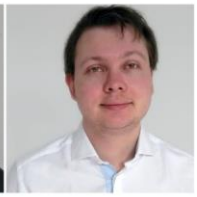
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

Teststand für ein dezentrales und Blockchain-basiertes Handelsnetzwerk für digitale Werte



Diplomierende
Levi Cailleret
Sascha Kyburz

Dozent
Stephan Neuhaus

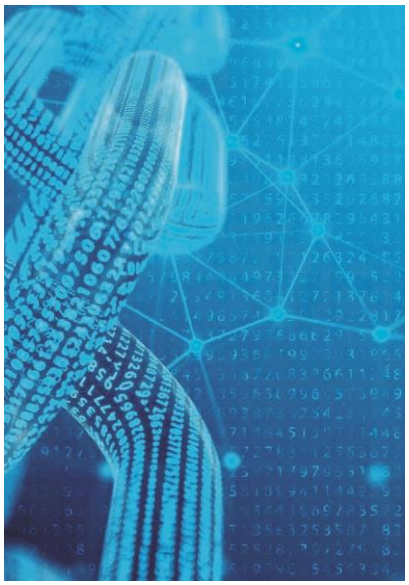
Wir untersuchen das Projekt DIVA.EXCHANGE und versuchen dabei mögliche Sicherheitsrisiken auszumachen. DIVA.EXCHANGE ist ein Open-Source-Projekt mit dem Ziel, mittels einer Blockchain ein vollständig verteiltes Handelsnetzwerk aufzubauen. Die eingesetzte Blockchain basiert auf Hyperledger Iroha und ist primäres Ziel der Forschungsarbeit und unserer Tests.

Auf einem lokalen Netzwerk wird eine Test-Blockchain von DIVA.EXCHANGE aufgebaut. Innerhalb dieser Testumgebung werden mehrere Tests durchgeführt und das Verhalten der Blockchain analysiert. Dabei liegt die Manipulation der Blockchain durch unehrliche Knoten im Fokus. Auch andere mögliche Angriffe auf DIVA.EXCHANGE werden dabei in Betracht gezogen.

Die wichtigsten Resultate zeigen, dass die auf Hyperledger Iroha basierende Blockchain die byzantinische Fehlertoleranz von mehr als zwei Drittel ehrlichen Knoten nicht einhält. Weiterhin zeigen die Resultate, dass der Konsensalgorithmus YAC, der den Hyperledger Iroha verwendet, zu langen Wartezeiten bei der Erstellung von Blöcken innerhalb des Netzwerks hat, wenn nicht alle Netzwerkteilnehmer durchgehend verfügbar sind.

Wir folgern aus den Daten, dass Hyperledger Iroha deutliche Sicherheitsrisiken aufweist, da byzantinische Fehler nicht ausgeschlossen werden können. Dieser Umstand muss verbessert werden, damit Transaktionen von Wertmitteln im öffentlichen Rahmen risikolos stattfinden können. Wir kommen zum Schluss, dass Hyperledger Iroha sich als Blockchain-Technologie für DIVA.EXCHANGE nicht eignet. DIVA.EXCHANGE plant als dezentrales Handelsnetzwerk Benutzern zugänglich zu sein, die nicht immer erreichbar sind. Dieses Verhalten der Benutzer führt bei Hyperledger Iroha allerdings zu langen Verzögerungen.

DIVA.EXCHANGE ist seit Q1/2021 an der Entwicklung einer eigenen Blockchain-Technologie, der «divachain». Die Sicherheit von «divachain» soll in einer weiteren Forschungsarbeit untersucht werden.



Sicherheit einer Blockchain (sinnbildlich).