Dokumentation Blockchainbasierendes Votingsystem

Inhaltsverzeichnis

Stand der Länder

Estland

Seit 2005 können die Menschen in Estland sowohl das nationale, als auch das europäische Parlament digital wählen.

Das digitale Wahlverfahren läuft in mehreren Stufen ab. Auf einer extra dafür eingerichteten Website identifizieren sich die Wähler mit ihrem Personalausweis oder ihrem Mobiltelefon. Nach der Identifikation können sie aus einer Liste von Parteien und ihren Mitgliedern ihren Wunschkandidaten auswählen. Die Auswahl kann beliebig oft angepasst werden, sodass eine falsche Auswahl kein Problem darstellt. Durch das Bestätigen einer weiteren Kontrollnummer kann die Wahl abgeschickt werden. Hier gilt das Prinzip der letzten Wahl. Bis zum Wahlzeitpunkt kann die Wahl beliebig oft neu abgeschickt werden. Alle älteren Wahlen werden gelöscht. Falls doch noch eine Wahl vor Ort oder per Brief eingeht, werden diese vorgezogen. Über einen QR-Code lässt sich überprüfen, ob die Wahl erfolgreich eingereicht wurde.

Hauptgrund für die Einführung von digitalen Wahlen war eine höhere Wahlbeteiligung durch eine einfachere Durchführung der Wahl zu ermöglichen. Da seit einem Hackerangriff 2007 die Cybersicherheit höchste Priorität hat, machen sich die Wähler kaum Sorgen um ihre Daten. Hinzu kommt, dass die Wahlsoftware für jeden als Open Source einsehbar ist. Estland gilt europaweit als Vorreiter in der Digitalisierung. Heute wählen etwa ein Drittel der Estländer digital.

Schweiz

In der Schweiz steht momentan kein E-Voting-System zur Verfügung, weswegen kein E-Voting möglich ist. In zehn Schweizer Kantonen wurde bis Anfang 2019 E-Voting angeboten. Es stand das System des Kantons Genf und das der Schweizerischen Post zur Auswahl. Beide Systeme wurden mit dem Hinweis auf Verbesserungsmaßnahmen abgeschaltet. Genannt wurden vor allem Sicherheitslücken in den bestehenden Systemen.

Die Bundeskanzlei befindet sich gerade gemeinsam mit den Kantonen in der Erstellung eines neuen E-Voting Konzepts. Hierzu gehört vor allem die Anpassung von rechtlichen Voraussetzungen. Die Abschaltung der Systeme hatte direkte Auswirkungen auf nachfolgende Wahlen. So verringerte sich die Wahlbeteiligung von im Ausland lebenden Schweizern um etwa 10%.

Deutschland

In Deutschland wurden erstmals im Jahr 1999 elektronische Wahlgeräte zur Europawahl eingesetzt. Die damaligen Wahlgeräte wurden jedoch im Nachhinein für ungültig erklärt, da die Wähler nicht einsehen konnten, ob die Wahlergebnisse korrekt ausgezählt wurden. Alle

wesentlichen Schritte einer Wahl müssen in Deutschland öffentlich überprüfbar sein. Das daraus resultierende Urteil verbietet solche Wahlgeräte. E-Voting im Allgemeinen wäre jedoch grundsätzlich möglich.

Ein Hindernis in Deutschland sind fehlende rechtliche Grundlagen. So müssten Gesetze angepasst werden, um Onlinewahlen durchführen zu können. Ein weiteres Problem stellt die erforderliche Akzeptanz der Bevölkerung dar. Im Gegensatz zu Estland besteht bei den Deutschen weniger Vertrauen in die Informationstechnologie. Zudem haben einige Bürger Bedenken beim Umgang mit ihren personenbezogenen Daten.

