

Smart Contracts basierend auf Blockchain Technologien

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B. Sc.)“ im Studiengang
Wirtschaftswissenschaften der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität
Hannover

vorgelegt von

Name: Bauer



Vorname: Alexander



Prüfer: Prof. Dr. M. H. Breitner

Betreuer: Rouven Wiegard

Hannover, den 16.11.2017

Inhaltsverzeichnis

Abkürzungsverzeichnis	I
Abbildungsverzeichnis	II
1. Einleitung	1
1.1 Motivation und Relevanz des Themas.....	1
1.2 Zielsetzung und Aufbau der Arbeit	2
2. Grundlagen und Funktionsweise von Blockchain Technologien	3
2.1 Motivation und Hintergrund	3
2.2 Definition und historischer Hintergrund.....	4
2.3 Unterscheidungsmerkmale und Grundfunktionen von Blockchains	5
2.4 Blockchain Plattformen	7
2.4.1 Bitcoin und Ethereum.....	8
2.4.2 Guardtime und Hyperledger.....	8
2.5 Funktionsweise der Blockchain Technologie am Beispiel Bitcoin	9
2.5.1 Transaktionsfähigkeit des Bitcoin-Netzwerks	10
2.5.2 Transaktionslegitimität und kryptographische Verfahren.....	12
2.5.3 Blöcke und Kettenstruktur	15
2.5.4 Konsensprotokoll und Mining.....	17
2.5.5 Verwaltung des Bitcoin-Systems	20
3. Smart Contracts	22
3.1 Definition.....	22
3.2 Grundlagen und Funktionsweise	23
3.3 Chancen von Smart Contracts	27
3.4 Risiken und Limitationen von Smart Contracts	29
3.5 Rechtliche Aspekte	31
3.6 Beispielhafter Programmcode eines Smart Contracts	34
4. Anwendungsmöglichkeiten von Smart Contracts	35
4.1 Finanzsektor.....	35
4.1.1 Wertpapierhandel und Bankwesen.....	35
4.1.2 Versicherungen.....	37
4.1.3 Onlinehandel und weitere Anwendungsmöglichkeiten.....	38
4.2 Internet of Things	39

4.2.1 ADEPT	40
4.2.2 Slock.it.....	41
4.2.3 Blockchain als IoT Plattform	42
4.3 Supply Chain	43
4.3.1 Skuchain.....	44
4.4 Patente und Lizenzierung.....	45
4.4.1 Anmeldung von Patenten	45
4.4.2 Lizenzierung von Musik und Kunst	46
4.5 Dezentrale Autonome Organisationen.....	47
4.5.1 The DAO	49
5. Diskussion und Beantwortung der Forschungsfrage.....	51
6. Limitation.....	55
7. Fazit und Ausblick	56
Literaturverzeichnis.....	58

1. Einleitung

1.1 Motivation und Relevanz des Themas

Technische Innovationen treiben die digitale Transformation heutiger Gesellschaften an. Eine Digitalisierung kann in vielen Bereichen des alltäglichen Lebens beobachtet werden. Dies trifft auch auf den rechtlichen Bereich zu, welcher sich verglichen mit dem Digitalisierungslevel anderer Gebiete noch am Anfang des Digitalisierungsprozesses befindet. Fortschritte in der Sicherung und Aufbereitung von Daten und Informationen, explizit der Popularitätsgewinn sogenannter *Blockchain Technologien* während des letzten Jahrzehnts, haben das Potenzial eine grundlegende Veränderung zahlreicher Geschäftsbereiche zu bewirken. Nach dem Hype-Zyklus des IT-Marktforschungsunternehmens Gartner aus dem Jahr 2017 haben die Erwartungen an Blockchain Technologien stark zugenommen, obwohl sich diese noch in einem frühen Entwicklungsstadium befinden. Langfristig gesehen erwartet Gartner, dass ganze Branchen durch Blockchain umgestaltet werden.¹ Alleine im ersten Quartal des Jahres 2017 wurden bereits über 100 Millionen USD an Venture Capital in Startups aus dem Bereich Blockchain investiert.² Ein besonderer Fokus ist dabei auf die Abwicklung von Verträgen zu legen. Der bereits länger bestehende Ansatz, dass sich Verträge basierend auf enthaltenen Bedingungen und Verpflichtungen durch die Umsetzung in Programmcode selbst ausführen, hat im Rahmen der erwähnten technologischen Fortschritte stark an Attraktivität gewonnen.

