**Bachelorarbeit**

**WS2021/2022**

gemäß §19 der Prüfungsordnung für die

Bachelor-Studiengänge der Fachrichtung Wirtschaftswissenschaft

in der Fassung vom 27. Februar 2014

Fakultät HW, Universität des Saarlandes

Generalthema: Distribute Ledger Technologies

Titel: Integration von Schnittstellenprozessen der Finanzverwaltung mithilfe der Blockchain-Technologie

Gestellt von: Prof. Dr. Peter Loos

Betreuer: M.A., M.Sc. Allesandro Benke

Bearbeitet von: Florian Feibel,

Adresse: Kaiserstr.26, 66111 Saarbrücken;

Matrikelnummer: 2568339

Studiengang: Bachelor Wirtschaftsinformatik

Inhalt

[1 Einleitung (Motivation, Forschungsfrage, Methodik, Hypothese) - 1 -](#_Toc96104436)

[1.1 Hinführung und Kontext der Arbeit - 1 -](#_Toc96104437)

[2 Grundlagen / Forschungsstand - 5 -](#_Toc96104438)

[2.1 Prozess zwischen F,S,S - 5 -](#_Toc96104439)

[2.2 Verwendete Technologien und Blockchain - 6 -](#_Toc96104440)

[2.2.1 Blockchain - 6 -](#_Toc96104441)

[2.2.2 Hyperledger Firefly - 8 -](#_Toc96104442)

[2.3 Heraklit - 9 -](#_Toc96104443)

[3 Modellierung des Szenarios - 10 -](#_Toc96104444)

[3.1 Anforderungsdefinition - 10 -](#_Toc96104445)

[3.2 HERAKLIT: technische Komponenten / Module und deren Zusammenspiel Prozessengin Module - 10 -](#_Toc96104446)

[4 Implementierung - 11 -](#_Toc96104447)

[5 Kritische Würdigung - 12 -](#_Toc96104448)

[6 Fazit und Ausblick - 13 -](#_Toc96104449)

[7 Abbildungsverzeichnis II](#_Toc96104450)

[8 Literaturverzeichnis III](#_Toc96104451)

# Einleitung (Motivation, Forschungsfrage, Methodik, Hypothese)

Dieses Kapitel erläutert die Herangehensweise an die Arbeit, sowie den Aufbau der Arbeit und gibt einen thematischen Überblick über das Thema Blockchain-Technologien.

## Hinführung und Kontext der Arbeit

Durch den Wandel der Digitalisierung fallen immer größere Datentransaktion an. Ob es sich bei den Transaktionen um digitale Währungen, Daten oder einfach Textnachrichten handelt, ist dabei egal. In jedem Fall will man, dass Transaktionen schnell, günstig und vor allem sicher ablaufen. Nicht allein deswegen, sondern auch weil das Vertrauen in zentrale Institutionen immer geringer wird, sind die Erwartungen an Distributed Ledger Technologien enorm hoch. Solche Technologien wie zum Beispiel Blockchains bieten Lösungen für genau solche Fälle an. Sie bieten eine dezentral verteilte Infrastruktur, mit der Transaktionen vertrauensvoll und vollkommen transparent verifiziert und abgeschlossen werden können.

Der wohl in der heutigen Zeit bekannteste Anwendungsfall ist der des 2008 erschienene Bitcoin-White-Paper von Satoshi Nakamoto (*Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute*, o. J.). Das Ziel seines Papers war es ein solches peer-to-peer Netzwerk zu schaffen, sodass online Transaktionen direkt zwischen den beteiligten Parteien hin und her gesendet werden können, ohne dass eine weitere Institution dazwischensteht. (Zitat mit Seitenzahl)

