Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

TECHNOLOGIEÜBERBLICK BLOCKCHAIN

VERSION 1.0 – 20.10.2016

Alexander Marsalek – alexander.marsalek@a-sit.at
Bernd Prünster – bernd.pruenster@a-sit.at

Zusammenfassung: Die Blockchain wurde als zentrales, aber dezentralisiert verwaltetes, sequentielles Transaktionsregister im Rahmen der Kryptowährung *Bitcoin* entwickelt. Die Blockchain-Technologie ermöglicht Transaktionen zwischen Parteien, die einander nicht vertrauen, ohne dass eine zentrale, vertrauenswürdige Instanz benötigt wird. Anstelle von Vertrauen treten kryptografische Algorithmen und mathematische Beweise, welche eine korrekte Transaktionsabwicklung garantieren. Die Einsatzmöglichkeiten von Blockchain-basierten Systemen gehen jedoch weit über Szenarien im Rahmen von Kryptowährungen hinaus. Auf Grund der vielseitigen Einsatzmöglichkeiten der Technologie könnten sich durch den Einsatz der Blockchain im Umfeld traditioneller Zahlungssysteme, Börsen und Devisenmärkte signifikante Einsparungen ergeben. Das vorliegende Dokument beschreibt die Grundlagen der Blockchain-Technologie und legt eine Reihe von Anwendungsmöglichkeiten dieses Systems abseits von Kryptowährungen dar. Durch die geringe Gesamtmarktkapitalisierung von nur wenigen Milliarden US-Dollar sind Kryptowährungen ungeachtet ihrer Anwendungsmöglichkeiten nach wie vor als Nischenprodukt anzusehen. Da jedoch das Wissen um die Funktionsweise von Kryptowährungen notwendig ist, um sich mit einer von derartigen elektronischen Währungssystemen entkoppelten Blockchain auseinanderzusetzen, wird auch deren Funktionsweise beschrieben.

Dokument-Historie

Version	Datum	Autor	Änderungen
0.5	13.05.2016	Alexander Marsalek, Bernd Prünster	Erster Entwurf
0.6	17.05.2016	Thomas Zefferer	Internes Feedback
0.7	20.05.2016	Alexander Marsalek, Bernd Prünster	Interne Vorabversion
0.8	26.05.2016	Herbert Leitold	Review
0.9	20.09.2016	Alexander Marsalek, Bernd Prünster	Einarbeitung Feedback OeNB
1.0	20.10.2016	Alexander Marsalek, Bernd Prünster	Energieverbrauch und Miningprozess ergänzt

Inhaltsverzeichnis

1. Einleitung

Laut Schätzungen von Autonomous Research LLP belaufen sich die Gesamtkosten für Banken im Bereich Sales and Trading auf USD 136 Mrd. jährlich, wobei rund ein Drittel davon auf den weltweiten Zahlungsverkehr bzw. dessen Abwicklung entfällt [1]. Hauptgründe hierfür sind struktureller Natur: Durch den teilweise historisch gewachsenen zentralisierten Aufbau des aktuellen Bankensystems fallen signifikante administrative Kosten an, nur um die notwendigen Transaktionsregister aktuell zu halten. Des Weiteren sind im globalen Finanzmarkt in vielen Bereichen Mittelsmänner für die Durchführung bzw. Absicherung von Transaktionen notwendig. Augenscheinlich fallen auf Grund derartiger Strukturen sowohl direkt substantielle Kosten an, jedoch ist in diesem Zusammenhang auch der Zeitfaktor relevant: Jede weitere Instanz, die im Rahmen der Abwicklung einer Transaktion involviert ist, schlägt sich auch in der Dauer der Transaktionsabwicklung nieder. Dezentralisierte Systeme wie *Bitcoin*, welche die *Blockchain* (alternativ auch *Block Chain*) als zentrales, jedoch dezentralisiert verwaltetes Transaktionsregister einsetzen, benötigen keine zentralen Instanzen, Treuhänder, oder ähnliche Konstrukte. Trotzdem garantieren sie einen verlässlichen, raschen, sicheren und vor allem lückenlos nachvollziehbaren Zahlungsverkehr. Durch die Tatsache, dass der Weg jeder Währungseinheit unwiderruflich in einem zentralen Transaktionsregister protokolliert ist, bzw. sein muss, lassen sich viele Vorgänge automatisieren. Weiters garantiert die Struktur der Blockchain und deren fortlaufende Nutzung die Integrität der in ihr protokollierten Transaktionsdaten. Autonomous Research LLP schätzt die möglichen Gesamtersparnisse eines vollständigen Umstiegs auf blockchainbasierte Transaktionsabwicklung auf bis zu USD 16 Mrd. jährlich.

Auch abseits des Bankensektors gibt es erhebliches Interesse an der Blockchain. Google und IBM beispielsweise forschen daran, wie gewerbliche Kredite mittels der Blockchain-Technologie automatisch an den aktuellen Zinssatz angepasst werden können. Dadurch würde ein effizienteres System entstehen, da viele Schritte automatisiert ausgeführt werden könnten [2]. Einschätzungen über die Höhe potentieller Ersparnisse sind jedoch mit Vorsicht zu genießen, da nach wie vor in vielen Bereichen Unklarheit über die Anwendungsmöglichkeiten und das tatsächliche Potential von Blockchain als Technologie für den globalen Finanzmarkt herrscht. Oft liegen konservative Schätzungen auch schlicht in einem mangelnden Verständnis der involvierten Technologien begründet. Doch gerade deshalb ist die Aufmerksamkeit, die der Blockchain-Technologie gewidmet wird, gerechtfertigt. Erst ein ausreichendes Verständnis ermöglicht überhaupt eine aussagekräftige Abschätzung des potentiellen Einflusses von Blockchain auf die Finanzwelt. Zum jetzigen Zeitpunkt existieren diesbezüglich jedoch vorwiegend Modelle, die nicht alle Aspekte befriedigend abdecken.

Die Blockchain selbst wurde in ihrer Urform 2008 von Satoshi Nakamoto[1] im Zuge von Bitcoin entwickelt [3]. Ursprünglich wurde sie als sequentielle Transaktionsdatenbank konzipiert, deren Einträge im Nachhinein weder verändert noch gelöscht werden können. Bitcoin selbst versteht sich als dezentrale *Kryptowährung* (C*ryptocurrency*), auf Basis derer sich ein von traditionellen Währungen entkoppelter Wirtschaftsraum entwickelt hat. Die grundlegenden Konzepte von Kryptowährungen, sowie auch die Struktur des darunterliegenden Netzwerks werden im Rahmen dieser Studie ebenfalls beschrieben.