Wahlarten

Lokale Wahlen

Vorteile:

- Jede Person mit Wahlberechtigung kann teilnehmen
- Im nächstgelegenen Wahlbüro der Wahlberechtigten Person
- Kann offiziell vorzeitig ausgewertet werden
- Gemeinschaft kann Personen zum Wählen animieren
- Fester Termin der Wahlabgabe

Nachteile:

- Bei manchen Personen ist selbst das nächstgelegene Wahllokal weit entfernt
- Personen müssen vor Ort ins Wahllokal kommen
- Wahlzettel können invalide abgegeben werden bzw. invalidiert werden
- Die Gemeinschaft kann leicht Druck auf eine einzelne Person ausüben
- Man ist vom Wahltermin abhängig. Dieser kollidiert oft mit privaten Plänen

Briefwahlen

Vorteile:

- Hat sich in der Vergangenheit bewährt
- Kann von zu Hause aus in Ruhe ausgefüllt werden
- Offizielles Dokument welches Vertrauen schafft
- Geschützt durch das Briefgeheimnis
- Ermöglicht es Zielgruppen, bei denen eine Wahl vor Ort nicht möglich ist, trotzdem wählen zu können

Nachteile:

- Altmodisch, was für jüngere Generationen unattraktiv ist
- Keine kryptographische Sicherung, was Manipulationen erleichtert
- Kann durch staatliche Instrumente gefälscht werden
- Muss beantragt werden
- Brief muss manuell abgegeben werden

Digitale Wahlen

Vorteile:

- Eine automatische Auswertung geht viel schneller als langwieriges - teils notwendiges mehrmaliges - Auszählen von Hand.
- Eine gute und sichere Software macht zudem in der Regel weniger Fehler beim Auszählen.
- Mittel- bis langfristig könnte E-Voting auch Geld sparen. Die Entwicklung und Wartung der technischen Systeme kostet zwar Geld, dafür entfallen auf lange Sicht Ausgaben für den Stimmzetteldruck, mögliche Raummieten für Wahllokale und die Bezahlung für Wahlhelfer.
- Durch bequemes E-Voting wird das Wählen niederschwelliger und mehr ehemalige Nichtwähler geben ihre Stimme ab.
- E-Voting schafft für manche Menschen mit Behinderung überhaupt einen Zugang zur Wahl. Der gegebenenfalls beschwerliche Weg zum Wahllokal wird überflüssig.
- Die Wähler sind bei der Online-Wahl flexibler als bei der Urnenwahl. Sie können ihre Stimme – ähnlich wie bei der Briefwahl – schon vor dem Wahltag abgeben. Außerdem können sie an jedem Ort mit Internetzugang wählen, selbst außerhalb von Deutschland.

Nachteile:

- Mangelnde Transparenz, da selbst Open Source Projekte nur technikaffine Menschen verstehen.
- Hohe Anfangskosten, da die Programmierung einer komplexen Software erforderlich ist.
- Die Gefahr, sich zu verklicken.
- Wahlen und Abstimmungen können durch Hacker manipuliert werden.
- Hardware muss zur Verfügung gestellt werden
- Menschliche Unterstützung bei bestimmten Zielgruppen; Ältere Menschen, Menschen mit körperlichen/geistigen Einschränkungen, usw. erforderlich.

Blockchain

Vorteile:

- Dezentral, deshalb ausfallsicherer als andere Technologien.
- Anonymität ist durch Kryptografie gewährleistet.

- Wahlbetrug ist schwieriger, da um eine Stimme zu manipulieren, die ganze Blockchain bis zur Stimme manipuliert werden muss
- Transaktionssicher, dadurch bleibt eine Stimme permanent auf der Blockchain erhalten
- Erhöhte Sicherheit durch kryptographische Sicherung wie z.B. Zero Trust Proves
- Online verfügbar

Nachteile:

- Hardware muss zur Verfügung gestellt werden
- Benötigt viel Speicherplatz, da eine Stimme auf allen Rechnern in der Blockchain gespeichert werden muss
- Hoher Energie- bzw Rechenaufwand bei neuem Eintrag in der Blockchain
- Nach jeder Transaktion dauert es lange Zeit bis zur synchronisierung

Aktuelle Projekte

Agora

E-Voting-System, welches die Blockchain als Dienst nutzt. Das System wurde in März in Sierra Leone Parlamentswahlen 2018. Agora verwendet einen eigenen Token auf der Blockchain für Wahlen, wo Regierungen und Institutionen diese Token für jeden einzelnen Wahlberechtigten kaufen.

