Blockchain bassierte Smart Contracts: Grundlagen, Prozessunterstützung und Bewertung

Andreas Rauscher und Zoran Cupic

Hochschule Ravensburg-Weingarten
andreas.rauscher@hs-weingarten.de
zoran.cupic@hs-weingarten.de

Abstract. Motiviert durch das stark gestiegene Interesse rund um die Blockchain, wird mit dieser Arbeit geprüft, ob und wie die Blockchain im Bereich der Geschäftsprozesse geeignet ist. Blockchains ermöglichen es, ein verteiltes Peer-to-Peer-Netzwerk zu betreiben, in dem nicht vertrauenswürdige Mitglieder ohne vertrauenswürdige Mittler auf eine überprüfbare Weise miteinander interagieren können. Grundlegend soll erklärt werden wie dieser Mechanismus funktioniert, bedingt durch Automatisierung von mehrstufigen Prozessen wird die Prozessunterstützung sowie der Smart Contract im Ganzen bewertet. Weiter wird die Bewertung spezifisch für die Geschäftsrozess-Domäne mithilfe einer Blockchain Geschäftsprozess Kombination durchgeführt. Hier werden Vor- und Nachteile bewertet, welche sich durch die gemeinsame Nutzung der Ressourcen in und außerhalb eines Unternehmens zwischen Prozessen ergeben. Weiterhin wird durch die Nutzung von Blockchain-Geschäftsprozess-Kombination ermöglicht, mehrere existierende, zeitaufwändige Workflows kryptographisch verifizierbar zu automatisieren. In dieser Arbeit möchten wir auf elementare Bedingungen und Aspekte aufmerksam machen, die vor der Einrichtung eines Blockchain-Netzwerkes in einem Geschäftsprozess-Setting berücksichtigt werden sollten: von der transaktionalen Privatsphäre bis hin zum erwarteten Wert der digitalisierten Assets, die im Netzwerk gehandelt werden. Es werden Lösungen und Abhilfemaßnahmen zu den jeweiligen Sachverhalten dargelegt. Unsere Schlussfolgerung ist, dass die Blockchain-Geschäftsprozess-Kombination leistungsstark ist und signifikante Transformationen über mehrere Branchen hinweg bewirken kann, was den Weg für neue, vorallem disruptive, Geschäftsmodelle und neuartige, verteilte Anwendungen ebnet.

Schlüsselwörter: Blockchain, Smart Contracts, Geschäftsprozesse

1 Motivation

Blockchain stellt laut dem Gartner Hypecycle des Jahres 2017 eine der vielversprechendsten Technologien dar [1]. Erstmalig 2008 wurde die Technologie der

Blockchain als nutzbares verteiltes Datenbankmanagementsystem durch Satoshi Nakamoto im White Paper zu Bitcoin beschrieben [2]. Die Idee der Blockchain gab es jedoch bereits im Jahr 1991 [3]. Im Jahr darauf veröffentlichte Satoshi Nakamoto die erste Implementierung der Bitcoin-Software und startete dadurch die erste öffentlich verteilte Blockchain. Hierbei war es das Ziel, eine virtuelle Währung mit einem transparenten und verteilten Buchungssystem ohne zentrale Abwicklungsstelle zu erstellen [2]. Speziell der Aspekt, dass es in der Blockchain keine zentrale Abwicklungsstelle gibt, macht diese so vielversprechend. So können zum Beispiel monetäre Überweisungen getätigt werden, ohne dass eine Bank als Abwicklungsstelle für die Überweisung nötig wäre. Die Validierung der Überweisung würde hierbei in der Blockchain vollautomatisiert geschehen [4]. Jedoch ist die Blockchain nicht nur auf die virtuelle Währung Bitcoin beschränkt. Vielmehr ist diese eine Technologie, welche die transparente und robuste Abwicklung von Transaktionen in einem verteilten Peer-to-Peer Netzwerk ohne zentrale Abwicklungstelle garantiert. Der Inhalt und Ausführungszweck dieser Transaktionen spielt dabei keine Rolle. Durch diese Eigenschaft wird Einsatz der Blockchain für viele Branchen und Gebiete ermöglicht [5].

Mittlerweile haben sich weitere Blockchain Plattformen etabliert, welche einen erweiterten Funktionsumfang anbieten. Zu diesen gehört die Ethereum Plattform, welche eine stark optimierte Transaktionsabwicklung bietet. Die auf der Ethereum Plattform basierende virtuelle Währung Ether ist neben Bitcoin die am häufigsten genutzte und gehandelte virtuelle Währung. Im Gegensatz zu Bitcoin steht bei der Ethereum Plattform die Verwendung als Bezahlmittel jedoch nicht im Vordergrund. Vielmehr versteht sich Ethereum als eine Plattform für sogenannte Smart Contracts. Diese sind digitale Verträge, deren Vertragsbedingungen mittels einer Programmiersprache definiert werden. Nachdem der Vertrag erfolgreich abgeschlossen wurde, prüft dieser fortlaufend und selbstständig, ob eine der vorher definierten Vertragsbedingungen eingetreten ist. Sobald dies der Fall ist, erfüllt der Vertrag den anderen Teil automatisch. Hierdurch verspricht man sich schnelle und kosteneffiziente Verträge. So können zum Beispiel automatisierte Kaufverträge geschlossen werden, bei denen die Zahlung automatisch angewiesen wird, wenn die Post erfolgreich das Paket mit der Ware geliefert hat. Auch Versicherungsverträge könnten so zumindest teilweise automatisiert werden. So denkt die Blockchain Insurance Industry Initiative (B3i), die aus mehreren großen Versicherern besteht, darüber nach, die Vertragssumme einer Elementarschädenversicherung automatisch auszuzahlen, wenn am Ort des versicherten Gebäudes ein Erdbeben oder eine Überschwemmung stattfindet [6]. Mehrere Smart Contracts können auch zusammengefasst werden, so dass sie sich gegenseitig bedingen oder ausschließen. Prinzipiell könnte so ein komplett autonom handelndes, dezentrales Unternehmen entstehen.

Smart Contracts werden allerdings nicht nur in der Finanzbranche eingesetzt. In der Ethereum Plattform ist es zum Beispiel möglich für den Anwender sogenannte digitale Tokens zu erstellen. Diese digitalen Tokens werden in Smart Contracts

eingebunden. Durch den Einsatz der Tokens ist es zum Beispiel möglich reale Waren und Güter über die Blockchain zu verfolgen und den Besitz zu bestätigen [7, S. 2296]. Gerade für hochpreisige oder schützenswerte Waren wie Gold oder Schmuck ist der Einsatz daher prädestiniert. Auch staatliche Register, wie z. B. das Patentregister oder das Grundbuch, können durch digitale Tokens und damit digitalisierte Assets ersetzt werden. Anstatt eines zeitraubenden Prozesses vor dem Notar und dem Grundbuchamt, würde die Übereignung eines Grundstückes so nur noch wenige Sekunden brauchen. In Form eines digitalen Kettengliedes auf einer Festplatte, transparent und nachvollziehbar.

