FOM Hochschule für Ökonomie & Management München

Berufsbegleitender Studiengang
Wirtschaftsinformatik, 1. Semester

Seminararbeit

über das Thema

Herausforderungen und Potentiale der Blockchain-Technologie dargestellt am Beispiel von Smart-Contracts

Betreuer: Prof. Dr. Thomas Städter

Autor: Florian Hofsäss
Matrikelnr.: 332025
Abgabe: 28.02.2018

Inhaltsverzeichnis

Abbildungsverzeichnis **IV**

1. Einleitung **1**

2. Ziel der Arbeit **1**

3. Methodik **2**
3.1. Vorgehen . . . 2
3.2. Literaturrecherche . . . 2
3.3. Forschungsfragen . . . 3

4. Definition und Abgrenzung **3**
4.1. Bestandteile der Blockchain . . . 3
4.1.1. Peer to Peer Networking . . . 3
4.1.2. Asymmetrische Kryptographie . . . 4
4.1.3. Kryptografisches Hashing . . . 4
4.1.4. Aufbau eines Blocks . . . 5
4.1.4.1. Version . . . 5
4.1.4.2. Referenz . . . 5
4.1.4.3. Zeitstempel . . . 6
4.1.4.4. Schwellenwert . . . 6
4.1.4.5. Nonce . . . 6
4.1.5. Aufbau der Transaktionen . . . 6
4.2. Konsensfindung . . . 7
4.2.1. Proof of Work . . . 7
4.2.2. Proof of Stake . . . 8
4.3. Kryptoassets . . . 8
4.4. Smart-Contracts . . . 8

5. Rechtliche Anforderungen nach BGB **9**
5.1. Ziel durch den Einsatz von Blockchaintechnologien . . . 9
5.2. Vertragsgrundlagen nach BGB . . . 9
5.2.1. Geschäftsfähigkeit . . . 10
5.2.2. Willenserklärungen . . . 10
5.2.3. Rechte und Pflichten aus einem Vertragsverhältnis . . . 10
5.2.4. Mängelansprüche . . . 10

5.3. Erfüllbarkeit durch Smart-Contracts 10
5.3.1. Geschäftsfähigkeit 11
5.3.2. Willenserklärungen 11
5.3.3. Rechte und Pflichten 11
5.4. Zwischenfazit 12
5.5. Möglichkeiten von Smart-Contracts 13
5.5.1. Bedingungen durch Smart-Property 13
5.5.2. Entscheidungsfindung durch Orakel 14

6. SWER Analyse **14**
6.1. Stärken 15
6.1.1. Dezentralität 15
6.1.2. Integrität 16
6.1.3. Open Execution 16
6.2. Schwächen 16
6.3. Risiken 16
6.3.1. Zentralisierung durch Orakel 16
6.3.2. Entlohnung der Full Nodes 17
6.3.3. Sicherheit 17
6.3.3.1. 50 + 1 17
6.3.3.2. Selfish Mining 18
6.4. Erwartungen 19
6.4.1. Multisig 19
6.4.2. Alternative Konsensfindungsmodelle 19
6.4.3. Schiedsstellen 20
6.4.4. Verteilte Orakel 21

7. Fazit **22**

Literaturverzeichnis **V**

A. Glossar **VII**

B. Ehrenwörtliche Erklärung **VIII**

Abbildungsverzeichnis

1. Zusammenhang zwischen privatem und öffentlichem Schlüssel 4
2. Blockaufbau und deren Beziehung untereinander 5
3. Smart-Contracts ohne externe Ereignisse 13
4. Zusammenhänge in einem Smar-tContracts unter Verwendung von Orakel 15
5. Selfish Mining 18

1. Einleitung

Am 17.12.2017 steigt der Kurs der Bitcoin auf Tagesbasis auf 19.290 US-Dollar und zieht mit einer Rendite von 1832% seit Jahresbeginn nicht nur das Interesse von Anlegern auf sich.[1] Auch Andere wollen an der Entwicklung dieser Technologie partizipieren, wie die Netzwerkleistung des Bitcoin-Netzwerkes zeigt. Mit einer Rechenleistung von rund 9,3 Mio. Tera Hashes pro Sekunde, bildet das Netzwerk eine Rechenleistung von rund dem 1.3 Millionenfache eines herkömmlichen Vierkernprozessors ab.[2] Zusätzlich sind auch viele Unternehmen, vor allem im Finanzsektor, an dieser Technologie interessiert. Neben der Landesbank Baden-Württemberg und Daimler AG haben sich auch der französische Versicherer AXA sowie ein Konsortium bestehend aus den Großbanken Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale und UniCredit unter Mitarbeit von IBM für die Blockchain ausgesprochen und großes Interesse am Einsatz dieser Technologie bekundet und diese teilweise bereits umgesetzt.[3] Vor diesem Hintergrund stellt sich die Frage, welche Besonderheiten und damit verbundene Möglichkeiten und Herausforderungen diese Technologie mit sich bringt.

2. Ziel der Arbeit

Ziel der Arbeit ist, neben der ausführlichen Erläuterung der Blockchain Technolgie, eine Gegenüberstellung von Herausforderungen und Möglichkeiten am Beispiel von Smart-Contracts, welche im weiteren Verlauf der Arbeit näher erläutert werden. Die Arbeit soll daher einen Leitfaden bieten, mit dem Unternehmen eine objektive Bewertung vornehmen können, ob die Blockchain eine geeignete Technologie für die angestrebte Lösung ist.

[1] o.V. 2017.
[2] Ebd.
[3] Daimler AG 2017, Hüfner 2017, Williams-Grut 2017

3. Methodik

Zu Beginn wurde eine ein breites Spektrum an Fachliteratur gesichtet um den Umfang und die Funktionsweise der Blockchain im Detail zu beleuchten. Dabei wurde sich aufgrund des schnelllebigen Umfelds der Thematik vor Allem auf die Aktualität sowie auf die Qualität der Literatur konzentriert.

3.1. Vorgehen

Als Forschungsdesign wird die Grounded Theory gewählt. Dabei soll über eine umfassende Literaturrecherche eine neue These gebildet und Forschungsfragen abgeleitet werden.

3.2. Literaturrecherche

Bei der Literaturrecherche werden folgende Datenbanken verwendet:

1. JSTOR
2. SpringerLink
3. WISO
4. statista.de
5. GoogleScholar
6. EDS (EBSCO Discovery Services)

Mit einer vowärtsgerichteten Suche, ausgehend von dem Basispapier der Technologie von Satisho Nakamato aus dem Jahr 2009, wurde eine Vielzahl der Treffer erhoben. Ausgehend von deren Relevanz wurden mit einer rückwärtsgerichteten Suche weitere valide und relevante Ergebnisse hinzugefügt. Ergänzend wurde ebenfalls über oben aufgeführte Datenbanken eine umfassende Suche durchgeführt die sich mit folgenden Keywords befasste:

1. *Blockchain*
2. *Smart Contracts* AND *Blockchain*
3. *Proof of Stake* AND *Proof of Work*
4. *private Blockchain* AND *public blockchain*
5. *Ethereum* AND *Smart Contracts*
6. *Oracles* AND *Smart Contracts*

3.3. Forschungsfragen

Als zentrale Forschungsfragen der Arbeit und somit als Leitfaden dienten:

> Inwieweit ermöglichen Smart-Contracts rechtverbindliche Verträge vor dem Hintergrund geltender Gesetze?
>
> Inwiefern ermöglichen Smart-Contracts einen Fortschritt in der Vertragsgestaltung und -erfüllung?

Im Laufe der Literaturrecherche kristallisierten sich dabei folgende Hypothesen heraus:

- Smart-Contracts erlauben ein gültiges Rechtsgeschäft im Sinne des BGB.
- Bedingungen zur verlässlichen Erfüllung eines Smart Contracts können sich nur auf interne Blockchain-Ereignisse beziehen.

4. Definition und Abgrenzung

Im Folgenden soll die Technologie Blockchain erläutert werden. Ebenso wird der Begriff Smart-Contracts spezifiziert und von anderen artverwandten Begriffen abgegrenzt.

