Entwicklung und Analyse einer dezentralisierten Terminbörse auf Basis der Blockchain-Technologie

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M. Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Weber Vorname: David Jonathan Julian Benedikt

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. Hans Jörg von Mettenheim Betreuer: Dipl. Ök. Rouven-B. Wiegard

Ort, den: Hannover, den 30.09.2016

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation und Relevanz

Mit seinem White Paper zum Bitcoin hat Satoshi Nakamoto (2008) erstmalig ein Konzept einer digitalen Kryptowährung vorgestellt, die Überweisungen Peer-to-Peer über ein verteiltes Rechnernetzwerk ohne zentrale Abwicklungsstelle möglich macht.
Bereits seit Anfang der 2000er befindet sich der Zahlungsverkehr im Umbruch. Dieser Trend ist eng verknüpft mit der Verbreitung des Internets und eines starken Wachstums des E-Commerce (Sharma und Gupta (2009)). Dieser hat eine Notwendigkeit nach schnellen, sicheren und einfachen Zahlungsmethoden, die den speziellen Anforderungen geschäftlicher Transaktionen im Internet gerecht werden, hervorgerufen (Botha et al. (2008)). Neben den herkömmliche Bezahlverfahren, wie Bargeld oder Kartenzahlung und Überweisungen, wurden neue Online-Bezahlsysteme entwickelt.
Im Zuge dieser Entwicklung sind neue, auf die Abwicklung von Zahlungstransaktionen im Internet spezialisierte, Anbieter und Plattformen entstanden, die mit herkömmlichen Anbietern wie Banken konkurrieren. Ein populäres Beispiel für ein Online-Bezahlsystem, das ursprünglich speziell für den E-Commerce entwickelt wurde, ist PayPal. Das Unternehmen hat laut eigener Angaben inzwischen über 230 Millionen Mitgliedskonten und im Jahr 2015 einen Umsatz von 9,25 Mrd. Dollar erzielt (PayPal (2016)).

Trotz fortschreitender Digitalisierung im Zahlungsverkehr war man bei Transaktionen vor der Entwicklung von Bitcoins auf die Infrastruktur von Banken oder anderer zentraler Institutionen angewiesen.
Der bargeldlose Zahlungsverkehr, sowohl bei Online-Bezahlverfahren, als auch bei Überweisungen, Kreditkarten oder Lastschriftverfahren wird letztlich über Buchgeld abgewickelt (Hartmann-Wendels et al. (2013)). Buchgeld liegt nicht materiell vor, sondern als Aufzeichnung in Kontobüchern der Banken(Sixt (2016)). Für den Umlauf von Buchgeld müssen bei einer Transaktion Zahlungsinformationen übermittelt und Buchungsakte zwischen den Kontobüchern der betreffenden Banken vorgenommen werden (Adrian und Heidorn (2013)). In diesem Zusammenhang sorgen Clearinghäuser oder Zahlungsverkehrssysteme wie TARGET 2 für die Weiterleitung der Zahlungsinformation und Buchung auf den Konten der beteiligten Banken (Hadeler et al. (2013)). Diese Infrastruktur ist notwendig, da Buchgeld nicht in einem gemeinsamen Register erfasst ist. Durch die Vielzahl an Intermediären und Zwischenschritten wird die korrekte Abwicklung gewährleistet. Die Prüfung der Korrektheit gespeicherter Informationen in den Kontobüchern erfolgt dabei unter anderem durch Wirtschaftsprüfer.

