Electronic vote using Blockchain driven Identity Management

Matrikelnummer 01023355, 2562 Wörter

(Dated: 30. Juli 2018)

Die technische Umsetzung einer Wahl hat sich in den letzten Jahrhunderten in einem Großteil der europäischen Länder nur marginal geändert. Den amtlichen Stimmzettel durch ein elektronisches Abstimmungsmittel zu ersetzen, erscheint eine zeitgemäße Überlegung zu sein. Das Wählen mithilfe eines Smart Contracs wäre durch die Datenstruktur einer Blockchain, die Sicherheit gewährleistet, eine Option. Wir wollen die zugrunde liegenden Konzepte eines *Ballot Contracts* aufzeigen und dann die gewonnene Erkenntnis nutzen, um das Wählen mithilfe eines Smart Contracts mit der traditionellen Wahl zu vergleichen. Dieser Ansatz führt uns zu der Erkenntnis, dass wir entweder ein hohes Maß an Integrität auf Kosten der Benutzerfreundlichkeit erhalten und damit potentiell Wähler diskriminieren, oder mit Sicherheitsproblemen konfrontiert werden, die uns bereits von der elektronischen Wahl ohne Blockchain bekannt sind. Unsere Erkenntnis bestätigt bisherige Forschungsergebnisse: E-Voting stellt in der derzeit umsetzbaren Form eine Gefährdung der Demokratie dar. Wir sehen dennoch potentielle Einsatzmöglichkeiten in der Zukunft.

Keywords: Electronic Vote, Digital Identity, Blockchain, Smart Contract

I. EINLEITUNG

Die Welt hat sich im Laufe der letzten Jahrzehnte drastisch verändert. Das *Internet of Things - Zeitalter* hat begonnen. Der Einfluss neuer Technologien auf unsere Gesellschaft ist unverkennbar. Die allgemeine Verfügbarkeit des Internets und die Verbreitung von Smartphones waren erst der Anfang. Doch dieser Wandel ist nicht nur auf unser Privatleben beschränkt, diese Änderungen haben auch Auswirkungen auf die Verwaltungsstruktur vieler Staaten. Viele Anträge, für die vor wenigen Jahren noch ein Behördengang erforderlich war, lassen sich heute mithilfe eines *Online Formulars* über das Internet abwickeln. Die Europäische Kommission nennt den *Einsatz der Informations- und Kommunikationstechnologien (IKT) in öffentlichen Verwaltungen in Verbindung mit organisatorischen Änderungen und neuen Fähigkeiten, um öffentliche Dienste und demokratische Prozesse zu verbessern und die Gestaltung und Durchführung staatlicher Politik zu erleichtern*, E-Governance [5]. Doch die Wahlen, das demokratiepolitisch wichtigste Verfahren, haben sich in den letzten Jahren nur marginal geändert.[1] Wahlen sind das grundlegende Entscheidungswerkzeug einer jeden Demokratie. In den meisten Fällen entscheiden wahlberechtigte Staatsbürger über ihre demokratisch legitimierten Repräsentanten. In einer Demokratie gilt es den ordnungsgemäßen Ablauf einer Wahl zu gewährleisten, ansonsten ist die demokratische Legitimation infrage zu stellen. Dies gilt natürlich sowohl für das traditionelle Wählen, als auch für das elektronische Pendant. Einen sehr guten Einblick in das Thema *Electronic Voting* liefern M. Mursi und G. Assassa [1]. Wir werden die dort beschriebenen notwendigen Sicherheitskriterien für das E-Voting als Diskussionsgrundlage verwenden. Wir wollen in der folgenden Arbeit **Blockchain basiertes E- Voting** vorstellen und auf dessen Vor- und Nachteile eingehen. Besonders in den letzten Jahren hat die Verwendung des Begriffs *Blockchain* nahezu inflationären Charakter angenommen. Oft wird dieser Begriff besonders im Zusammenhang mit Kryptowährungen wie Bitcoin oder Ether genannt. Mit dieser Thematik hat Blockchain basiertes E- Voting nur insofern Ähnlichkeiten, als dass die selbe Datenstruktur zugrunde liegt. Eine Blockchain ist ein verteiltes Datenbankmanagementsys-

[1] https://en.wikipedia.org/wiki/Electronic_voting_by_country

tem, das von Satoshi Nakamoto (Pseudonym) vorgestellt wurde [4]. Durch kryptographische Verfahren und der dezentralen Speicherung auf vielen gleichberechtigten Rechnern erhält man eine *byzantine fault tolerant database*. In dieser Datenbank werden getätigte Transaktionen und Programme, sogenannte *Smart Contracts*, gespeichert.

