E-Voting – schon wieder? Das funktioniert doch nicht …

Die Kontroversen um E-Voting sind wohl so alt wie E-Voting selbst, also schon 2-3 Jahrzehnte - je nachdem, was genau man alles unter dem Begriff E-Voting subsummiert.

E-Voting-Systeme verschiedenster Art wurden bereits in vielen Ländern bei offiziellen Wahlen eingesetzt, eine Auflistung dazu findet man etwa hier (englischsprachige Wikipedia).

In Österreich jedoch gibt es bis auf eine als Fehlschlag betrachtete ÖH-Wahl bisher noch keine praktische Erfahrung mit E-Voting. Woran liegt das? Sind wir zu rückständig?

Die nicht-polemische Antwort lautet: nein, wir sind nicht rückständig, sondern – ähnlich wie andere Länder auch, etwa Deutschland, – in dieser Angelegenheit sehr vorsichtig.
Die meisten bisherigen E-Voting-Systeme haben einen großen Haken: mangelnde Transparenz.
Für weitere Einblicke in die Thematik empfiehlt sich die dediziert E-Voting-kritische Plattform papierwahl.at.

… oder doch? Und warum brauchen wir das überhaupt?

These: E-Voting mit hinreichender Manipulationssicherheit und Wahrung der Privatsphäre ist möglich – und wünschenswert. Im nächsten Kapitel wird weiter auf das Wie eingegangen. Doch zuvor kurz zur Frage: wozu überhaupt, wenn wir doch eine funktionierende, erprobte Alternative haben?

Was bei der Diskussion um E-Voting oft unter den Tisch fällt: Die Papierwahl ist auch nicht perfekt und die Briefwahl noch viel weniger, deshalb macht eine differenzierte Auseinandersetzung mit der Thematik Sinn, auch wenn dies anstrengender ist als eine dogmatische Herangehensweise.

Transparenz und Manipulationssicherheit

Wir halten die Papierwahl deshalb für sicher, weil wir die persönliche Erfahrung gemacht haben, dass sie funktioniert. Einzelfälle von (stark begrenzter) Manipulation, wie etwa 2002 in Dachau können als seltene Ausnahme von der Regel verbucht werden.
Die Integrität von Wahlen ist jedoch stark vom gesellschaftlichen Kontext abhängt, in dem sie stattfinden. In vielen nicht-demokratischen und schein-demokratischen Ländern gibt es Wahlen mit oft fragwürdigen Ergebnissen – ob auf Papier oder elektronisch, ist dabei eher zweitrangig.

Anonymität

Sind wir uns sicher, dass im Wahllokal nicht irgendwo eine kleine, hochauflösende Kamera versteckt ist?
Und dass der abgegebene Stimmzettel später nicht auf Fingerabdrücke gescannt wird?

Absolute Sicherheit haben wir nicht. Aber wir halten es für hinreichend unwahrscheinlich – wahrscheinlich haben sich die meisten Wähler über diese Möglichkeiten noch nichtmal

Gedanken gemacht.

Kosten

Ein häufiges Argument für E-Voting sind vermeintliche Kosteneinsparungen.

Die intuitive Schlussfolgerung, dass ein elektronisches System günstiger sein muss, ist nicht zwangsläufig korrekt, wie etwa eine diesbezügliche Analyse um US-Bundesstaat Maryland gezeigt hat.

Überhaupt sollte der Kosten-Aspekt nicht überbewertet werden, da die Kosten von Wahlen im Verhältnis zu den Budgets, über die die Gewählten zu verfügen haben, in der Regel eher vernachlässigbar sind, weshalb eine korrekte Abhaltung auf keinen Fall aufgrund von Kosteneinsparungen gefährdet werden sollte.

Anderes

Weitere potentielle Vorteile von E-Voting-Systemen sind etwa die Geschwindigkeit (Wahlergebnisse schneller verfügbar), Genauigkeit (knappe Papierwahl-Ergebnisse sind oft umstritten, weil Wiederauszählung erfahrungsgemäß meist zu marginal verschiedenen Zahlen führt) und bessere Eignung für Menschen mit Beeinträchtigungen.