Einer der Gründe für die weite Verbreitung und das Interesse an Bitcoin ist die Attraktivität des Systems für Händler: Einerseits sind die Transaktionsgebühren im Allgemeinen niedriger als beispielsweise bei Kreditkartenzahlungen, andererseits werden diese vom Kunden getragen, wodurch für den Händler keine Kosten anfallen. Darüber hinaus ist Bitcoin auch auf Grund anderer Eigenschaften attraktiv. Die Unwiderrufbarkeit, bzw. Unveränderbarkeit getätigter Transaktionen und die eindeutige Identifikation jeder Währungseinheit führen dazu, dass der Weg aller Währungseinheiten seit deren Entstehung öffentlich einsehbar und inhärent unzweifelhaft nachvollziehbar ist. Die Ausschüttung von neuem Kapital und der Transaktionsgebühren an jene Teilnehmer des Bitcoin-Netzwerks, welche erfolgreich Transaktionen in die Blockchain als zentrales Transaktionsregister aufnehmen (siehe Abschnitt 2.5), führt zu einem gewollten Konkurrenzkampf innerhalb des Netzwerkes. Daraus ergibt sich ein Gleichgewicht, da viele voneinander unabhängige Teilnehmer auf ein gemeinsames Ziel hinarbeiten, ohne jedoch einander vertrauen zu müssen. Auf Grund dessen ist die Blockchain vor Manipulationen geschützt. Dieses hohe Maß an Integrität macht die Blockchain-Technologie auch als Datenbank für Anwendungen abseits von Kryptowährungen

[1] Satoshi Nakamoto ist ein Pseudonym. Die wahre Identität des Bitcoin-Erfinders ist nicht gesichert bekannt. Jüngst hat Craig Steven Wright anhand erster Bitcoin Transaktionen behauptet, dies zu sein.

interessant.
Besonderes Augenmerk bei der Entwicklung von Bitcoin und Blockchain galt der eben erwähnten Unumkehrbarkeit und somit der Integrität von Transaktionen. Das Sicherheitskonzept der Blockchain basiert im Kontext von Kryptowährungen zu einem signifikanten Teil auf der Ausschüttung von neuem Kapital an Teilnehmer des Netzwerks. Abseits solcher Zahlungssysteme müssen Alternativen die Integrität des Systems garantieren. Doch gerade dieser essentielle Aspekt wird weitgehend vernachlässigt, wenn es darum geht, solche sich selbst regulierenden Systeme, auf den Bankensektor umzulegen.
Mangels empirischer Daten und auf Grund von teilweise unzureichend spezifizierten Modellen werden im Rahmen dieser Studie zwar diesbezügliche Beispiele und Konzepte dargelegt, deren Potential jedoch nicht bewertet. Im folgenden Abschnitt wird auf die Konzepte von Bitcoin eingegangen. Da sich dieses System in nahezu allen entscheidenden Punkten von traditionellen Zahlungssystemen unterscheidet, ist ein grundlegendes Verständnis von Kryptowährungen eine Voraussetzung, bevor die technischen Details der Blockchain diskutiert werden können. Nachfolgend wird die Blockchain, wie sie in ihrer Urform im Rahmen der Kryptowährung Bitcoin zum Einsatz kommt, detailliert beschrieben. Im Anschluss werden mögliche Anwendungsfälle abseits von Kryptowährungen skizziert und abschließend wird ein Ausblick auf mögliche zukünftige Entwicklungen gegeben.

2. Bitcoin

Der Begriff *Bitcoin* wird oft als Synonym für unterschiedliche Komponenten und Aspekte des Systems Bitcoin verwendet. Tatsächlich umfasst dieses ein Bezahlsystem basierend auf einer Kryptowährung, die Kryptowährung selbst, ein *Peer-to-Peer-Netzwerk*[2], sowie eine Referenzimplementierung der Software. Diese wird benötigt um diesem Netzwerk beizutreten und Transaktionen abwickeln zu können. Weiters ist auch die *Blockchain* als zentrales Transaktionsregister und Eckpfeiler des Bezahlsystems ein zentraler Bestandteil von Bitcoin. Oft wird auch der Begriff *Kryptowährung* als Synonym für die Gesamtheit eines solchen Systems verwendet. Durch die enge Koppelung aller Komponenten ist es schwierig, diese isoliert zu betrachten, weshalb in diesem Abschnitt die Grundlagen des Systems Bitcoin in seinen wesentlichen Aspekten basierend auf [4] beschrieben werden.

Zur Veranschaulichung des grundlegenden Ablaufs und der Begriffe werden in Abbildung 1 jene Begriffe und Schritte einer Transaktion erläutert, die für das Verständnis von Bitcoin wesentlich sind. Die Begriffe werden anschließend in Abschnitt 2.1 genauer erläutert bzw. eine Transaktion in Abschnitt 2.2 beschrieben.

Eine Grundlage ist, dass bestimmte selbsterklärte Teilnehmer des Bitcoin-Netzwerks (sog. „Miner“) Werte generieren, indem sie kryptografisch schwere Rätsel lösen. Durch die Lösung des Rätsels erhält der Miner einen (Daten)block der eine bestimmte Eigenschaft erfüllt. Dies dient als *proof-of-work.* Anschließend muss der Miner den erstellten Block an die ihm bekannten P2P-Teilnehmer schicken. Auf diese Weise baut sich bei jedem Teilnehmer dezentral ein öffentliches Transaktionsregister auf und jeder kann – über kryptografisch relativ einfache Funktionen – die Transaktionen überprüfen. Blöcke andere Miner – die wiederum Daten anderer Transaktionen verknüpfen – werden mit dem eben generierten verknüpft. Auf diese Weise sind alle Transaktionen miteinander verkettet.
Ein Benutzer, der Werte besitzt (sie in einer *Wallet* hält) gibt diese wiederum weiter, indem er eine Transaktion mit diesen eingehenden Werten generiert, signiert und weitergibt. Diese wird wiederum

[2] Ein *Peer-to-Peer-Netzwerk* (P2P-Netz) beschreibt eine dezentrale Netzwerkstruktur. Im Gegensatz zu hierarchischen Netzen (wie beispielsweise dem Telefonnetz) oder klassischen Client-Server Netzwerken sind P2P-Netze flach organisiert. Jeder Teilnehmer ist gleichzeitig Client und Server und trägt seinen Teil dazu bei, Informationen durch das Netzwerk zu leiten. Dadurch ergibt sich ein hohes Maß an Ausfallsicherheit, da es keinen Single Point-of-Failure gibt. Im Regelfall sind P2P-Netze logische Strukturen, welche auf bestehenden Netzwerken aufbauen; bestehende Infrastruktur wird verwendet, deren Organisation und Struktur jedoch verborgen. Den Teilnehmern eines P2P-Netzes erscheint ein solches Netzwerk so, als würde es sich tatsächlich um eine Gruppe von Teilnehmern handeln welche alle auf einer einzigen Ebene miteinander verbunden sind.

als Teil eines neuen verketteten Blocks im Transaktionsregister (d.h. der Blockchain) prüfbar protokolliert. (Rest-)Werte wie „Wechselgeld“ werden ebenfalls in die Transaktion aufgenommen.