Inzwischen wurde auch erkannt, dass durch die Blockchain bereits existierende Geschäftsmodelle komplett verändert werden können. So können mit Hilfe der Blockchain Prozesse systematisch und kontinuierlich dokumentiert werden. Hierdurch können einzelne Prozessschritte transparent erfasst und nachvollzogen werden. So könnten zum Beispiel Revisionen schneller und kostengünstiger abgewickelt werden, wenn alle für die Prüfung relevanten Informationen in die Blockchain geschrieben werden. Durch die resultierende Prozesstransparenz kann die operative Steuerung eines Unternehmens optimiert werden. Da Smart Contracts einen Vertrag zwischen mehreren Parteien abbilden, könnten somit auch unternehmensübergreifende Prozesse vollkommen automatisiert abgebildet werden.

Anhand dieser genannten Beispiele zeigt sich, dass die Blockchain eine Technologie ist, welche ein großes Potential hat unsere Wirtschatft, sowohl als auch unseren Alltag, effizienter zu gestalten.

Diese Arbeit erklärt im zweiten Kapitel die grundlegende Technik der Blockchain. Im folgenden Kapitel 3 werden die darauf aufbauenden Smart Contracts erläutert und eruiert. In Kapitel 4 erfolgt die Sicht auf die Smart Contracts für die Geschäftsprozesse. In Kapitel 5 werden die Vor- und Nachteile von Smart Contracts aufgezeigt. Im letzten Kapitel wird eine Zusammenfassung über die behandelten Themen durchgeführt.

2 Die Blockchain-Technologie

2.1 Grundlagen

Da die Blockchain eine recht neue Technologie ist, hat sich bisher keine einheitliche Definition durchgesetzt. Betrachtet man vorhandene Definitionen, wird die Blockchain oftmals als eine Art verteilte Datenbank oder elektronisches Register dargestellt. Hierbei werden Einträge der Blockchain als sogenannte Blöcke gruppiert. Diese Einträge können Transaktionen, Ereignisse oder Datensätze darstellen. Die Blöcke sind dabei wiederum über eine kryptografische Signatur miteinander verknüpft. Die Verknüpfung, Validierung und Speicherung der Blöcke wird in der Blockchain von mehreren unabhängigen Parteien in einem Peer-to-Peer Netzwerk durchgeführt [5, S. 7 f.]. Im Folgenden wird die konkrete

Funktionsweise der Blockchain anhand dem Beispiel Bitcoin detailliert erläutert. Die virtuelle Währung Bitcoin ist als ein Währungssystem zu verstehen, in dem Transaktionen ohne eine zentrale Verwaltungsstelle in einem Peer-To-Peer Netzwerk vollzogen werden. Die Blockchain wird hierbei als ein chronologisches Register genutzt, in welchem alle Transaktionen chronologisch gespeichert werden. Dieses Register wird wiederum bei allen Teilnehmern der Blockchain dezentral gespeichert und ebenfalls durch diese verwaltet. Die sichere Abwicklung von Transaktionen wird durch kryptografische Verfahren gewährleistet. Bei Bitcoin werden hierbei die Public-Key-Kryptographie und eine kryptographische Hashfunktion verwendet. Die konkrete Transaktionsabwicklung ist bei Bitcoin in mehrere Schritte unterteilt. In der folgenden Abbildung 1 werden die ersten zwei Schritte der Transaktionsabwicklung grafisch dargestellt und anschließend detailliert erläutert.

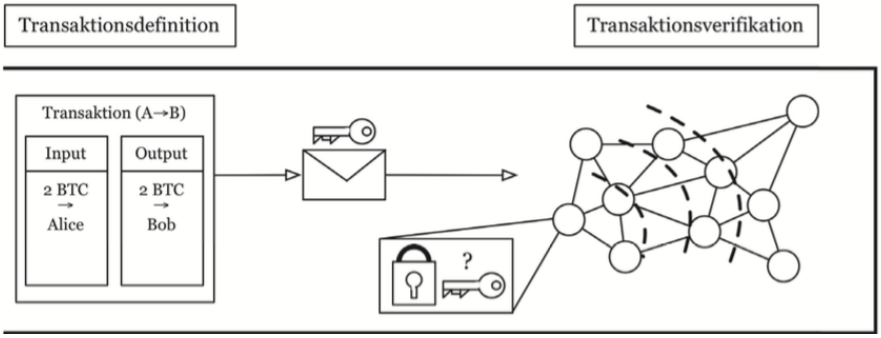

Abb. 1. Transaktionsdefinition und -verifikation in der Bitcoin Blockchain [5]

Um eine konkrete Transaktion im Bitcoin-Netzwerk abzuwickeln, muss diese von einem Absender an einen Empfänger gerichtet sein. Hierbei werden Absender und Empfänger jeweils durch eine Adresse referenziert. Die einzelnen Adressen ergeben sich jeweils aus dem Hash des öffentlichen Schlüssels des Empfängers oder des Absenders. Der konkrete Inhalt einer Transaktion wird hierbei durch den privaten Schlüssel des Absenders verschlüsselt. Durch die Verschlüsselung des Inhalts der Transaktion mit dem privaten Schlüssel des Absenders kann der Empfänger den Inhalt durch die Nutzung des öffentlichen Schlüssel des Absenders wieder öffnen. Ebenfalls wird durch die Nutzung der Public-Key-Kryptographie verifiziert, dass die Transaktion auch wirklich vom jeweiligen Absender stammt. Dieser Schritt nennt sich Transaktionsdefinition. Nach dem die Transaktion versandt wurde, wird diese auch an weitere Teilnehmer des Bitcoin-Netzwerks als sogenannte offenstehende Transaktion verteilt. Als offenstehende Transaktion werden Transaktionen bezeichnet, welche noch nicht in die Blockchain geschrieben wurden. Jeder Teilnehmer im Bitcoin Netzwerk besitzt einen Cache, in welchem noch offenstehende Transaktionen gespeichert werden. Der erste Teil-

