Sachdokumentation:

Signatur: DS 2313

Permalink: www.sachdokumentation.ch/bestand/ds/2313

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

up!schweiz

Baar, 27 Oktober 2018

BLOCKCHAIN-BASIERTE ABSTIMMUNGEN - EINE ANALYSE

1. Einleitung

In der Schweiz wird das Thema E-Voting seit längerem kontrovers diskutiert. Während die Befürworter die Effizienz erhöhen und die Fehleranfälligkeit des bestehenden Systems verbessern wollen, sehen die Gegner Sicherheitsrisiken und kritisieren die fehlende Nachvollziehbarkeit. Als dritter Weg zwischen dem bestehenden ineffizienten und intransparenten Papiersystem und einem fehleranfälligen zentralisierten Computersystem, könnte ein dezentralisiertes, blockchain-basiertes System dienen, das bereits in einigen Ländern erfolgreich getestet wird.

Im Folgenden stellen wir die Vor- und Nachteile von Papier- und E-Voting einander gegenüber und stellen ein mögliches Konzept für ein Blockchain-Voting-System vor.

Wichtig ist dabei zu beachten, dass die Blockchain nur das Wahlverfahren technisch verbessern kann. Die grundlegende Frage über die Legitimität von Abstimmungen (welche Kompetenzen solle das Individuum überhaupt an die abstimmende Mehrheit abgeben?) werden dabei nicht tangiert.

2. Herkömmliches E-Voting (ohne Blockchain)

Anbei haben wir die wichtigsten Vor- und Nachteile von E-Voting zusammengestellt:

Vorteile	Nachteile
• Einfacheres, besseres Wahlerlebnis (insb. für jüngere Generation) • Höhere Wahlbeteiligung • Kostensenkung • Reduktion von Fehlern (z.B. durch falsches Ausfüllen des Wahlzettels)	• Überforderung gewisser Wähler mit der elektronischen Abstimmung • Fehleranfälligkeit von IT-Systemen • Risiken von Hacking und Wahlbetrug • Fehlende Überprüfbarkeit der Resultat («Nachzählen»)

3. Blockchain als Lösung?

Die Problematik des E-Voting manifestiert sich vor allem im Misstrauen gegenüber einem zentralen, intransparenten System («Black Box») das vom Wähler nicht überprüft werden kann. Der Einsatz von Blockchain Technologie ist zu prüfen, da diese genau für jene Art von Problemen besonders gut geeignet ist.

Doch welche Probleme löst Blockchain genau und wie?

1. Eine klassische Blockchain (wie zum Beispiel die Bitcoin Blockchain) besteht aus einer Aneinanderreihung von Datenblöcken, welche durch ein Verschlüsselungssystem so miteinander verknüpft sind, dass der davorliegende Daten-Block nicht mehr verändert werden kann ohne den nachfolgenden Block ebenfalls zu verändern. Dadurch wird eine Datenbank geschaffen, welche im Vergleich zu einer herkömmlichen Datenbank extrem fälschungssicher ist. Die Blockchain könnte somit zur Speicherung von Wählerstimmen und der nachträglichen Überprüfbarkeit der Ergebnisse dienen.
2. Die «Distributed Ledger Technologie» (oftmals mit fälschlicherweise mit dem Begriff Blockchain gleichgesetzt) sieht vor, dass die Daten nicht auf einem zentralen Server, sondern gleichzeitig auf einer Vielzahl von Computern gespeichert werden. Jeder Wähler könnte somit sämtliche Wahlzettel auf seinem eigenen Computer speichern und somit das Wahlergebnis jederzeit selbst überprüfen.

Ein dezentralisiertes System kann somit die positiven Elemente von Papier-Voting und E-Voting verbinden:

	Papier-Voting	E-Voting	Blockchain-Voting
Dezentralisiert Kein zentraler Punkt, welcher angegriffen werden kann			
Elektronisch Effizient, günstig, benutzerfreundlich			

4. Ein mögliches blockchain-basiertes Abstimmungsmodell

Achtung: die vorliegende Abhandlung setzt grundlegende Kenntnisse der Blockchain Technologie, Cryptographic Hashing und DLT voraus. Die Grundlagen dieser Technologien zu erörtern würde den Rahmen dieses Papiers sprengen.

Im von uns vorgeschlagenen Modell wird das ganze Abstimmungsverfahren auf zwei separate Blockchains registriert: Eine Stimmrechts-Blockchain und eine Abstimmungs-Blockchain.

