Projektidee zur Ausschreibung Bachelorarbeit 2020/21

Ergänzende Informationen

Titel der Ausschreibung

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

Ausgangslage und Problemstellung

Ausgangslage

Das Ziel des Auftraggebers (Verein DIVA.EXCHANGE) ist die kontinuierliche Weiterentwicklung der freien Software "DIVA"[1]. Dabei handelt es sich um ein für alle zugängliches vollständig dezentrales, nicht-diskriminierendes und Privatsphäre-schützendes Handelsnetzwerk für digitale Werte (wie z.B. "Krypto-Anlagen"). Die wichtigsten Komponenten des Software Prototypen sind:

- I2P[2] (Anonymisierungsschicht)
- Iroha[3] (Datenschicht, Blockchain)
- Diva[4] (Handeln und Verwalten von digitalen Werten)

Die Anonymisierungsschicht (I2P) garantiert den Benutzern, dass Transaktionsdaten keine Rückschlüsse auf Identitätsdaten zulassen. Das Schreiben von Transaktionsdaten auf die Blockchain (Iroha), wird von Stellvertreterfunktionen durchgeführt, welche das Speichern im Auftrag der Sender übernehmen. Diese Implementation muss in Bezug auf die Stabilität und Anonymität untersucht werden. Darum wird ein Teststand benötigt.

Annahme

Ein vollständig *dezentrales* und *nicht-diskriminierendes* Handelsnetzwerk und -system für digitale Werte (wie z.B. "Krypto-Anlagen") mit einer *Privatsphäre-schützenden* Architektur ist vorteilhaft für alle Netzwerkteilnehmer. Ebenfalls soll das System "DIVA.EXCHANGE" *Stabilität* und *Resistenz* gegen Angriffe (z.B. Replay-Attacken) garantieren.

[1] Das quelloffenes Projekt ist hier verfügbar: https://codeberg.org/diva.exchange/
[2] Übersicht: https://geti2p.net. I2P wurde in einer Bachelorarbeit (Herbstsemester 2019) thematisiert und erläutert, https://codeberg.org/diva.exchange/academia
[3] Übersicht: https://iroha.readthedocs.io/en/latest. Iroha wurde in einer Bachelorarbeit (Herbstsemester 2019) thematisiert und erläutert, https://codeberg.org/diva.exchange/academia
[4] Benutzeroberfläche, die das Handeln und Verwalten von digitalen Werten ermöglicht

These

Dies sind die Eigenschaften des Software Prototypen:

- alle Daten und Prozesse sind vollständig dezentralisiert[5]
- nicht-diskriminierend, dazu gehören insbesondere die Eigenschaften Freier Software[6] sowie tiefstmögliche Installations- und Betriebskosten
- ein hinreichend[7] Privatsphäre-schützendes Netzwerk erlaubt den Handel (Tausch, d.h. Kauf und Verkauf) von Blockchain-basierten digitalen Werten (wie z.B. “Krypto-Anlagen”)
- die digitalen Werte sind vor unautorisierter Nutzung und Verfälschung geschützt (Stichworte: Diebstahl, “double spending”, Replay-Attacken)
- die Installation kann für jeden aktiven Teilnehmer im Netzwerk vorteilhaft sein

Der Software Prototyp stellt somit die These dar und wird vom Auftraggeber auf einer Linux Plattform zur Verfügung gestellt. Es ist möglich, dass der Prototyp Programmierfehler und Funktionsmängel aufweist. In den ersten zwei Wochen des Projektes muss festgelegt werden, wie mit Fehlern und Mängeln umgegangen wird.