4.1. Bestandteile der Blockchain

Wie der Name Blockchain bereits suggeriert, besteht die Blockchain aus miteinander verketteten Blöcken. Ein Block verhält sich als eine Art Container für verschiedene Transaktionen und bildet dabei eine Entität der Blockchain ab.[4]

4.1.1. Peer to Peer Networking

Bei der Blockchain oder auch „Distributed Ledger Technology“ handelt es sich um ein dezentrales Peer to Peer Netzwerk über welches kryptografisch signierte Transaktionen gespeichert werden. Charakteristisch für ein solches Peer to peer Netzwerk ist dabei, dass alle Netzwerkteilnehmer grundlegend gleichgestellt sind

[4] Berentsen et al. 2017, S. 95 ff. Dannen 2017, S. 1

und mehrere Verbindungen zu anderen Teilnehmern des Netzwerkes pflegen.[5] Bedingt dadurch, dass jeder Netzwerkteilnehmer eine aktuelle Version der ihm aktuell bekannten Blockchain speichert, ist die Blockchain eine vollständig dezentrale und kryptografische Datenbank.[6] Dabei stellt die dezentrale Struktur über mehrere Partner sowie das kryptographische Speichern der Daten den größten Unterschied zu bisherigen Datenbanklösungen dar.[7]

4.1.2. Asymmetrische Kryptographie

Für die Freigabe und Signierung von Transaktionen kommt asymmetrische Kryptographie in Form von Schlüsselpaaren zum Einsatz. Solche Schlüsselpaare haben die mathematische Eigenschaft, dass aus dem privaten Schlüssel der zugehörige öffentliche Schlüssel abgeleitet werden kann, dieser aber jedoch nicht zur Erstellung des privaten Schlüssels verwendet werden kann. Das Schlüsselpaar wird folglich durch eine Einwegfunktion verbunden, wie die Abbildung „Zusammenhang zwischen privatem und öffentlichem Schlüssel“ illustriert.[8] Auf diesem Weg wird die Legitimität der Transaktion sichergestellt.

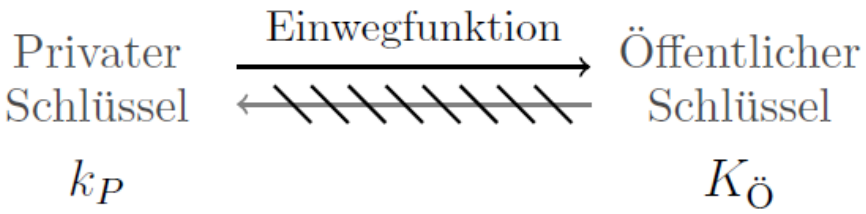

Abbildung 1: Zusammenhang zwischen privatem und öffentlichem Schlüssel
Quelle: Berentsen et al. 2017, S. 120

4.1.3. Kryptografisches Hashing

Um sicherzustellen, dass die Integrität der Blocks gewährleistet ist, muss jeder Block mit einer Prüfsumme (Hash) versehen werden. Dabei werden zur Generierung der Hashes alle Inhalte des jeweiligen Blocks herangezogen. Sollte sich

[5] Berentsen et al. 2017, S. 53.
[6] Yli-Huumo et al. 2016, S. 2f.
[7] Dannen 2017, S. 1.
[8] Berentsen et al. 2017, S. 144.

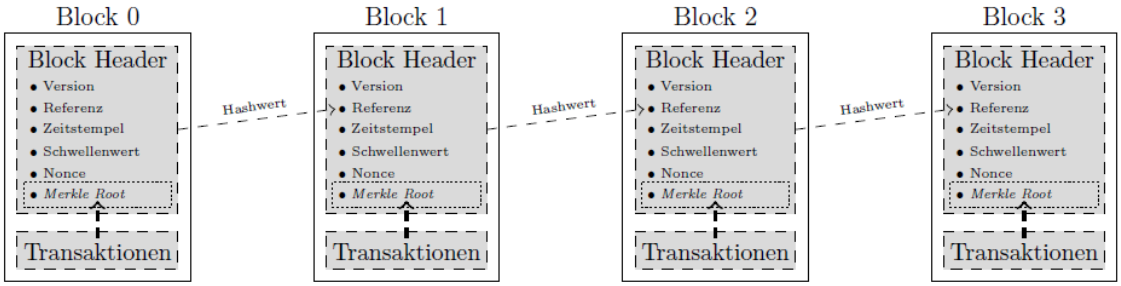

Abbildung 2: Blockaufbau und deren Beziehung untereinander
Quelle: Berentsen et al. 2017, S. 200

einer der Inhalte dabei ändern, ändert sich auch zwangsläufig die Prüfsumme des Blocks. Somit würde der berechnete Wert nach Veränderung des Blocks nicht mehr mit dem Inhalt des Blocks übereinstimmen und die Manipulation würde schnell bemerkt werden.[9]

4.1.4. Aufbau eines Blocks

Der Block ist der elementare Bestandteil der Blockchain und ist innerhalb dieser der Container für Transaktionen. Wie viele Transaktionen dabei in einen Block passen, hängt von der erlaubten Größe eines Blocks ab, die jede Blockchainimplementierung für sich selbst definieren kann.

4.1.4.1. Version In diesem Teil des Headers ist die Version der Blockchain vermerkt, unter welcher der Block erstellt wurde. Da im Laufe der Zeit die Regeln für die Validierung der Blockchain verschärft (Soft Fork) oder gelockert (Hard Fork) werden können, ist die Version relevant um die für den Block notwendigen Validierungskriterien heranziehen zu können.[10]

4.1.4.2. Referenz Die Referenz speichert den Hashwert des jeweils vorangegangenen Blocks. Wird in dem Beispiel aus Abbildung „Blockaufbau und deren Beziehung untereinander“ der Block 1 in seiner Integrität beschädigt, müsste die Referenz in Block 2 angepasst werden. Dadurch ändert sich auch dessen Hashwert und die in Block 3 gespeicherte Referenz müsste angepasst werden. Daraus folgt, dass bei einer Änderung der Referenz des Blocks n, alle Blöcke zwischen n und dem jüngsten Block neu errechnet werden müssten.[11]

[9] Dannen 2017, S. 4.
[10] Berentsen et al. 2017, S. 197f.
[11] Ebd., S. 197f.

4.1.4.3. Zeitstempel Dieser Wert repräsentiert das Datum und die Uhrzeit, an dem der Block erstmalig in die Kette aufgenommen wurde.

4.1.4.4. Schwellenwert Um einen Block einer bestehenden Kette hinzufügen zu können, müssen aktive Teilnehmer, sogenannte Miner, Hashes berechnen die bestimmten Kriterien entsprechen. Dieses Kriterium wird zentral vorgegeben und wird Schwellenwert oder auch „target“ genannt. Es gibt vor, dass ein gültiger Block einen Hash besitzen muss der kleiner als der Schwellwert ist. Ziel dieses targets ist es, die Zeit zwischen der Generierung zweier Blöcke dynamisch steuern zu können.[12]

4.1.4.5. Nonce Die Nonce ist eine - einmalig in der Blockchain vorkommende - Zufallszahl die sicherstellt, dass auch bei identischem Inhalt zweier Blöcke die daraus erstellten Hashes unterschiedlich sind.[13]

4.1.5. Aufbau der Transaktionen

Jede Transaktion hat mindestens einen Transaktionsinput, welcher Guthaben aus einer vorangehenden Transaktion referenziert. Der Transaktionsoutput ist das bei einer anderen Person entstehende Guthaben. Daher ist eine Bitcoin, die im eigenen Wallet zur Übertragung bereitsteht ein valider und noch nicht verwendeter Transaktionsoutput und wird bei einer neuen Transaktion zum Transaktionsinput. Im weiteren Verlauf der Arbeit wird daher häufiger von Transaktionsoutputs zu lesen sein, um allgemeingültige Aussagen treffen zu können.
Grundlegend gelten für Transaktionen folgende Kriterien:[14]

- Haben mindestens einen Transaktionsinput
- Haben mindestens einen Transaktionsoutput
- Es müssen alle erforderlichen Signaturen vorhanden sein
- Transaktionsinputs müssen gültige und noch nicht referenzierte Transaktionsoutputs referenzieren

Sollte eines dieser Kriterien nicht erfüllt sein, so wird die Transaktion vom gesamten Netzwerk ignoriert.