nehmer, den die offenstehende Transaktion erreicht, prüft nun ob diese valide ist. Dieser Vorgang wird als Transaktionsverifikation bezeichnet. Nach erfolgreicher Prüfung schickt dieser Teilnehmer die offenstehende Transaktion an möglichst viele weitere Teilnehmer [5, S. 9 f.]. Um die offenstehenden Transaktion endgültig in die Blockchain zu schreiben, werden die offenstehende Transaktionen eines bestimmten Zeitraums zu einem neuen Block zusammengefasst, welcher anschließend durch sogenannte Miner validiert und anschließend zur Blockchain hinzugefügt wird. Die Miner sind hierbei Teilnehmer der Blockchain, welche für die Validierung der Blöcke Rechenleistung zur Verfügung stellen. Die Validierung erfolgt durch ein Konsensverfahren, welches die Lösung einer kryptographischen Aufgabe beinhaltet. Das bei Bitcoin genutzte Konsensverfahren wird als Proof of Work bezeichnet. Das Proof of Work stellt in der Informatik eine Methode dar, welche den übermäßigen Gebrauch eines Dienstes verhindern soll. Hierzu wird der Nutzer aufgefordert eine mäßig schwere Aufgabe zu lösen. Die Lösung der Aufgabe kann durch Dritte ohne großen Aufwand nachgeprüft werden. Bei Bitcoin soll durch dein Einsatz des Proof of Work Vertrauen geschaffen werden, da es in der Blockchain keinen vertrauenswürdigen Mittler gibt [8]. Die Abbildung 2 stellt die Inputs und den Vorgang der zu lösenden kryptographischen Aufgabe vereinfacht grafisch dar.

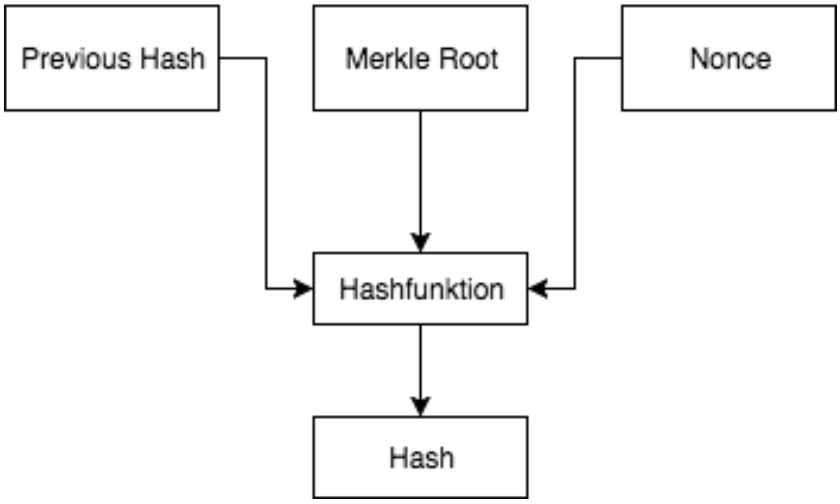

Abb. 2. Inputs und Vorgang der zu lösenden kryptographischen Aufgabe

Das Proof of Work der Bitcoin Blockchain und die damit verbundene Lösung der kryptographischen Aufgabe werden im Folgenden detailliert beschrieben. Wie in der Abbildung aufgezeigt, wird bei der kryptographischen Aufgabe eine Hashfunktion verwendet. Hierbei dienen drei Größen als Input, welche im Folgenden jeweils beschrieben werden.

Previous Hash Aktuellster Block der Blockchain als Anknüpfungspunkt für den zu validierenden Block

Merkle Root Ein Wert, welcher durch das paarweise hashen von den einzubindenden Transaktionen durch einen Hash-Baum/Merkle Tree erzeugt wird

Nonce Ein frei wählbarer Wert, welcher sicherstellt, dass überhaupt eine Lösung der kryptographischen Aufgabe gefunden werden kann

Der Output der kryptographischen Aufgabe muss laut dem Bitcoin-Protokoll wiederum ein neuer Hash sein, bei welchem die ersten 17 Bits mit Nullen belegt sind. Dieser Hash wird durch hashen der Inputs mit einer Hashfunktion erstellt. Um so einen Hash zu finden, wird solange durch die Miner ausprobiert und dabei die Nonce verändert, bis ein geeigneter Hash erstellt wurde. Der Proof of Work ist sehr rechenintensiv. Der Miner, welcher die Aufgabe als erstes gelöst hat und somit einen geeigneten Hash ermittelt hat, veröffentlicht den neuen Block zur Validierung im Netzwerk der Blockchain. Die Validierung erfolgt hierbei durch die anderen Teilnehmer der Blockchain, welche durch den Previous Hash, den Merkle Root und die vom Miner gewählt Nonce die Aufgabe nachrechnen. Nach erfolgreicher Validierung wird der Block unveränderbar zur Blockchain hinzugefügt und die Blockchain somit geupdatet. Der Miner erhält für die Lösung der Aufgabe einen gewissen Betrag in Bitcoin als Belohnung [9]. Die folgende Abbildung 3 verdeutlicht die gerade beschriebenen letzten zwei Schritte der Transaktionsabwicklung.

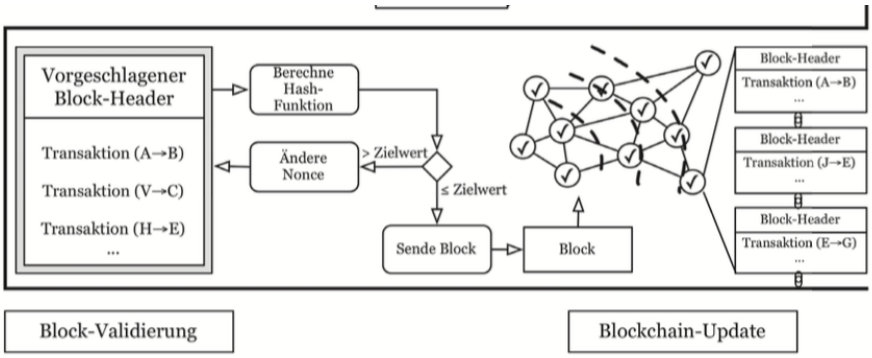

Abb. 3. Abwicklung von offenstehenden Transaktionen in der Bitcoin Blockchain [5]

2.2 Anwendungsbereiche

Momentan ist die Technologie vor allem durch ihren Einsatz bei virtuellen Währungen wie Bitcoin bekannt, jedoch ergeben sich in der Finanzbranche weitere Einsatzmöglichkeiten. So arbeitet die Deutsche Börse zurzeit in Kooperation mit der Deutschen Bank an einem Prototyp für die auf der Blockchain-Technologie basierende Abwicklung von Wertpapiertransaktionen [10].