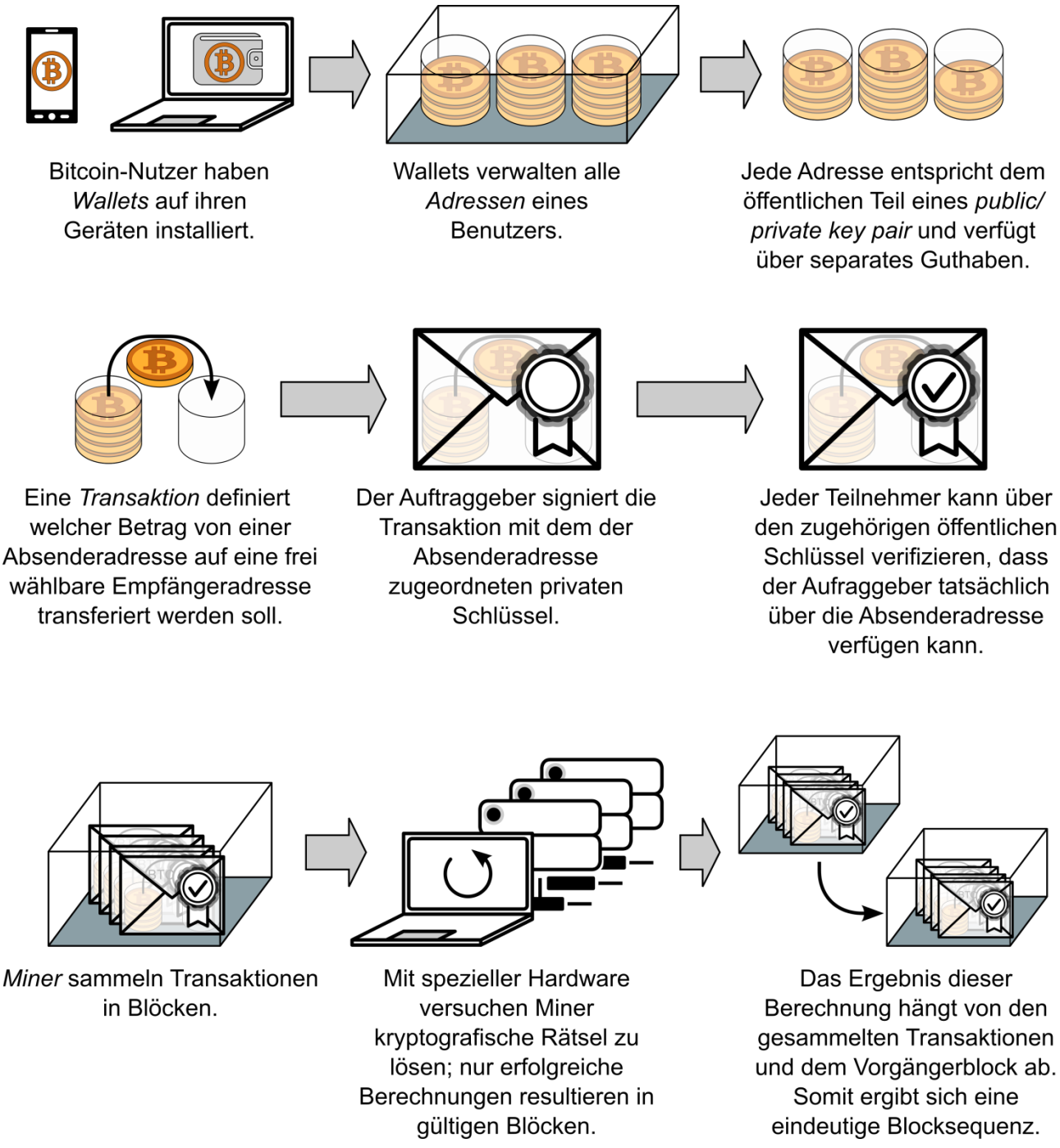

Abbildung 1: Illustration grundlegender Konzepte

2.1. Konzepte

Im Rahmen dieses Abschnitts werden grundlegende Konzepte von Kryptowährungen wie Bitcoin sowie die zugehörige Terminologie definiert. Nach Möglichkeit werden konkrete Beispiele angeführt. Besonderes Augenmerk wird jedoch auf die Zusammenhänge der Begrifflichkeiten untereinander gelegt, um ein möglichst vollständiges Bild des Bitcoin-Systems darzulegen. Aus diesem Grund folgt die Definition auch nicht alphabetisch, sondern in der Reihenfolge, welche die Zusammenhänge am besten zum Ausdruck bringt.

2.2. Adresse

Die *Adresse* kann am ehesten als Äquivalent zur Kontonummer bzw. IBAN in traditionellen Zahlungssystemen angesehen werden, da Guthaben auch im Rahmen von Kryptowährungen an Adressen gebunden ist. Eine weitere Parallele ergibt sich, da auch Bitcoin-Transaktionen Guthaben zwischen Adressen transferieren. Allerdings gibt es gravierende Unterschiede gegenüber traditionellen Zahlungssystemen. Aus der dezentralen Struktur von Bitcoin ergibt sich der Umstand, dass jeder Teilnehmer seine Adressen selbst erstellt und diese auch keine Personenbindung besitzen, daher gibt es auch kein Verzeichnis gültiger Adressen. Der Adressraum ist mit 2^{160} so groß, dass doppelte Adressen de-facto ausgeschlossen sind. Dieser Fall wird im Protokoll schlichtweg nicht behandelt, da er irrelevant ist; durch den großen Adressraum wird die „unkontrollierte" Selbstverwaltung von Adressen ohne zusätzlichen Aufwand erst ermöglicht.[3] Das bloße Erstellen von Adressen führt auch nicht dazu, dass diese anderen Teilnehmern bekannt sind. Die Adresse des Begünstigten muss durch die Applikation des Bezahlenden jeweils erfragt werden. Dieser Adressaustausch ist nicht Teil der Bitcoin-Protokolle, sondern erfolgt auf Applikationsebene. Üblich sind anklickbare Links und QR-Codes, welche die Empfängeradresse enthalten. Erst wenn eine Adresse als Empfänger im Rahmen einer Transaktion referenziert wird, gibt es öffentliche Aufzeichnungen über deren Existenz (aber eben nicht über die Person des Begünstigen).

Der größte Unterschied zu Kontonummer und IBAN ist jedoch die Tatsache, dass es sich bei Adressen um Einwegtoken handelt. Bitcoin ist darauf ausgelegt, dass jede Adresse nur für eine einzige Transaktion verwendet wird. Somit besteht im Gegensatz zu einem Bankkonto keine Langzeitbindung zwischen Adresse und „Kontoinhaber". Auch deshalb sind Adressen ihren Besitzern nicht zuordenbar, wenn diese sie nicht freiwillig bekannt geben. Tatsächlich gibt es im Rahmen von Bitcoin kein Äquivalent zum klassischen Bankkonto.

Aus technischer Sicht handelt es sich bei einer Adresse um den öffentlichen Teil eines kryptografischen Schlüsselpaars (eines *public/private key pair*, siehe Abschnitt A.2).