Vorteile:

- TAMPER-PROOF: Stimmzettel und Ergebnisse können nicht von Dritten geändert werden.
- TRANSPARENT: Der gesamte Abstimmungsprozess ist völlig transparent und öffentlich überprüfbar.
- PRIVATE: Die Wahlmöglichkeiten und die Identität der Wähler sind geschützt.
- ACCESSIBLE: Die Wähler können auf moderne, bequeme und faire Weise teilnehmen.
- AFFORDABLE: Die Digitalisierung von Papier und manuellen Prozessen senkt die Wahlkosten.
- TENSION-LESS: Beseitigung der durch fragwürdige Ergebnisse verursachten Gewalt.

Es handelt sich um eine Gruppe, die eine digitale Blockchain-Wahlplattform eingeführt hat. Sie wurde 2015 gegründet und bei den Präsidentschaftswahlen in Sierra Leone im März 2018 teilweise umgesetzt. Die Architektur von Agora basiert auf mehreren technologischen Innovationen: einer benutzerdefinierten Blockchain, einzigartiger partizipativer Sicherheit und einem legitimen Konsensmechanismus. Die Stimme ist der native Token im Ökosystem von Agora. Sie ermutigt Bürger und gewählte Gremien, die als Verfasser von Wahlen weltweit

dienen, sich für einen sicheren und transparenten Wahlprozess einzusetzen. Die Stimme ist der universelle Token des Agora-Ökosystems.

Dieser Test (Präsidentschaftswahlen in Sierra Leone im März 2018) wurde als eine teilweise Einsatz einer Blockchain. Die Wahlen wurden nur durch die Blockchain verifiziert, aber nicht durch die Blockchain betrieben. Agora lieferte eine unabhängige Stimmenauszählung, die mit der Hauptzählung verglichen wurde.

Voatz

Voatz ist eine gewinnorientierte, private Anwendung für die mobile Internet-Wahl. Das erklärte Ziel von Voatz ist es, die Stimmabgabe nicht nur zugänglicher und sicherer zu machen, sondern auch transparenter, überprüfbar und rechenschaftspflichtig.

Voatz nutzt die Blockchain-Technologie und die Biometrie, um die Identität der Wähler zu überprüfen, und verzichtet auf die Speicherung sensibler persönlicher Daten in einer Datenbank. Die Blockchain-Infrastruktur von Voatz umfasst 32 identisch angeordnete Verifizierungsserver, die über Amazons AWS und Microsofts Azure verteilt sind. Auf jedem Server läuft eine identische Kopie von Hyperledger, einer Open-Source-Blockchain-Software.

Der Ablauf für den Wähler

Sobald ein Nutzer die Voatz-App herunterlädt, verifiziert er seine Telefonnummer, legt einen Lichtbildausweis vor und macht ein "Selfie". Gesichtserkennung und Wählerlisten werden verwendet, um die Identität zu überprüfen und eine Übereinstimmung zwischen dem Foto und dem eingereichten Ausweis zu bestätigen. Nachdem dem Nutzer ein sicheres Token (das durch einen Fingerabdruck aktiviert wird) angeboten wurde, das für wählbare Wahlen gilt, werden die biometrischen Daten des Nutzers aus dem Voatz-System entfernt. Nachdem alle Stimmen an Voatz übermittelt wurden, werden die Stimmen auf einen Papierstimmzettel gedruckt und in eine Maschine eingegeben.