[12] Berentsen et al. 2017, S. 197f.
[13] Ebd., S. 197f.
[14] Ebd., S. 193ff.

Transaktionen können k Transaktionsinputs und j Transaktionsoutputs beinhalten. Ebenso müssen Transaktionen von allen benötigten Walletinhabern der Absenderadressen signiert werden. Meist reicht eine Signatur pro Absenderadresse. Es existieren jedoch weitere Arten von Adressen, sogenannte „Multisig-Adressen“ bei denen m private Schlüssel zum signieren einer abgehenden Transaktion vorhanden sind und mindestens n Signaturen vorliegen müssen um die Transaktion als gültig betrachten zu können, wobei stets $n \leq m$ gilt.[15]

4.2. Konsensfindung

In einem dezentralen Netzwerk, wie der Blockchain, ist es im Vergleich zu zentralisierten Systemen nicht möglich, eine Instanz nach dem aktuellen Stand zu fragen und sicher gehen zu können, dass es sich dabei auch tatsächlich um den aktuellsten Stand handelt. Als Beispiel dient jede Art von Register wie das Handels- oder das Grundbuchregister. So sind Änderungen erst mit Eintragung in das etwaige Register anerkannt, da diese Register den öffentlichen Glauben genießen.
Bei dezentralen System muss ein Prozess definiert werden, der ermöglicht, dass sich alle Netzwerkteilnehmer über den aktuell gültigen Stand einig sind und klargestellt ist, wie Informationen dem Netzwerk zufließen können. Grundsätzlich gelten bei allen Ansätzen folgende Kriterien:[16]

- Die längste im Netzwerk verfügbare Kette gilt als aktuelle Version
- Nur valide Blöcke können in die Blockchain aufgenommen werden
- Nur eine valide Historie der Blockchain, kann als gültige Blockchain in Betracht gezogen werden

Die folgenden beiden Ansätze, stellen die zwei dominierenden Ansätze dar, wie neue Blöcke der Blockchain zugeführt werden können.

4.2.1. Proof of Work

Bei dem Proof of Work-Ansatz gibt es für den Netzwerkteilnehmer der erfolgreich neue Informationen der Blockchain zuführt einen sogenannten Mining-Reward. Um dabei die Zeitintervalle steuern zu können in denen neue Blöcke der Blockchain zugeführt werden, wird den Teilnehmern eine schwer zu lösende Aufgabe

[15] Sixt 2017, S. 164,Berentsen et al. 2017, S. 184 f.
[16] Ebd., S. 54ff.

gestellt. Der Teilnehmer der die Aufgabe als erstes löst, kann die Lösung in den Block schreiben und diesen Block in das Netzwerk propagieren. Die Chance auf etwaige Rewards steigt somit mit zunehmender Rechenleistung im Verhältnis zum Gesamtnetzwerk.[17] Folglich ist der Proof of Work-Ansatz sehr rechenintensiv.

4.2.2. Proof of Stake

Beim Proof of Stake wird nicht auf Basis eines Arbeitsnachweises ein Konsens erzielt, sondern anhand der Verteilung des bisherigen Vermögens. Somit entspricht die Entscheidungskraft eines Netzwerkteilnehmers seinem Anteil am Gesamtvermögen der Kryptowährung.[18] Dieser Ansatz unterstellt, dass die Entscheider mit mehr Entscheidungskraft weniger Interesse an negativen Entscheidungsfolgen für das Netzwerk haben, da sie zu einem größeren Teil selbst davon betroffen wären.[19]

4.3. Kryptoassets

Als Kryptoassets bezeichnet man die Verknüpfung eines weiteren Zahlungsversprechens an die eigentliche Kryptoeinheit. Diese Möglichkeit besteht auch in der Bitcoin Implementierung. Hier spricht man von „Colored Bitcoins“. Beispielsweise kann ein solches Zahlungsversprechen die Übergabe von Wertpapieren oder einer beliebig anderen Leistungen sein. Hervorzuheben ist jedoch, dass dieses Zahlungsversprechen dem Kontrahentenrisiko unterliegt, da das Einlösen des angeknüpften Zahlungsversprechens durch den Partner selbst geschehen muss und nicht durch die Blockchain besichert werden kann.[20]

4.4. Smart-Contracts

Unter Smart-Contracts ist eine Transaktion zu verstehen, deren Transaktionsoutput keinen anderen Wallet, sondern einen Script-Hash referenziert. Dieser Hash repräsentiert ausführbaren Code, daher spricht man im Zusammenhang von Smart-Contracts auch von Open Execution, da das zum Hash passende Skript öffentlich ist. Bei einigen Implementierungen auf Basis der Blockchain ist die zu

[17] Zheng et al. 2017, S. 8,Berentsen et al. 2017, S. 205ff.
[18] Zheng et al. 2017, S. 9.
[19] Sixt 2017, S. 113 f.
[20] Berentsen et al. 2017, S. 282ff.

Grunde liegende Programmiersprache turingkomplett, wie die Sprache „Solidity“ der Blockchain Ethereum. Die Sprache Script, welche für die Bitcoin verwendet wird, ist dies hingegen nicht. Daher gilt Ethereum als vorherrschendes Beispiel für Smart-Contracts. [21] Elementar ist dabei, dass Smart-Contracts jederzeit wiederverwendet werden können, da der Vertragsinhalt gleich bleibt und sich lediglich die Vertragsparteien ändern, da mehr Anwendungsfälle abbildbar sind.

5. Rechtliche Anforderungen nach BGB

In diesem Kapitel soll die Hypothese geprüft werden, ob in Form von Smart-Contracts geschlossene Verträge den rechtlichen Erfordernissen des BGB (Bürgerliches Gesetzbuch) entsprechen.

5.1. Ziel durch den Einsatz von Blockchaintechnologien

Betrachtet wird in diesem Fall der Zweck, ob der Einsatz von Treuhändern durch den Einsatz der Blockchaintechnologie obsolet wird und der Vertragsschluss, unter Verwendung dieser Technologie, gesetzeskonform ist. Als Treuhänder wird „eine juristische oder auch natürliche Person [verstanden], die stellvertretend für einen Auftraggeber bestimmte zugewiesene Aufgaben wahrnimmt. Die Treuhandpflicht versteht sich als die Pflicht, eine Gefährdung oder Veruntreuung zu vermeiden (...)“[22]. Darüber hinaus ist der Treuhänder vertraglich oder gar gesetzlich dazu verpflichtet, Interessen eines anderen Rechtssubjekts wahrzunehmen.[23]

5.2. Vertragsgrundlagen nach BGB

Im Folgenden werden die grundlegenden Erfordernisse an einen Vertrag nach dem Bürgerlichen Gesetzbuch dargestellt. Anschließend wird geprüft, ob es möglich ist, diese Gegebenheiten in Smart-Contracts adäquat abzubilden.

[21] Dannen 2017, S. 89,Berentsen et al. 2017, S. 289ff.
[22] Birgitta Dennerlein 2017.
[23] Löhnig 2006, S. 1.

5.2.1. Geschäftsfähigkeit

Grundlegend muss für einen gültigen Vertrag sichergestellt sein, dass alle beteiligten Parteien geschäftsfähig sind. Nach § 104 BGB ist dies dann der Fall, wenn der Betroffene das siebte Lebensjahr vollendet hat und geistig vollständig in der Lage ist, geschäftlich tätig zu sein. In §107 BGB wird ausgeführt, dass Minderjährige für die Vertragsschließung eine Zustimmung der gesetzlichen Vertreter benötigt, insofern er nicht „lediglich einen rechtlichen Vorteil erlangt § 107 BGB“.