Allerdings ist das Anwendungsgebiet solcher Technologien längst nicht mehr nur auf solche Finanztransaktionen beschränkt. Heutzutage finde sie Anwendung in allen möglichen Bereichen wie dem Gesundheitswesen, dem Supply Chain Management oder auch bei digitalen Wahlen (*Wofür kann die Blockchain-Technologie eingesetzt werden?*, 2019). All diese Fälle haben eines gemeinsam. Sie wollen Daten sicher, schnell, und transparent austauschen. Und vor allem wird all das ermöglicht ohne Intermediäre, denen man vertrauen müsste. Auch im Bereich der Steuerabwicklung liegt Potenzial für die Anwendung von Blockchain-Technologien (*Die Blockchain macht die Finanzverwaltung effizienter*, 2021). In dieser Arbeit geht es um genau dieses Anwendungsgebiet und der Frage, kann eine Blockchain-Technologie dafür genutzt werden den Steuerprozess zu optimieren und die Kommunikation zwischen dem Steuerpflichtigen und der Finanzverwaltung, sowie ggf. einem Steuerberater erleichtern? Ein Grund warum die Anwendung in diesem Bereich sinnvoll sein könnte liegt in der manipulationssicheren und transparenten Vernetzung der beteiligten Parteien. Somit hat der Steuerpflichtige immer volle Kontrolle über seine Daten und kann (*Die Blockchain macht die Finanzverwaltung effizienter*, 2021). Außerdem kann man mit Hilfe von Smart Contracts gezielt Berechtigungen bzw. Vollmächte ausgestellt werden und diese sind dann auf der Blockchain verankert, wodurch der Steuerpflichtige wiederum mehr Kontrolle über den gesamten Prozess bekommt, da diese Verträge ebenfalls nicht manipulierbar sind.

(Weitere Forschungsfragen ..?)

Um den Kommunikationsfluss zwischen diesen drei beteiligten Parteien über eine Blockchain laufen zu lassen, wird in dieser Arbeit Hyperledger Firefly (*Home*, o. J.) verwendet. FireFly ist ein „Mehrparteiensystem“, welches Entwicklern ein schnelle Möglichkeit liefert Blockchain Anwendungen zu erstellen, idem man sich mehr auf die Geschäftslogik als auf die Infrastruktur konzentrieren kann (Quelle). In Kapitel 2.2 wird auf Firefly noch genauer eingegangen.

Die Arbeit ist folgendermaßen aufgebaut: In Kapitel 2 wird zunächst der Steuerkommunikationsprozess näher erläutert. Außerdem geht dieses Kapitel auf die Verwendeten Technologien ein und gibt noch einen überblick über die Blockchain-Technologie. Im letzten Teil des Kapitels geht es um das zur Modellierung des Prozesses verwendete Tool Heraklit. Im darauffolgenden Kapitel geht es dann um die Anforderungsdefinitionen sowie der eigentlichen Modellierung des Prozesses.In Kapitel 4 wird die Implementierung der Anwendung genauer betrachtet und detaillierter auf die zugrunde liegende Technologie eingegangen. Im Anschluss werden mit der kritischen Würdigung nochmal die Forschungsfragen aufgegriffen und beurteilt. Im letzten Teil gibt es dann nochmal ein zusammenfassendes Fazit, sowie einen Ausblick mit zukünftigen Verbesserungsmöglichkeiten.

# Grundlagen / Forschungsstand

( a) Prozess zwischenn F,S,S, Vollmacht, etc.

b) Verwendete Technologien und Blockchain

c) Heraklit)

In diesem Kapitel wird zunächst der Prozess genau betrachte und geschaut wie genau das Zusammenspiel der drei Parteien in diesem Prozess aussieht. Anschließend wird mit Hilfe der Heraklit Methode der gesamte Prozess Modelliert. Für das Jahr 2022 wäre das der

## Prozess zwischen F,S,S

Wer verpflichtet ist, eine Steuererklärung abzugeben, muss dies im Normalfall bis zu 31. Juli des Folgejahres tun *(Quelle)*. Somit ist jeder Steuerzahler dazu verpflichtet, einmal pro Jahr eine Steuererklärung beim Finanzamt abzugeben. Die Steuererklärung kann man entweder selber machen oder man beauftragt einen darauf spezialisierten Steuerberater, welcher sowohl die Steuererklärung für einen erstellen kann, als auch die gesamte Kommunikation mit dem Finanzamt für einen erledigen kann, je nach dem wie weit dieser dazu bevollmächtigt wurde.

