Vorgenommene Änderungen

Christoph Bieringer, Simon Schneider

27.10.2022

In diesem Dokument werden die im Rahmen dieser Arbeit am System vorgenommenen Änderungen aufgelistet und beschrieben.

Inhalt

[Einschränkung der Verfügbarkeit der Auszählfunktion 3](#_Toc119405067)

[Veröffentlichung der kompletten Blockchain 3](#_Toc119405068)

[Usability-Updates im Frontend 3](#_Toc119405069)

[Hinzufügen einer Verifikationsmöglichkeit für die Blockchain 3](#_Toc119405070)

# Einschränkung der Verfügbarkeit der Auszählfunktion

Da die permanente Verfügbarkeit der Auszählfunktion, wie im Dokument „Analyse und Schwachstellen“ beschrieben, eine potentielle Sicherheitslücke darstellt, wurde beschlossen, sie nur noch nach einem bestimmten Datum (gewissermaßen dem Ende der Wahl) verfügbar zu machen.

Dieser Zeitpunkt befindet sich in einem neu angelegten Config-File in BlockchainTIF19AGruppeC\dhbw-blockchain-encryption\config.json. Bei dieser Datei handelt es sich um eine JSON-Datei, die ein Objekt mit dem Key „end“ enthält. Der zugehörige Value ist ein String, der einen ISO-8601-konformen Timestamp in UTC enthält. Der Wahlserver liest diesen Wert beim Start einmal ein (der für dieses Feature zuständige Code befindet sich in config\_management.py). Wird nun eine Auszählanfrage vor dem in „end“ gespeicherten Zeitpunkt gestellt, so antwortet der Server (semantisch korrekt) mit dem Antwortcode 403 (Zugriff verweigert) sowie einem JSON-Objekt, dass den Fehlergrund angibt („Election still in progress“). Eine Anfrage nach dem Ende der Wahl wird normal beantwortet.

# Veröffentlichung der kompletten Blockchain

Damit die Manipulationssicherheit der Blockchain gewährleistet ist, muss ihr Inhalt öffentlich von Dritten überprüft werden können. Hierfür wurde im Register ein neuer API-Endpoint (/api/getFullChain) geschaffen. Analog zu /api/getTransactions enthält dieser einen JSON-Array mit einem Objekt für jeden Block der Blockchain. Diese Objekte enthalten jeweils die Blocknummer, die Transaktionen (als Array), den Hash des Vorgängerblocks, und den Hash des Blocks. Mit diesen Informationen kann eine Anwendung die Integrität der Blockchain unabhängig überprüfen, indem sie die Hashwerte für jeden Block selbst berechnet und mit den in der Blockchain gespeicherten vergleicht.

Diese Änderung ist ein wichtiger Schritt, um die globale Verifizierbarkeit und Manipulationssicherheit der Wahl sicherzustellen.

# Usability-Updates im Frontend

Im Frontend des Systems (d.h. den Websites im Ordner dhbw-blockchain-website) wurden verschieden Updates durchgeführt, die das System leichter benutzbar machen sollen. Einige der durchgeführten Updates sind u.a.:

* An verschiedenen Stellen wurden erklärende Text hinzugefügt.
* Die File-Input-Elemente auf der Verifikationsseite wurden so verändert, dass sie dem Benutzer anzeigen, ob schon eine Datei ausgewählt wurde (und wenn ja, welche). Zudem wird der Button zum Starten des Verifikationsprozess nun erst dann freigeschaltet, wenn der Benutzer beide der benötigten Dateien bereitgestellt hat.
* Die technisch nicht zu rechtfertigende Beschränkung der PIN auf eine sechsstellige Zahl wurde aufgehoben und durch eine neue Bedingung ersetzt. Ein PIN muss nun mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern enthalten. Auf diese Weise wird verhindert, dass Benutzer einfach zu erratende PINs (etwa ihr Geburtsdatum) verwenden, und Brute-Force-Angriffe zur Deanonymisierung von Wählern werden erschwert.

# Hinzufügen einer Verifikationsmöglichkeit für die Blockchain

Im Frontend wurde eine vierte Seite erstellt. Auf dieser kann sich der Benutzer die gesamte Blockchain (von /api/getFullChain auf dem Register) anzeigen lassen. Clientseitiger Code überprüft die Blockchain vollautomatisch (mithilfe der Web Crypto API) und informiert den Benutzer, falls einer der Hash-Wert in der Blockchain nicht korrekt ist. Auf diese Weise kann sich jeder Benutzer selbst davon überzeugen, dass die Blockchain nicht manipuliert wurde und alle Stimmen korrekt gespeichert sind, ohne dabei einer anderen Komponente (Wahlserver/Register) vertrauen zu müssen. Dies ist ein wichtiger Schritt hin zur vollständigen Verifizierbarkeit.