2.3. Wallet

Bei der *Wallet* handelt es sich um eine Endbenutzersoftware, welche Adressen sowie deren zugehörige private Schlüssel verwaltet und die Erstellung von Transaktionen ermöglicht. Aus Benutzersicht entspricht die Wallet am ehesten dem Bankkonto im Kontext traditioneller Zahlungssysteme. Nachdem im Rahmen von Bitcoin Währungseinheiten (die auch als *Bitcoins* oder kurz BTC bezeichnet werden) in der Blockchain (dem konzeptionell zentralen aber topologisch verteilten Transaktionsregister) gespeichert sind, kann nicht davon gesprochen werden, dass das eigene Guthaben in einer Wallet abgelegt ist. Die Wallet sammelt lediglich die in der Blockchain gespeicherten Informationen und wertet jene Transaktionen aus, welche zu den von der Wallet verwalteten Adressen passen um daraus einen „Kontostand" zu berechnen und dem Benutzer anzuzeigen. Die Informationen der Blockchain werden jedoch unter anderem aus Gründen der Performance lokal am Endgerät zwischengespeichert. Zudem speichert die Wallet die zu den Adressen gehörenden *private keys*. Diese Schlüssel dienen als Beweis, dass man der Eigentümer der zugehörigen Bitcoins ist und diese verwenden darf. Eine weitere Kernaufgabe der Wallet ist die Generierung von Adressen für auszuführende Transaktionen, um die Mehrfachverwendung bestehender Adressen zu vermeiden.

2.4. Transaktionen, UTXO

Bitcoin-Transaktionen unterscheiden sich grundlegend von Transaktionen im Rahmen traditioneller Zahlungssysteme. Transaktionen werden vollständig dezentral durchgeführt: Die einzigen in einer Zahlung direkt involvierten Parteien sind Auftraggeber und Empfänger. Statt auf vertrauenswürdige Dritte zu setzen, beruht die Sicherheit und Integrität des Systems auf kryptografischen Beweisen. Dritte sind nur dahingehend involviert, dass Transaktionen in der (in allen Wallets vorliegenden)

[3] Adressen werden zufällig generiert. Kommt ein unzureichender Zufallsgenerator zum Einsatz, kann es zu Adresskollisionen kommen. Es gibt keine Möglichkeit zwischen „Original" und „Duplikat" einer Adresse zu unterscheiden, da es eine Adresse nur einmal geben kann. Wird eine bereits existierende Adresse erneut generiert, besitzen zwei Teilnehmer den zu dieser Adresse passenden privaten Schlüssel und können somit über das an diese Adresse gebundene Guthaben verfügen.

Blockchain protokolliert werden. Die Integrität einer Zahlung ist somit formal garantiert. Daher ist ein Wissen um die grundlegenden Konzepte asymmetrischer Kryptografie eine Voraussetzung, um die Funktionsweise von Bitcoin-Transaktionen nachvollziehen zu können. Entsprechende Informationen sind Anhang A zu entnehmen.

Eine Transaktion besteht aus einem eindeutigen *Identifier*, Werten in Form von mindestens einem *Input*, mindestens einem *Output* sowie *Freigabebedingungen*. In den meisten Fällen verlangen die Freigabebedingungen schlichtweg den zur Empfängeradresse passenden privaten Schlüssel, um über die in der Transaktion referenzierten Werte verfügen zu können. Dies trifft auf *Pay-to-Public-Key–*, bzw. *Pay-to-Address–, und Multisignature*-Transaktionen (siehe Abschnitt 4.3) zu. Der Identifier kann als eine Art Auftragsnummer angesehen werden. Im Gegensatz zu Auftragsnummern im Endkundengeschäft hierarchischer Bankensysteme sind Identifier innerhalb des gesamten Zahlungssystems eindeutig. Pay-to-Public-Key-Transaktionen machen den Großteil der Transaktionen aus. Neben diesen werden noch *Pay-to-Script-Hash*, *OP_Return* sowie *Non-Standard* Transaktionen unterstützt, welche sich vor allem anhand ihrer Freigabebedingungen unterscheiden.
Non-Standard-Transaktionen spielen im regulären Zahlungsverkehr keine Rolle und sind für spezielle Anwendungen vorgehsehen. Im Gegensatz dazu können die Freigabebedingungen von Pay-to-Script-Hash-Transaktionen vom Auftraggeber innerhalb eines vorgegebenen Rahmens frei definiert werden um *Smart Contracts* umzusetzen (siehe Abschnitt 4.5). OP_Return-Transaktionen dienen ausschließlich zur Datenspeicherung innerhalb der Blockchain.

Bei Inputs und Outputs handelt es sich um „unverbrauchte“ bzw. noch nicht ausgegebene Währungseinheiten – Werte – welche entsprechend als *Unspent Transaction Outputs* (UTXO) (umgangssprachlich auch als „Bitcoins“, bzw. schlichtweg Guthaben) bezeichnet werden. Kryptowährungseinheiten können genau wie traditionelle Zahlungsmittel nicht verbraucht werden, sondern lediglich den Besitzer wechseln. Besitzt jemand UTXO, bedeutet das schlicht, dass diese Partei über einen bestimmten Betrag frei verfügen kann. Unverbrauchtes Guthaben wird ausgegeben, indem es als Input in eine Transaktion aufgenommen wird und als Output an einen Empfänger „ausbezahlt“ wird. Auftraggeber und Empfänger werden nicht als Personen deklariert, lediglich deren Adressen. Transaktionen sind strukturell angelehnt an doppelte Buchführung (siehe Tabelle 1).

Input	**Adresse**	**Wert**		Output	Adresse	**Wert**
Input 1	A	0,15		Output 1	X	0,90
Input 2	B	0,20		Output 2	Y	0,25
Input 3	C	0,35				
Input 4	D	0,50				
Summe Inputs		1,20		Summe Outputs		1,15
		Inputs	1,20			
	–	Outputs	1,15			
			0,05	(implizite Transaktionsgebühr)		

Tabelle 1: Schematische Darstellung einer Transaktion

UTXO sind nicht aufteilbar, genauso wenig wie ein Teil einer Banknote einen Teil des Werts einer unversehrten Banknote repräsentiert. Stattdessen wird bei Bitcoin-Zahlungen genau wie im Rahmen traditioneller Zahlungssysteme „Wechselgeld gegeben“, indem ein entsprechender Wert in Form neuer UTXO als Output einer Transaktion angegeben wird, welche eine Adresse des Auftraggebers als Empfänger referenziert. Der Output einer Transaktion kann als Input in einer anderen Transaktion verwendet werden. Genau wie Banknoten durch Seriennummern gekennzeichnet sind, besitzen auch UTXO eine Art Seriennummer und sind somit eindeutig identifizierbar. Dadurch ist auch die gesamte Historie einer jeden Währungseinheit im zentralen Transaktionsregister protokolliert. Die Differenz aus der Summe der Outputs und der Summe der Inputs einer Transaktion

ergibt die (implizite) Gebühr, welche für diese Transaktion anfällt. Deren Höhe wird vom Auftraggeber festgelegt. Abschnitt 2.7 behandelt Transaktionsgebühren im Detail.