Zunächst gehen wir vom einfachsten Fall aus. Hierbei betrachten man nur den Steuerzahler und das Finanzamt ohne den dazwischen liegenden Steuerberater. In diesem Fall muss der Steuerpflichtige bis zu einem bestimmten Stichtag, wie im ersten Teil bereits erwähnt, seine Steuererklärung mit allen benötigten Dokumenten bei dem Finanzamt einreichen. Hat das Finanzamt die Steuererklärung erhalten, wir diese geprüft, woraufhin das Finanzamt entweder Unterlagen bei Bedarf nachfordern kann oder wenn alles in Ordnung ist, einen Steuerbescheid ausstellt und diesen an den Steuerpflichtigen zurücksendet. Anschließend hat dieser das Recht den Steuerbescheid zu prüfen und ggf. Einspruch einzulegen. Dabei muss beachtet werden, dass auch für das Einreichen des Einspruches eine Frist vorlieft. Diese Einspruchsfrist beträgt einen Monat nach Bekanntgabe des Steuerbescheides. „Kommt der Bescheid per Post, gilt er gemäß § 122 Abs. 2 AO am dritten Tag, nachdem das Finanzamt ihn mit einfachem Brief zur Post gegeben hat, als bekannt gegeben“( <https://www.steuernetz.de/lexikon/einspruch-gegen-den-steuerbescheid)>“. „Fällt das **Ende** der Dreitagefrist oder der Einspruchsfrist auf einen **Samstag, Sonntag oder gesetzlichen Feiertag,** läuft die Frist erst mit Ende des darauf folgenden Werktags ab (§ 108 Abs. 3 AO; BFH-Urteil vom 14.10.2003, IX R 68/98, BStBl. 2003 II S. 898).“( <https://www.steuernetz.de/lexikon/einspruch-gegen-den-steuerbescheid)>“.). Hat der Steuerpflichtige bis zum Ende der Einspruchsfrist keinen Einspruch eingelegt, wird der Steuerbescheid bestandskräftig.

Im nächsten Fall gehen wir davon aus, dass der Steuerpflichtig einen Steuerberater beauftragt hat seine Steuererklärung anzufertigen. Da der Steuerberater aber keine Vollmacht erhält, läuft die gesamte Kommunikation mit dem Finanzamt wie im vorherigen Fall über den Steuerpflichtigen.

Hat der Steuerpflichtige einen Steuerberater beauftragt und diesem auch noch eine allgemeine Vollmacht erteilt, ist dieser berechtigt seinen Mandanten gegenüber dem Finanzamt zu vertreten. Das bedeutet, das die Kommunikation in erster Linie nur noch über den Steuerberater läuft. Nur der Steuerbescheid geht direkt an den Mandanten. Erhält der Steuerberater zusätzlich noch eine Empfangsvollmacht, läuft nicht nur die Kommunikation über ihn, sondern er ist auch derjenige, an den der Steuerbescheid gehen muss.

Die ausgestellten Vollmächte können zu jedem Zeitpunkt vom Steuerpflichtigen widerrufen werden, wodurch man dann wieder in dem Basisfall landet.

## Verwendete Technologien und Blockchain

Im den Folgenden Abschnitten werden die verwendete Technologie näher erläutert.

### Blockchain

Blockchain ist zunächst einmal eine technische Lösung, um Daten manipulationssicher und ohne zentrale Instanz zu speichern (*Blockchain macht Daten praktisch unveränderbar*, o. J.). Entstanden ist die Blockchain als Lösung für das Double-Spending-Problem. Bei diesem Problem geht es darum, dass man Geld nicht mehrfach ausgeben kann. Um zu gewährleisten, dass Geld oder eben auch digitale Währungen nicht doppelt ausgegeben werden, hat man normalerweise Intermediäre die solche Betrugsversuche verhindern. In seinem Bitcoin Paper hat Satoshi Nakamoto eine Möglichkeit vorgestellt, wie man das Double-Spending-Problem ohne eine zentrale Behörde lösen kann(bitcoin).