[5] Einfache, kurze Zusammenfassung: https://de.wikipedia.org/wiki/Dezentrales_Netzwerk
[6] https://de.wikipedia.org/wiki/Freie_Software. Die Freiheiten verunmöglichen u.a. explizit die Zensur von Software.
[7] Definiert als: der Bruch der Anonymität des Netzwerkes ist “mit sehr hohen Kosten verbunden”. Im Rahmen der Projektdefinition müssen “sehr hohe Kosten” quantifiziert werden. Ausführliche Diskussion, siehe Nguyen Phong Hoang, Panagiotis Kintis, Manos Antonakakis, and Michalis Polychronakis. 2018. An Empirical Study of the I2P Anonymity Network and its Censorship Resistance. https://www.researchgate.net/publication/327445307_An_Empirical_Study_of_the_I2P_Anonymity_Network_and_its_Censorship_Resistance

Technologien des Prototypen

Der Software Prototyp basiert auf folgenden Technologien:

- Diva-Komponente - Eigenentwicklung
- Hangout-Komponente[8] - Eigenentwicklung
- Logger-Komponente[9] - Eigenentwicklung
- I2P-Komponente (Darknet) - Externe Verwendung
- Iroha-Komponente - Externe Verwendung
- mehreren, fundamental unterschiedlichen Blockchain-Implementationen; mit einer mittleren Wahrscheinlichkeit sind dies Bitcoin[10], Monero[11], Ethereum[12] und Ripple[13] und damit vermutlich sechs handelbare Krypto-Anlage-Paare
- zahlreichen quelloffenen Entwicklungen von unterschiedlichen Autoren

Alle Komponenten des Prototypen müssen quelloffen[14] sein und werden auf der Codeberg-Repository[15] veröffentlicht.

[8] Ermöglicht bidirektionale Verbindung zwischen zwei Knoten in einem privaten Netzwerk
[9] Generische Logger Komponente
[10] https://bitcoin.org
[11] https://www.getmonero.org
[12] https://www.ethereum.org
[13] https://ripple.com
[14] Mögliche Software Lizenzen: GPL, BSD, MIT, Apache Foundation, Creative Commons
[15] https://codeberg.org/diva.exchange

Architektur des Prototypen

Der Prototyp der Software besteht aus drei Kern-Funktionalitäten innerhalb eines Knotens des Netzwerkes:

1. einer Funktion für das Handeln mit Krypto-Anlagen (“Auftragsfunktion”, engl. “order placement”)
2. einer Funktion zur Vermittlung von 2..n Aufträgen zwecks Vertragserstellung zwischen zwei Aufträgen (“Vermittlungsfunktion”, engl. “matching”)
3. einer Funktion zwecks Feststellung des Zustandes (korrekt oder fehlerhaft) der Vertragserfüllung (“Abwicklungsfunktion”, engl. “settlement”)

Jeder Netzwerkteilnehmer, d.h. ein Knoten, kann ein beliebiges Set von Funktionen bereitstellen. Die Netzwerkteilnehmer können soweit anonym bleiben wie dies der unterliegende Anonymisierungslayer (I2P) erlaubt. Jede einzelne Nachricht im Netzwerk muss zustandslos[16] sein. Je nach Funktionsbündel des Netzwerkteilnehmers fallen Gebührenaufwände und/oder -erträge an. Der Handel mit Krypto-Anlagen kann sowohl in Echtzeit wie auch Auktionsbasiert stattfinden.

Hypothesen

Dies sind Vorschläge von Hypothesen, welche im Rahmen des Projektes mit geeigneten Methoden zu falsifizieren sind:

1. die implementierte Auftragsfunktion garantiert die Anonymität (gemäss Gary T. Marx[17]) jedes DIVA.EXCHANGE Benutzers
2. die implementierte Vermittlungsfunktion garantiert die Anonymität (gemäss Gary T. Marx) jedes DIVA.EXCHANGE Benutzers
3. die implementierte Auftragsfunktion ist resistent gegen Replay-Attacken
4. die implementierte Vermittlungsfunktion ist resistent gegen Replay-Attacken

Der Auftraggeber ist offen für weitere oder andere Hypothesen. Die definitiven Hypothesen werden im Rahmen des Projektes definiert.

