Milojkovic M, Mohler J (2018) BroncoVote – secure voting system using Ethereum's blockchain. In: *Proceedings of the 4th international conference on information systems security and privacy, ICISSP 2018*, Funchal, Madeira, Portugal, January 22–24, 2018, S 96–107
- Delaune S, Kremer S, Ryan M (2010) Verifying privacy-type properties of electronic voting protocols. In: Chaum D, Jakobsson M, Rivest FL, Ryan PA, Benaloh J (Hrsg) *Towards trust-worthy elections – new directions in electronic voting*. Springer, Berlin, S 274–288
- Hardwick FS, Gioulis A, Akram RN, Markantonakis K (2018) E-voting with blockchain – an E-voting protocol with decentralisation and voter privacy. In: *2018 IEEE international conference on internet of things, IEEE green computing and communications, IEEE cyber, physical and social computing, and IEEE smart data; July 30 till August 3, 2018, Halifax, NS, Canada*. <Https://Arxiv.Org/Abs/1805.10258>. Zugegriffen am 04.02.2019
- Kaskina A (2018, September) A fuzzy-based user privacy framework and recommender system – case of a platform for political participation. PhD Thesis, Faculty of Science, University of Fribourg
- Ladner A, Meier A (2014) Digitale politische Partizipation – Spannungsfeld zwischen MyPolitics und OurPolitics. *HMD Zeitschrift der Wirtschaftsinformatik*, Jahrg. 51, Heft 6, Dezember 2014. Springer, Heidelberg, S 867–882
- Liu Y, Wang Q (2017) An E-voting protocol based on blockchain. *IACR cryptology ePrint archive*. <https://eprint.iacr.org/2017/1043.pdf>. Zugegriffen am 04.02.2019
- McCorry P, Shahandashti SF, Hao F (2017) A smart contract for boardroom voting with maximum voter privacy. https://www.researchgate.net/publication/317843497_A_Smart_Contract_for_Boardroom_Voting_with_Maximum_Voter_Privacy. Zugegriffen am 04.02.2019
- Meier A, Kaufmann M (2019) SQL- & NoSQL-databases: models, languages, consistency options and architectures for big data management. Springer, Heidelberg
- Meier A, Stormer H (2012) eBusiness & eCommerce – Management der digitalen Wertschöpfungskette. Springer, Heidelberg
- Meier A, Stormer H (2018) Blockchain = distributed ledger + consensus. In: Kaufmann M, Meier A (Hrsg) *Blockchain*. HMD Praxis der Wirtschaftsinformatik, Jhrg. 55, Heft 6, Dezember 2018. Springer, Heidelberg, S 1139–1154
- Meier A, Teran L (2019) eDemocracy & eGovernment – stages of a democratic knowledge society. Springer, Heidelberg
- Meier A, Kaskina A, Teran L (2018) Politische partizipation – eSociety anders gedacht. *HMD Praxis der Wirtschaftsinformatik*, Jahrg. 55, Heft 3, Juni 2018. Springer, Heidelberg, S 614–626

- Nasser Y, Okoye C, Clark J, Ryan PYA (2018) Blockchain and voting – somewhere between hype and panacea (a position paper). <https://www.semanticscholar.org/paper/Blockchains-and-Voting-%3A-Somewhere-between-hype-and-Nasser-Okoye/397f569d89af9c35f5fa67c738e2f705bb328368>. Zugegriffen am 04.08.2019
- Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In: International conference on the theory and application of cryptographic techniques, Prague, Czech Republic, May 2–6, 1999, Lecture notes in computer science, Bd 1592. Springer, Berlin, S 223–238
- Portmann E, Meier A (2019) Fuzzy Leadership – Trilogie Teil I: Von den Wurzeln der Fuzzy-Logik bis zu smarten Gesellschaften. essential. Springer Vieweg, Wiesbaden
- Schaub H-P (2014) Landsgemeinde oder Urne – was ist demokratischer? Ein Vergleich der demokratischen Qualitäten von Urnen- und Versammlungsdemokratien in den Schweizer Kantonen. Dissertation der Universität Bern
- Tarasov P, Tewari H (2017) The future of E-voting. IADIS Int J Comput Sci Inform Syst 12(2):148–165
- VEIEs (2018, Juli) Verordnung der Bundeskanzlei über die elektronische Stimmabgabe vom 13. Dezember 2013. Stand 1. <https://www.admin.ch/opc/de/classified-compilation/20132343/index.html>. Zugegriffen am 05.08.2019
- Yu B, Liu J, Sakzad A, Nepal S, Steinfeld R, Rimba P, Au MH (2018) Platform-independet secure blockchain-based voting system. <https://eprint.iacr.org/2018/657.pdf>. Zugegriffen am 04.02.2019
- Zadeh LA (1965) Fuzzy sets. Inform Control 8:338–353
- Zhao Z, Chan THH (2015) How to vote privately using bitcoin. In: Proceedings of the international conference on information and communications security. Springer, Heidelberg, S 82–96

Prof. em. Dr. sc. techn. ETH Andreas Meier war von 1999 bis 2018 Professor für Wirtschaftsinformatik an der wirtschafts- und sozialwissenschaftlichen Fakultät der Universität Fribourg, Schweiz. Seine Forschungsgebiete sind eBusiness, eGovernment und Informationsmanagement. Nach Musikstudien in Wien diplomierte er in Mathematik an der ETH in Zürich, wo er später doktorierte und habilitierte. Er forschte am IBM Research Lab in Kalifornien/USA, war Systemingenieur bei der IBM Schweiz, Direktor bei der Großbank UBS und Geschäftsleitungsmitglied bei der CSS Versicherung.