Bewertung BA ba21_neut_02
Teststand für ein dezentrales und Blockchain-basiertes Handelsnetzwerk für digitale Werte von Levi Cailleret und Sascha Kyburtz

Stephan Neuhaus

2021-06-14

1 Fortschritt, Leistung, Arbeitshaltung

Die Kandidaten haben zu Anfang einen Plan erstellt, den sie tatsächlich eingehalten haben. Das ist ungewöhnlich, denn normalerweise überlebt so ein Plan den Kontakt mit der Wirklichkeit nur selten. Dabei haben die Kandidaten stets über Risiken informiert und erschienen jederzeit gut vorbereitet zu den vereinbarten Treffen.

Hinter dem scheinbar glatten und einfachen Fortschritt steht offenbar ein erheblicher Teil Arbeit, der auftretende Schwierigkeiten durch grossen Arbeitseinsatz beseitigte oder umschiffte. Das ist insbesondere deshab bemerkenswert, weil die Arbeit einen erheblichen Unsicherheitsfaktor hatte, nämlich die Einarbeitung in die Blockchain-Technologie, die einen erheblichen Anteil an dem zu untersuchenden DIVA.EXCHANGE-Netzwerk hat.

Wenn man hier überhaupt Kritik anbringen kann, dann die, dass die Kandidaten den erzielten Fortschritt wenn überhaupt als zu leicht haben erscheinen lassen. Der grosse dahinter stehende Arbeitseinsatz ist erst sichtbar, wenn man in das Repository schaut.

Note: 6.0, Gewicht 25%.

2 Qualität der Resultate

In dieser Arbeit sollte ein Teststand entwickelt werden, um das Handelsnetzwerk DIVA.EXCHANGE bestimmten Angriffen unterziehen zu können. Dabei sollten einige Hypothesen untersucht werden. Dieser Teststand wurde erstellt und die Hypothesen wurden untersucht.

Ein Ergebnis der Untersuchungen war, das die ursprünglich zum Einsatz gekommene Blockchain Hyperledger Iroha wegen Performanceproblemen nicht geeignet ist. Der Nachweis dieser Performanceprobleme ist so überzeugend gelungen, dass das Projekt DIVA-EXCHANGE nun eine eigene Blockchain entwickelt. Der in dieeser Arbeit erstellte Testdtand und die in dieser Arbeit

erzielten Ergebnisse haben dazu massgeblich beigetragen und werden auch die neue Blockchain einem Performancetest unterziehen. Dass eine BA einen solch massiven Einfluss auf das Hauptprodukt eines Kooperationspartners hat, ist sehr aussergewähnlich.

Die wichtigste der gefundenen Lücken ist jedoch, dass Hyperledger Iroha anscheinend nicht den sogenannte "'$3f+1$"'-Konsens unterstützt, sondern lediglich "'$2f+1$"'. Das ist ein ausgezeichnetes Resultat, das man von einer Bachelorarbeit nicht erwarten durfte.

Note: 6.0, Gewicht 25%.

3 Form und Inhalt des Berichts

Der Bericht besteht aus 99 Seiten (A4, schmale Ränder, 10-Punkt-Schrift), bestehend aus 8 Seiten front matter (Titel, Abstracts, Vorwort), 59 Seiten eigentlichen Bericht, 2 Seiten Literaturverzeichnis, 3 Seiten andere Verzeichnisse und 26 Seiten Anhängen (Aufgabenstellung, Zeitplan, Protokolle, Codeübersicht). Die 49 Literaturreferenzen sind mehr als ausreichend und sehr gut ausgewählt. Der Bericht enthält alle Abschnitte, die man erwartet.

Ber Bericht beschreibt ausführlich—und korrekt!—, was byzantinische Fehlertoleranz und Konsesalgorithmen sind, wie sich diese voneinander unterscheiden und wie der zum Zeitpunkt der Arbeit verwendete Algorithmus YAC funktioniert. Nur den Titel von Abschnitt 2.5 ist mit "'Historische Aufarbeitung"' missverständlich gewählt :-)

Sodann werden verschiedene praktische Angriffe auf ein blockchain-basiertes Handelsnetzwerk skizziert, die ebenfalls sehr detailliert beschrieben und mit Beispielen illustriert sind.

Um mögliche Sicherheitslücken zu finden, verwenden die Kandidate Abuse Cases und Data Flow-Diagramme und die daraus entstehende Bedrohungsmodellierung, aus denen erst Sicherheitsanforderungen und dann mägliche Angriffe abgeleitet werden. Das ist mustergültig.

Diese Angriffe werden dann in einem Testnetzwerk umgesetzt und ausgewertet. Dabei werden einige recht deutliche Lücken gefunden (siehe vorhergehenden Abschnitt).

Der Bericht ist in einem gut verständlichen deutsch geschrieben. Der Text ist der Textsorte angemessen formuliert.

Note: 5.5, Gewicht 50%.

Gesamtnote: 5.75, gerundet 6.0