„Code is law“³ (Lessig 2000)

Bereits im Jahr 2000 hat der US-amerikanische Verfassungswissenschaftler Lawrence Lessig im Rahmen eines Aufsatzes erläutert, welchen starken Einfluss Technologien wie das Internet auf das alltägliche Leben haben. Anders ausgedrückt beeinträchtigen Software und Hardware die Gesellschaft in einem solchen Ausmaß, dass der zugrundeliegende Softwarecode wegen seiner Einflussnahme als eine Art Regelwerk oder Gesetz angesehen werden kann. Durch die Entwicklung sogenannter *Smart Contracts*, die auf Basis von Programmcode rechtliche Verträge abwickeln können und damit zumindest teilweise die Rolle des heutigen Rechtssystems in Frage stellen, kommt die Gesellschaft der Vision Lessigs ein Stück näher. Nach Wright und de Filippi haben Smart Contracts das größte disruptive Potential auf die alltägliche Ausübung des Rechts seit der Erfindung der Druckerpresse.⁴ Der innovative Einfluss dieser Smart Contracts ist jedoch nicht nur auf die Abwicklung von Verträgen beschränkt. Auch die automatisierte Kommunikation zwischen Maschinen im Rahmen des Internet of Things bis hin zur Entstehung autonom agierender Organisationen sind unter Anwendung von Smart Contracts denkbar. Besonders im finanzwirtschaftlichen Bereich versuchen etwa Banken Smart Contracts zu nutzen, um durch die grundlegende Änderung klassischer Geschäftsprozesse Kostenersparnisse und Effizienzsteigerungen zu erreichen. Nach einer Studie könnten in

¹ Vgl. Gartner Inc. 2017b

² Vgl. CoinDesk 2017

³ Lessig 2000

⁴ Vgl. Wright und de Filippi 2015, S. 10.

diesem Bereich durch die Implementierung von Blockchain Technologien aufgrund von sinkenden Infrastrukturkosten bis 2022 Ersparnisse von bis zu 20 Milliarden USD pro Jahr realisiert werden.⁵ Die Marktführer des Finanzdienstleistungsbereichs forcieren daher in Initiativen und Kooperationen die Weiterentwicklung von Blockchain Technologien und Smart Contracts, um ihre Positionen weiter zu festigen. Bei aller Euphorie zeichnen sich jedoch auch Risiken bezüglich der Nutzung von Smart Contracts ab, gerade im rechtlichen Bereich besteht hier noch Klärungsbedarf.

1.2 Zielsetzung und Aufbau der Arbeit

Diese Arbeit soll die diversen Anwendungsmöglichkeit von Smart Contracts untersuchen. In der wissenschaftlichen Literatur existieren bis dato kaum Arbeiten, die das enorme Spektrum der Einsetzbarkeit solcher Smart Contracts aufzeigen und genauer untersuchen. Dies ist vor allem auf die Neuartigkeit der zugrundeliegenden Technologien zurückzuführen. Unternehmen haben erst kürzlich begonnen, das große Potential von Smart Contracts zu realisieren. Daher existieren bis dato nur wenige praktische Use Cases, die meisten Unternehmen befinden sich noch in der Entwicklung und Ausarbeitung praktischer Anwendungen von Smart Contracts. In der Literatur finden sich zumeist eher theoretische Ansätze und Ideen, wobei erwartet werden kann, dass sich dies in den nächsten Jahren im Zuge der aktuell forcierten Entwicklung von Smart Contracts ändern wird. Diese Arbeit soll dazu beitragen, genannte Forschungslücke zu verkleinern und das innovative Potenzial von Smart Contracts zu verdeutlichen. Ziel ist es, folgende Forschungsfrage zu beantworten.

Wie können Smart Contracts in verschiedenen Anwendungsbereichen eingesetzt werden?

Zur Beantwortung dieser zentralen Fragestellung werden Ansätze aus Wissenschaft und Praxis gleichermaßen betrachtet. Eine reine Literaturobwertung zur Beantwortung der Forschungsfrage ist aus den eben genannten Gründen eher ungeeignet. Wissenschaftliche Ausarbeitungen zu dieser Thematik beziehen sich meist allgemein auf die Verwendung von Blockchain Technologien und behandeln Smart Contracts eher nebensächlich, wohingegen im Rahmen dieser Arbeit explizit der Einsatz von Smart Contracts untersucht werden soll. Aus diesem Grund versucht diese Arbeit wissenschaftliche Theorien mit Anwendungen aus der Praxis zu hinterlegen. Aufgrund des offenen Charakters der Forschungsfrage wird für deren Beantwortung eine Fallstudie durchgeführt. Im zweiten Kapitel wird als notwendige Voraussetzung für die Verwendung von Smart Contracts zunächst das Konzept der Blockchain detailliert diskutiert. Dazu wird der Begriff definiert und historisch eingeordnet, anschließend werden zentrale Grundfunktionen und Plattformen vorgestellt, welche auf Blockchain Technologien beruhen. Um das komplexe Zusammenspiel der einzelnen Komponenten genauer zu erläutern, wird daraufhin anhand des populären Bitcoin-Systems die grundlegende Funktionsweise von Blockchain Technologien erklärt. Das dritte Kapitel thematisiert allgemein das Konzept der Smart Contracts, nach einer Begriffsklärung werden besondere Charakteristika

⁵ Vgl. Belinky et al. 2015, S. 15.