Die Voatz-App bietet eine Schnittstelle, die den Verwaltern der Wahl zur Verfügung steht, die Voatz einbezieht. Wahlhelfer können Stimmzettel einsehen, Wähler hinzufügen und bei Bedarf Ergebnisse veröffentlichen. Voatz erlaubt es den Wählern nicht, mit den Blockchain-spezifischen Funktionen der mobilen Anwendung zu interagieren. Anstelle von Wallet-Adressen, Token oder privaten Schlüsseln können die Wähler einen 6-stelligen Code eingeben oder eine biometrische Verifizierung als privaten Schlüssel verwenden.

Schwachstellen:

(MIT-Ingenieure warnen vor Lücken im Voatz-Wahlsystem. Siehe: https://www.blockchain-insider.de/mit-ingenieure-warnen-vor-luecken-im-voatz-wahlsystem-a-911749/)

Die MIT-Ingenieure Michael A. Specter, James Koppel und Daniel Weitzner haben das Voatz-Wahlsystem auf seine Sicherheit hin überprüft. Dazu nahmen die Experten die Voatz-Android-App per Reverse Engineering auseinander und setzen einen eigenen Server auf.

In einem ausführlichen Bericht kommen sie zum Schluss, dass ein Angreifer mit Root-Zugriff auf ein Smartphone die Sicherheitsmaßnahmen des Systems umgehen und Wahlstimmen fast beliebig einsehen und verändern könnte. Zudem kritisieren die MIT-Ingenieure das verwendete Netzwerkprotokoll, das Rückschlüsse auf die Stimmabgabe erlaubt, sowie den fehlenden Schutz vor Server-basierten Attacken.

Polays

Die POLYAS Online-Wahl fand im Sommer 1996 in Finnland mit 30.000 Wahlberechtigten in drei Sprachen statt. Im 2012 entstand das Unternehmen POLYAS GmbH. Im März 2016 wurde Polyas mit der Version CORE 2.2.3. vom Bundesamt für Sicherheit in der Informationstechnik(BSI) zertifiziert und ist die erste Online-Wahlsoftware, die die Anforderungen des internationalen Schutzprofils nach Common Criteria erfüllt. Die Services der POLYAS GmbH werden im POLYAS Online-Wahlmanager zusammengeführt, um intelligente Schnittstellen zwischen der Nominierungsplattform, der Online-Wahl und dem Live-Voting zu ermöglichen und damit die Effizienz für die Wahlleitung weiter zu steigern.

POLYAS gewährleistet das Wahlgeheimnis für die Wahlberechtigten:
Digitale Abstimmungen und Wahlen mit POLYAS sind nicht nur sicher, sie sind auch geheim. Eingeloggte Wahlberechtigte werden mit kryptografischen Verfahren anonymisiert. Gleichzeitig werden die Wahlberechtigten eindeutig identifiziert und authentifiziert, so dass Mehrfachabstimmungen verhindert werden. Außerdem bietet POLYAS verschiedene Möglichkeiten der sicheren Authentifizierung, so dass Wahlveranstalter die Methode wählen können, die zu den Anforderungen des Wahlsystems, dem zugrunde liegenden Sicherheitsniveau und den Bedürfnissen vom Wählerschaft passt.

Mögliche Authentifizierungsmethoden

- Anmeldung mit einer ID und einem Passwort
- SecureLink in dem eigenen Intranet
- Authentifizierung durch digitalen Personalausweis

Unabhängige Überprüfung der Wahlergebnisse

Die Wähler und die Wahlveranstalter können die Richtigkeit der Online-Wahl überprüfen und sich vergewissern, dass die Wahl reibungslos verlaufen ist. Dabei gibt es zwei verschiedene Arten der Überprüfung: die allgemeine Überprüfung und die individuelle Überprüfung.