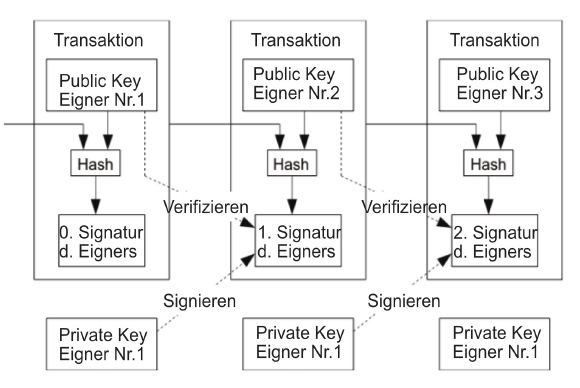
Grundvoraussetzung dafür sind zwei kryptographische Bausteine die im Weiteren kurz erläutert werden, zum einen kryptografische Hashfunktionen und zum anderen digitale Signaturen (blockchain, kurz & gut).

Mit Hilfe von kryptografischen Hashfunktionen kann man sicherstellen, dass ein Originaltext, auch bei Übertragungen, nicht verwendet wurde (Hashfkt: B&H). Um diese Eigenschaft zu gewährleisten wir ein String mit Hilfe einer Hashfunktion, wie zum Beispiel der SHA-256, in einen 256 Bit großen Hashwert umgewandelt (3 Hashfunktionen).

Eine digitale Signatur ist dafür da, damit sich der Empfänger einer Nachricht versichern kann, dass die Nachricht auch tatsächlich vom erwarteten Absender stammt und nicht zwischendurch geändert wurde (blockchain, kurz&gut), also sozusagen ein Ersatz der handschriftlichen Unterschrift. Die Signatur benötigt zwei Schlüssel, einen Signaturschlüssel und einen Verifizierungsschlüssel (whitepaper-signatur). Mit dem Signaturschlüssel kann der Absender seine Nachricht signieren, muss diesen aber geheim halten. Und mit dem Verifizierungsschlüssel, welcher öffentlich gemacht werden kann, kann die Signierung beim Empfänger versifiziert werden. (eventuell deutlicher die Eigenschaften darstellen, Unfälschbares Signaturschema).

Mit diesen Grundlagen kann man jetzt sicher Nachrichten wie in Abbildung 1 versenden. Allerdings ist damit das Double-Spending-Problem noch nicht gelöst. Um das Problem zu lösen, hat Satoshi Nakamoto eine Zeitliche Reihenfolge der Transaktionen festgelegt und einen Proof-of-Work. Um diese Zeitliche Reihenfolge zu sichern benötigt man einen digitalen Zeitstemple(bitocoin).

Jede Transaktion erhält zu ihrem eigenen Hash zusätzlich noch einen Hash aus der Signatur des Zeitstempels, welcher durch einen Server generiert wurde, sowie aus dem Hash des vorherigen Zeitstempels. Damit lässt sich leicht feststellen ob im Nachhinein in dieser verketteten Liste etwas manipuliert wurde, indem man die Hashwerte überprüft. Je mehr solcher Zeitstempel ausgestellt und der Liste hinzugefügt wurden umso Fälschungssicherer wird diese Hash Liste



Um das Double-Spending-Problem nun vollständig zu lösen, fehlt nur noch der Proof-of-Work.

### Hyperledger Firefly

Hyperledger Firefly ist ein „Multiparty-System für Prozessdatenflüsse“ (HFF ) auf der Basis der Blockchain Technologie (Quelle). Das bedeutet, es ist eine Sammlung verschiedener Softwaretechnologien, welche in der Lage sind Transaktionen zwischen mehreren Parteien, sicher auf einer privaten Blockchain zu ermöglichen. Firefly unterscheidet auserdem zwischen privaten Nachrichten innerhalb des Netzwerkes und der Übertragung von Transaktionen an alle im Netzwerk beteiligten Parteien. Firefly bietet dabei Entwicklern die Möglichkeit die komplexe Logik dahinter zu umgehen und bietet eine Programmierschnittstelle wodurch sich diese volständig auf die eigentlich Geschäftslogik fokusieren könne. Firefly erlaubt damit eine schnelle, sichere und unabhängige Übertragung von Transaktion zwischen verschiedenen Partner eines Netzwerkes mit Hilfe einer privaten Blockchain. Dadurch ist Firefly für alle Anwendungbereiche interesssant, für die man in irgendeiner Weise ein Haupbuch bzw. einen Nachweis von verschiedensten Transaktionen benötigt und verschieden Organistationen zusammen arbeiten müssen ohne, dass sich dies vollständig Vertrauen. Auch heute findet Firefly schon Anwendung in verschiedensten Bereichen die genau diese Bedingungen mitbring. Dazu zählen unteranderem Bereich wie das Gesundheitswesen , das Versicherungswesen, Immobilien und Finanzen oder auch Wohltätigkeitszwecken.