II. METHODOLOGIE

Wir wollen im folgenden Abschnitt Konzepte vermitteln, die für das Verständnis dieser Arbeit notwendig sind.

Privater und öffentlicher Schlüssel

Es seien d_k und e_k *kryptographische* Funktionen mit folgenden Eigenschaften

- $d_k \circ e_k = e_k \circ d_k = id$
- $d_j \circ e_k \neq id$ and $e_k \circ d_j \neq id$ (uvm.)

Wir nennen d_k den privaten und e_k den öffentlichen Schlüssel.

A. Protokoll einer digitalen Signatur

Es seien d_{Alice}, e_{Alice} der private und öffentliche Schlüssel von Alice und m eine Nachricht

1. Alice signiert die Nachricht mit ihrem privaten Schlüssel $c := d_{Alice}(m)$
2. Alice sendet das Tupel (m, c) zu Bob (über einen unsicheren Kanal)
3. Bob besitzt den öffentlichen Schlüssel e_{Alice} von Alice
4. Bob überprüft die Gleichung $m = e_{Alice}(c)$
   (a) Gleichung falsch: Das Tupel (m, c) wurde beim Versenden manipuliert $m \neq e_{Eve}(c) = e_{Eve}(d_{Alice}(m))$
   (b) Gleichung richtig: Integritätsprüfung der Nachricht erfolgreich. Digitale Identität bestätigt.

Eine digitale Signatur ermöglicht die verlässliche Feststellung der Authentizität einer Nachricht. Einerseits kann der Urheber einer Nachricht nicht bestreiten, diese versendet zu haben, andererseits ist es nicht möglich, im Namen eines anderen Nachrichten zu versenden. Dieses Prinzip schützt somit unsere digitale Identität. Nun wollen wir darauf hinweisen, dass eine digitale Signatur *nur* die Authentizität einer Nachricht bestätigt. Wenn wir nun Transaktionen mit unserer Wahlentscheidung (signiert) auf einer öffentlich zugänglichen Datenbank speichern, könnten diese von einem Angreifer mühelos gelöscht werden. Der Einsatz der digitalen Signatur allein bietet für unseren Zweck somit nicht die notwendige Sicherheit.

B. Blockchain

Eine Blockchain besteht aus vielen *verbundenen* Datenblöcken. Jeder Block besitzt einen (fortlaufenden) Index, einen Timestamp, seinen abgeleiteten Hashcode, den Hashcode seines Vorgängerblocks und Daten. Angesichts der Tatsache, dass jeder Block den eigenen und den Hashcode des Vorgängerblocks gespeichert hat, ist eine lückenlose Abfolge der Blöcke gewährleistet. Dies ist die für diese Datenstruktur namensgebende Eigenschaft: Wir erhalten eine *block chain*. Wir wollen diese Datenstruktur im Folgenden grob skizzieren, für eine ausführlichere Charakterisierung empfehlen wir dem interessierten Leser [2][4][7]. Eine Blockchain ist dezentral auf einem Rechnernetz gespeichert. Solange diese Rechner eine exakte Kopie der Blockchain besitzen, ist das Netzwerk im Konsens.

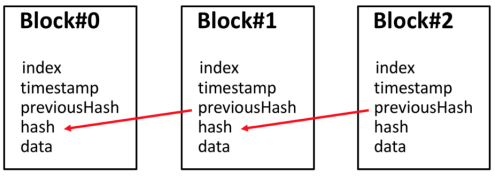

Abbildung 1. Struktur Blockchain

Ausstehende Transaktionen werden von den sogenannten *Minern*, die eine finanzielle Vergütung erwarten, in einem neuen Block zu der Kette hinzugefügt. Für das sogenannte *hashen* ist viel Rechenleistung notwen-

dig[2], deshalb treten die meisten Miner sogenannten *Miningpools* bei, einer großen Gruppe von Minern, um die Varianz des erwarteten Gewinns zu verkleinern.

Der Mining Prozess kann vereinfacht wie folgt dargestellt werden:

1. Neue Transaktionen werden von den Urhebern signiert und an alle Miner versendet
2. Transaktionen werden von den Minern gesammelt
3. Miner sammeln Transaktionen und versuchen einen gültigen hash zu berechnen
4. Ein gültiger Block wird an alle Miner versendet
5. Dieser Block wird von den anderen Minern nur akzeptiert, wenn der
   (a) Hashcode des Blocks korrekt berechnet wurde,
   (b) alle Transaktionen signiert wurden und die
   (c) Datenkonsistenz gewahrt wird.
6. Erfüllt ein Block diese Eigenschaften, so wird dieser von den anderen Minern akzeptiert und der Hashcode des Blocks in die Blockchain aufgenommen.