[16] Kurze Einführung: https://de.wikipedia.org/wiki/Zustandslosigkeit
[17] Gary T. Marx definiert sieben Identifikationsmerkmale: https://web.mit.edu/gtmarx/www/identity.html. Eine Bachelorarbeit (Herbstsemester 2019) hat diese Punkte ebenfalls thematisiert, https://codeberg.org/diva.exchange/academia

Zusammenarbeit

Carolyn Bächler-Schenk und Konrad Bächler arbeiten während der gesamten Projektdauer zu 100% mit. Sie sind verantwortlich für alle Aspekte der Software ("DIVA") und insbesondere für Veränderungsvorschläge. Die Veränderungen am Software Prototypen finden in einer Versions-kontrollierten Umgebung (Codeberg) statt, damit die Hypothesen korrekt gegen spezifische Versionen getestet werden können. Arbeitsort ist entweder Baar (in den modernen Büroräumlichkeiten der Kopanyo AG an der Schochenmühlestrasse 4) oder wahlweise in den Räumlichkeiten der Hochschule oder im "Homeoffice". Die Räumlichkeiten müssen ein konzentriertes, stilles Arbeiten in moderner Umgebung[18] erlauben. Es ist für den Auftraggeber (Verein DIVA.EXCHANGE) und für den Studierenden von Vorteil, wenn während der Arbeit eng miteinander zusammengearbeitet wird[19].

Verwandte Projekte und Abgrenzung

Seit einigen Jahren werden "verteilte Anwendungen" intensiv auf verschiedenen Ebenen diskutiert. Ob dies nun eine verteilte Börse für Krypto-Anlagen (z.B. "bisq"[20] oder "resistance"[21]) oder ein verteiltes soziales Netzwerk (z.B. "solid"[22]) darstellt. In diesem Kontext rücken dann oft auch rechtliche Fragestellungen ins Zentrum, unter anderem die Fragestellung nach der Rechtmässigkeit einer spezifischen Technologie. Zusammengefasst lauten die Abgrenzungen wie folgt:

- In diesem Projekt spielen rechtliche Fragestellungen keine Rolle
- Alle bestehenden Projekte, welche in irgendeiner Form eine zentrale Stelle aufweisen (eine zentrale ökonomische Einheit, eine Form von zentraler Regulation oder ein zentraler technischer Standard), können per Definition nicht mit diesem Projekt verwandt sein
- Fiatgeld[23] wird in diesem Projekt nicht berücksichtigt

[18] Schneller, unbeschränkter Netzwerkzugang; höhenverstellbare Tische; ergonomische Stühle; moderne Hardware mit Linux Betriebssystemen; eigene Konferenzräume mit Raum für mindestens vier Personen

[19] Im Herbstsemester 2019 wurde bereits eine Bachelorarbeit von einem Studierenden verfasst. Rückblickend war die enge Zusammenarbeit ein wichtiger Punkt für den erfolgreichen Abschluss des Forschungsprojektes.

[20] https://bisq.network

[21] https://resistance.io

[22] https://github.com/solid/information

[23] https://de.wikipedia.org/wiki/Fiatgeld

Kreativität, Varianten, Innovation

Die empirischen Tests der Hypothesen stehen in einer Wechselwirkung mit der Weiterentwicklung des Software Prototypen.
Im Rahmen der These des Projektes sind alle Ideen und Varianten willkommen. Inwiefern spezifische empirische Vorgehensweisen (z.B. offensive Netzwerk-Tests) in diesem Projekt ethisch akzeptabel sind, wird in einem kurzen “Manifest”/“Code of Conduct” zu Beginn gemeinsam festgelegt.

Kein Tagesgeschäft

Da das Projekt ein wissenschaftliches Forschungsprojekt ist, hat es nichts mit dem Tagesgeschäft zu tun.

Innovation in Reinform

Gemäss Wissensstand der Projektauftraggeber existiert per Januar 2020 kein “vollständig dezentrales und nicht-diskriminierendes Handelssystem für digitale Werte mit einer hinreichend Privatsphäre-schützenden Architektur”. Es ist Neuland.