5.2.2. Willenserklärungen

Nach § 126 III BGB i.V.m. § 126a BGB ist eine elektronische Form zur Vertragsschließung gültig, insofern das Gesetz keine Formvorschrift verlangt.

5.2.3. Rechte und Pflichten aus einem Vertragsverhältnis

Gemäß § 433 BGB „wird der Verkäufer einer Sache verpflichtet, dem Käufer die Sache zu übergeben und das Eigentum an der Sache zu verschaffen. Der Verkäufer hat dem Käufer die Sache frei von Sach- und Rechtsmängeln zu verschaffen. Der Käufer ist verpflichtet, dem Verkäufer den vereinbarten Kaufpreis zu zahlen und die gekaufte Sache abzunehmen § 433 II BGB.“

5.2.4. Mängelansprüche

Nach § 437 BGB steht dem Käufer im Falle eines Mangels das Recht auf Nacherfüllung nach § 439 BGB beziehungsweise der Vertragsrücktritt nach §§ 440, 323 BGB oder 326 V BGB oder Kaufpreisminderung nach § 441 BGB zu.
In diesem Rahmen wird Konformität des Vertragsschlusses sowie der Möglichkeit der Substitution eines Treuhänders erörtert. Da Mängelansprüche weder Teil des gültigen Vertragsschlusses sind noch Aufgabe des Treuhänders, wird auf deren Erfüllbarkeit durch Smart-Contracts verzichtet.

5.3. Erfüllbarkeit durch Smart-Contracts

Im Folgenden soll geprüft werden ob den ermittelten rechtlichen Anforderungen nach BGB beim Einsatz von Smart-Contracts nachgekommen werden kann.

5.3.1. Geschäftsfähigkeit

Die Geschäftsfähigkeit der Parteien im Rahmen von Smart-Contracts sicherzustellen ist alleinig durch die Blockchain nicht möglich, da die beteiligten Parteien einer Blockchaintransaktion lediglich durch Hashes repräsentiert werden. Die Zuordnung zu einer natürlichen oder juristischen Person - also die Legitimation -, welche die Geschäftsfähigkeit sicherstellt, muss dabei im Vorfeld getroffen werden, wie auch die Autoren Pesch et. al. vor dem Hintergrund der Geldwäscheprävention verdeutlichen.[24]

5.3.2. Willenserklärungen

Eine Willenserklärung ist nach § 116 I BGB „nicht deshalb nichtig, weil sich der Erklärende insgeheim vorbehält, das Erklärte nicht zu wollen § 116 I BGB“. Daraus lässt sich schließen, dass eine Willenserklärung nicht ausdrücklich kund getan werden muss um gültig zu sein. § 133 BGB untermauert diese Einschätzung mit dem Hinweis, dass bei der „Auslegung einer Willenserklärung (...) der wirkliche Wille zu erforschen § 133 BGB“ sei. Mit dem Verweis auf ein BGH Urteil lässt sich eine Willenserklärung durch „Artikulierung (...) aber auch stillschweigend durch konkludentes Handel oder ausnahmsweise durch Schweigen“ abgeben.[25]

Durch das Signieren und Publizieren einer Transaktion kann daher hinreichend davon ausgegangen werden, dass der Betroffene eine gültige Willenserklärung im Sinne des BGB abgegeben hat.

5.3.3. Rechte und Pflichten

Das Recht des Käufers am Eigentum an dem erworbenen Gut, sowie die Pflicht zur Abnahme und Zahlung des vereinbarten Kaufpreises ist im Rahmen der Blockchain möglich. Da sowohl die Übertragung des Guts sowie die Zahlung des Kaufpreises innerhalb einer Transaktion in das Netzwerk propagiert werden können, ist eine gleichzeitige Erfüllung der Pflichten gewährleistet. Sollte eine Transaktion abgelehnt werden, wird keine der Parteien in die Pflicht genommen. Problematisch könnten lediglich angeknüpfte Zahlungsversprechen sein, die unabhängig von der Durchführung der Transaktion sind.

[24] Pesch et al. 2017.
[25] juraforum.de 2017 nach BGHZ 111, 97, 101

Somit sind unter Verwendung der Blockchaintechnologie die grundlegenden Bestandteile eines Kaufvertrags nach BGB umsetzbar. Die Willenserklärungen der Vertragsparteien sind nach vorangegangener Legitimierung hinreichend als solche erkennbar und durch die persistierende Eigenschaft von Transaktionen innerhalb der Blockchain ausreichend dokumentiert. Die Erfüllung der Pflichten aus dem Kaufvertrag werden gleichzeitig von beiden Parteien erfüllt oder von beiden - aufgrund einer abgelehnten Transaktion - nicht erfüllt. Es ist jedoch sichergestellt, dass keiner der Partner schlechter gestellt ist als zuvor, wodurch ein gesondert bestellter Treuhänder obsolet ist.

5.4. Zwischenfazit

Daher ist festzuhalten, dass sich Smart-Contracts auf Basis der Blockchaintechnologie für die grundlegende Abbildung von Kaufverträgen eignen. Es ist jedoch deutlich darauf hinzuweisen, dass „Kaufverträge“, welche eine Gegenleistung in Kryptowährungen anstatt in Fiat-Geld vorsehen, rechtlich nicht als „Kaufverträge“ sondern als Tauschverträge gemäß § 480 BGB gelten.[26] Da § 480 BGB regelt: „Auf den Tausch finden die Vorschriften über den Kauf entsprechende Anwendung. § 480 BGB“ sind alle Erläuterungen parallel zum dargelegten Kaufvertrag gültig. Abseits der Bestimmungen des BGB, erläutert Sixt umfassend, dass rechtsgültige Verträge auf Basis von Bitcoin, daher auf Basis von Blockchaintechnologie, konform zu dem deutschen Grundgesetz sind.[27]

Folglich kann die Hypothese, dass mittels Blockchaintechnologie rechtsgültige Kaufverträge, beziehungsweise Tauschverträge, geschlossen werden können, bekräftigt werden.

[26] Sixt 2017, S. 121 ff.
[27] Ebd., S. 121 ff.