Relevant ist nun, dass das Erstellen eines neuen Blocks künstlich erschwert wurde - die Kontrolle, ob ein Block ordnungsgemäß erstellt wurde, erfordert nur minimalen Aufwand.
Die Datenkonsistenz der Blockchain wird durch die große Anzahl an Minern gewährleistet. Das *Löschen* von Daten ist nicht möglich. Da alle Transaktionen digital signiert wurden, ist auch eine Manipulation dieser Daten nicht möglich - ein Block mit verfälschten Daten würde von den anderen Minern schlicht abgelehnt werden.

C. Smart Contract

Ein Smart Contract ist ein Programm, das auf einer Blockchain gespeichert ist und dort auch ausgeführt werden kann. Smart Contracts werden meist in der Programmiersprache Solidity geschrieben, die für den Einsatz auf Ethereum entwickelt wurde. Diese Programme werden auf der Ethereum Virtual Maschine betrieben[3]. Mithilfe von Transaktionen kann man gezielt auf Funktionen und Instanzen eines Smart Contracts zugreifen. Die spezielle Struktur der Blockchain garantiert, dass Smart Contracts von den Minern ordnungsgemäß ausgeführt werden. Die Programmintegrität wird dadurch gewährleistet.

D. E- Voting

Elektronisches Wählen beinhaltet jede Form der Stimmabgabe, die mithilfe eines elektronischen Hilfsmittels erfolgt. Wir werden unseren Focus auf Blockchain basiertes E-voting legen. Wir wollen nun ein paar der notwendigen Anforderungen [1], die eine Wahl erfüllen muss, vorstellen.

- Wahlrecht: Stimmabgabe nur möglich mit Wahlberechtigung
- Authentifikation: Feststellung der Identität
- Wahlgleichheit: Nur einmalige Stimmabgabe möglich
- Wahlgeheimnis: Es dürfen keine Rückschlüsse auf die individuelle Stimmabgabe möglich sein
- Transparenz: Der Wähler sollte grobe Züge des Wahlsystems verstehen
- Verifizierbarkeit: Möglichkeit zu prüfen, ob die eigene Stimme korrekt verarbeitet wurde
- Einfach: Wählen muss für jeden Wahlberechtigten möglich sein und darf somit kein besonderes Wissen voraussetzen
- Exaktheit: Das Wahlsystem muss die Stimmen korrekt aufzeichnen
- Integrität: Wahlmanipulation darf nur mit Einschränkungen möglich sein (dh. wenn diese sofort erkannt wird).

[2] Diese Rechenaufgabe wurde künstlich erschwert i.e. Proof of Work

[3] https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial

All diese Kriterien sollten sowohl bei einer traditionellen Wahl mit Stimmzettel, als auch bei einer elektronischen erfüllt sein.

E. Ballot Contract

Ein *Ballot Contract* ist ein Smart Contract, der speziell für die Vorbereitung und Durchführung einer Wahl geschrieben wurde. Ein solches Programm benötigt ein Wählerverzeichnis, in unserem Fall heißt diese Liste *voters*. Diese Liste ist auf der Blockchain gespeichert, deshalb spricht man auch von *Blockchain driven Identity Management*. In das Wählerverzeichnis kann man von einem Wahlbeauftragten eingetragen werden i.e. *giveRightToVote()*.

```
mapping (address => bool) voters;

// has to be Initialized
address chairman;

function giveRightToVote(address newVoter){
        if (msg.sender != chairman){
                voters[newVoter] = true;
        }
}
```

Mithilfe eines sogenannten *modifiers*, der die Identität überprüft, wird gewährleistet, dass nur Menschen mit Wahlrecht auch wählen können. Analog können mithilfe eines Modifiers auch andere Anforderungen überprüft werden. Dies ist wichtig, denn die Funktion *vote()* ist für jeden Benutzer der Blockchain sichtbar.

```
modifier canVote() {
        if (!voters[msg.sender])
                throw;
}

function vote() external canVote  {
        // Vote  here
}
```

III. ERGEBNISSE

Wir wollen nun die technischen Erkenntnisse verwenden, um die ebenfalls beschriebenen Anforderungen, die an E-Voting gestellt werden, zu diskutieren. Dem aufmerksamen Leser ist bestimmt aufgefallen, dass wir bisher nur die Datenbank für elektronisches Wählen beschrieben haben. Der Sicherheitsaspekt ist aber natürlich stark abhängig von der spezifischen Umsetzung, dem Framework, mit dem wir auf der Blockchain operieren. Wir wollen auf zwei verschiedene Implementationsmöglichkeiten einer auf Blockchain basierten Wahl eingehen:

- Supportives Modell: Wahlen werden in einem Wahllokal durchgeführt. Anstatt des Wahlzettels wird mithilfe eines Wahlcomputers, der mit der Blockchain verbunden ist, gewählt.