Die allgemeine Überprüfung ermöglicht es dem Wahlveranstalter, den ordnungsgemäßen Ablauf der Wahl und die Richtigkeit der Stimmenauszählung zu überprüfen. Andererseits kann der Wahlberechtigte durch die individuelle Überprüfung sicherstellen, dass seine Stimme nicht

manipuliert wurde, als sie in der digitalen Wahlurne ankam, und dass sie gezählt wurde. Bei beiden Methoden bleibt das Wahlgeheimnis gewahrt.

Sicherheit bei der Stimmabgabe

Sowohl bei POLYAS CORE 2.5.0 als auch bei POLYAS CORE 3.0 erfolgt die Stimmabgabe ausschließlich über eine TLS-verschlüsselte Verbindung per Serverzertifikat der D-Trust GmbH. Dies verhindert, dass Stimmzettel bei der Übertragung über das Internet manipuliert werden können. Bei POLYAS CORE 3.0 erfolgt die Verschlüsselung auch im Browser des Wählers, um sicherzustellen, dass die Stimmzettel bei der Erstellung, dem Transport und der Speicherung verschlüsselt sind.

Datenschutz bei POLYAS

- Personenbezogene Daten werden immer verschlüsselt übertragen.
- Der Zugang zu all Benutzerdaten ist passwortgeschützt.
- Daten, die zu unterschiedlichen Zwecken erhoben werden, werden getrennt gespeichert

Kaspersky

Kaspersky ist ein globales Unternehmen für Cybersicherheit und digitalen Datenschutz, das 1997 gegründet wurde. Kasperskys tiefgreifende Erkenntnisse über Bedrohungen und seine Sicherheitsexpertise werden ständig in innovative Sicherheitslösungen und -dienste umgewandelt, um Unternehmenskritische Infrastrukturen, Regierungen und Verbraucher auf der ganzen Welt zu schützen. Das umfassende Sicherheitsportfolio von Kaspersky umfasst einen führenden Schutz für Endgeräte sowie eine Reihe von spezialisierten Sicherheitslösungen und -diensten zur Bekämpfung anspruchsvoller und sich weiterentwickelnder digitaler Bedrohungen. Mehr als 400 Millionen Anwender werden durch Kaspersky-Technologien geschützt und wir helfen 240.000 Firmenkunden dabei, das zu schützen, was ihnen am wichtigsten ist.

Die US-Regierung behauptet, dass Kaspersky seine Virensoftware dazu benutzt hat, für die russische Regierung zu spionieren, und verbot die Verwendung seiner Software durch Bundesbehörden.

Am 27. Februar 2020 präsentierte Kaspersky das Projekt Polys.
Polys, ein Projekt des Kaspersky Innovation Hub, das eine sichere Online-Wahlplattform für Unternehmen, Universitäten und politische Parteien entwickelt, hat einen Prototyp seines neuen Voting-Systems vorgestellt. Das System ist das erste seiner Art, das Blockchain-Technologien einsetzt und mit dem Online-Wahlsystem Polys zusammenarbeitet, so dass alle Stimmen - ob sie in Wahllokalen oder auf persönlichen Geräten abgegeben werden, auf sichere Weise übertragen und gemeinsam verarbeitet werden. Dies gibt den Wahlteilnehmern die Möglichkeit zu wählen, wie sie ihre Stimme abgeben wollen, und gewährleistet gleichzeitig, dass die Organisatoren eine sichere Online-Wahloption mit garantiertem Datenschutz einführen können. Die Online-Wahlsoftware wurde bei manchen Wahlen in Russland verwendet. Beobachter haben festgestellt, dass keine Blockchain-Transaktionen von der Website für die Online-Wahl

heruntergeladen werden können und außerdem konnten sie nicht sehen, wie das System von innen funktioniert, und sind daher nicht in der Lage, die Integrität der Wahlen zu bewerten. Die Passdaten der Wähler waren nicht ausreichend geschützt und online verfügbar, was dazu führte, dass einige Wähler doppelt im System erfasst waren, während andere mit ungültigen Pässen wählen konnten.