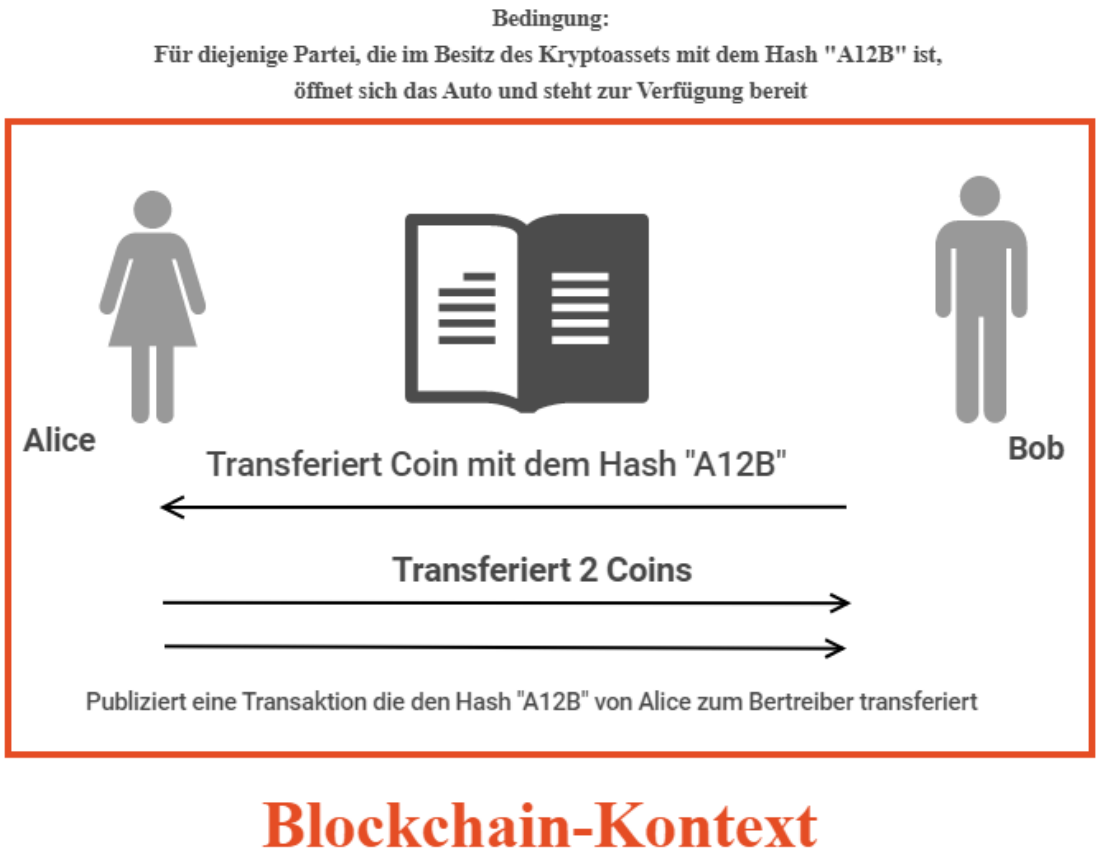

Abbildung 3: Smart-Contracts ohne externe Ereignisse
Quelle: eigene Abbildung

5.5. Möglichkeiten von Smart-Contracts

Neben den bereits dargestellten Transaktionen erlaubt die Technologie der Smart-Contracts „Script-to-Hash“-Transaktionen (siehe Abschnitt 4.4 „Smart-Contracts“ auf Seite 8). Dieses Skript ist für die Auslösung an Bedingungen geknüpft. [28]

5.5.1. Bedingungen durch Smart-Property

Ein bekannter Anwendungsfall für Smart-Contracts, beziehungsweise in dem Fall der Subkategorie Smart-Property auf die auch die Autoren Berentsen et. al. zu sprechen kommen, ist Car-Sharing.[29] Dabei enthält eine der Coins ein angeknüpftes Versprechen. Das Versprechen ist, dass sich dem Besitzer der Coin mit diesem Hash ein bestimmtes Fahrzeug öffnet.

[28] Dannen 2017, S. 89 ff.Berentsen et al. 2017, S. 292 ff.Kaulartz 2016, S. 34 ff.
[29] vgl. Berentsen et al. 2017, S. 286f.

Möchte Alice nun ein Auto unter Verwendung der Blockchaintechnologie mieten, so muss der Betreiber ihr das notwendige Kryptoasset mit dem erwartenden Hash verschaffen - hier: „A12B“ -. Im Gegenzug propagiert Alice eine Transaktion, welche den Mietpreis enthält. Zusätzlich wird eine weitere Transaktion in das Netzwerk propagiert, welche zum Ende der Mietzeit die Coin mit dem Hash „A12B“ an den Car-Sharing-Betreiber gutschreibt.
Für die Entscheidung ob Alice der Zugang zu dem Auto gewährt werden kann, ist zu keinem Zeitpunkt die Information über externe Zustände notwendig.[30] Es muss lediglich geprüft werden, ob der Anfragende im Besitz des notwendigen Kryptoassets „A12B“ ist.

5.5.2. Entscheidungsfindung durch Orakel

Um Bedingungen in einem Smart-Contract, welche an externe Zustände wie Aktienkurse, Kontobewegungen oder Sportergebnisse geknüpft sind, auswerten zu können, werden von der Blockchain unabhängige Instanzen benötigt, denen für die Entscheidungsfindung vertraut werden kann.[31]

Die Abbildung „Zusammenhänge in einem Smar-tContracts unter Verwendung von Orakel“ zeigt die Zusammenhänge unter den Vertragspartnern Alice und Bob, die unter Verwendung eines Smart-Contracts eine Wette abschließen. Um bewerten zu können, ob der Aktienkurs gefallen oder gestiegen ist, müssen externe Zustände einbezogen werden. Für die Bewertung solcher Zustände werden sogenannte „Orakel“ (*engl. Oracles*) verwendet.[32]
Je nach Einschätzung des Orakels, wird eine Bedingung des Smart-Contracts erfüllt und die Auszahlungstransaktion wird angestoßen.

6. SWER Analyse

Neben der ausgearbeiteten Hypothese soll im Folgenden eine SWER-Analyse durchgeführt werden, die Stärken (*S*trengths), Schwächen (*W*eaknesses), Erwartungen (*E*xpectations) und Risiken (*R*isks) beleuchtet. Es werden bewusst zuletzt die Erwartungen thematisiert, da bestehende Risiken elementaren Einfluss auf die Erwartungen bezüglich der Weiterentwicklung der Blockchaintechnologie haben.

[30] Spancken et al. 2016, S. 58f.
[31] Kaulartz 2016, S. 34ff,Spancken et al. 2016, S. 59f.
[32] vgl. Berentsen et al. 2017, 294.ff.

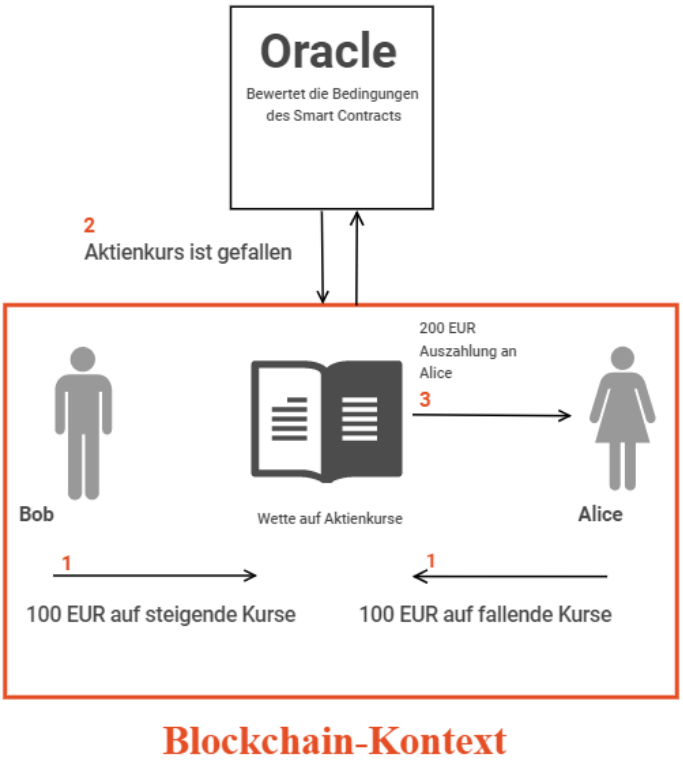

Abbildung 4: Zusammenhänge in einem Smar-tContracts unter Verwendung von Orakel
Quelle: eigene Abbildung

6.1. Stärken

Als Stärken gehen vor allem die charakteristischen Eigenschaften der Blockchain-technologie hervor.

6.1.1. Dezentralität

Unter der Annahme einer Nicht-Privaten Blockchainlösung, also einer öffentlichen oder zumindest konsortialen Variante, ist die Dezentralität ein großer Vorteil von Smart-Contracts. Dadurch kann gewährleistet werden, dass der Vertragsschluss auf einer neutralen Basis geschlossen wird und keiner der Vertragsparteien der anderen Vertragspartei Vertrauen beim Vertragsschluss entgegenbringen muss. Ebenso ist die Blockchain durch die verteilte Struktur resistent gegen DDoS-Attacken (Distributed Denial of Service) oder Manipulationsversuchen von Teilnehmern des Netzwerks.[33]

[33] Dannen 2017, S. 175 f.