- Off- booth Modell: Das Wählen ist ortsunabhängig. Der Zugriff auf den Ballot Contract erfolgt z.B. über den Browser.

Wir wollen zuerst auf die Variante mit Wahlcomputer in einem Wahllokal eingehen und werden die beschriebenen Anforderungen behandeln:
Das Supportive Modell ermöglicht doppelte Kontrolle des Wahlrechts. Der Wahlbeisitz sucht, so wie heute, jeden Wahlgänger im Wählerverzeichnis und überprüft somit das Wahlrecht. Der Ballot Contract selbst akzeptiert zudem nur zulässige Wähler.
Ähnlich verhält es sich bei der Authentifikation. Der Wahlbeisitz kontrolliert die Identität des Wahlgängers (mit Hilfe des Passfotos)- zusätzlich ist am Wahlcomputer die Authentifizierung mit dem privaten Schlüssel notwendig. Das Prinzip der digitalen Signatur ermöglicht an diesem Punkt den höchsten Grad an Sicherheit- diese steht in keiner Relation zu der Frage, ob der Wahlgänger dem vorgelegten Passfoto ähnlich sieht.
Selbst ein oberflächliches Verständnis von Smart Contracs und Blockchain Technologie erfordert Fachwissen; ob die erforderliche Transparenz dieses Wahlsystems gewährleistet bleibt, ist zu hinterfragen. Besonders in Zeiten gezielter Desinformation könnte dieses System somit Angriffen ausgesetzt sein. Für schlecht informierte Wähler könnte es sehr schwer sein, den richtigen Schluss zu ziehen.

In Österreich sind ein paar Fälle bekannt, in denen Bürger und Bürgerinnen den Ansatz einer Möglichkeit gehabt hätten, mehr als eine Stimme abzugeben. [4] Ein fehlerfreier Ballot Contract würde dies nicht zulassen. An diesem Punkt möchten wir aber auf den DAO-Bug verweisen, der es einem Dieb ermöglichte, wiederholt sein Konto zu leeren, ohne seinen Kontostand zu verändern [3]. Er erbeutete damit 50 Millionen Dollar. Dieser Bug löste intensive Forschung in der Smart Contracts *Programm Verifikation*[5] aus.

Bei der auf Stimmzettel basierten Wahl ist es üblich, dass von jeder antretenden Partei ein Wahlbeisitz das Auszählen der Stimmen überwacht. So soll gewährleistet werden, dass die Wahlzettel korrekt ausgezählt werden. Bei auf Blockchain basierten Wahlen ist der Ballot Contract öffentlich. Daher ist *jedem* die Funktionsweise bekannt und es kann zumindest die korrekte Evaluation der Wahl als gegeben angenommen werden. Weiters wäre es möglich, von zuhause selbst zu überprüfen, ob die abgegebene Stimme korrekt dokumentiert wurde. Dies erfordert den privaten Schlüssel und steht somit nicht im direkten Widerspruch zum Wahlgeheimnis. Auch wenn diese Option demokratiepolitisch romantisch klingen mag, ist dennoch zu hinterfragen, ob dieses Feature die möglichen negativen Aspekte aufwiegen kann, dh. ob man es letztendlich anbieten möchte. So könnten Wähler sehr leicht genötigt werden, für eine bestimmte Partei zu stimmen. Der Handel von Wählerstimmen könnte sich zu einem Geschäftszweig entwickeln, der nahezu nicht rückverfolgbar wäre.

Das Supportive Modell verändert die technische Anforderung beim Wahlgang nur marginal. Theoretisch könnte sogar ein mechanischer Gegenstand den privaten Schlüssel *speichern*, um den Prozess zusätzlich zu erleichtern. Menschliche Ungenauigkeit, besonders unter dem Einfluss von Stress, wird immer dazu führen, dass marginale Fehler beim Auszählen bzw. bei der Aggregation der Stimmen passieren - das Wählen mit Wahlcomputer ist exakt.