Alle Transaktionen, sowie die Gesamtmenge aller Währungseinheiten (alle jemals existierenden UTXO) sind im System in der Blockchain als zentralem Transaktionsregister festgehalten. Daher sind auch alle Transaktionsdaten öffentlich bekannt. Gutgeschrieben werden kann der im Output einer Transaktion deklarierte UTXO jedoch nur der Adresse, welche in den definierten Freigabebedingungen der Transaktion referenziert ist.

Da es sich bei Bitcoin-Adressen um den öffentlichen Teil eines kryptografischen Schlüsselpaares handelt, lauten die Freigabebedingungen im Allgemeinen sinngemäß „der Besitz des privaten Schlüssels des Begünstigten“. In diesem Fall kann nur der Ersteller einer Adresse über die im Output einer Transaktion deklarierten UTXO verfügen und diese allenfalls in Form einer neuen Transaktion ausgeben. Hierfür wird eine neue Transaktion erstellt und mit dem der Adresse zugehörigen privaten Schlüssel signiert, wodurch bewiesen ist, dass man den dazugehörigen privaten Schlüssel besitzt.

Obwohl keine weiteren Parteien direkt an der Transaktionsabwicklung beteiligt sind, welche eine „in Auftrag gegebene“ Transaktion ausführen, ist die Bezeichnung *Auftraggeber* von einem bestimmten Standpunkt aus nach wie vor zutreffend, wenn man die Freigabebedingungen näher betrachtet: Im einfachsten Fall verlangen diese schlicht den der Adresse zugehörigen privaten Schlüssel. Es ist jedoch möglich, zusätzliche Bedingungen zu definieren. Im Rahmen von Bitcoin sind diese zwar begrenzt, allerdings existieren andere Systeme, die auf dem gleichen Prinzip beruhen und darauf ausgelegt sind, dass der Empfänger vom Auftraggeber festgelegte Operationen, sogenannte *Contracts* durchführt bzw. erfüllt und als Entlohnung für diesen Aufwand die deklarierten UTXO erhält (siehe Abschnitt 4.5). Diese Bedingungen sind so strukturiert, dass deren Einhaltung von allen Teilnehmern verifizierbar ist. Das trifft auch auf die eben beschriebenen, regulären Transaktionen zu: Die Überprüfung digitaler Signaturen (siehe Abschnitt A.3) kann und wird von allen Teilnehmer unabhängig voneinander durchgeführt, um zu gewährleisten, dass nur legitime Transaktionen vom System anerkannt werden. Ein beispielhafter Transaktionsablauf ist in Abschnitt 2.9 beschrieben.

2.5. Blockchain, Blöcke und Mining

Die Blockchain ist das zentrale Transaktionsregister von Kryptowährungen wie Bitcoin. Wie der Name vermuten lässt, besteht diese aus einzelnen Blöcken. Blöcke sind kryptografisch miteinander verkettet, woraus sich eine eindeutige Reihenfolge ergibt. Details hierzu sind Abschnitt 3 zu entnehmen. Transaktionen werden in Blöcken zusammengefasst und dadurch validiert. Neue Blöcke können nur erstellt werden, indem ein kryptografisches Problem gelöst wird, dessen Lösung schwierig zu finden, aber einfach zu verifizieren ist. So ist es zum Beispiel auch schwierig ein Sudoku-Rätsel korrekt zu lösen, die Korrektheit einer Lösung ist jedoch von jedermann sehr einfach durch simple Additionen verifizierbar. Dasselbe Prinzip kommt auch beim Erstellen von Blöcken zum Einsatz. Durch die Schwierigkeit des zu lösenden Problems und der von jedem Teilnehmer unabhängig durchführbaren Verifikation der Lösung (und somit des Blocks) ist die Blockchain vor Manipulationen geschützt und deren Integrität garantiert. Auf Grund des Umstands, dass jeder Block (ebenso wie jede Transaktion) von allen Teilnehmern unabhängig voneinander überprüft wird, können sich ungültige oder gezielt gefälschte Blöcke nicht im Netzwerk verbreiten, da diese verworfen werden. Offensichtlich handelt es sich hierbei um freiwilliges Verhalten aller Teilnehmer. Der Grund hierfür ist schlichtweg, dass man jederzeit selbst Opfer eines Betrugs werden kann, wenn man UTXO empfängt, welche nicht korrekt verarbeitet wurden. Genau wie bei Falschgeld, besteht die Gefahr, dass diese Outputs nicht angenommen werden. Die Chance hierfür ist jedoch um ein Vielfaches höher. Im Gegensatz zu Banknoten werden UTXO nicht auf optische und haptische Merkmale überprüft, sondern automatisiert nachprüfbare kryptografische und mathematische Beweise bestätigen bzw. widerlegen deren Authentizität.

Als Anreiz neue Blöcke zu erstellen dient das mit einem Erfolg einhergehende frische Kapital in Form neu erstellter UTXO. Dazu erstellt der Erzeuger des Blocks (im Kontext von Kryptowährungen als *Miner* bezeichnet) eine sogenannte *Coinbase* Transaktion. Die *Coinbase*-Transaktion ist immer die erste Transaktion die in einen neuen Block aufgenommen wird. Setzt sich der Block durch, bekommt der Ersteller die Belohnung ausgeschüttet. Ob und wann sich ein Block etabliert hängt von mehreren

Faktoren ab. Im einfachsten Fall setzt sich der Block durch, welcher zuerst erzeugt wurde. Wenn es jedoch konkurrierende Blöcke gibt, welche auf demselben Vorgängerblock aufbauen, wird der Block mit dem höheren proof-of-work anerkannt (Details hierzu werden in Kapitel 3 behandelt). Im ersten Moment kann diese Tatsache den Eindruck vermitteln, dass jeder nach Belieben „Geld drucken“ kann. Tatsächlich ist dies aber streng reglementiert, da die Menge an ausgeschüttetem Kapital im System (d.h. in der Software aller Teilnehmer) definiert ist. Auch an dieser Stelle werden wieder kryptografische Verfahren – Hashfunktionen auf Basis von SHA-256 [3] – eingesetzt, mit deren Hilfe jeder Teilnehmer die Validität eines neuen Blocks überprüfen kann (Details zum proof-of-work-Konzept sind in Abschnitt 3.2 ausgeführt). Somit wird sichergestellt, dass der Ersteller eines Blocks auch tatsächlich das vorgegebene kryptografische Rätsel gelöst hat und somit nicht beliebig „Geld nachdrucken“ kann.

