Titel: Referenzmodell: Blockchain für Patientendaten

Einleitung: Die elektronische Verarbeitung von Patientendaten erfolgt in Österreich mit der „Elektronischen Gesundheitsakte“ (ELGA). Hierbei entstehen ca 140.000.000 Patientenkontakte pro Jahr. Die Daten werden dezentral auf den Standorten gespeichert, bei denen sie entstehen. Durch diesen Aufbau ergeben sich zwei entscheidende Nachteile: Einerseits besteht bei einem (lokalen) Netzausfall kein Zugriff auf die vorhandenen Patientendaten. Neben dem Problem der Verfügbarkeit, kann auch durch eine nicht-redundante Speicherung die Datenintegrität nicht gewährleistet werden. Dies bedeutet, dass ein Angreifer oder eine Angreiferin bei einem erfolgreich geglückten Manipulationsversuch alternative Datenbestände hinterlegen kann.
Durch den Aufbau und die Funktionsweise einer Blockchain-Struktur lassen sich beide Schwachstellen vermeiden. Hierbei werden alle Transaktionen auf allen berechtigten Knoten gespeichert, was einen Datenverlust ausschließt. Gleichzeitig garantiert ein entsprechendes Konsensprotokoll den gültigen Letztstand der Blockchain über alle Knoten hinweg.
Das bedeutet, dass Daten weder gelöscht oder manipuliert werden können und zusätzlich zu jeder Zeit überall zur Verfügung stehen.

Ziel: Die Aufgabe dieser Arbeit war es, eine Blockchain-Struktur zu entwickeln, welche die erwähnten Risikofaktoren minimiert und gleichzeitig die bestehenden Anforderungen an ELGA sowie der letztgültigen DSGVO erfüllt werden sollten. Technische Optimierungen (als Beispiel sei der Energieverbrauch oder Speicherbedarf genannt) wurden als Nicht-Ziel definiert und stellen somit eine logische Weiterentwicklung der Ergebnisse dar.

Methode: Die Beantwortung der Forschungsfrage erfolgte durch die Erstellung eines Referenzmodelles anhand der Vorgaben der „Design Science Methodologie“ welches einen „Blueprint“ für ähnliche Problematiken darstellen soll.
Im ersten Schritt wurde das Modell „step-by-step“ anhand der vorhandenen Anforderungen erstellt. Dieses untergliederte sich in die entsprechenden Prozesse welche durch die Modellierungssprache UML abgebildet wurden. Um sicherzugehen, dass auch alle ursprünglichen Anforderungen erfüllt waren, wurden den fertigen Prozessen die zutreffenden Anforderungen in einer Anforderungsmatrix zugewiesen und verifiziert.
Als zweiter Schritt musste das erstellte Modell anhand eines bereits existierenden Beispiels demonstriert werden. Im konkreten Fall bedeutete dies, dass eine ähnliche Lösung

„Medicalchain“ mithilfe des Referenzmodelles abgebildet und wiederum mit Hilfe einer Anforderungsmatrix validiert wurde.

Ergebnisse: Entwickelt wurde eine private Blockchain-Struktur, welche die Teilnehmer in mehrere Rollen und somit unterschiedliche Berechtigungen und Aufgaben unterteilt:
Patienten: Diese Personen erhalten lediglich Zugriff auf die von ihnen benötigten Daten.
Gesundheitsdatenanbieter (GDA): Können Patientendaten (sprich Transaktionen) erstellen und an Patienten sowie an andere GDAs weiterleiten. Ebenso sind in diesen Accounts alle Transaktionen gespeichert.
Miners: Diese erstellen durch das Protokoll der „Mining Rotation“ einen neuen Block, welcher alle neu erstellten Transaktionen beinhaltet. Ein Miner erstellt, alle anderen Miner validieren daraufhin diesen Block auf Gültigkeit und signieren diesen mit ihrer digitalen Signatur. Im Anschluss erstellt der nächste Miner einen Block.
Anchorer: Ein gültiger Block wird zusätzlich in einer öffentlichen Blockchain publiziert. Hierbei wird der Hash des Blockheaders zB. in einer Bitcoin Transaktion eingefügt.
Dieser Ablauf garantiert, dass die Daten nur auf den Knoten, auf denen sie benötigt werden, gespeichert sind, dass Daten sicher und anonym in einem Block integriert werden können und die Richtigkeit (Datenintegrität) der privaten Blockchain mit Hilfe der öffentlich publizierten Header jederzeit validiert werden kann, ohne Einsicht in die kreierten personenbezogenen Daten zu gewährleisten.
Im Gegensatz zu der bestehenden Lösung von „Medicalchain“ werden die gesamten Patientendaten in einer einzigen Blockchain verschlüsselt gespeichert, während bei „Medicalchain“ Transaktionsdaten und Unterlagen (zB: Röntgenbilder, MRI-Daten) in zwei unterschiedlichen Blockchains abgelegt werden.

Diskussion/Conclusio: Es konnte gezeigt werden, dass das erstellte Referenzmodell alle Anforderungen gemäß der DSGVO und ELGA erfüllte, sowie durch dessen Aufbau die Schwachstellen der zurzeit vorherrschenden Lösung verringert werden konnten. Sowohl die Verfügbarkeit als auch die Integrität der Daten wurde dadurch erhöht.
Die Forschungsfrage konnte somit positiv beantwortet werden.

Zusammenfassung und Ausblick: Obgleich sich eine Blockchain eignet, Patientendaten verschlüsselt, anonym, nachvollziehbar und de facto ausfallsicher zur Verfügung zu stellen, können die in den Hypothesen definierten Verbesserungen vorerst nur theoretisch bestätigt werden. Es folgt zwar, dass eine höhere Ausfallssicherheit und Replikation der Daten die

Verfügbarkeit und Integrität erhöht. Dennoch wird nicht jeder e-Befund unmittelbar nach der Erstellung benötigt. Ein kurzfristiger Systemausfall könnte hier eventuell zu keinen nennbaren Einbußen für GDAs oder Patienten führen, obwohl die Daten theoretisch nicht zur Verfügung standen.

Ebenso ließen sich zusätzliche Verschlüsselungsmethoden (Hybridverschlüsselung) oder alternative Konsensprotokolle in das Referenzmodell als eine Art Baukastensystem integrieren. Eine Entwicklung eines Prototyps würde sich aufbauend auf diese Arbeit ebenso anbieten. Hierbei könnte man Spezifikationen, wie die Benutzeroberfläche für Pateinten, GDA und Behörde, die zu verwendende Skriptsprache und dessen Befehle sowie Steuerung der Berechtigungsstruktur konkretisieren und die allgemeine Funktionalität der vorliegenden Lösung zu verbessern.