Eigenes Projekt

Ausgangssituation

Aufgrund der besonderen Relevanz der Blockchain Technologie bei demokratischen Wahlen, wurde unsere Gruppe mit diesem Thema betraut. Die ursprüngliche Aufgabe war es, das Projekt eines vorherigen Teams zu übernehmen und Erweiterungen umzusetzen. Als Erweiterungen sollten umgesetzt werden:

- Anonymes Wählen
- Aufrufen der eigenen Wahl
- Auszählung zu festem Zeitpunkt

Hierbei kam allerdings das Problem auf, dass das Projekt der Vorgänger dem Team nicht lauffähig zur Verfügung gestellt werden konnte. Obwohl dies nicht Bestandteil der Aufgabe war, wurde etwa ein Monat gemeinsam mit den Dozenten versucht, das Programm zum Laufen zu bringen. Leider ohne Erfolg.

Aufgrund der begrenzten noch übrigen Zeitspanne wurde schließlich der Arbeitsauftrag für die Gruppe geändert. Es sollte als ein separater Baustein das Aufrufen trotz Anonymität mittels Tor Routing umgesetzt werden. Darüber hinaus wurde der Gruppe auch kreativer Freiraum bei der weiteren Aufgabenbearbeitung gewährt.

So entschied sich die Gruppe nach der Fertigstellung des Tor-Routings dazu, die gesamte Anwendung nochmals komplett neu zu schreiben. Hierdurch konnten alle gewünschten Punkte, bis auf die Auszählung, zu einem festen Zeitpunkt umgesetzt werden. Die exakte Lösung hiervon gelang nur konzeptionell. Im Projekt wurde eine Lösung in Form eines Admin-Servers als Workaround umgesetzt. Durch diesen kann die Auszählung manuell zu einem bestimmten Zeitpunkt gestartet werden.

Projektziele

Simulation einer Blockchain in Python

Der Aufbau der Blockchain-Datenstruktur basiert auf SHA-256 als Hashing-Methode. In Python kann die Hashlib-Bibliothek verwendet werden, um jede Transaktion mit einem geeigneten Hash fester Länge zu definieren. Außerdem wurde die Klasse "Block" in Python mit den folgenden Eigenschaften erstellt:

- Block-Nummer gibt jedem Block eine eindeutige ID.
- Der vorherige Hash wird als Überprüfungsmethode betrachtet, um eine Manipulation und Bearbeitung der vorherigen Blöcke zu verhindern.
- “Transaktionen” enthält die realen Werte und in diesem Fall hat jede Transaktion zwei Parameter. Der erste Parameter ist die gehashte Identität des Benutzers und der zweite Parameter ist die verschlüsselte Wahl.
- Der Hash wird mit der Hashlib-Bibliothek erstellt und aktualisiert, wenn eine Änderung an der Transaktion auftritt.
- Der tatsächliche Hash enthält den ersten Wert des ursprünglichen Hashs, um ihn später mit dem aktuellen Hash zu vergleichen.

Einholen der Authentifizierung bzw. der Wahlberechtigung des Benutzers

Damit eine Person zum Wähler werden kann, muss sie bestimmte Kriterien erfüllen. Am Beispiel der Bundesrepublik Deutschlands kann davon ausgegangen werden, dass jede Person, die das Alter von 18 Jahren erreicht hat, auf Bundesebene bei Bundestagswahlen wahlberechtigt wird. Dazu zählen noch andere Faktoren wie z.B. Staatsangehörigkeit, mögliche schwere Straftaten usw. Dadurch muss sichergestellt werden, dass nur Personen, die diese Wahlbestimmungen erfüllen, die technische Möglichkeit haben, ihre Stimme abzugeben.