Dass die ganze Abstimmung auf der Blockchain registriert wird, heisst nicht, dass die Abstimmung künftig nur noch elektronisch erfolgen soll. Jeder Stimmbürger soll die Wahl erhalten, ob er weiterhin papierbasiert oder neu elektronisch abstimmen will:

1. Stimmrechts-Blockchain

Der erste Teil des Modells ist der Registrierungsprozess. Die Verifizierung des Wählers ist unerlässlich für die Schaffung eines sicheren Systems. Es geht darum, sicherzustellen, dass die Identität des Wählers nicht von jemand anderem missbraucht werden kann.

Vor einer Abstimmung erhalten die Stimmberechtigten einen Stimmrechtsausweis per Post oder verschlüsselt eine hinterlegte E-Mail-Adresse. Darin erhalten ist ein Passwort («Private Key») das sie zur Stimmabgabe für diese spezifische Abstimmung oder Wahl berechtigt.

Anschliessend werden die stimmberechtigten Personen in einer Stimmrechts-Blockchain registriert.

Jeder Stimmbürger kann die Stimmrechts-Blockchain einsehen. Er sieht nur die verschlüsselten Informationen und keine Namen und Adressen der Stimmberechtigen. Er kann jedoch nachprüfen, wie viele Stimmrechtsausweise insgesamt versendet wurden.

Die Stimmrechts-Blockchain selbst enthält keine Wahlresultate. Sie dient nur dazu, zu überprüfen, ob alle abgegebenen Stimmen von berechtigten Wählern abgegeben wurden.

2. Abstimmungs-Blockchain / Wahlkreise und / Wahlbüros

Für die Abstimmung selbst werden drei verschiedene Stufen verwaltet:

- Die nationale Abstimmungs-Blockchain
- Die kantonalen und regionalen Wahlkreise
- Die lokalen Wahlbüros

Die nationale Abstimmungs-Blockchain ist eine dezentrale Datenbank, auf welcher alle abgegebenen Stimmen abgespeichert sind. Die abgebenden Stimmen werden mit einem komplexen Passwort verschlüsselt, welches nur den Wahlkreisen bekannt ist. Nach der Abstimmung werden die Wahlkreise ihre Passwörter veröffentlichen und die Stimmen auf der Blockchain können ausgezählt werden. Wichtig: Wer im Besitz dieser Passwörter ist, kann zwar die Stimmen auszählen, sie aber nicht manipulieren. Die abgegebenen Stimmen sind unveränderlich auf der Blockchain abgespeichert.

Die nationale Abstimmungs-Blockchain wird durch eine Gruppe von Servern verwaltet. Diese Server können bei staatlichen Stellen als auch bei staatlichen und privaten Unternehmen und

bei Einzelpersonen untergebracht sein (z.B. Swisscom, Post, Bund, Kantone etc.). Durch einen dezentralisierten Konsens-Mechanismus wird sichergestellt, dass keine Partei die Daten auf der Blockchain manipulieren kann (nur wenn sich Bund, Kantone und viele Unternehmen gegen die Demokratie verschwören würden, wäre eine Manipulation möglich).
Jeder Wahlkreis produziert vor den Wahlen ein zufälliges Master-Passwort («Private Key»).

Aus diesem Private Key werden durch einen Hashing-Algorithmus einen «Public Key» chiffriert, welche dann den lokalen Abstimmungsbüros zur Verschlüsselung der Wählerstimmen abgegeben wird. Mit diesem Public Key können die Wahlbüros die abgegebenen Wählerstimmen verschlüsseln, bevor sie diese an die Abstimmungs-Blockchain melden. Sollte ein Public Key gehackt werden, könne die Wahlergebnisse eines Abstimmungsbüros vorzeitig bekannt werden. Sollte ein Private Key gehackt werden, können die Abstimmungsergebnisse eines ganzen Wahlkreises vorzeitig ausgezählt werden. Eine Veränderung der Stimmabgabe ist jedoch auch dann nicht möglich.

3. Stimmabgabe

Am Tag der Stimmabgabe geht der Wähler wie bisher zu seinem Wahlbüro (oder er gibt seine Stimme brieflich oder per E-Mail an den Wahlkreis ab). In allen Fällen benötigt er dazu:

- Seine ID / Pass
- Sein Passwort (welches er vor der Wahl vom Einwohneramt erhalten hat)
- Seinen Stimmzettel (welchen er vor der Wahl vom Wahlkreis erhalten hat)

Wichtig: Der Stimmbürger kann seine Stimme nur beim eigenen Wahlkreis abgeben. Jeder Wahlkreis verfügt über eine eigene Internetadresse. Es gibt keine zentrale Stelle, welche die Stimmzettel und die Stimmabgabe verwaltet.
Das Wahlbüro, welches gleichzeitig die Funktion eines lokalen Knotens in einem dezentralen Netzwerk des gleichen Wahlkreise einnimmt, nimmt die Stimme entgegen. Als nächstes wird das Wahlbüro auf der Stimmrechts-Blockchain überprüfen, ob der Wähler wirklich stimmberechtigt ist und ob er seine Stimme nicht bereits per E-Mail, schriftlich oder in einem anderen Wahlbüro abgegeben hat.