Ein weiterer potentieller Anwendungsbereich für die Blockchain ist die Musikindustrie. Die Verwaltung von Musikrechten stellt eine komplizierte Aufgabe dar, an welche sich bislang nur Labels und nationale Verwertungsgesellschaften wie die Gema herantrauen. Der Grund hierfür ist, dass Musikrechte oftmals von mehreren Anteilseignern gehalten werden. Hierdurch entsteht eine komplizierte Rechtestruktur und Lizensierung. Durch den Einsatz der Blockchain lassen sich bereits bestehende Rechte oder Lizenzen transparent darstellen und eine Vergabe von neuen Rechten oder Lizenzen ist transparent, sicher und unkompliziert möglich. Mittlerweile wurde ein Start-up mit dem Namen Peertracks gegründet, welches die Bezahlmodalitäten für Musikrechte und -lizenzen mit Hilfe der Blockchain vereinfachen und die Rechtehaltung transparenter gestalten möchte [11].

Ebenfalls bietet die Blockchain im Bereich von staatlichen Institutionen vielerlei Anwendungsbereiche. Die Isle of Man hat sich im Jahr 2015 dazu entschlossen, das erste staatliche Blockchain Projekt zu starten. Hierbei wird die Blockchain zur automatischen Unternehmensregistrierung genutzt [12]. Große Handelsunternehmen untersuchen ebenfalls die Potentiale der Blockchain-Technologie. Hierbei wird überlegt, inwiefern sich Versorgungsketten einfacher und robuster mit Hilfe der Blockchain-Technologie gestalten lassen. Durch den Einsatz der Blockchain-Technologie könnte in der Versorgungskette jeder einzelne Schritt eines Produktes aufgezeichnet werden. Hierdurch kann der Herkunftsort von Produkten und der Produktionsprozess bzw. Beschaffungsprozess transparent für die Käufer dargestellt werden [12]. Ein sehr interessantes Pilotprojekt wurde von dem Finanzhaus Broadridge in den USA durchgeführt. Hierbei wurde eine Wahl mittels einer Blockchain auf einer Aktionärshauptversammlung durchgeführt. Bei diesem Pilotprojekt waren die wichtigsten Aspekte ein schnelles Ergebnis zu erzielen und von überall auf der Welt abstimmen zu können. Auch die Europäische Union erforscht den potentiellen Einsatz der Blockchain für Wahlen. Hierbei wird untersucht, ob die Blockchain für Wahlen eine revolutionäre Technologie darstellt oder ob diese nur unterstützend wirken kann [13].

Ein weiterer, bereits in der Motivation beschriebener, Anwendungsbereich der Blockchain sind die sogenannten Smart Contracts. Diese werden im folgenden Kapitel detailliert erläutert.

3 Smart Contracts

3.1 Funktionsprinzip

Ein Smart Contract ist ein Computerprotokoll, welches die Verhandlung oder Ausführung eines Vertrags erleichtern, verifizieren oder durchsetzen soll. Der Begriff Smart Contracts wurde erstmalig in den 90 Jahre von Nick Szabo verwendet [14]. Wer in der Zukunft einen Versicherungs-, Notarvertrag oder Hauskauf abschließen möchte, kann dies mithilfe eines Smart Contracts umsetzen. Ein Smart Contract kann in der Theorie jeden Mittelsmann (Anwalt, Notar oder Serviceanbieter) ersetzen und damit zu enormen Kosteneinsparungen führen. Die Informationen über das Haus wären bereits auf der Blockchain verfügbar. Bietet nun ein Käufer den geforderten Preis für das Objekt, wird der Smart Contract automatisch ausgeführt. Es sind keine weiteren Notar- oder Behördengänge mehr erforderlich, da die Papierarbeiten entfallen weitgehend. Einfach ausgedrückt ist ein Smart Contract eine ausführende Regel mit einer Bedingung. Beispielhaft "wenn GeldEingang() > 4312 €, dann AccountFreischalten()". Ein Smart Contract erlaubt es nun diese Regel dezentral beliebig zu erweitern und mit einer beliebig großen Menge an Bedingungen zu verknüpfen. Die Bedingungen definieren, wann der Vertrag vollständig zustande gekommen ist [14]. Dezentral bedeutet, dass die Speicherung von Informationen oder das Treffen von Entscheidungen nicht durch ein einzelnes Individuum, sondern in einer Gemeinschaft durchgeführt wird. Die Notwendigkeit einer dezentralen Schiedsstelle im Vertragswesen ergibt sich aus den verschiedenen Verlangen und Zielen der Vertragspartien. Die Verwendung einer dezentralen Schiedsstelle, in diesem Fall für Services, bringt gleichzeitig allgemeine und bekannte Hürden mich sich. Diese Hürden schränken die Nutzbarkeit grundsätzlich stark ein. Diese Hürden werden im Folgenden erläutert.

- Attacker Collusion: Angreifer schließen sich zusammen. Durch eine Mehrheit in der Gruppe können Trustwerte gegenseitig erhöht werden und so Entscheidungen bezweckt werden, welche sonst nicht möglich wären [15, S. 32 f.].

- Data Fudging: Angreifer nutzen betrügerische Aktivitäten, sogenanntes Daten-Fudging, so dass echte Nutzer betrogen werden. Das Ziel dieser Aktion ist die Minderung des Vertrauens in das System [15, S. 32 f.].

- Denied Denial of Service (DDOS): Dies ist einer der wichtigsten Angriffsarten in jeder dezentralisierten Umgebung. Diese Art von Angriffen deaktiviert die Funktionalität. Dieser Angriff macht das System unbrauchbar während der Zeit des Angriffs. Spamming und Flooding von echten Usern mit unerwünschten Nachrichten in Form von Aufrufen können auch in diesem Zusammenhang auftreten [15, S. 33 f.].

- Fälschung: Angreifer versuchen, eine vertrauenserweckende Identität zu verkörpern und können als legitime und verifizierte Benutzer im System handeln [15, S. 33 f.].

– Fremde Entitäten: Bedingt durch mehrere Einstiegsknoten, welche für das Nutzen der zentralisierten Umgebung notwendig sind, wird Angreifern ein neues Einfallstor für Angriffe geboten. Siehe dazu die Veranschaulichung in Abbildung 4. Angreifer errichten einen eigenen Einstiegsknoten und manipulieren Eingaben, tätigen eigene Transaktionen oder hören bei vertrauenswürdigen Informationen mit [15, S. 33 f.].

Die Blockchain bietet nun ein Gesamtkonzept als Struktur zur Verwendung an, welches die aufgelisteten Probleme mit technologischen Funktionen löst. Da der Fokus dieser Arbeit auf Smart Contracts im Prozessmanagement liegt, werden die genutzten Funktionen und Einzelkonzepte innerhalb dieser Arbeit nicht näher erläutert. Näher soll die Funktionsweise eines Smart Contracts beschrieben werden. Wie in Abbildung 4 dargestellt, lässt sich ein Vertrag direkt in der Blockhain vergleichen.