Zusätzlich zum frischen Kapital erhält ein Miner auch die Transaktionsgebühren aller in einen Block aufgenommenen Transaktionen. Über beides kann der Ersteller eines Blocks frei verfügen. Das Erstellen gültiger Blöcke wird (angelehnt an das Schürfen von Gold) als *Mining* bezeichnet. Die Schwierigkeit des zu lösenden kryptografischen Problems wird laufend an die Rechenleistung des Bitcoin-Netzwerkes angepasst. Bei zunehmender Popularität steigt somit die Gesamtrechenleistung und damit einhergehend auch der Energieverbrauch. Ziel ist es, dass alle 10 Minuten ein neuer Block erstellt wird. Da jeder Block vom vorherigen Block und den enthaltenen Transaktionen abhängt, ist eine Vorberechnung unmöglich. Im folgenden Abschnitt wird der Energieverbrauch betrachtet.

2.6. Energieverbrauch

Der Energieverbrauch des Bitcoin-Netzwerkes lässt sich nur sehr ungenau abschätzen, da die verwendete Hardware der Miner unbekannt ist. Dementsprechend gehen die Abschätzungen weit auseinander. So schätze Bergmann 2014 den Stromverbrauch auf 125-200 Megawatt [5], während Allied Controll auf 250-500 Megawatt kommt [6] und O’Dwyer und Malone auf 0,1-10 Gigawatt [7]. Die Schätzung von O’Dwyer und Malone würde in etwa dem Energieverbrauch von Irland (3GW) entsprechen. Im Jahr 2015 schätzte Malmo den Stromverbrauch auf 215 Megawatt [8]. Das Goverment Office of Science ging 2016 von einem Stromverbrauch von einem Gigawatt aus. Es gibt auch Prognosen für den zukünftigen Stromverbrauch, so schätzt beispielsweise Deetman, dass Bitcoin im Jahr 2020 zwischen 417 Megawatt und 14,6 Gigawatt an Energie benötigen wird [9]. Dies würde in etwa dem Energieverbrauch von Dänemark (14 GW[4]) entsprechen.
Die große Schwankungsbreite ergibt sich durch die unterschiedliche Effizienz der eingesetzten Hardware. Beispielsweise schafft eine herkömmliche CPU[5] weit unter einer Million Hashoperationen pro Joule, während eine Anwendungsspezifische integrierte Schaltung (ASIC)[6] über 1700 Millionen Hashoperationen pro Joule durchführen kann [7].
Da sich der Stromverbrauch des Bitcoin-Netzwerkes nur sehr ungenau abschätzen lässt ist auch ein Vergleich mit bestehenden Zahlungssystemen sehr schwer. Je nachdem welche Annahmen man trifft kann man sowohl zeigen, dass Bitcoin um 99,8% weniger Emissionen hat als das Bankensystem [10], als auch das Bitcoin pro Transaktion etwa 5033 mal so viel Energie benötigt wie eine VISA-Transaktion [8]. Beide Aussagen sollten mit Vorsicht betrachtet werden.

2.7. Transaktionsgebühren

Da Transaktionen ohne den Einbezug Dritter erstellt werden, fallen zumindest theoretisch keine Transaktionsgebühren an. Im Rahmen des Miningprozesses können allerdings nicht beliebig viele Transaktionen in einen neuen Block aufgenommen werden. Folglich werden jene Transaktionen priorisiert, welche die höchsten Transaktionsgebühren abwerfen. Deren Höhe ergibt sich schlicht aus der Differenz zwischen der Summe der Inputs und der Summe der Outputs einer Transaktion. Wenn eine Transaktion beispielsweise UTXO im Wert von 10 Währungseinheiten als Inputs und UTXO im Wert von 9 Währungseinheiten als Outputs enthält, ergibt sich *Collateral* (angelehnt an den finanziellen Terminus Sicherheit bzw. *Collateral*) im Wert einer Währungseinheit. Collateral wird an den Miner, der eine Transaktion in einen Block aufnimmt ausbezahlt, bzw. an eine seiner

[4] http://www.tsp-data-portal.org/Breakdown-of-Electricity-Capacity-by-Energy-Source#tspQvChart abgerufen am 20.10.2016
[5] Core i7 950 (0.126 Mhash/J)
[6] Monarch BPU 600 C (1714 Mhash/J)

Adressen gebunden. Miner werden daher Transaktion mit höheren Transaktionsgebühren bevorzugt in ihre Blöcke aufnehmen. Somit kann der Ersteller einer Transaktion über die Höhe der Transaktionsgebühren die Priorisierung von Transaktionen beeinflussen. Tatsächlich spielt dieser Aspekt jedoch eine verschwindend geringe Rolle und muss vom Durchschnittsnutzer nicht weiter beachtet werden, da die Wallet-Applikation sinnvolle Standardwerte verwendet.

2.8. Das Bitcoin-Netzwerk

Kryptowährungen wie Bitcoin sind dezentral organisiert. Der komplette Datenbestand an Transaktionen wird zwar in der Blockchain gesichert, welche als zentrales Transaktionsregister fungiert, jedoch wird die Blockchain selbst nicht an einem zentralen Ort gespeichert oder zentral verwaltet, sondern eben durch den Prozess des Minings stetig fortgeführt. Bitcoin spezifiziert ein Protokoll, welches alle Teilnehmer des Bitcoin-Netzwerks nutzen um untereinander ständig Informationen auszutauschen und dadurch ein stets aktuelles Abbild der Blockchain zu verbreiten.

Wenn eine Transaktion durchgeführt wird, so wird diese vom Auftraggeber an jene Teilnehmer übermittelt, die ihm momentan bekannt sind. Diese leiten die eben erhaltenen Informationen wiederum an die ihnen bekannten Teilnehmer weiter. Somit propagieren alle, egal an welchem Punkt im Netzwerk erstellten (Transaktions-)Informationen durch das Netzwerk und erreichen nach wenigen Sekunden alle Teilnehmer. Dies entspricht dem Flooding-Ansatz, welcher auch von klassischen Routing-Protokollen verwendet wird. Da es sich dabei um kontrolliertes Flooding handelt, skaliert dieser Ansatz [11]. Die Integrität aller ausgetauschten Informationen, somit auch die Integrität neu erstellter Blöcke wird von jedem Teilnehmer des Netzwerks unabhängig verifiziert. Grundlage hierfür sind ebenfalls Verfahren aus dem Bereich der asymmetrischen Kryptografie. Wird eine Transaktion empfangen, welche bereits ausgegebene Währungseinheiten oder sonstige Unregelmäßigkeiten aufweist, wird diese nicht weitergereicht. Da Miner nur von gültigen Transaktionen in Form von Transaktionsgebühren profitieren, werden ungültige Transaktionen auch nie in neue Blöcke aufgenommen werden.

Im nachfolgenden Abschnitt wird der Ablauf einer Bezahlung von der Erzeugung einer Transaktion bis zu deren Einbettung in die Blockchain beschrieben.

2.9. Transaktionsablauf

In diesem Abschnitt wird ein beispielhafter Transaktionsablauf beschrieben, der zum einen den Transaktionsablauf an sich veranschaulichen, aber auch die Praxistauglichkeit von Kryptowährungen wie Bitcoin illustrieren soll. Zur Veranschaulichung wird auf die einleitend gegebene Abbildung verwiesen.