7. Fazit und Ausblick

Ziel dieser Arbeit war es zu untersuchen, auf welche Art und Weise Smart Contracts in verschiedenen Anwendungsbereichen eingesetzt werden können. Zunächst wurden elementare technische Grundlagen von Blockchain Technologien und Smart Contracts dargestellt. Anschließend wurden Einsatzmöglichkeiten und praktische Anwendungsfälle von Smart Contracts untersucht. Dabei wurde ein verstärkter Fokus auf den Einsatz im Finanzsektor, im Rahmen des IoT, in Lieferketten, in der Lizenzierung sowie in der Verwaltung von Organisationen gelegt. Dabei wurden gleichermaßen wissenschaftliche und praktische Ansätze betrachtet. Innerhalb einer anschließenden Diskussion wurden die Ergebnisse dieser Untersuchung kritisch betrachtet und auf dieser Basis wurde die Forschungsfrage beantwortet. Im Ergebnis konnten bei der Verwendung von Smart Contracts bis dato nur wenige echte Durchbrüche erzielt werden. Trotzdem sehen sowohl Wissenschaft als auch Wirtschaft großes Potenzial in der Verwendung von Smart Contracts, vor allem im Hinblick auf mögliche Kostenersparnisse und Effizienzsteigerungen durch die Automatisierung von Workflows.

Trotz des verhältnismäßig frühen Entwicklungsstadiums von Blockchain Technologien und Smart Contracts existieren bereits zahlreiche theoretische und praktische Implementierungsansätze. Besonders im Finanzbereich ist die Entwicklung am weitesten fortgeschritten, so sind bereits erfolgreiche Testläufe der automatischen Abwicklung von Wertpapiergeschäften durchgeführt worden. Dass die Steuerung von Geräten durch Smart Contracts innerhalb eines IoT Systems funktionieren kann, verdeutlicht ein Pilotprojekt von IBM und Samsung. Dabei wurde eine Waschmaschine in die Lage versetzt, mithilfe von Sensoren die Knappheit von Waschmittel festzustellen und dieses selbstständig durch die Nutzung von Smart Contracts nachzubestellen. Die Vision einer Sharing Economy, der flexiblen Vermietung einer Vielzahl von Alltagsgegenständen, wird durch die Integration von Smart Contracts und IoT ein Stück realistischer. Das Startup Slock.it hat ein intelligentes Türschloss entwickelt, welches die effiziente Vermietung von Wohnraum durch Smart Contracts ermöglicht. Bis diese sogenannten Slocks allerdings Serienreife erreicht haben, werden noch einige Jahre vergehen. Im Rahmen der prognostizierten enormen Zunahme der Anzahl IoT-fähiger Geräte werden sich in Zukunft weitere Anwendungsfälle von Smart Contracts in IoT Ökosystemen ergeben. Lieferketten können durch die automatische Transaktionsabwicklung und die verbesserte Ortungsfähigkeit von Produkten transparenter gestaltet werden. Eine gerechte Zahlungsabwicklung von Tantiemen in der Musikindustrie kann durch die Verwendung von Smart Contracts ermöglicht werden, wie das Startup Ujo verdeutlicht. Sogar die Verwaltung ganzer Organisationen ist durch die Implementierung organisationsspezifischer Regeln in Smart Contracts möglich.

Die Weiterentwicklung der vorgestellten Ansätze ist vor einer praxistaugliche Anwendung von Smart Contracts notwendig. Allerdings belegen erfolgreiche Pilotprojekte und Use Cases, dass bereits erhebliche Fortschritte im Einsatz von Smart Contracts erzielt werden konnten. Leistungsfähigkeit und Robustheit von Blockchain Technologien, welche die Basis für die Verwendung von Smart Contracts bilden, müssen verbessert werden. Die Klärung rechtlicher Fragestellungen, welche sich aus der Verwendung von Smart Contracts ergeben, ist

Voraussetzung für eine Alltagsreife. Smart Contracts werden das bestehende Rechtssystem nicht revolutionieren, allerdings ist eine Veränderung des Aufgabenbereichs von Anwälten denkbar. Sollte es künftig möglich sein, durch Smart Contracts bindende Verträge nach dem Rechtsinn einzugehen, müssten Anwälte die Erstellung von Smart Contracts beaufsichtigen oder selbst durchführen.

Die zugrundeliegenden Blockchain Technologien sind erst vor wenigen Jahren in den Fokus von Wissenschaft und Wirtschaft geraten. Daher ist es verständlich, dass sich Smart Contracts noch am Anfang eines langen Entwicklungsprozesses befinden und noch nicht ihr volles Potenzial entfalten konnten. Die Standardisierung von Smart Contracts ist erforderlich, um eine breite Akzeptanz und Nutzung zu ermöglichen. Es wird auch in Zukunft eine Vielzahl von Verträgen und Vereinbarungen geben, welche nicht durch Smart Contracts abgebildet werden können, sondern menschliche Kommunikation erfordern. Zusätzlich zu den vorgestellten Anwendungsbereichen gibt es bereits heute zahlreiche weitere Ansätze, etwa im Gesundheitswesen und im Aufbau von Strommärkten. Es kann erwartet werden, dass sich in den kommenden Jahren weitere spannende Anwendungsmöglichkeiten von Smart Contracts ergeben.