Modernität

Der Einsatz von neuen Technologien sollte kein Selbstzweck sein, wenn es um ein so sensibles Thema geht.
Gleichzeitig macht es aber Sinn, Entwicklungen zu beobachten und nach Potential für Verbesserungen Ausschau zu halten.

Das Jahr 2016 war politisch recht turbulent und hat bei vielen die Frage aufgeworfen, ob das demokratische System selbst in einer Krise steckt.
Vor diesem Hintergrund ist vielleicht auch die Frage angebracht, ob es nicht an der Zeit für eine Modernisierung demokratischer Strukturen und Prozesse ist. Dabei geht es nicht um isolierte Fragen wie etwa Papierwahl oder E-Voting, sondern darum, ob und wie wir verfügbare Technologien so einsetzen können und wollen, dass das demokratische Prinzip wieder an Vertrauen und Legitimation gewinnt.
Die Digitalisierung hat viele Lebensbereiche und -gewohnheiten grundlegend verändert. Die Frage, was dies für die Demokratie bedeutet, ist bisher nur ungenügend beantwortet. Brauchen wir eine digitale Version der Agora?

Blockchain + Kryptographie = transparenter als Papierwahl

E-Voting-Systeme können nicht gleichzeitig Transparenz und Anonymität gewährleisten, so lautet ein zentraler und ernstzunehmender Kritikpunkt.

Bei klassischen Wahlcomputern ist dies wohl zutreffend. Mit einer Kombination von aktueller Kryptographie und Blockchain-Technologie ist es aber mittlerweile möglich, E-Voting so zu konstruieren, dass trotz Anonymität die Transparenz höher als bei

Papierwahlen ist. Der englische Fachbegriff für solche Systeme lautet End-to-end auditable voting systems (E2E).

E2E-Systeme nutzen Kryptographie für die Wahrung der Anonymität. Dadurch entfällt die Notwendigkeit, die elektronischen Stimmzettel geheimzuhalten, indem sie in einer unzugänglichen “black box” gespeichert werden, deren korrekter Funktionsweise man vertrauen muss.

Stattdessen werden elektronische Stimmzettel vor der Abgabe vom Wähler verschlüsselt und signiert. Abgegebene Stimmen werden in dieser verschlüsselten Form veröffentlicht. Es ist somit für jeden leicht nachvollziehbar, wieviele Stimmen abgegeben wurden. Wähler können sich außerdem vergewissern, dass der eigene virtuelle Stimmzettel auch darunter ist. Auch die Überprüfung, ob die eigene Stimme korrekt zugeordnet wurde, ist prinzipiell überprüfbar. Diese Eigenschaft will man aber im Allgemeinen nicht, weil Wähler erpressbar werden, wenn es eine Möglichkeit gibt, das eigene Stimmverhalten nachzuweisen. Diese Überprüfung sollte also nur in einem geschützten Rahmen ermöglicht werden, etwa an eigens dafür eingerichteten Stellen.

Wie kann die Stimmberechtigung eines anonymen Wählers geprüft werden?

Der Wähler erhält vor der Stimmabgabe ein von einem elektronischen Wählerregister signiertes Token aus einem elektronischen Wahlregister. Dies könnte z.B. über eine Erweiterung der elektronischen Bürgerkarte oder Handysignatur realisiert werden.

Dieses signierte Token wird Teil des elektronischen Stimmzettels.

Über die Signatur kann verifiziert werden, ob ein Stimmzettel von einem Wahlberechtigten stammt. Durch Verwendung von Blindsignaturen wird gleichzeitig eine Identifizierung des Wählers verunmöglicht.

Warum dann überhaupt den Stimmzettel verschlüsseln?

Prinzipiell wäre eine Verschlüsselung nicht für die Wahrung der Anonymität nötig, weil bereits die Blindsignatur die Identität vom Stimmzettel entkoppelt.

Eine zusätzliche Verschlüsselung gewährt aber folgende Eigenschaften:
- Geheimhaltung des vorläufigen Ergebnisses vor Wahlende (etwa wenn zur Verschlüsselung ein von der Wahlbehörde ausgegebener Schlüssel verwendet wird)

- Nicht-Erpressbarkeit, weil einzelne Wähler nicht nachweisen können, wie sie gewählt haben

Wie können verschlüsselte Stimmzettel verifiziert werden?