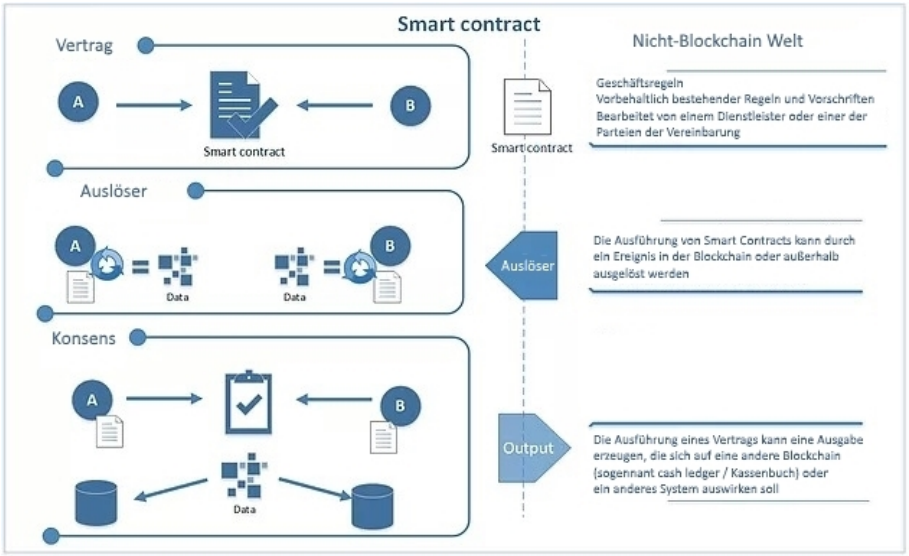

Abb. 4. Darstellung eines Smart Contracts im Vergleich [16]

Der Smart Contract entspricht im wesentlichem einer abstrahierten Ansicht einer Businesslogik eines Unternehmens bzw. eines Prozesses im Unternehmen (z. B. Zahlungsprozess, Einkaufsfreigabeprozess). Die eigentliche Vertragsdurchführung wird durch entsprechende Ereignisse, sogenannte Trigger, ausgelöst. Trigger entsprechen z. B. einer E-Mail oder einem Anruf in der bisherigen Geschäftswelt. In der Blockchain können Trigger entsprechende Hooks sein, welche in dem Geschäftsprozess eingeklinkt werden und durch auslösen, weitere Prozesse oder Vertragsbestandteile durchführen und abschließen. Wird durch die Trigger die

Vertragsdurchführung erfolgreich abgeschlossen, können durch die Blockchain weitere Ereignisse folgen. Ein Beispiel hierfür ist das Freigeben eines Geldbetrags nach Erhalt einer Ware. Vergleichbar mit dem bisherigen Geschäftsprozessen ist der Versand von Waren an einen Kunden nach Geldeingang.

3.2 Beispiel

Als Beispiel dient der E-Commerce Bereich im Zusammenspiel mit einem Logistikunternehmen (vgl. Abbildung 5). Wird durch einen Endverbraucher Ware bei einem Verkäufer bestellt, liefert dieser die Ware an den Logistikunternehmer. Diese Schritte unterscheiden sich auf den ersten Blick nicht vom einem konventionellen Geschäftsprozess. Der Unterschied jedoch ist, dass es eine vertragliche Vereinbarung gibt, welche die Zahlung des Kaufpreises an den Verkäufer freigibt, sobald der Paketdienstleister die Ware ausgeliefert hat. Sobald nun die Ware vollständig ausgeliefert wurde, ist der Vertrag und die Vertragsbedingung von Seiten des Verkäufers erfüllt. Der Vorteil für den Endkunden entsteht dadurch, dass er das Geld nicht im Voraus transferieren muss und somit kein Risiko eingeht. Das Geld wird freigegeben sobald die Lieferung eingetroffen ist. Der Händler hat den Vorteil, dass er das Geld sicher direkt nach der Lieferung erhält. Heutzutage wird dieses Risiko häufig durch einen weiteren Zahlungsdienstleister abgefangen. Der Zahlungsdienstleister lässt sich dieses Risiko entsprechend vergüten. Durch Smart Contracts wird dieser Kostenfaktor eliminiert.

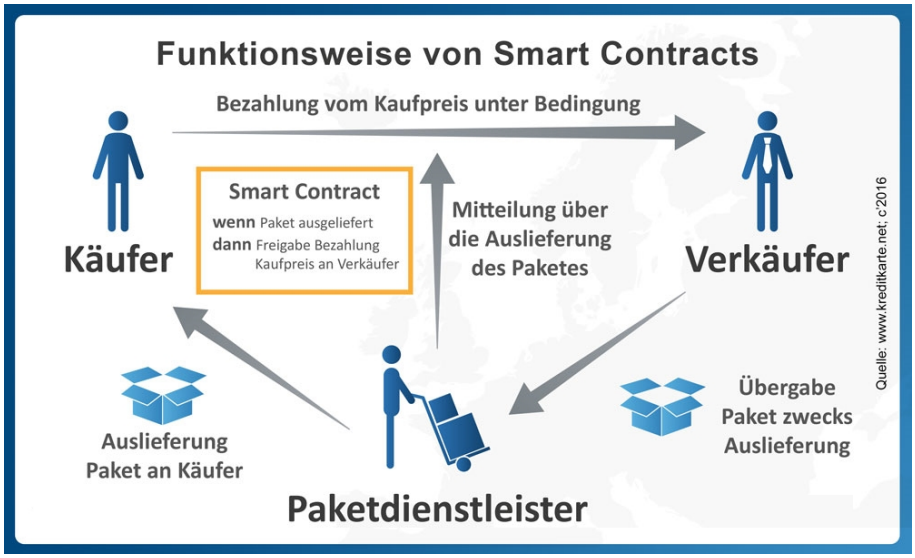

Abb. 5. Darstellung eines Smart Contracts Beispiel im E-Commerce [17]