6.1.2. Integrität

Durch die Tatsache, dass jeder Block seinen vorangehenden Block referenziert (ausgeführt in Abschnitt 4.1.4.2 „Referenz“ auf Seite 5), ist der Austausch oder das nachträgliche Verändern von Transaktionen nur schwer möglich. Somit sind die in der Transaktion definierten Zahlungsströme, sowie die Willenserklärungen in Form von Signaturen als auch der Vertragsinhalt in Form des hinterlegten Smart-Contracts-Skript-Hashes persistiert. Im Vergleich zu herkömmlichen Methoden in Papierform, ist somit eine nachträgliche Prüfung des Vertragsinhaltes leichter möglich.

6.1.3. Open Execution

Da der Inhalt der Smart-Contracts für Jedermann einsehbar ist, können alle Vertragsparteien im Vorfeld alle Vertragsbedingungen einsehen. So ist für Beteiligte nachhaltig und öffentlich einsehbar, unter welchen Bedingungen die Zahlung zu seinen Gunsten ausgelöst wird.

6.2. Schwächen

Den Stärken, die vor Allem auf Aspekte der Transparenz und der Einhaltung von Rechten und Pflichten abzielen, stehen jedoch Schwächen gegenüber.

Vor allem die Thematik rund um Skalierbarkeit scheint ein größeres Hemmnis für die Einführung von blockchainbasierten Systemen zu sein. Aufgrund der Vorgehensweise, bei der Erstellung jedes neuen Blocks alle bisherigen Blocks validieren zu müssen, nimmt die Performanz mit zunehmender Anzahl an Blocks ab.[34] Ein weiterer Nachteil entsteht durch Proof of Work gestützte Systeme, da diese Art des Minings ressourcenintensiv und zeitaufwendig ist.[35]

6.3. Risiken

6.3.1. Zentralisierung durch Orakel

Das Berücksichtigen von externen Ereignissen für Smart-Contracts scheint elementar zu sein, um Smart-Contracts für eine breite Masse an Nutzern interessant zu

[34] Sixt 2017, S. 95ff., 99f.Berentsen et al. 2017, S. 250 ff.
[35] Zheng et al. 2017.

machen, da sich hierdurch eine Vielzahl von Anwendungsfällen ergibt.[36] Auf entsprechende Risiken durch Manipulationen aufgrund zentralisierter Orakel weisen jedoch sowohl Kaulartz[37] als auch Berentsen hin.[38]

6.3.2. Entlohnung der Full Nodes

Die Interessen der Full-Nodes - Teilnehmer an der Blockchain die nicht nur Transaktionen in das Netzwerk propagieren, sondern zur Findung eines Konsens (Abschnitt 4.2 „Konsensfindung“ auf Seite 7) beitragen -, sind meist konträr zu den Interessen der Nutzer der Blockchain. Die Interessen der Full-Nodes sind meist monetär begründet, während die Nutzer eine möglichst kostengünstige Abwicklung ihrer Transaktion erwarten. Eine der bekanntesten blockchainbasierten Technologien ist „Bitcoin“. Das Bitcoin-Netzwerk benötigte vergangenes Jahr Strom im Wert von rund 40.000 USD pro Sekunde.[39]. Um die Beteiligung für „Full-Nodes“ weiterhin interessant zu machen, bedarf es daher zusätzlicher Erlöse die über Transaktionsentgelte oder Mining Rewards generiert werden müssen. Letztendlich zahlen jedoch die Nutzer für das Bestehen der Blockchain. Ist diese Bereitschaft der Nutzer nicht vorhanden, gehen die Zahlen der Full-Nodes - wie bei Bitcoin - stetig zurück und reduzieren damit die Vorteile der Transparenz und Dezentralität.[40]

6.3.3. Sicherheit

6.3.3.1. 50 + 1 Die in Abschnitt 4.2 „Konsensfindung“ auf Seite 7 dargelegte Vorgehensweise zeigt, dass im statistischen Mittel die Mehrheit des Netzwerkes über die Gültigkeit und Validität von Blocks und damit von Transaktionen entscheidet. Sollte es einer Partei gelingen die Mehrheit des Systems zu übernehmen, so ist die Sicherheit der Blockchain nicht mehr gewährleistet.[41] Vor allem durch die Bildung von sogenannten Mining-Pools, also von Zusammenschlüssel mehrerer Miner, wird das Problem zunehmend relevanter, da die Gefahr einer Zentralisierung steigt.[42] Dass bereits bei der Kryptowährung Bitcoin eine relevante

[36] Berentsen et al. 2017, S. 294.
[37] Kaulartz 2016, S. 34ff.
[38] Berentsen et al. 2017, S. 294.
[39] Ebd., S. 213.
[40] Sixt 2017, S. 100 ff.
[41] Berentsen et al. 2017, S. 59.
[42] Eyal et al. 2013, S. 4f. Yli-Huumo et al. 2016, S. 14f.

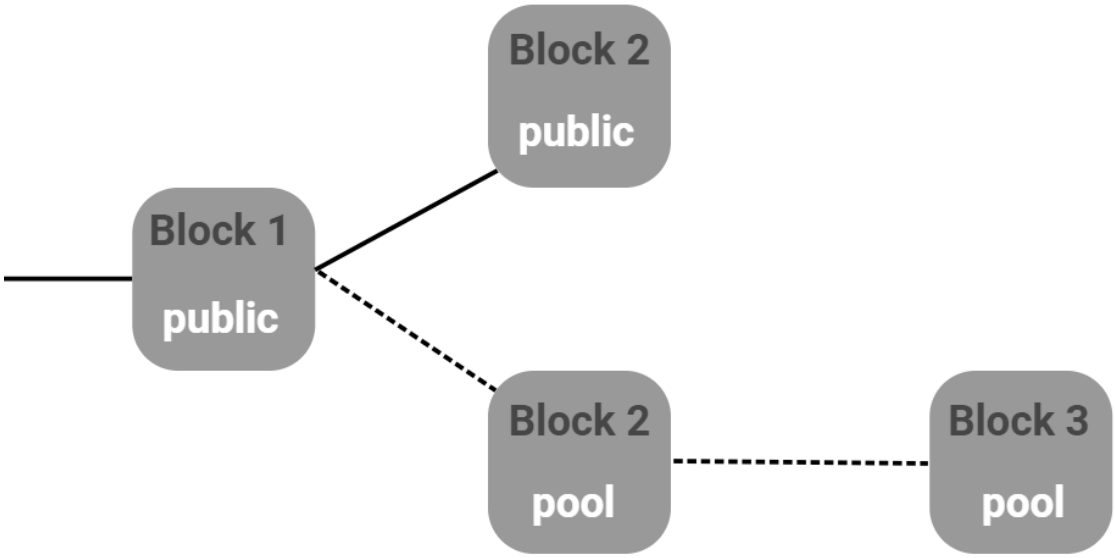

Abbildung 5: Selfish Mining
Quelle: Eigene Abbildung in Anlehnung an Eyal et al. 2013, S. 9

Zentralisierung stattgefunden hat, haben die Autoren Beikverdi et. al. in ihrer Studie nachgewiesen.[43]

6.3.3.2. Selfish Mining Unter Selfish Mining versteht man den Ansatz, die grundlegende Regel, stets an der längsten Kette der Blockchain zu minen, zu missachten.

Die Abbildung 5 „Selfish Mining“ auf Seite 18 zeigt geminte Blöcke und nummeriert sie anhand der Position. Angenommen sei folgende zeitliche Abfolge:

1. Block 1 wurde gemined und ein Team aus Minern (Pool) mined auf Basis dieses Blocks
2. Block $2_{(pub)}$ wurde von der Öffentlichkeit gemined, der Pool ignoriert diesen
3. Block $2_{(pool)}$ wurde vom Pool gemined und **nicht veröffentlicht**
4. Block $3_{(pool)}$ wurde vom Pool gemined und veröffentlicht

Die Konsequenz aus vorangegangener Vorgehensweise ist nun, dass die Öffentlichkeit auf Basis der längsten gültigen Kette - die mit dem letzten Element $3_{(pool)}$ - als Grundlage für den nächsten Block (4) betrachten wird. Dadurch würde Block $2_{(pub)}$ nicht in die Kette mit aufgenommen werden. Dass diese Vorgehensweise nicht nur theoretisch zum Erfolg führt, sondern eine tatsächliche Schwachstelle

[43] Beikverdi et al. 2015, S. 4.

des Mining Konzepts ist, haben die Autoren Eyal in ihrer Arbeit „Majority is not enough“ hinreichend aufgezeigt.[44]

6.4. Erwartungen

Auf Basis der dargestellten Stärken und Schwächen sowie der grundlegenden Möglichkeit Smart-Contracts als rechtsgültige Form zur Abbildung und Persistierung bereits geschlossener Verträge in Betracht zu ziehen, sind folgende zukünftige Entwicklungen der Blockchaintechnologie zu erwarten.

