Thesis-Seminar im Bachelor-Studium – monatliche Berichterstattung

Berichtszeitraum: 01.03.2019 – 31.03.2019

Thema der Thesis:	Anwendung von Blockchain Technologien zur kryptografischen Absicherung von Auditdaten.
Bearbeiter:	Kevin Hertfelder
Kontakt: kevin.hertfelder@hs-furtwangen.de	

Durchgeführte Arbeiten

Im ersten Monat habe ich die meiste Zeit mit Recherche und Papers lesen verbracht, um einen allgemeinen Einblick in den Stand der Technik und die verwendeten Methoden und Verfahren, in meinem Thesis-Thema, zu bekommen. Hierbei behandelte Themen waren Audit-Logging im Allgemeinen: welche Informationen sind für ein Audit zu speichern, Gesetzlicher Hintergrund im europäischen und deutschen Recht, sowie diverse DINs und andere Richtlinien. Welche Art von Dokumenten werden auditiert und wie lange müssen / dürfen die entsprechende Datei aufgehoben werden. Schließlich noch die Technische Umsetzung und konkrete Datenstrukturen zur Speicherung und Verifikation solcher Daten: Verwendung von Hashverifikation, Signaturverfahren und die Verwendung in dezentralen, verteilten Systemen. Im späteren Teil des Monats habe ich dann eine vorläufige Spezifikation für das Softwaremodul, welches Hauptbestandteil meiner Thesis darstellt, erstellt. Zur Planung der Architektur habe ich unterschiedliche UML Diagramme, von System- bis Klassensicht, erstellt. Zuletzt habe ich die Arbeiten an der Implementierung eines ersten Prototyps begonnen, der eine möglichst einfache Implementierung benutzt und später als Vergleichspunkt zu aufwendigeren und interessanten Verfahren dient.

Erzielte Ergebnisse

- Aneignung von Basiswissens zum Stand der Technik und dem Thema allgemein
- Wissen über einige spezialisierte Verfahren
- Ermittelte Anforderungen
- UML Systemdiagramm
- UML Datenflussdiagramm
- UML Klassendiagramm
- REST Schnittstellenbeschreibung
- Angefangene Implementierung von Interfaces für ersten Prototypen.

Abweichungen / Probleme

Probleme sind bis jetzt keine aufgetreten, jedoch habe ich schon eine Vorahnung was sich eventuell als problematisch herausstellen könnte. Audit-Logging ist in den meisten Fällen durch eine zentrale Einheit in einem Servercluster umgesetzt. „neverpile eureka“, das Softwareprodukt von levigo, für welches das Audit-Logging implementiert werden soll, ist aber ein dezentrales Cluster ohne Koordination durch eine übergeordnete Instanz. Ohne diese übergeordnete Instanz ergeben sich einige Probleme wie „Total Ordering“ zwischen Events einzelner Instanzen und ähnliches. Diese Eigenschaft von neverpile eureka ist aber essenzieller Bestandteil der Software und bietet auch viele Vorteile wie leichte und schnelle Skalierbarkeit und Verfügbarkeit durch den Einsatz von Containerisierung. Konkrete Probleme, die dadurch verursacht werden, zeigen sich erst im weiteren Verlauf, sind aber jetzt schon absehbar.

Ausblick über die geplanten Tätigkeiten und Ergebnisse des nächsten Berichtszeitraums

Für den nächsten Monat ist die Fertigstellung der Basisimplementierung und Interfaces geplant. Der erste Prototyp soll auf Basis einer simplen Hashchain implementiert werden und als Basis-Benchmark für spätere Implementierungen dienen. Als nächster Schritt soll dann ein geeignetes Verfahren gewählt werden, welches

Verbesserungen in den Bereichen Geschwindigkeit, Speicherplatz oder Sicherheit bietet. Diese Verbesserungen sollen dann anhand eines End-To-End Tests nachgewiesen werden.