4 Smart Contracts und Prozessunterstützung

Mit der voranschreitenden Digitalisierung sollen Geschäftsprozesse immer weiter digitalisiert, vereinfacht und automatisiert werden. Die Smart Contracts und die Blockchain haben ein sehr großes Potential für die Digitalisierung, Vereinfachung und Automatisierung von Geschäftsprozessen. Ein Grund hierfür ist, dass mit dem Einsatz eines Smart Contracts ein vollkommen automatisierter Vertrag zwischen einer bestimmten Anzahl von Parteien abgeschlossen wird. Diese Parteien können zum Beispiel Abteilungen von Unternehmen oder sogar ganze Unternehmen sein. Der Vertrag würde dann beispielsweise zwischen Abteilungen von Unternehmen gelten oder sogar zwischen einzelnen Unternehmen abgeschlossen werden. Der Vertrag kann eine gewisse Geschäftslogik beinhalten, welche innerhalb des Smart Contracts implementiert wird. Diese Geschäftslogik würde einem ganzen Geschäftsprozess oder Teilen eines Geschäftsprozesses entsprechen. Innerhalb des Smart Contracts werden einzelne Prozessschritte durch die abgebildete Geschäftslogik verarbeitet. Die bei der Abwicklung des Geschäftsprozesses entstehenden Daten werden sicher, transparent, integer und nachvollziehbar in der Blockchain persistent gespeichert. Dies alles würde ganz ohne zentrale Abwicklungs- und Prüfstelle in dem verteilen Netzwerk der Blockchain verlaufen. Durch das verteilte Netzwerk ist die Ausfallsicherheit für die Abwicklung von Geschäftprozessen ebenfalls gewährleistet. Für die Steuerung von Geschäftsprozessen können die gespeicherten Daten aus der Blockchain ausgelesen werden. Diese Aspekte machen die Nutzung von Smart Contracts für Geschäftsprozesse interessant. Die Smart Contracts und die Blockchain haben somit das Potential in Zukunft bestehende Technologien zur Abwicklung und Steuerung von Geschäftsprozessen abzulösen. Da ein Smart Contract ein Vertrag ist, welcher zwischen mehreren Parteien gebildet wird, können somit sogar unternehmensübergreifende Geschäftsprozesse durch Smart Contracts abgebildet werden.

Im Folgenden wird ein vereinfachtes Beispiel für einen Geschäftsprozess aufgezeigt, welcher durch den Einsatz eines Smart Contracts vereinfacht, automatisiert und somit optimiert wird. Hierzu wird als Geschäftsprozess eine vereinfachte Form des SEPA-Lastschriftverfahren für eine Bestellung bei einem Versandhändler betrachtet. Der konventionelle Geschäftsprozess wird in der folgenden Abbildung grafisch als BPMN-Diagramm dargestellt.

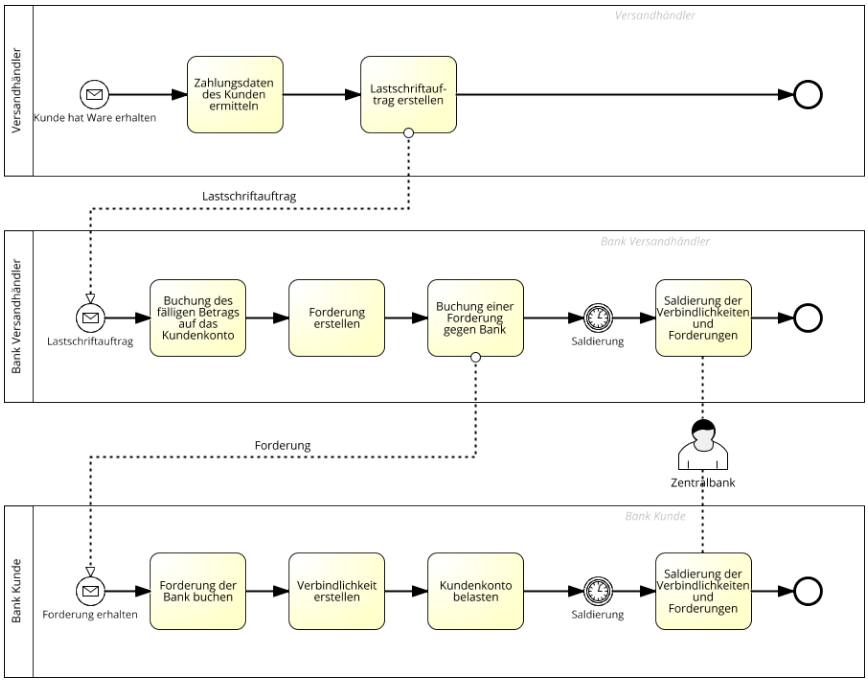

Abb. 6. SEPA-Lastschriftverfahren ohne Smart Contract

Der in der Abbildung 6 dargestellte Geschäftsprozess stellt das SEPA-Lastschriftverfahren für eine Bestellung bei einem Versandhändler ohne Smart Contract dar. Der Geschäftsprozess wird gestartet, indem der Kunde seine Ware erhalten hat. Diese Information kann automatisiert von dem genutzten Logistikunternehmen bereitgestellt werden oder durch einen Sachbearbeiter des Versandhändlers mittels einer Prüfung festgestellt werden. Anschließend werden die Zahlungsdaten des jeweiligen Kunden ermittelt und ein Lastschriftauftrag wird erstellt. Diese Prozessschritte können ebenfalls automatisiert oder durch einen Sachbearbeiter abgewickelt werden. Der Lastschriftauftrag wird anschließend an die Bank des Versandhändlers übermittelt. Hier wird der fällige Betrag dem Konto des Vertragshändlers gutgeschrieben und eine Forderung gegenüber der Bank des Kunden des Versandhändler erstellt. Diese Forderung wird anschließend an die Bank des Kunden des Vertragshändlers übertragen. Die Forderung wird anschließend bei der Bank des Kunden des Versandhändlers gebucht und in eine Verbindlichkeit transformiert. Das Kundenkonto wird anschließend mit dem Betrag der Verbindlichkeit belastet. Um schlussendlich den Geschäftsprozess zu beenden, müssen die ausstehenden Verbindlichkeiten bzw. Forderungen zwischen den Banken abgeschlossen werden. Dieser Vorgang wird als Saldierung bezeichnet. Erst bei der Saldierung werden die fälligen Beträge zwischen den Banken ausgeglichen.

Die Saldierung wird hierbei von einer zentralen Institution, in diesem Beispiel die Zentralbank, vorgenommen [18, S. 829 f.]. In der folgenden Abbildung 7 wird der zuvor dargestellte Geschäftsprozess durch einen mit der Blockchain agierenden Smart Contract erweitert, welcher den Geschäftsprozess vereinfacht, automatisiert und somit optimiert. Dieser erweitere Geschäftsprozess ist ebenfalls als BPMN-Diagramm grafisch dargestellt.