Hierzu verwenden wir einen generellen Ansatz, wie er auch in der Verwaltung verwendet wird. Es besteht pro Zuständigkeitsregion (eine Region, in der der Wähler seine Stimme abgeben kann) ein zentraler Authentifizierungsserver zur Verfügung. Dieser Server ist vor der Allgemeinheit verborgen und enthält eine Liste an Personalnummern, welche die zugelassenen Wähler repräsentieren. Falls nun ein Wähler seine Stimme abgeben möchte, wird eine Anfrage an den Server gesendet und dieser gibt eine Antwort, ob die Person wahlberechtigt ist. Da in dieser Tabelle keine Namen gespeichert werden, muss eine eindeutige, vom Benutzer bekannte Personalnummer als Identifikationsmittel verwendet werden. Damit andere Personen, welche kein Stimmrecht im Fall derjenigen Person besitzen, versuchen, für diejenige Person abzustimmen, muss eine zweite Authenfizierungsschicht erstellt werden. Dies

wird mit Hilfe von einer sechsstelligen Pin geregelt. Diese wird dem Benutzer von den Behörden zusammen mit der Wahlbenachrichtigung zugeschickt.

Verschleiern der Wähler-Identität durch Hashing

Damit der Wähler nicht durch seine Wahl zurückverfolgt werden kann und seine Identität herausgefunden werden kann bzw. seine Wahl mit seiner ungehashten Personalnummer assoziiert werden kann, muss die Personalnummer zusammen mit der sechsstelligen, selbst gewählten Pin gehasht werden. Dadurch kann von dieser neuen, eindeutigen Identifikationsnummer nicht mehr auf den Wähler zurückgeschlossen werden. Nur der Wähler selbst kann diesen Zustand mit seinen “Secrets” (also seiner Personalnummer und der PIN) wiederherstellen.

Zum Hashing wird ein Verfahren verwendet, welches Argon2 heißt und durch einen Wettbewerb entwickelt wurde und als derzeit sicherstes Hashing-Verfahren bekannt ist.

Argon2 hat drei Varianten: Argon2i, Argon2d und Argon2id. Argon2d ist schneller und verwendet einen datenabhängigen Speicherzugriff, was es sehr widerstandsfähig gegen GPU-Cracking-Angriffe macht und für Anwendungen geeignet ist, bei denen keine Bedrohung durch Seitenkanal-Timing-Angriffe besteht (z. B. Kryptowährungen). Argon2i verwendet stattdessen einen datenunabhängigen Speicherzugriff, der für das Hashing von Passwörtern und die passwortbasierte Ableitung von Schlüsseln bevorzugt wird, aber langsamer ist, da es zum Schutz vor Tradeoff-Angriffen mehr Durchläufe im Speicher macht. Argon2id ist ein Hybrid aus Argon2i und Argon2d, der eine Kombination aus datenabhängigem und datenunabhängigem Speicherzugriff verwendet, was Argon2i einen Teil seiner Widerstandsfähigkeit gegen Seitenkanal-Cache-Timing-Angriffe und Argon2d einen Großteil seiner Widerstandsfähigkeit gegen GPU-Cracking-Angriffe verleiht. Durch diese Eigenschaften und eine Kombination beider Vorteile ist Argon2id der derzeit beste Algorithmus, welche für Hashing im Online-Voting verwendet werden kann.

Die gehashte Personalnummer in Verbindung mit der PIN wird zum Schluss in die Blockchain geschrieben, davor wird jedoch überprüft, ob die Person mit der gewissen Personalnummer bereits gewählt hat und ob die angegebene Autorisierungs-PIN richtig war.

Verschlüsseln der Online-Wahl mit Public und Private Key durch “Elliptic Curve Cryptography”

Elliptic Curve Cryptography ist ein Ansatz zur Public-Key-Kryptografie, der auf der algebraischen Struktur elliptischer Kurven über endlichen Feldern basiert. ECC erlaubt kleinere Schlüssel im Vergleich zu Non-EC-Kryptografie (basierend auf einfachen

Galois-Feldern), um gleichwertige Sicherheit zu bieten. In diesem Projekt wurde die ECIES-Bibliothek verwendet, um die Schlüsselpaare zu generieren. Mit dem Public Key kann die Wahl jedes Users verschlüsselt werden und an die Blockchain als zweiten Parameter der Transaktion weitergegeben werden. Der private Schlüssel wird dem Benutzer in Form eines QR-Codes angezeigt, damit der Benutzer seine Wahl entschlüsseln und überprüfen kann.