6.4.1. Multisig

Multisig - also Wallets zu denen m private Schlüssel gehören und mindestens n Signierungen die für eine Transaktion notwendig sind - (siehe Aufbau der Transaktionen) eignen sich für das Abbilden von Berechtigungskonzepten.
Beispielsweise ist es bei der Erteilung einer Prokura notwendig, diese im Handelsregister des entsprechenden Unternehmens nachtragen zu lassen und den Banken die Information über die Eintragung zukommen zu lassen um zu ermöglichen, dass der Prokurist Geldtransfers tätigen kann. Im Rahmen von Blockchaintransaktionen könnten Prokuristen einen privaten Schlüssel zu dem Wallet bekommen. Dabei würden m Schlüssel (für jeden Prokuristen und Vollmachtsträger) verteilt werden und $n = 1$ gewählt werden, so dass jeder Prokurist alleinig verfügen kann. Soll gewährleistet sein, dass nur 2 Prokuristen miteinander verfügen dürfen, kann $n = 2$ gewählt werden um dieses Konzept abzubilden.
Aufgrund des geringeren Aufwands im Vergleich zu bisherigem Vorgehen, scheinen Multisig-Wallets eine komfortable Option für Unternehmen zu sein, Berechtigungs- und Freigabekonzepte abzubilden.

6.4.2. Alternative Konsensfindungsmodelle

Wie bereits in Abschnitt 6.2 „Schwächen“ auf Seite 16 erläutert, ist der Proof of Work-Ansatz sehr ressourcenintensiv und skaliert schlecht. Der Proof of Stake erlaubt hingegen keine Umverteilung der Machtverhältnisse, wie z.B. der Proof of Work-Ansatz durch das Zuführen neuer Rechenleistung.[45]

[44] vgl. Eyal et al. 2013.
[45] Sixt 2017, S. 114,Zheng et al. 2017, S. 9

Mit dem Ziel ein skalierbares, öffentliches, performantes und dennoch sicheres System zu etablieren, müssen neue Konsensfindungsmodelle entwickelt werden.

Ein Beispiel für ein energiesparsames Konsensfindungsmodell ist „Ripple“.

Bei Ripple wird zwischen Server und Client unterschieden. Während der Server für die Validierung zuständig ist, kümmern sich die Clients ausschließlich um das Transferieren selbst. Dabei verfügt jeder Ripple Server über eine Unique Node List (UNL). Alle hier gelisteten Nodes werden für die Konsensfindung gefragt und liefern zurück, ob die Transaktion in die Blockchain aufgenommen werden soll oder nicht. Nur wenn die Zustimmung bei $\geq 80\%$ liegt, wird die Transaktion aufgenommen.[46]

Auch wenn das Ripple Protokoll ein guter Ansatz zu sein scheint, da er schneller und skalierbarer als bisher umgesetzte Proof of Work-Ansätze ist und bisherige Bedenken des Proof of Stake Ansatzes hier nicht relevant sind, muss bedacht werden, dass der Gedanke der Dezentralität hier eingeschränkt ist, da die UNLs teilweise zentralisiert ausgegeben werden.[47]

Ein weiterer Vorteil von Ripple scheint die Resistenz gegen byzantinische Fehler zu sein. Rund ein Fünftel aller beteiligten müssten falsche Aussagen liefern, um dem Netzwerk schaden zu können.[48] Bei dem Proof of Work Ansatz ist das Problem allgegenwärtig und bei dem Proof of Stake Ansatz abhängig von der Vermögensverteilung.

6.4.3. Schiedsstellen

Kaulartz schlägt vor etwaige Programmierfehler durch zuvor im Smart-Contract verankerte Schiedsstellen festzustellen und entsprechend abwickeln zu lassen.[49] Für eine solche Schiedsstelle kommt, ähnlich wie ohne Smart-Contracts die Treuhänder, „jede Person oder Institution in Betracht, auf die sich die Parteien im Vorfeld als neutralen Dritten verständigen.“[50] Als weiterer Anwendungsfall könnten Fehlentscheidungen durch Orakel berichtigt werden.
Gerade vor dem Hintergrund, dass Fehlentscheidungen durch Orakel als zentrale Schwachstelle der Smart-Contracts betrachtet werden kann, scheint eine neutrale

[46] Zheng et al. 2017, S. 89 f.
[47] Schwartz et al. 2014, S. 7.
[48] Ebd., S. 4.
[49] Kaulartz 2016, S. 36.
[50] Ebd., S. 36.

Instanz sinnvoll um solche Entscheidungen selektiv korrigieren zu können. Zu beachten ist dennoch, dass die Anzahl der Einsätze von Schiedsstellen geringer ist als die Anzahl der dafür notwendigen Treuhänder im Falle der Nichtverwendung von Smart-Contracts. Pro Smart-Contract müsste einmalig eine Schiedsstelle aktiv werden, während Treuhänder für jeden Vertragsschluss einberufen werden.

6.4.4. Verteilte Orakel

Da das Einbinden externer Zustände oder Ereignisse als Bedingungen für das Auslösen von Smart-Contracts wichtig ist, ist es notwendig, die in Abschnitt 6.3.1 „Zentralisierung durch Orakel“ auf Seite 16 dargestellten Risiken zu reduzieren.

Spancken liefert hier im Rahmen seiner Arbeit einen Vorschlag zu sogenannten „Distributed Oracles“. Dabei schlägt er vor, dass beide Vertragsparteien sich auf den Einsatz von n Oracles verständigen und je nach Art der Bedingung eine $\frac{2}{3}$ Mehrheit zur Anerkennung des Ergebnisses wählen oder bei Werten wie Aktienkursen das arithmetische Mittel unter Eliminierung der Extrema verwenden.[51]. Der Vorschlag würde das Problem zwar hinsichtlich dessen lösen, dass ein Orakel den Ausgang des Smart-Contracts beeinflussen kann, verlagert das Problem jedoch nur. Denn auch in dieser Vorgehensweise, wäre bspw. der Datenlieferant in der Lage die Ausgänge zu manipulieren. Des Weiteren müsste in diesem Fall alleinig dem Dienstleister vertraut werden können, der die Orakel zu Verfügung stellt.

Einen anderen Ansatz arbeiteten Pedro et. al. aus. Sie entwickelten „Witnet“, ein Protokoll basierend auf einem dezentralen Orakelnetzwerk, das selbst auf einer Blockchain basiert. Dabei wird jede Node, der „Witness“, das Ergebnis für einen Task, die Bedingung für einen Smart-Contract, auswerten. Entsprechend dem Proof of Stake-Ansatz einigen sich die Witnesses auf ein finales Ergebnis. Alle Witnesses, deren Ergebnis mit dem Finalen übereinstimmt, erhalten Reputationspunkte und werden bei der nächsten Entscheidung stärker berücksichtigt. Somit können sich Orakel unter Beweis stellen und haben im Vergleich zu neuen Orakeln eine höhere Bedeutung.[52]

[51] Spancken et al. 2016, S. 60.
[52] De Pedro et al. 2017, S. 6.

7. Fazit

Die erste Hypothese, dass Smart-Contracts auch nach BGB gültige Rechtsgeschäfte zulassen konnte bestätigt werden und ist eine der Grundlagen dafür, dass sich Smart-Contracts als Vertragsvariante sowohl im B2C, B2B als auch in der Machine-to-Machine-Kommunikation durchsetzen können.