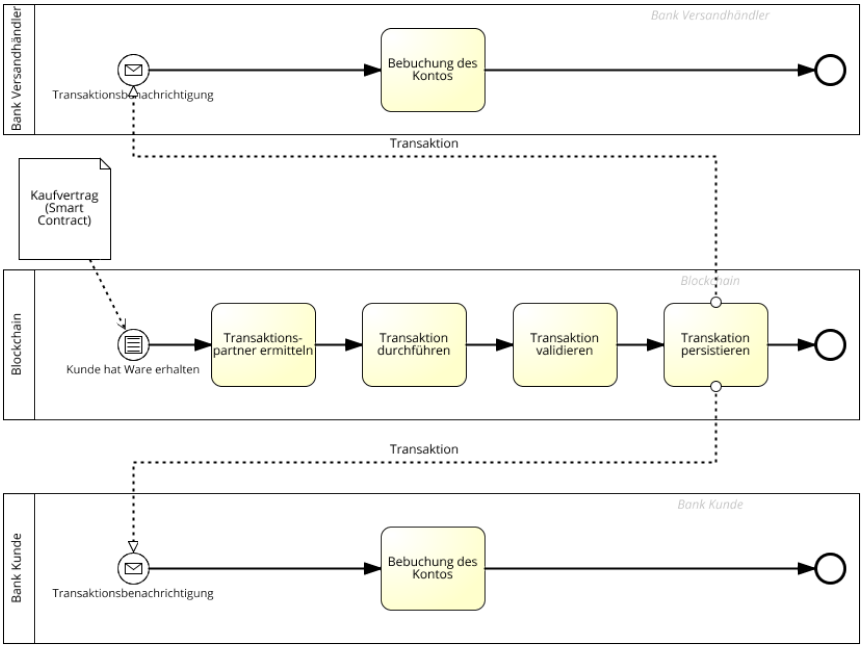

Abb. 7. SEPA-Lastschriftverfahren mit Smart Contract

Wie an diesem Geschäftsprozess zu erkennen ist, wurden wichtige Teile des SEPA-Lastschriftverfahrens in die Blockchain ausgelagert. Beim Kauf wird automatisch ein Kaufvertrag zwischen dem Kunden und dem Versandhändler abgeschlossen. Dieser ist als Smart Contract in die Blockchain implementiert. Hierbei prüft der Smart Contract fortlaufend den aktuellen Status des Kaufes. Tritt ein bestimmtes Ereignis ein, wird der dazu passende Geschäftsprozess angestoßen. In diesem Beispiel wird der Geschäftsprozess des SEPA-Lastschriftverfahrens angestoßen, wenn der Kunde die Ware erhalten hat. Der Geschäftsprozess wird dabei größtenteils in der Blockchain abgewickelt. Hierzu werden zuerst die Transaktionspartner ermittelt, welche in diesem Fall die Bank des Versandhändlers und die Bank des Kunden darstellen. Anschließend wird die Ausführung der Transaktion gestartet. Innerhalb der ausgeführten Transaktion wird der zu begleichende

Betrag von der Bank des Kunden an die Bank des Versandhändlers übertragen. Im Anschluss wird die Transaktion innerhalb der Blockchain vollkommen automatisch validiert und in die Blockchain persistent gespeichert. Die Banken werden benachrichtigt und führen anschließend die jeweiligen Buchungen intern durch. In diesem Schritt werden die jeweilige Konten belastet bzw. begünstigt.

Wie man an diesem beispielhaften Geschäftsprozess erkennen kann, können durch Smart Contracts Geschäftsprozesse optimiert werden. Vor allem die hier aufgezeigte Automatisierung durch den Einsatz eines Smart Contracts und der Blockchain führt zu einer Vereinfachung des Geschäftsprozesses. Hierdurch werden Aufwände und Kosten für die Geschäftsprozessabwicklung gesenkt. Ebenfalls wird die Durchlaufzeit eines Geschäftsprozesses signifikant reduziert.

Ebenfalls wird an diesem Beispiel ersichtlich, dass Smart Contracts und die Blockchain nicht ohne einen gewissen Änderungsaufwand in bestehende Geschäftsprozesse eingebunden werden können. Es muss ein Business Process Reengineering durchgeführt werden. Durch das Business Business Process Reengineering werden Geschäftsprozesse optimiert und bestmöglich auf die organisatorischen und technologischen Veränderungen abgestimmt [19].

5 Vorteile und Nachteile von Smart Contracts

Wie bei jeder Technologie, bringt auch der Einsatz von Smart Contracts gewisse Vorteile und Nachteile. Die wichtigsten Vor- und Nachteile werden in folgender Tabelle 1 zusammenfassend dargestellt und im Folgenden jeweils detailliert erläutert.

Vorteile	**Nachteile**
transparente, kostengünstige und automatisierte Abwicklung von Geschäftsprozessen	nicht vorhandene Rechtswirksamkeit
durchgehende Verfügbarkeit von Dienstleistungen	keine Interpretationsmöglichkeit
Vetrauensgewinnung	Fehler bei der Programmierung

Tabelle 1. Vorteile und Nachteile von Smart Contracts

Ein Vorteil beim Einsatz von Smart Contacts in Geschäftsprozessen, ist die hierdurch entstehende schnelle, sichere, transparente, kostengünstige und automatisierte Abwicklung von Geschäftsprozessen. Diese Aspekte wurden vor allem im vorherigen Kapitel detailliert dargestellt.

Ein weiterer Vorteil, welcher beim Einsatz von Smart Contracts entsteht, ist die durchgehende Verfügbarkeit von Dienstleistungen. So sind Prozessschritte, welche in einen Smart Contract implementiert werden, wie z.B. das Annehmen einer Anfrage, rund um die Uhr verfügbar. Da ein Smart Contract in dem verteilen Netzwerk der Blockchain agiert, ist ebenfalls die Ausfallsicherheit des Smart Contracts garantiert [20].

Der Einsatz eines Smart Contracts stellt auch ein gewisses Vertrauen zwischen Parteien her. So wird ein vertrauenswürdiger Handel zwischen Menschen ermöglicht, welche sich nicht kennen und entsprechend noch kein Vertrauen zueinander aufgebaut haben [21]. Dies ist beispielsweise bei Auktionsplattformen der Fall.

Ein Nachteile von Smart Contracts ist die durch die Programmierung beschränkte Abbildungsmöglichkeit von Sachverhalten. Vor allem komplexe Sachverhalte lassen sich nur sehr schwer und mit viel Aufwand abbilden [22].

Aktuell ist die Rechtswirksamkeit eines Smart Contracts nicht vorhanden. Der Grund hierfür ist das Formerfordernis, welches fordert, dass ein Vertrag von Menschen lesbar ist. Da der Smart Contract in Programmcode implementiert wird, können eine Vielzahl von Menschen den Vertrag nicht lesen und somit nicht verstehen, wofür sie ihre Zustimmung geben würden. Die Lösung ist hier zuerst einen rechtswirksamen Vertrag zu erstellen und diesen anschließend als Smart Contract zu implementieren. Die Abwicklung des Vertrages würde anschließend durch den Smart Contract geschehen [22].