Generierung der Qr-Codes von Benutzerinformationen zur Autorisierung

Mithilfe der Python-Bibliothek "qrcode" werden die gehashte Identität, den privaten Schlüssel und den öffentlichen Schlüssel des Benutzers in Form eines QR-Codes erstellt. Diese drei QR-Codes werden dem Nutzer nach erfolgreicher Auswahl angezeigt. Der Benutzer kann diese QR-Codes dann an die Anwendung jederzeit eingeben, um seine Auswahl aufzurufen und zu prüfen.

Verschlüsseln des Benutzerschlüssels zur Erhaltung des Wahlrechts

Um die Wahl zum Schluss auszuzählen werden alle Private-Keys der Benutzer benötigt, da durch diese Private-Keys die verschlüsselte Wahl in der Blockchain überhaupt entschlüsselt werden kann. Durch einen vordefinierten Administratorschlüssel sollen alle Benutzerschlüssel verschlüsselt werden, damit eine vorzeitige Wahlauszählung nicht möglich ist.

Dieser Administratorschlüssel wird zentral unabhängig von den Wahlregionen abgespeichert und wird zur Verschlüsselung der Benutzerschlüssel nicht benötigt. Dadurch bleibt der private Schlüssel des Administrators von Anfang an, bis hin zur Auszählung versteckt.

Verteilung der Zuständigkeit durch eine Distribution der Infrastruktur

Die Server sollen auf verschiedene Wahlbezirke verteilt werden. Dazu sollen die Server auf verschiedenen Maschinen deployed werden. Dadurch kann der Benutzer in seiner eigenen Region wählen gehen. Wenn eine Anfrage durch einen Server geht, wird diese an davor vordefiniert viele, zufällige Server geschickt, welche eine Art von Verschleierung bieten. Dadurch kann am Ende nicht mehr herausgefunden werden, wo die ursprüngliche Nachricht herkam.

Quellen

- https://www.tagesschau.de/ausland/estland-wahl-cyber-101.html
- https://www.bpb.de/shop/zeitschriften/apuz/255967/e-voting-in-estland-vorbild-fuer-deutschland/
- https://www.valimised.ee/et/e-haaletamine/e-haaletamise-juhised/e-haaletamise-etapid-valijarakenduses
- https://www.ch.ch/de/abstimmungen-und-wahlen/e-voting/
- https://www.swissinfo.ch/ger/kein-e-voting-mehr--stimmbeteiligung-der-fuenften-schweiz-gesunken/47754936
- https://ch.galileo.tv/life/e-voting-online-wahlen-auch-bald-in-deutschland/
- https://www.kaspersky.de/about/press-releases/2021_blockchain-basiertes-wahlsystem-polys-neue-abstimmungsformen-und-noch-benutzerfreundlicher
- https://www.kaspersky.com/about/press-releases/2020_polys-from-kaspersky-innovation-hub-presents-first-blockchain-based-voting-machine
- https://www.kaspersky.com/about/press-releases/2021_the-blockchain-based-voting-boom-online-sessions-increased-threefold-during-year-of-lockdown
- https://dgap.org/en/research/publications/online-elections-russia
- https://www.ledgerinsights.com/kaspersky-blockchain-voting-machine/
- https://www.kaspersky.de/about/press-releases/2020_kaspersky-innovation-hub-praesentiert-wahlcomputer-auf-blockchain-technologie
- https://voatz.com/
- https://www.polyas.de/
- https://www.agora.vote/about