Mit der Entwicklung und Einführung von Bitcoins wurde ein für alle zugängliches monetäres System geschaffen, in dem für die Abwicklung von Zahlungstransaktionen bisherige

Intermediäre nicht benötigt werden (Lee (2015)). Den direkten Zahlungsverkehr zwischen den Nutzern möglich macht ein, von Satoshi Nakamoto konzipiertes, verteiltes dezentrales Datenbanksystem, die Blockchain (Nakamoto (2008)). Die Blockchain ist ein digitales, transparentes Register, in dem alle Transaktionen festgehalten werden (Swan (2015)). Die Blockchain wird nicht zentral geführt, sondern von allen angeschlossenen Rechnern gemeinsam verwaltet (Platzer (2014)). Jeder Rechner hat eine eigene Kopie der Datenbank lokal gespeichert. Neue Transaktionen werden automatisch verifiziert, in Datenblöcken gespeichert und an die vorherigen Datenblöcke gereiht (Antonopoulos (2014)). Im Bitcoin System ist die Blockchain das gemeinsame Kassenbuch aller Teilnehmer. Da durch die öffentliche Dokumentation innerhalb der Blockchain jeder die gleiche Information besitzt und nachvollziehen kann, wer welche Geldeinheit besitzt und ausgegeben hat, ist eine Zahlungstransaktion ohne Intermediäre möglich. Die Prüfung der Korrektheit von Informationen basiert bei Bitcoins vollständig auf kryptografischen Verfahren (Platzer (2014)).

Laut Statista (2016) betrug im September 2016 die Marktkapitalisierung von Bitcoins über 9,7 Milliarden US Dollar . Neben Bitcoin gibt es inzwischen weitere Peer-to-Peer Zahlungsnetzwerke die Blockchain als Grundlage verwenden. Ein Beispiel ist Ripple, welches von der gewinnorientierten Gesellschaft Ripple Labs 2012 entwickelt wurde und ähnlich wie Bitcoin funktioniert [1]. Die Besonderheit bei Ripple ist, dass es zusätzlich zum Zahlungsverkehr einen angeschlossenen Devisenmarkt hat. Ripple arbeitet mit Banken zusammen und hat laut eigener Angabe im Juli 2016, zusammen mit SAP, der kanadischen Bank ATB Financial und der ReiseBank die erste Echtzeitüberweisung von Kanada nach Deutschland getätigt (Ripple (2016)).

Durch die Transparenz schafft die Blockchain weiterhin eine Möglichkeit, Vertrauen und Integrität zwischen zwei Gegenparteien herzustellen, ohne Notwendigkeit eines Intermediärs (MacDonald et al. (2016)). Grund ist das die Blockchain Transaktionen unwiderruflich abwickelt und jede für die Anbahnung von Verträgen benötigte Information in der Blockchain nachvollziehbar gespeichert sind, ohne Informationsasymmetrien zwischen einzelnen Teilnehmern (Deutsche Bank (2015)) . Die potenziellen Einsatzmöglichkeiten einer Blockchain gehen daher weit über den Austausch von Geld hinaus. Über die Kryptowährung Bitcoin können bereits heute eine Vielzahl von Finanztransaktionen und Finanzgeschäften abgebildet und direkt abgewickelt werden, für die es im herkömmlichen Finanzsystem noch mehrerer zwischengeschalteter Instanzen bedarf. Dieses Potenzial hat die Finanzindustrie erkannt. Eine Studie der Großbank Santander (2016) hat verschiedene Anwendungsbereiche bei Wertpapiergeschäften, Krediten, Swaps und Derivaten identifiziert. Im Ergebnis kommt die Studie zu dem Schluss, dass mithilfe der Blockchain bis 2022 15-20 Milliarden Euro an Infrastrukturkosten in der Finanzindustrie eingespart werden könnten.