Da es sich bei dem Smart Contract um ein in einer Programmiersprache entwickeltes Programm handelt, ist keine Interpretationsmöglichkeit gegeben. Gerade bei bestimmten Anfragen oder Auslegungen ist menschliches Urteilsvermögen nötig. Für solche Fälle sind Smart Contracts ungeeignet. Zum Beispiel würde die Anfrage eines wichtigen Kunden gleichberechtigt wie anderen Anfragen behandelt werden. Man könnte gewisse Spielräume einprogrammieren, jedoch würde dies die Komplexität enorm steigern [20].

Ebenfalls können, wie bei der Entwicklung von konventioneller Software, auch Fehler bei der Programmierung von Smart Contracts entstehen. Diese würden sich geschäftskritisch auswirken [22].

6 Zusammenfassung

Innerhalb dieses Papers wurde untersucht, inwieweit sich Blockchain basierte Smart Contracts für die Prozessunterstützung eignen. Hierfür wurden die Grundlagen und das Funktionsprinzip der Blockchain und der Smart Contracts erläutert. Ebenfalls wurden verschiedene Anwendungsbereiche für die Blockchain und ein Beispiel für einen Smart Contract aufgezeigt.

Im Kapitel 4 wurde detailliert untersucht und aufgezeigt, dass bestehende Geschäftsprozesse durch den Einsatz von Smart Contracts optimiert werden können. Durch den Einsatz der Blockchain im Hintergrund entstehen viele Vorteile, wie z.B. die Transparenz, Sicherheit und schnelle Abwicklung von Geschäftsprozessen.

Wie bei jeder neuen und disruptiven Technologie stellt sich die Frage, welche Auswirkungen diese auf die heutige Welt haben wird und inwieweit diese Akzeptanz findet. Aktuell wird die Blockchain größtenteils für den Handel von Kryptowährungen genutzt. Der Einsatz in Unternehmen wird noch erprobt oder mittels Pilotprojekten getestet.

Die Vorteile von Smart Contracts überwiegen, jedoch sind diverse Nachteile geschäftskritisch. Zum Beispiel würde sich eine Fehlprogrammierung katastrophal auf das Unternehmen und seine Geschäftsbeziehungen auswirken.

Zusammenfassend betrachtet haben Blockchain bassierte Smart Contracts ein großes Potential bestehende Geschäftsprozesse zu verändern und sogar neue Geschäftsmodelle hervor zu bringen.

Literatur

1. Panetta, Kasey: Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017. (2017). https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/
2. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. (2008). https://bitcoin.org/bitcoin.pdf
3. Hudson, Richard P. ; Augsten, Stephan: Blockchain – eine Einführung in die Konzepte. In: *Dev Insider* (2017). https://www.dev-insider.de/blockchain-eine-einfuehrung-in-die-konzepte-a-624577/
4. Seibel, Karsten: Dieses System macht Überweisungen blitzschnell. (2016). https://www.welt.de/finanzen/article157915297/Dieses-System-macht-Ueberweisungen-blitzschnell.html
5. Schlatt, Vincent ; Schweizer, André ; Urbach, Nils ; Fridgen, Gilbert: Blockchain: Grundlagen, Anwendungen und Potenziale. In: *Fraunhofer FIT* (2016). http://www.fim-rc.de/wp-content/uploads/Blockchain_WhitePaper_Fraunhofer_FIT_2016.pdf
6. Re, Munich: Blockchain-Initiative B3i gewinnt weltweit neue Mitglieder. In: *Munichre* (2017). https://www.munichre.com/de/media-relations/publications/company-news/2017/2017-02-06-company-news/index.html
7. K. Christidis, M. D.: Blockchains and Smart Contracts for the IoT. (2016). http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408
8. BTC-ECHO: Was ist Proof-of-Work? In: *BTC-ECHO* https://www.btc-echo.de/tutorial/was-ist-proof-of-work-wie-funktioniert-konsens-mechanismus/
9. Ruess, Sandra: So funktioniert Blockchain. In: *Computerwoche* (2017). https://www.computerwoche.de/a/so-funktioniert-blockchain,3331391
10. Group, Deutsche B.: Blockchain - Neue Impulse für die Finanzmärkte. http://deutsche-boerse.com/dbg-de/ueber-uns/gruppe-deutsche-boerse/geschaeftsfelder/blockchain-business-areas
11. Bader, René ; Deckers, Thorsten: Technik und Uses Cases der Blockchain - Wie die Blockchain funktioniert. In: *CIO* (2017). https://www.cio.de/a/wie-die-blockchain-funktioniert,3264958,2
12. Schafft, Pascal: 7 aufregende Anwendungen der Blockchain Technologie. In: *Zweiblog* (2016). http://www.zweiblog.com/2016/06/7-aufregende-anwendungen-der-blockchain-technologie/
13. Müller, Lara M.: BLOCKCHAIN - Wie eine Technologie unser Wahlsystem revolutionieren könnte. In: *Handelsblatt* (2017). http://www.handelsblatt.com/politik/deutschland/bundestagswahl/alle-schlagzeilen/blockchain-wo-man-die-blockchain-schon-zum-abstimmen-einsetzen-kann/20366520-2.html
14. Szabo's, Nick: Exploding Onto The Web. (1996). https://archive.is/zWbhL#selection-607.412-607.427
15. author, Unkown: The Next Galaxy. (2016). The Advantages and Disadvantages of Decentralization. (2016)
16. author, Unknown: TheFundsChain White Paper extract 4: Smart Contracts. (2017)
17. Kreditkarte.net: Smart Contracts – selbsterfüllende Verträge. (2017)
18. Deubel, Marco ; Moormann, Jürgen ; Holotiuk, Friedrich: Nutzung der Blockchain-Technologie in Geschäftsprozessen: Analyse am Beispiel des Zahlungsverkehrs. In: *Notes in Informatics (LNI)* (2017). https://dl.gi.de/bitstream/handle/20.500.12116/4105/B10-5.pdf?sequence=1

19. Schewe, Prof. Dr. G.: Business Process Reengineering. (2016). http://wirtschaftslexikon.gabler.de/Definition/business-process-reengineering.html
20. Bitz, Sebastian: Smart Contracts – Was steckt hinter den smarten Verträgen. In: *double Slash Blog* (2017). https://blog.doubleslash.de/smart-contracts-was-steckt-hinter-den-smarten-vertraegen/
21. Tiedemann, Michaela: Smart Contracts: Anwendungsszenarien, Vorteile und Potenzial von smarten Verträgen. In: *alexanderthamm Blog* (2017). https://www.alexanderthamm.com/artikel/smart-contracts-anwendungsszenarien-vorteile-und-potenzial-von-smarten-vertraegen/
22. Hellinger, Axel: Smart Contract | Wirksamkeit & Unwirksamkeit von Vertragsprogrammen. In: *HELLINGER.LEGAL* (2016). https://hellinger.eu/smart-contract/