Hier kommt fortgeschrittene Kryptographie zum Einsatz.

Mit “zero knowledge proofs” (ZKP) etwa können überprüfbare Aussagen gemacht werden, ohne zugrundeliegende „Klartext“-Daten zu veröffentlichen.
So könnte etwa die Wahlbehörde über solche ZKPs das Ergebnis veröffentlichen. Dieses könnte von jedem verifiziert werden, indem die kryptographische Korrektheit der Aussage

über alle verschlüsselten Stimmzettel hinweg berechnet wird.

Wozu Blockchain?

Eine Schwachstelle von existierenden E2E-Systemen wie z.B. Helios ist, dass für einzelne Wähler zwar überprüfbar ist, ob die eigene Stimme gezählt wurde, nicht aber, ob auch alle anderen Stimmen berücksichtigt wurden.

Wenn davon ausgegangen werden kann, dass genug Wähler ihre eigene Stimme verfolgen und öffentlich machen, wenn diese „verlorengegangen“ ist, wäre dies kein großes Problem. Wenn aber zusätzlich alle verschlüsselten Stimmzettel auf eine öffentliche Blockchain geschrieben werden, wird eine Unterschlagung unmöglich. Der einzelne Wähler (bzw. die auf seinem Gerät laufende Wahl-Software) müsste sich bei der Stimmabgabe nur noch vergewissern, dass die Stimme auch in die Blockchain geschrieben wurde. Dadurch wird für jeden Wähler verifizierbar, ob auch alle anderen „Stimmzettel“ korrekt ausgewertet wurden.

Und die Mathematik?

Wenn von solchen „Trustless“-Systemen die Rede ist, wird immer impliziert, dass man der Mathematik vertraut, die den kryptographischen Verfahren zugrunde liegt.
Diese ist meist so kompliziert, dass nur sehr wenige Menschen zu Recht behaupten können, sie wirklich zu verstehen. Also nicht wirklich transpartent.
Aber ist das wirklich die Art von Transparenz, um die es geht?
Ist dies nicht eher vergleichbar mit dem Wissen, wie Papier hergestellt wird, wie Bleistifte hergestellt werden, und welche chemischen und physikalischen Vorgänge dazu führen, dass der Bleistift auf dem Papier permanent eine sichtbare Markierung hinterlässt?
Wie können wir ohne dieses Wissen sicher sein, dass nicht jemand ein Papier konstruiert hat, bei dem sich die Markierung selbstständig ändert? Oder vielleicht gibt es ja auch Geheimbleistifte, nicht nur Geheimtinten ;-)

Die Frage ist hier möglichweise, ab wann wir Gegebenheiten aus der digitalen Welt mit der gleichen Gewissheit betrachten wie Gegebenheiten aus der materiellen Welt. Akzeptanz für eine Technologie entsteht dadurch, dass sie sich auf Dauer bewährt.

Was ist Blockchain?

„Blockchain“ (Kette von Blöcken) ist eine 2008 mit der Schaffung von Bitcoin eingeführte Technik, mit der erstmals das sogenannte „double spending“-Problem gelöst wurde.

Bitcoin ist die erste Blockchain-Anwendung.

Eine Blockchain ist konzeptuell gesehen eine verteilte Datenbank, die aus einer zeitlich fortlaufenden Folge von Datenblöcken besteht, die miteinander verkettet sind. Diese Datenblöcke enthalten die Transaktionen, die im jeweiligen Zeitfenster angefallen sind.

Die Verkettung erfolgt dadurch, dass jeder Datenblock eine kryptographisch abgesicherte Referenz (implementiert über Hashes) auf den vorausgehenden Datenblock enthält.
Diese Absicherung beinhaltet auch die Transaktionen, die dadurch fälschungssicher werden.