Ausgangspunkt ist, dass Alice mittels Bitcoin ein Produkt von Bob erwerben will. Beide haben ihre Wallets bereits eingerichtet, Alice in Form einer App für ihr Smartphone und Bob betreibt seine Wallet auf dem Kassenrechner. Die Wallets verwalten alle Adressen und die dazugehörigen privaten Schlüssel des jeweiligen Benutzers. Wenn Alice nun ein Produkt von Bob erwerben will, wird Bobs Wallet eine neue Adresse generieren. Diese wird zusammen mit dem zu zahlenden Betrag Alice übermittelt oder – z.B. als QR-Code kodiert – präsentiert. Der QR-Code kann mittels der Wallet-App gescannt werden, alternativ kann die Information auch abgetippt werden. In jedem Fall hat die Wallet nun alle benötigten Informationen und wählt eine oder mehrere Adressen von Alice als Input aus. Mehrere Adressen werden benötigt, falls das Guthaben einer einzelnen Adresse nicht ausreicht. Als Output wird die von Bobs Wallet generierte Adresse angegeben. Zusätzlich generiert die Wallet-App von Alice eine neue Adresse auf die das Wechselgeld übertragen wird. Je nach Konfiguration wird die Wallet einen kleinen Betrag als Transaktionsgebühren vom Wechselgeld abziehen. Die soeben generierte Transaktion wird anschließend mit den zu den Input-Adressen gehörenden privaten Schlüsseln signiert. Da Alices Adresse vom zugehörigen öffentlichen Schlüssel abgeleitet ist und der Public Key Teil der Transaktion ist, kann jeder Teilnehmer des Bitcoin-Netzwerkes verifizieren, das Alice über dieses Guthaben verfügen darf [12]. Die erstellte Transaktion wird nun über das Bitcoin-Netzwerk weiterverbreitet. Kurz darauf wird diese Transaktion von Bobs Wallet empfangen.

Je nach Konfiguration kann Bobs Wallet die Transaktion als Beweis für die Bezahlung akzeptieren oder warten, bis die Transaktion in einen neuen Block aufgenommen wurde. Die sofortige Akzeptanz

der Transaktion birgt ein gewisses Risiko: Wird die Transaktion nicht in einen Block aufgenommen, bekommt Bob sein Geld nie. Dieser Fall kann beispielsweise dann eintreten, wenn keine Transaktionsgebühren deklariert werden, oder sonstige Unregelmäßigkeiten auftreten. Um sicher zu gehen, müsste Bob folglich warten, bis die Transaktion in einen neuen Block aufgenommen wird. Wenn Bob jedoch über ein hinreichend aktuelles Abbild der Blockchain verfügt, reicht bei Kleinstbeträgen die Transaktion selbst im Regelfall als Beweis aus. Bei größeren Beträgen wird jedoch meist abgewartet, bis die Transaktion in einen Block aufgenommen wurde und auch weitere auf diesem Block aufbauende Blöcke erstellt wurden. Je mehr Blöcke hinzukommen, umso schwieriger wird es für einen Betrüger oder Angreifer, eine bereits abgewickelte Transaktion nachträglich zu verändern. Details hierzu sind Abschnitt 3.2 zu entnehmen.

Neu erstellte Blöcke werden genau wie Transaktionen auch an alle Teilnehmer des Bitcoin-Netzwerks weitergeleitet. Alle Teilnehmer die einen Block empfangen, überprüfen ob es sich um einen gültigen Block handelt und ob die enthaltenen Transaktionen gültig sind. Nach kurzer Zeit wird der Block, der Alices Transaktion enthält folglich auch von Bobs Wallet empfangen. Bobs Wallet erkennt automatisch, dass dieser Block die Transaktion enthält, die als Bezahlung für das zuvor verkaufte Produkt dient. Somit hat Bob nach einer kurzen Wartezeit die Bestätigung, dass die Transaktion korrekt abgewickelt wurde. Eine korrekte und benutzerfreundliche Wallet ist somit eine Grundvoraussetzung für eine breite Akzeptanz der Technologie, da es nicht zumutbar wäre diese Schritte manuell durchzuführen. Die im Rahmen dieser Beispieltransaktion beschriebenen Konzepte sind in Abbildung 1 illustriert.

2.10. Bitcoinbörsen und Bitcoin im Endkundengeschäft

Auf Grund der steigenden Popularität von Kryptowährungen wie Bitcoin haben sich eine Reihe an Bitcoin-Börsen entwickelt, welche es ermöglichen Bitcoins zu kaufen. Beispiele hierfür sind *CoinBase, Inc.* [13] und *Bitcoin Deutschland AG* mit Services wie *bitcoin.de* [14]. Da der Bitcoin-Kurs in den letzten Jahren stark gestiegen ist, jedoch nach wie vor merklich schwankt (siehe Abbildung 2), hat sich ein eigener Markt um Kursspekulationen von Bitcoin entwickelt. Ähnlich wie bei Fiat-Währungen hängt der Kurs von Angebot und Nachfrage bzw. dem Vertrauen in die Währung ab.