Die Hypothese, dass zur verlässlichen und nachvollziehbaren Erfüllung eines Smart-Contracts nur interne Ereignisse berücksichtigt werden, konnte so nicht bestätigt werden. Auch wenn das Einbinden externer Ereignisse durch das Kanalisieren von Orakel Risiken und diverse Vertrauenschwierigkeiten mit sich bringt, scheint es Lösungen zu geben, die dem Vertrauensniveau der Blockchain selbst entsprechen. So scheint Witnet den Erwartungen an vertrauenswürdige Entscheidungen der Orakel gerecht zu werden und eliminiert dabei das Risiko durch Manipulation. Basis hierfür bildet ein Reputationssystems für Orakel, welches Orakeln mit bereits richtigen Entscheidungen einen höheren Anteil an der gesamten Entscheidungskraft gewährt, als Orakel mit einer niedrigeren Erfolgsquote.

Deutlich wurde jedoch auch, dass vor Allem im Bereich der Konsensfindung neue Ansätze geschaffen werden müssen, um den Einsatz der Blockchaintechnologie in Unternehmen zu vereinfachen. Denn während der Proof of Work-Ansatz zu ressourcenintensiv ist, ist der Proof of Stake-Ansatz zu einseitig. Hier könnten Ausgestaltungen wie das Ripple-Protokoll Grundlagen für weitere zielführende Lösungsansätze bieten.

Ansonsten scheint die Blockchaintechnologie vor Allem für Vertragsparteien die sich kaum oder nur wenig vertrauen können, eine sinnvolle und kostengünstige Alternative zu sein. Auch die Abbildbarkeit und sofortige Gültigkeit von Berechtigungen und Kompetenzen könnte in Zukunft ein relevanter Mehrwert der Blockchaintechnologie sein.

Literaturverzeichnis

[1] Beikverdi, A.; Song, J.: „Trend of centralization in Bitcoin's distributed network“, in: *IEEE/ACIS 16th International Conference on Software Engineering*, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), (Takamatsu), IEEE, 2015, S. 1–6.

[2] Berentsen, A.; Schär, F. (2017): Bitcoin, Blockchain und Kryptoassets, Erste Auflage, BoD - Books on Demand, Norderstedt.

[3] Birgitta Dennerlein (2017), Treuhänder.
URL:
http://wirtschaftslexikon.gabler.de/Archiv/14143/treuhaender-v12.html (besucht am 27. 12. 2017).

[4] Daimler AG (2017), Daimler und LBBW: Erfolgreicher Einsatz von Blockchain | Daimler.
URL: https://www.daimler.com/investoren/refinanzierung/blockchain.html (besucht am 05. 11. 2017).

[5] Dannen, C. (2017): Introducing Ethereum and Solidity, Erste Auflage, Apress, Berkeley, CA.

[6] De Pedro, A. S.; Levi, D.; Cuende, L. I. (2017): Witnet: A Decentralized Oracle Network Protocol.

[7] Eyal, I.; Sirer, E. G. (2013): Majority is not Enough: Bitcoin Mining is Vulnerable. In: *CoRR*.

[8] Hüfner, D. (2017), Tschüss, Schadensmeldung: Axa startet Versicherungspolice per Blockchain.
URL: http://t3n.de/news/axa-blockchain-versicherung-857073/ (besucht am 05. 11. 2017).

[9] juraforum.de (2017), Konkludentes Handeln.
URL: https://www.juraforum.de/lexikon/konkludentes-handeln (besucht am 12. 12. 2017).

[10] Kaulartz, M. (2016): Blockchain: Rechtliche Hürden für "Smart Contracts". In: *bank und markt* Ausg. 12 S. 34.

[11] Löhnig, M. (2006): Treuhand: Interessenwahrnehmung und Interessenkonflikte: Zugl.: Regensburg, Univ., Habil.-Schr., 2006, Mohr Siebeck, Tübingen.

[12] o.V. (2017), Market Price (USD).
URL: https://blockchain.info/de/charts/market-price?timespan=all (besucht am 02. 01. 2018).

[13] Pesch, P.; Böhme, R. (2017): Datenschutz trotz öffentlicher Blockchain?. In: *Datenschutz und Datensicherheit - DuD* Ausg. 41 no. 2 S. 93–98.

[14] Schwartz, D.; Youngs, N.; Britto, A. (2014): The Ripple Protocol Consensus Algorithm, hrsg. von Ripple Labs Inc.

[15] Sixt, E. (2017): Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie, Springer Gabler, Wiesbaden.

[16] Spancken, M.; Hellenkamp, M.; Brown, C.; Thiel, C. (2016): Abschlussbericht zum Forschungs- und Entwicklungsprojekt 2015/2016, Münster.

[17] Wallace, N. (2017): „Fiat Money“ in: *The New Palgrave Dictionary of Economics*, Palgrave Macmillan UK, London, S. 2079–2087.

[18] Williams-Grut, O. (2017), IBM landed a big win in the race to sell blockchain to Wall Street.
URL: http://www.businessinsider.de/blockchain-digital-trade-chain-ibm-hyperledger-deutsche-bank-hsbc-soc-gen-2017-6?r=UK&IR=T (besucht am 05. 11. 2017).

[19] Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. (2016): Where Is Current Research on Blockchain Technology?-A Systematic Review. In: *PloS one* Ausg. 11 no. 10 e0163477.

[20] Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. (2017): Blockchain Challenges and Opportunities: A Survey.

A. Glossar

Fiat-Geld Fiat Geld beschreibt ein Tauschmittel ohne eigenen, also inneren, Wert. Es dient als allgemein anerkanntes Tauschmittel, um Waren möglichst liquide zu handeln.[53]

Byzantinischer Fehler Als „Byzantinischer Fehler“ bezeichnet man den Zustand, in dem ein Partner innerhalb eines Systems Fehlinformationen liefert. Der byzantinische Fehler illustriert nun die Situation, dass der Informationsempfänger unterschiedliche Informationen aus unterschiedlichen Quellen erhält und nicht beurteilen kann, welche Information die Falschinformation ist. Der Fehler besteht solange, solange :
Lieferanten von Fehlinformation $< \frac{1}{3}$ aller Lieferanten

Forks Berentsen et. al. erklären: „Durch Forks entstehen konkurrierende Register, die nach ihren jeweiligen Regeln parallel die längste Registerversion darstellen können.“[54] Sie entstehen durch Regeländerungen für die Definition gültiger Blöcke. Dabei wird zwischen sogenannten „Softforks“ und „Hardforks“ unterschieden. Hardforks sind solche Abspaltungen, bei welchen nach Aufspaltung der Register neu erstelle Blöcke nach alten Regeln nicht gültig sind. Somit ist eine Fortführung unter neuen Regeln nicht möglich, da die gesamte Blockchain nach neuen Regeln nicht mehr gültig wäre. Ein Software hingegen verschärft die Regeln für neue Blocks. Neue Blocks sind somit auch nach alten Regeln gültig. Somit bleibt die gesamte Blockchain auch nach der Regeländerung in ihrer Gesamtheit gültig.[55]

[53] Wallace 2017, S. 2ff.
[54] Berentsen et al. 2017, S. 73.
[55] Ebd., S. 74ff.

B. Ehrenwörtliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbstständig und ohne unerlaubte Hilfe angefertigt worden ist, insbesondere dass ich alle Stellen, die wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen sind, durch Zitate als solche gekennzeichnet habe. Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Weiterhin erkläre ich, dass die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde/Prüfungsstelle vorgelegen hat. Ich erkläre mich damit einverstanden, dass die Arbeit der Öffentlichkeit zugänglich gemacht wird. Ich erkläre mich damit einverstanden, dass die Digitalversion dieser Arbeit zwecks Plagiatsprüfung auf die Server externer Anbieter hoch geladen werden darf. Die Plagiatsprüfung stellt keine Zurverfügungstellung für die Öffentlichkeit dar.

München, 28.02.2018
(Ort, Datum)

Florian Hofsäss
(Eigenhändige Unterschrift)