Für die Entwicklung einer auf Firefly basierenden Softwarlösung bietet die Hyperledger Foundation das Firefly-Cli an, mit welchem auch die in dieser Arbeit gearbeitet wurde. Das Firefly-Cli dient dazu einen private Blockchain in ihrem privaten Netzwerk zu simulieren. Dabei kann man einen sogenannten Stack individuell konfigurieren. Ein Stack representiert dabei ein gesamtes Firefly Netzwerk. Dabei wird mit Hilfe von Dockercompose die zugrunde liegende Infrastruktur generiert. Per default und auch die in dieser Arbeit verwendete Blockchain Technologie ist eine private Ethereum Blockchain. Bei der initialisierung eines Stack wird der „Genosis Block“ der neuen privaten Blockchain erstellt und alle Identitäten auf die Blockchain gepusht. Sobald ein Stack initialisiert wurde kann man mit Hilfe der Programmierschnittstellen auf diesen zugreifen. Dabei hat jede der Organisationen des Netzwerks einen eigenen Api Endpoint.

Firefly bietet mit dem Firefly-Cli eine einfache Möglichkeit einen lokalen FireFly-Stack, zur Entwicklung einer Blockchain basierten Anwendung zu generieren. Dabei wird für jeden Member ein FireFly-Knoten erzeugt. Ein solcher Knoten ist eine Sammlung vieler Mikroservices mit einer HTTPS/Websocket-API welche durch den Kern des Knoten verfügbar ist. Die FireFly-API liefert ein Interface für die Blockchain-Ebene die vollkommen erweiterbar/kompatibale(plugable, erkläten was damit gemeint ist?) ist. Dabei ist es möglich zwischen 3 großen Blockchain-Protokollen zu wählen, Hyperleder Fabric, Enterprise Ethereum oder R3 Corda. In dieser Arbeit liegt der Fokus auf einer Ethereum Blockchain. Sowohl Hyperledger Fabric als auch Enterprise Ethereum sind eine generell gut Wahl, R3 Corda dagegen ist speziell für den Finanzsektor entwickelt worden. Um mit der FireFly-Cli zu starten benötigt man zunächst eine aktuelle Go- und eine Docker-Version. Mit diesem Command-Line-Interface ist es möglich ein Stack zu erzeugen welcher sich auf die Menge aller Laufzeiten bezieht, die zur Simulation eines Multiparty-Netzwerkes auf dem lokalen Rechner nötig sind und diese automatisch in Verbindung bringt. Ein Stack ist individuell konfigurierbar.

## Heraklit

„Heraklit ist die Infrastruktur zur Modellierung rechnerintegrierter Systeme“. Die Grundlage von Heraklit bilden symbolische Petri-Netze, welche den Daten und Kontrollfluss, und damit das Verhalten dynamischer Systeme modellieren. Jedes Heraklit-Modul besteht im inneren aus diesen Petri-Netzen und hat nach außen sichtbare rechte und linke Schnittstellen, mit denen Heraklit-Module mit gleichbenannten Schnittstellen miteinander komponiert werden können. Damit lassen sich verschiedene Abstraktionsebenen und Abhängigkeiten zwischen den Modulen modellieren. Außerdem können Heraklit-Module gegenüber wichtiger Anforderungen formal bewiesen werden.

# Modellierung des Szenarios

( a. Anforderungsdefinition

b. Heraklit: technische komponenten / Module un deren Zusammenspiel Prozessengin Modul)

In diesem Kapitel wird zunächst auf die Anforderungsdefinitionen eingegangen und anschließend wir der Prozess mit Hilfe von Heraklit modelliert.

## Anforderungsdefinition

## HERAKLIT: technische Komponenten / Module und deren Zusammenspiel Prozessengin Module

# Implementierung

Dieses Kapitel beschreib die Implementierung der Software.

# Kritische Würdigung

# Fazit und Ausblick

# Abbildungsverzeichnis

**Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.**

# Literaturverzeichnis

**Im aktuellen Dokument sind keine Quellen vorhanden.**