[1] https://ripple.com

Ein weiteres Signal, das die Blockchain-Technologie in den Fokus der Finanzindustrie rückt, ist ein bis heute einmaliger globaler Zusammenschluss von inzwischen 45 Unternehmen der Finanzbranche, im Blockchain Startup R3CEV [2]. In Rahmen dieser Kooperation erforscht das Unternehmen die Entwicklung und Anwendung der Blockchain-Technologie im globalen Finanzsystem. Es wurde 2014 gegründet und ist ansässig in New York. Erste Unternehmen, die sich an R3 CEV beteiligten, waren Barclays, BBVA, die Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, State Street und UBS. Inzwischen sind unter anderem auch die Deutsche Bank und die Commerzbank mit eingestiegen.
Im August 2016 wurde zu dem bekannt, dass eine Bankenallianz mit UBS, der Deutschen Bank und der Santander Bank an einer eigenen Cyberwährung "Utility Settlement Coin" arbeiten (UBS (2016)). Diese soll zum Einsatz kommen, um Geschäfte innerhalb der Blockchain abwickeln zu können. Die "Utility Settlement Coin" soll ein wertneutrales, digitales Währungssubstrat sein, das technologisch benötigt wird, aber kein monetäres Eigenleben hat. Die digitale Münze soll nach außen hin nicht als Zahlungsmittel einsetzbar sein und repliziert bestehende Geldeinheiten. Die Besonderheit ist, dass für jeden "Utility Settlement Coin" eine reelle Währungseinheit bei der Zentralbank hinterlegt werden soll. Am 30. Dezember 2015 kündigte Nasdaq, die gemessen an der Zahl gelisteter Unternehmen, größte elektronische Börse der USA, die Entwicklung von Linq an. Linq ist ein Blockchain basierter Service, der die Ausgabe von Aktien auf Blockchain-Basis ermöglichen soll. Nasdaq sieht das Potential. Die vollständige Abwicklung von bis zu drei Tagen auf 10 Minuten zu reduzieren. Gleichzeitig könnten papierbasierte Zertifikate dieser Aktien abgeschafft und administrative, manuelle Prozesse automatisiert werden (Nasdaq (2015)).

Auch durchgeführte Studien von McKinsey (2015), Euroclear und OliverWyman (2016) sind zu dem Ergebnis gekommen, dass es Anwendungsfelder im Bereich des Kapitalmarktes gibt. Die Unternehmen sehen dabei besonderes Einsparpotenzial durch eine Verschmelzung der Handels-, Clearing- und Settlementprozesse sowie der Automatisierung im Backoffice.

Ein klassisches Finanzgeschäft, mit einem aufwendigen Abwicklungsprozess und einer Vielzahl zwischengeschalteter Intermediäre, sind Future-Kontrakte, die an Terminbörsen gehandelt werden (Adrian und Heidorn (2013)). An der Terminbörse findet kein direkter Handel zwischen Teilnehmern statt, sondern über eine zwischengeschaltete Clearingstelle (Hull (2013)). Die Studie der Großbank Santander (2016) sieht hierbei Möglichkeiten für ein direktes Clearing- und Settlement zwischen einzelnen Markteilnehmern durch den Einsatz der Blockchain-Technologie und Smart Contracts. In der Studie zeigen die Autoren dies modellhaft auf.

[2] siehe https://r3cev.com

An den Ergebnissen dieser Studie soll die Masterarbeit anschließen und untersuchen, wie eine technische Umsetzung auf einem existierenden Protokoll aussehen könnte. Gegenstand dieser Masterarbeit ist daher die Ausarbeitung und Analyse einer technischen Infrastruktur für eine Terminbörse auf Blockchain-Basis, die eine Peer-to-Peer Abwicklung von Future-Kontrakten ermöglicht.

Buterin (2014) zeigt Schwächen im Bitcoin Scripting auf, welche die Umsetzung einer solchen Anwendung auf diesem Protokoll erschweren. Daher wird in der Arbeit ein Modell für eine technische Umsetzung auf dem Ethereum Protokoll ausgearbeitet. Bei der Entwicklung von Ethereum wurden bekannte Scripting Schwächen des Bitcoin Protokolls berücksichtigt und vermieden. Ethereum wurde 2015 erstmals in Betrieb genommen. Als Plattform für programmierbare Smart Contracts bietet Ethereum eine Infrastruktur für die Abbildung bedingter Verträge, wie Futures oder Optionen, und ist daher geeignet eine Börsenapplikation auf Blockchain-Basis abzubilden.
Die Forschungsfragen der Masterarbeit lautet:

- **Wie kann eine Terminbörse in der Blockchain abgebildet werden und welche Vor- und Nachteile, sowie Herausforderungen, ergeben sich für einen Einsatz in der Praxis?**

1.2 Forschungsmethodik und Aufbau der Arbeit

Ziel der Arbeit ist die Entwicklung eines konzeptionellen Modells zur technischen Umsetzung eines Ethereum-Prototypen, der die Abwicklung von Terminkontrakten Peer-to-Peer ermöglicht. Im Modell sollen Strukturen, Funktionen und Abläufe einer späteren Ethereum-Anwendung beschrieben werden. Die Forschungsmethodik in dieser Arbeit orientiert sich an dem Design-Science Ansatz nach Peffers et al. (2007). Das langfristige Ziel ist, einen Prototypen zu entwickeln um zu testen, ob die Blockchain für einen Einsatz an Terminbörsen geeignet ist. In einer Vorarbeit müssen dafür bestehende Prozesse analysiert, ein konzeptionelles Modell entwickelt und eine technische Umsetzung aufgezeigt werden. Diese Vorarbeit soll in der Masterarbeit geleistet werden. Design-Science ist ein gestaltungsorientierter, problemzentrierter Forschungsansatz, der iterativ sechs Schritten folgt. Bei Design-Science ist das Ziel ein Artefakt zu schaffen, mit dem ein vorher identifiziertes Problem behoben werden kann (Vaishnavi und Kuechler (2015)). Der Design-Science Prozess nach Peffers et al. (2007) sieht wie folgt aus:

Protokolle wurden nicht untersucht. Ethereum wurde für diese Arbeit ausgewählt, da es frei zugänglich und Turing-vollständig ist, und eine eigene Programmiersprache für Smart Contracts implementiert hat. Neben Ethereum gibt es weitere kostenpflichtige und freie Blockchain-Plattformen. Im Rahmen der Arbeit wurde im Vorfeld nicht untersucht, ob Ethereum die beste verfügbare Alternative für den Anwendungsfall an einer Terminbörse ist. Möglicherweise gibt es bereits Blockchain-Plattform die einige der diskutierten Herausforderungen nicht aufweisen.

Weiterhin wurde im Anwendungsfall lediglich gezeigt, wie sich ein Futures technisch als Smart Contract abbilden lassen würde. Eine Terminbörse bietet jedoch eine Vielzahl an Produkten an. Auch wenn in Ethereum die technische Umsetzung eines Smart-Futures möglich erscheint, könnten andere bestehende Produkte schwieriger zu implementieren sein. Für eine Anwendung in der Praxis ist jedoch entscheidet, dass sich eine Vielzahl der heute gehandelten Produkte als Smart Contracts abbilden lassen.

8 Fazit und Ausblick

In der Einleitung wurde die Forschungsfrage aufgeworfen, wie eine Terminbörse in der Blockchain abgebildet werden könnte und welche Vor- und Nachteile, sowie Herausforderungen, sich für einen Einsatz in der Praxis ergeben.

Um den ersten Teil der Forschungsfrage zu beantworten, wurde ein technisches Umsetzungsmodell entwickelt für den Aufbau einer Konsortium-Blockchain in Ethereum, auf der dezentralisiert Smart-Futures abgewickelt werden können. In diesem Zusammenhang wurde gezeigt, wie eine Konsortium Blockchain in Ethereum aufgesetzt wird und wie durch eine Applikation eine Anbindung zum Nutzer entsteht. Weiterhin erfolgte die Ausarbeitung eines Modells für eine Infrastruktur aus verschiedenen Smart Contracts, die auf der Konsortium-Blockchain die Abwicklungsprozesse ausführen. Darüber hinaus wurde aufgezeigt, wie ein Future in Ethereum als Smart-Contract implementiert werden könnte, der das Clearing und Settlement eigenständig durchführt.