Sollte das Wahlbüro die abgegebene Stimme für gültig befunden haben, so wird die Stimme als elektronische Transaktion an alle anderen Knoten im selben Wahlkreis übermittelt, welche ebenfalls eine Verifikation vornehmen. Erst wenn sich die Mehrheit der Knoten einig sind, wird die Stimme verschlüsselt und an die nationale Abstimmungs-Blockchain gesendet und dort festgeschrieben. Gleichzeitig wird eine Transaktion an die Stimmrechts-Blockchain gesendet, damit der Wähler seine Stimme kein weiteres Mal abgeben kann:

4. Auszählung

Nach Schliessung der Wahlurnen werden die letzten Transaktionen verifiziert und auf der Abstimmungs-Blockchain registriert. Danach publizieren alle Wahlkreisknoten ihre Private Keys. Mit diesen können alle abgegebenen Stimmen entschlüsselt werden und die Stimmen können durch einen Computer ausgezählt werden. Da die Stimmen elektronisch und öffentlich verfügbar sind und auch die Private Keys öffentlich gemacht werden, kann jeder Bürger die Stimmen mit seinem eigenen PC nachzählen. Einen Rückschluss auf die Person, welche die Stimme abgegeben hat ist nicht möglich, da diese Daten nicht auf der Abstimmungs-Blockchain gespeichert werden.

5. Beurteilung der Sicherheit

Das vorgeschlagene System scheint uns deutlich sicherer und transparenter als das bisherigen System sowie die vorgeschlagenen E-Voting Lösungen. Eine hundertprozentige Sicherheit bietet jedoch auch dieses System nicht. Genauso wie heute jemandem ein Stimmrechtsausweis aus der Post gestohlen werden kann, könnte auch zukünftig jemand das Passwort entwenden. Auch die elektronische Stimmabgabe könnte durch einen Hacker auf einzelnen Computern verfälscht werden.

Allerding dürften solche Angriffe im Vergleich zum heutigen System aufgrund der erhöhten Transparenz und Dezentralisierung viel eher und viel schneller erkannt werden.

Auch eine blockchain-basierte Lösung ist jedoch nur dann sicher, wenn sie korrekt implementiert ist. Um dies überprüfen zu können, muss der verwendete Softwarecode ("Smart Contracts") komplett offen gelegt werden und jeder Bürger muss sich als Node an den Verifizierungsmechanismen beteiligen können, um die Korrektheit des Abstimmungsvorganges überprüfen zu können.

Auch darf nicht (wie in einzelnen Ländern versucht) die Stimme über ein zentrales Portal abgegeben und erst dann auf eine Blockchain geschrieben werden. Dann nämlich würde das zentrale Portal für Hackerangriffe anfällig. Der Schlüssel liegt in der möglichst weitgehenden Dezentralisierung des gesamten Wahl- und Abstimmungsprozesses.

Anwendungsbeispiele (Auswahl):

Zug	Die Stadt Zug hat im Sommer 2018 in einem Pilotprojekt eine Test-Abstimmung mit einer blockchain-basierten Lösung durchgeführt.
Agora	Das Schweizer Unternehmen Agora (https://agora.vote) hat ein blockchain basiertes Wahlsystem entwickelt und dieses bei den Präsidentschaftswahlen in Sierra Leone in 2018 getestet (als Wahlbeobachter parallel zu den herkömmlich durchgeführten Wahlen.
West Virginia	Der US-Bundesstaat West Virginia hat im Frühling 2018 ein blockchain basiertes Wahlsystem via Handy-App eingeführt, allerdings nur für Angehörige des Militärs, welche an einer Wahlteilnahme verhindert waren.
Kolumbien	Die Democracy Earth Foundation hat 2016 in Kolumbien eine Blockchain-Abstimmung zum Friedensvertrag durchgeführt (siehe OECD-Bericht). Die Teilnahme war auf im Ausland wohnhafte Personen beschränkt.
Procivis	Das Schweizer Start-up Procivis entwickelt zusammen mit der ETH eine blockchain basierte E-Voting-Lösung.