Die Integrität einer E-Vote kann auf zwei verschiedenen Ebenen verletzt werden. Einerseits kann ein Angreifer versuchen, die Datenbank zu manipulieren, andererseits kann das darauf operierende Abstimmungsframework zum Angriffsziel werden. Die Datenstruktur einer Blockchain macht, wie beschrieben, eine Manipulation auf Datenbankebene nahezu unmöglich. Nicht einmal eine sogenannte 51% - Attacke[6] wäre eine ernstzunehmende Gefahr. Diese ist unmöglich geheim zu halten und eine Wahl könnte annulliert werden. Wird der Blockchain ein korrekter privater Schlüssel übermittelt, aber eine, durch Schadsoftware auf dem Wahlcomputer manipulierte Stimme abgegeben, so wird diese akzeptiert. Der Wahlcomputer ist an dieser Stelle das schwächste Glied in der Kette. Dies stellt eine ernstzunehmende Gefahr dar, die vom klassischen elektronischen Wählen ohne Blockchain bereits bekannt ist.

Wir wollen nun unseren Focus auf das Off - booth Modell legen. Manche Argumente stimmen mit den bereits getätigten überein - wir werden diese somit nicht erneut erwähnen. Dieses Modell erfordert keinen Kontakt mit anderen Menschen - gewählt wird mit direktem Zugriff auf die Blockchain, sei es mithilfe eines Programms oder einer Homepage [7]. Dies wirft einige Probleme auf, denn man kann demokratiepolitisch weder verlangen, dass jeder Wähler einen Computer besitzt, noch kann man erwarten, dass jeder die notwendige Medienkompetenz besitzt, um seine Stimme abzugeben. Man vermag nun zu argumentieren, man könne kommenden Generationen abverlangen, den Umgang mit dieser Technologie zu erlernen. Um wählen zu können, muss die Adresse des Ballot Contracts bekannt sein. Diese Adresse müsste somit von Seiten einer staatlichen Institution verbreitet werden - ein Angreifer könnte dies für seine Zwecke missbrauchen und gezielt Missinformationen verbreiten z.B.: Wähler an einer Fake- Wahl teilnehmen lassen und ihnen suggerieren, gewählt zu haben. Der Zugriff auf die Blockchain über den Browser bietet natürlich erneut einen Angriffspunkt, doch durch die große Anzahl an unterschiedlichen Interaktionsmöglichkeiten mit einer Blockchain wäre ein unglaubliches Maß an Integrität gewährleistet.

[4] diepresse.com/home/innenpolitik/nationalratswahl/5292824/
[5] Hoare Logics
[6] i.e. man erlangt die Kontrolle über mehr als 50 % der Miner
[7] vgl. https://remix.ethereum.org

IV. DISKURS UND CONCLUSIO

Beide der von uns beschriebenen Modelle offenbaren Schwächen. Das Supportive Modell kann die notwendige Integrität nicht gewährleisten. Der Wahlcomputer ist ein mögliches Angriffsziel - dadurch sind wir mit einem klassischen Problem der elektronischen Wahl konfrontiert, das durch das Operieren auf der Blockchain nicht gelöst wird. Wahlcomputer bilden ein System von homogenen Rechenanlagen mit nahezu identer Hardware und Softwareausstattung - dies bietet ernstzunehmende Möglichkeiten für einen gezielten Angriff. Wir wollen an dieser Stelle auf [2] verweisen. Das Off- booth Modell bietet ein hohes Maß an Integrität. Diese wird einerseits durch die Datenstruktur der Blockchain gewährleistet, andererseits durch die große Anzahl an verschiedenen Computersystemen, die für das Wählen verwendet werden. Hinzu kommt die Vielfalt an Interaktionsmöglichkeiten mit der Blockchain. Ein gezielter Angriff ist in diesem Fall schwer möglich [6]. Dieses Modell setzt eine solide Medienkompetenz voraus, die heutzutage von einem Gutteil der Bevölkerung nicht erwartet werden kann. Somit würde diese Wahltechnik Bürger mit Wahlrecht diskriminieren und ist demokratiepolitisch nicht tragbar. Es bleibt weiterhin zu hinterfragen, ob diese notwendige Medienkompetenz in Zukunft von einem mündigen Bürger erwartet werden kann, aber auch ob dies überhaupt notwendig ist.

LITERATUR

[1] M. Mursi. G. Assassa. On the Development of Electronic Voting: A Survey. 2013.

[2] E.Wall. G.Malm. Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository. 2016.

[3] I. Sergey. A. Hobor. A Concurrent Perspective on Smart Contracts. 2017.

[4] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

[5] Publications Office. E-government: Elektronische behördendienste, 2003. URL `https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=LEGISSUM:124226b`.

[6] D. Jefferson. A. Rubin. B. Simons. Analyzing internet voting security. 2004.

[7] Y.Liu. Q. Wang. An e-voting protocol based on blockchain. 2017.