Die Erzeugung von neuen Datenblöcken erfolgt dezentral. Rechner, die Teil des Blockchain-Netzwerks sind, arbeiten an schwierigen kryptographischen Rätseln. Nur durch das Lösen eines solchen Rätsels kann ein gültiger Block generiert werden. Die Schwierigkeit des Rätsels passt sich immer automatisch so an, dass ungefähr die gleiche Frequenz von erzeugten Blöcken pro Zeiteinheit beibehalten wird – bei Bitcoin etwa im Durchschnitt ein Block alle 10 Minuten.

Das Finden eines gültigen Blocks wird mit virtuellem Geld belohnt, außerdem können – je nach Blockchain – auch Transaktionsgebühren an den sogenannten „Miner“ ausgezahlt werden. Dieser wirtschaftliche Anreiz zur Suche nach neunen Blöcken sorgt dafür, dass Blockchain-Netzwerke viel Rechenleistung anziehen – je nach Werthaltigkeit der zugrundeliegenden Crypto-Währung. Die Sicherheit des Netzwerkes ergibt sich daraus, dass das Überprüfen von Transaktionen und Blöcken viel einfacher ist als das Fälschen.

Sobald eine Transaktion in einem Block „verewigt“ wurde, ist sie quasi bis in alle Ewigkeit in Stein gemeißelt. Um eine solche Transaktion zu fälschen, müssten nämlich – aufgrund der kryptographisch abgesicherten Verkettung – alle nachfolgenden Blöcke ebenfalls manipuliert werden. Das wäre nur mit enormem Rechenaufwand möglich – der Manipulator müsste über mehr als die Hälfte der Gesamtrechenleistung des Netzwerks verfügen.

Das Auftauchen von Bitcoin hat einen verstärkten Fokus auf Kryptographie und verteilte Netzwerke bewirkt. Teilweise wurden für bereits bekannte, aber bisher nur in akademischen Kreisen relevante Technologien neue Einsatzbereiche gefunden, teilweise wurden und werden neue Technologien entwickelt. Gerade im Ethereum-Ökosystem findet laufend viel Innovation statt, siehe z.B. ethresear.ch.
Ein wichtiger Meilenstein in der Weiterenwicklung der Blockchain-Technologie war und ist der Umstieg auf sogenannte Proof-of-Stake-Algorithmen. Diese ermöglichen gleiche oder sogar höhere Netzwerk-Sicherheit ohne den immensen Stromverbrauch, der Proof-of-Work-basierten Algorithmen – wie z.B. von Bitcoin verwendet – innewohnt.
Die Ethereum-Blockchain wird mittelfristig von Proof-of-Work auf Proof-of-Stake umsteigen. Einige kleinere Blockchain-Netzwerke wie z.B. das Ethereum-basierte ARTIS benutzen bereits heute Proof-of-Stake.

Im Laufe der vergangenen Jahre wurde zunehmend besser verstanden, was die Erfindung der Blockchain konzeptionell bedeutet. Es wird damit möglich, weit über digitales Geld hinaus ein „Internet der Werte“ zu bauen. Bisher waren für den digitalen Transfer von Werten zentrale Vertrauensinstanzen nötig. Die Überweisung von digitalem Geld etwa wird klassisch über zentrale, hoch gesicherte Server, gesteuert. Solche Zentralisierung schafft immer ein Machtgefälle und damit Potential für Missbrauch verschiedenster Art, etwa Zensur, Manipulation, Wucher usw.

Mit der Blockchain besteht jetzt die Möglichkeit, dezentrale Finanzsysteme, Versicherungen, Notariate, Grundbücher, Rechtsprechungen, Wahllokale, usw. zu bauen.

Obwohl das Thema gerade sehr präsent ist, befindet sich die Technologie noch immer in

einer frühen Phase – vergleichbar etwa mit dem Internet Anfang der 00er Jahre.

Was ist diese Web-Applikation?

„Die unendliche Wahl“ ist eine Hommage an die österreichische Bundespräsidentenwahl 2016.

Diese Applikation ist eine einfache technische Demonstration für eine Blockchain-basierte Online-Wahl. Die grafische Oberfläche wurde möglichst schlicht und verständlich gehalten, während im Hintergrund mit Ethereum sehr ausgefeilte Technologie zum Einsatz kommt.