Schlagwörter

verteiltes System, dezentrales Netzwerk, Blockchain, digitale Werte, Krypto-Anlagen, Kryptographie, Handelssystem, Börse, I2P, Darknet, Privatsphäre, Anonymität

Bachelorarbeit oder Masterarbeit

Die Projektidee kann auch im Rahmen einer Masterarbeit ausgearbeitet werden.

Im Herbstsemester 2019 wurde die erste Bachelorarbeit zum Thema “Untersuchung eines vollständig dezentralen, nicht-diskriminierenden und Privatsphäre-schützenden Handelsnetzwerk für digitale Werte (wie z.B. «Krypto-Anlagen») von Stefan Maric verfasst[24].

[24] Bachelorarbeit Stefan Maric, siehe auch https://www.diva.exchange/forschung

Die Arbeit wurde im Januar 2020 abgegeben und von der HSLU mit “sehr gut” bewertet. Dies ist der Auftrag zu einem weiteren Folgeprojekt.

Projektart und Schwerpunkte

Es ist ein “Innovationsprojekt/Forschungsprojekt” mit den Schwerpunkten “Security/Privacy” sowie “Software-Erstellung”.

Auftraggeberin

Unternehmen

Firma:	Verein DIVA.EXCHANGE
Ansprechperson:	Carolyn Bächler-Schenk, Konrad Bächler
Funktion:	Gründungsmitglieder und Vorstandsmitglieder
Strasse:	Schochenmühlestrasse 4
PLZ, Ort:	6340 Baar
Telefon:	079 423 25 48
Email:	carolyn@diva.exchange
Website:	www.diva.exchange

Über die Autoren dieser Projektidee

Die Autoren dieser Projektidee sind Konrad Bächler und Carolyn Bächler-Schenk. Sie verfügen über jahrelange Erfahrung als Unternehmer, Softwareentwickler und Innovatoren.

Carolyn Bächler-Schenk

www.linkedin.com/in/carolyn-baechler-schenk

Konrad Bächler

- lic. oec. publ. Uni Zürich, abgeschlossen 12.1997 mit cum laude. Liz-Arbeit: Fixed Income Instruments with Embedded Options.
- Stationen: Schweizer Börse, Hugin/ThomsonReuters, Gründer und Unternehmer ab 2003: Entwickler/Architekt von https://marCo.ch, erfolgreicher Unternehmensverkauf der Tensid AG (rund 16 Mitarbeiter) im 2015.
- Gewinner Innovationspreis Kanton Zug, 2011: https://www.luzernerzeitung.ch/zentralschweiz/zug/zuger-innvationspreis-2011-geht-an-tensid-ld.38155
- Software-Entwickler seit >30 Jahren (Sprachen: Assembler, C/C++, Pascal, PHP, JS, SQL, HTML/CSS; OS: Linux). Expertenstatus im Bereich Softwarearchitektur/Microservices/API, modernes PHP (OO), zugehörige Test-Frameworks, persistente Datenspeicherung mit ORMs und Linux. Entwickler eigener sehr fortgeschrittener Backend-Frameworks und eines eigenen ORM für den Einsatz im Bereich hochfrequenter Datenverarbeitung (Forschungsprojekt: verteilte Kryptobörse).
- Einige öffentliche Referate u.a. an der Verleihung Jungunternehmerpreis 2012 in Zug zum Thema "Datenmissbrauch durch Cloud-Dienste", 2016 zum Thema TOR/I2P/Darknet in Zug im Rahmen des Technologieforums Zug oder 2017 zum Thema "Support Vector Models (Machine Learning)" ebenfalls für das Technologieforum Zug
- Aktuelle Tätigkeitsgebiete: Forschungsprojekt “DIVA.EXCHANGE”: ein vollständig dezentrales, nicht-diskriminierendes und Privatsphäre-schützendes Handelsnetzwerk für digitale Werte (“Krypto-Anlagen”)