Der Entwicklungsprozess des technischen Umsetzungsmodells erfolgte in Anlehnung an die ersten drei Stufen des Design-Science Ansatzes nach Peffers et al. (2007). In einem ersten Schritt wurde der Aufbau, die Intermediäre und Abwicklungsprozesse heutiger Terminbörsen analysiert. Zusätzlich erfolgte die Untersuchung verschiedener Produkte, die an Terminbörsen gehandelt werden. Anschließend wurden die Funktionalitäten einer Terminbörse, die in der Blockchain abgebildet werden müssten, abgeleitet. Auf Grundlage dieser Analyse erfolgte die Ausarbeitung eines möglichen Abwicklungsprozesses von Ter-

mingeschäften in der Blockchain und die Entwicklung des technischen Umsetzungsmodells.

Für die Untersuchung der Praxistauglichkeit reicht es jedoch nicht aus, aufzuzeigen, dass eine Terminbörse in der Blockchain theoretisch implementierbar wäre. Daher wurden in Kapitel 6 technische, sicherheitsrelevante und regulatorische Fragestellungen untersucht und Vor- und Nachteile einer Terminbörse auf Blockchain-Basis diskutiert. In diesem Abschnitt der Arbeit wurde der zweite Teil der Forschungsfrage beantwortet. Eine wichtige Erkenntnis ist, dass durch den Einsatz der Blockchain-Technologie großes Einsparpotenzial bei den Nachhandelsprozessen und redundanten Datenbanksystemen besteht. Jedoch gibt es heute noch große Hürden für einen Umsetzung in der Praxis. Terminbörsen sind streng reguliert und für den Einsatz der Blockchain-Technologie sind aktuell noch viele Fragestellungen aus aufsichtsrechtlicher Perspektive ungeklärt. Eine wichtige technische Herausforderung, die gelöst werden muss ist die Skalierbarkeit. Für eine Anwendung an einer Terminbörse müsste eine Blockchain in der Lage sein, tausende von Transaktionen pro Sekunde zu verarbeiten. Heutige Blockchain-Plattformen sind dazu technisch nicht in der Lage. Die Blockchain befindet sich aktuell jedoch noch in einem frühen Entwicklungsstadium. Viele Unternehmen und Branchen investieren in die Erforschung und Entwicklung neuer Blockchain-Plattformen. Daher könnte es sein, dass es für heutige technische Hürden schon bald erste Lösungen gibt, die eine Anwendung in der Praxis ermöglichen. Es bleibt abzuwarten, wie der Gesetzgeber auf die neue Situation reagiert und in welchem Umfang rechtliche Rahmenbedingungen geschaffen werden. Vor allem in der Finanzindustrie suchen Unternehmen bereits die Zusammenarbeit mit den staatlichen Aufsichtsbehörden.

Die Masterarbeit versucht, einen Beitrag zu leisten, um bisherige theoretische Forschungsergebnisse in die Praxis zu überführen. Ein weiterführender Forschungsansatz kann die Entwicklung eines Prototypen auf Grundlage des technischen Umsetzungsmodells sein, um so den begonnen Design-Science Prozess nach Peffers et al. (2007) abzuschließen. Im Rahmen einer Evaluation könnte ein Lasttest durchgeführt werden. Bei diesem könnte schrittweise ein sehr hohes Transaktionsvolumen simuliert werden. Aus den Testergebnissen könnten weitere technische Herausforderungen abgeleitet werden, für die es Lösungen hinsichtlich einer Anwendung in der Praxis bedarf. Darüber hinaus könnte der gleiche Prototyp in andere Blockchain-Plattformen implementiert werden, um diese bezüglich ihrer Leistungsfähigkeit miteinander zu vergleichen. Auch könnten neben Futures die Implementierung weiterer Börsenprodukte als Smart Contracts untersucht werden.