Die vorliegende Implementierung basiert auf anonym abgegebenen Stimmen, bei denen der digitale Stimmzettel verschlüsselt ist. Dies gewährleistet, dass erst am Wahlende ausgezählt werden kann.

Die Authentifizierung ist noch nicht implementiert.

Es fehlt auch noch die Implementierung eines Backend-Services, das ein elektronisches Wahlregister abbildet.

Diese Online-Wahl zu Demonstrations-Zwecken läuft in einer Schleife immer weiter, wobei die Abstimmung täglich (um Mitternacht) neugestartet wird..

Wie würde eine fertige Wahl-Applikation aussehen?

Eine einsetzbare Version müsste vor allem Benutzer authentifizieren und ihre Wahlberechtigung prüfen.

Die Authentifizierung könnte zum Beispiel über die Handysignatur erfolgen. Anschließend müsste über ein elektronisches Wählerregister sichergestellt werden, dass eine Wahlberechtigung vorliegt.

Die Anonymität bei der Stimmabgabe könnte dadurch gewahrt werden, dass Wähler das zufällig erzeugte „Token“ verschlüsselt an das elektronische Wählerregister senden und von diesem signieren lassen – eine sogenannte „Blindsignatur“.

Bei Stimmabgabe würde dann ein smart contract der Blockchain überprüfen, ob das Token gültig signiert ist. Die Ethereum-EVM erlaubt seit dem Byzantium-Hardfork effiziente Signatur-Überprüfung.

Bleibende Probleme

Eine solche Lösung wäre noch nicht sehr erpressungs-resistent, weil jede Transaktion einen ausgehenden Account hat und über die Kenntnis des dazupassenden privaten Schlüssels die Urheberschaft bewiesen werden kann.

Auch die Anonymität wäre in einem naiven Setting noch nicht optimal, etwa weil ein Blockchain-Node die IP-Adressen zu eingehenden Transaktionen aufzeichnen und rückverfolgen könnte. Dies ließe sich zum Beispiel über Verwendung des Tor-Netzwerkes

oder Wahl eines Blockchain-Nodes des Vertrauens vermeiden.

Ein potentielles Problem ist auch die Vertrauenswürdigkeit von gängigen Endgeräten. Eine Schadsoftware auf dem Gerät des Wählers könnte – potentiell unbemerkt – das Wahlverhalten beliebig manipulieren und/oder ausspähen.
Die Manipulation wäre immerhin nicht unbemerkt, weil der einzelne Wähler sich aufgrund der Transparenz des Systems nach Stimmabgabe vergewissern kann, ob der abgegebene Stimmzettel wirklich der eigenen ausgedrückten Intention entspricht.
Ausspähung hingegen könnte auch unbemerkt geschehen.

Noch problematischer ist, dass in so einem System der massenhafte Ankauf von digitalen Stimmzetteln wesentlich erleichtert würde. Eine mögliche Strategie dagegen könnte sein, Widerstandsfähigkeit durch Vielfalt der eingesetzten Client-Software zu erreichen. So könnte z.B. jeder Wahlsprengel (oder wie auch immer eine Untereinheit im digitalen Raum genannt würde) eine eigene Client-Software zur Verfügung stellen.

What next?

Die aktuell verfügbaren Zutaten in Form von Kryptographie und Blockchain laden dazu ein, den Möglichkeitsraum etwas genauer zu erforschen. Kurzfristig könnte Online-Voting vor allem als Alternative zur Briefwahl in Erwägung gezogen werden.

Auf technischer Seite sollte die Frage im Mittelpunkt stehen, wie man die Risiken in Bezug auf unsichere Endgeräte und Stimmenkauf minimieren kann.

Längerfristig sollte der Fokus vielleicht darauf liegen, zu erforschen, welche zeitgemäßen Formen von demokratischer Beteiligung eine Digitalisierung dieser Art ermöglichen würde.

Nachdem dies keine technische Fragestellung ist, sollte dafür ein interdisziplinärer Informations- und Ideenaustausch stattfinden. Ergebnisse könnten dann experimentell in begrenztem Rahmen ausprobiert werden.