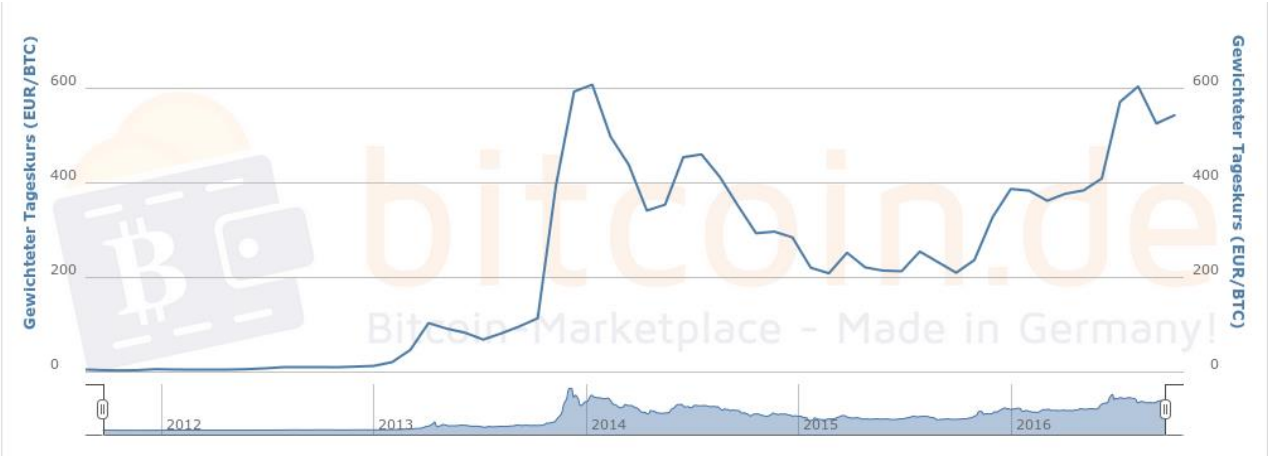

Abbildung 2: Bitcoin-Kursentwicklung seit 2012 laut Bitcoin Deutschland AG

Die Mehrheit der Bitcoin-Börsen ist aus technischer und organisatorischer Sicht konservativ umgesetzt und baut auf zentralen Datenbanken und zentral verwalteten Servern in Rechenzentren auf, welche alle Abwicklungen koordinieren. Hervorzuheben ist in diesem Zusammenhang die dezentrale Bitcoin-Börse *Bitsquare* [15], welche analog zu Bitcoin auf ein P2P-Netzwerk und eine dezentrale Organisation setzt. Wie auch bei Kryptowährungen, soll die dezentrale Struktur einen Single Point-of-Failure, Zensur und Manipulation verhindern. Hierbei handelt es sich aber nach wie vor um ein Nischenprodukt. Der Bitcoinkurs selbst beläuft sich laut Coinbase, Inc. momentan (Stand 20.09.2016 11:00 Uhr) auf USD 609,01 bei einer Gesamtmarktkapitalisierung von rund USD 10 Mrd. (woraus sich eine Gesamtmenge von rund 16 Mio. Bitcoins ergibt). Vergleicht man diese Zahlen beispielsweise mit dem BIP von Österreich sind auch Kryptowährungen selbst nach wie vor als Nischenprodukt anzusehen, da die Umsätze im Vergleich zu den Vermögenswerten der restlichen

Weltwirtschaft nicht ins Gewicht fallen. Nichts desto trotz setzen sich Kryptowährungen zunehmend im Endkundengeschäft durch. Unter anderem ist es mittlerweile möglich online Essen zu bestellen und mit Bitcoin zu bezahlen. Um eine rasche Abwicklung zu garantieren, verarbeitet in solchen Fällen meist ein Zwischenhändler wie z.B. *BitPay, Inc.* [16] die Bitcoin-Zahlung und zahlt dem Händler den entsprechenden Betrag in der Landeswährung aus. Des Weiteren wird versucht Bitcoin-ATMs zu etablieren. Technisch gesehen handelt es sich hierbei lediglich um einen Terminal, welcher direkt an eine Bitcoin-Börse angebunden ist und gegen Geld Bitcoin-Gutschiften auf eine Adresse tätigt.

Im nachfolgenden Abschnitt wird näher auf die Struktur der Blockchain und deren zu Grunde liegendes Sicherheitsmodell im Kontext von Kryptowährungen eingegangen.

3. Blockchain-Grundlagen

Die Blockchain als zentrales Transaktionsregister für das Bitcoin-System entspricht im Prinzip einer sequentiellen Datenbank, in welcher Informationen in Blöcken zusammengefasst protokolliert werden, wobei diese Blöcke unumkehrbar miteinander verkettet sind; jeder Block ist von allen vorhergehenden Blöcken abhängig. Im Rahmen der Kryptowährung Bitcoin handelt es sich bei den verarbeiteten Informationen im Wesentlichen um Transaktionsprotokolle, wobei theoretisch beliebige Informationen in die Blockchain aufgenommen werden können. Derzeit ist die von Bitcoin genutzte Blockchain ca. 80GB groß [17]. Eines der Alleinstellungsmerkmale der Blockchain ist das dezentrale Sicherheitskonzept, das im Folgenden in seiner Urform an Hand von Bitcoin beschrieben wird.

3.1. Blockchain im Kontext von Bitcoin

Bei der Blockchain, bzw. bei Bitcoin handelt es sich um vollständig dezentralisierte Systeme mit flacher Hierarchie (wesentliche Systemfunktionen und eine Kopie des zentralen TX-Registers Blockchain liegt am Endkundengerät); kein Teilnehmer steht über einem anderen. Weiters gibt es keine zentralen Instanzen, welche für die Verwaltung des Systems, Abwicklung von Transaktionen, oder Buchführung verantwortlich sind. In derartigen Szenarien ergeben sich neue Herausforderungen und Sicherheitsprobleme. Fragen wie Bonität und Integrität (sowohl von Geschäftspartnern, als auch von Datensätzen) lassen sich nicht über den Einbezug Dritter klären. Besonders die Integrität der Blockchain als zentrales Transaktionsregister, in dem die gesamte Historie jeder einzelnen Währungseinheit nachvollziehbar ist, muss garantiert werden können, ohne dass zentrale Entscheidungsträger dafür bürgen. Folglich ist auch die Frage der Verantwortung im Falle manipulierter Daten nicht einfach zu klären. Im Rahmen von Bitcoin wurde dieses Problem wie folgt gelöst: Transaktionen werden als validiert anerkannt, wenn diese in die Blockchain als Teil eines neuen Blocks aufgenommen wurden. Ein neuer Block kann jedoch nur erstellt werden, indem ein kryptografisches Problem gelöst wird. Im Fall von Bitcoin liegt diesem das Überwinden der Einwegcharakteristik einer kryptografischen Hashfunktion (siehe Abschnitt A.1) zu Grunde. Weitere Details hierzu sind in Abschnitt 3.2 beschrieben. Nachdem die Einwegcharakteristik per Definition nur mit immensem Rechenaufwand überwunden werden kann, ist auch dieses Problem entsprechend schwer lösbar.

Einige Teilnehmer[7] des Bitcoin-Netzwerks, die *Miner*, stellen hierfür Rechenleistung zur Verfügung und „rechnen um die Wette“. Obwohl sich prinzipiell jeder Teilnehmer als Miner versuchen kann, ist dieses Unterfangen mit hohen Kosten verbunden. Unter anderem, da die aufgebrachte Rechenleistung hohe Stromkosten verursacht (siehe unten). Der erste Teilnehmer, welcher das kryptografische Problem lösen kann, kann einen neuen Block erstellen, Transaktionen in diesen aufnehmen, den Block an die vorhandene Blockchain anhängen und, diese Information (mittels Flooding) im Netzwerk verbreiten und so veröffentlichen. Alle anderen Teilnehmer können mit geringem Rechenaufwand überprüfen, dass der Block gültig ist und das kryptografische Problem

[7] Die genaue Anzahl an Minern lässt sich aus technischen Gründen nicht feststellen, Schätzungen aus dem Jahr 2014 [5] legen jedoch nahe, dass es einige zehntausende Miner im gesamten Bitcoin-Netzwerk gibt. Diese stehen einigen hunderttausend aktiven Nutzern gegenüber, wobei sich auch diese Zahl nur schwer belegen lässt.

somit tatsächlich korrekt gelöst wurde. Da diesem Problem, bzw. der Überprüfung keine Signatur, sondern eine Hashfunktion zu Grunde liegt, wird hierfür kein Schlüsselmaterial benötigt (entsprechende Details sind dem nachfolgenden Abschnitt zu entnehmen). Nachdem jeder Block von allen vorherigen abhängig ist und alle vorangegangenen Blöcke öffentlich bekannt sind, lässt sich auch leicht sicherstellen, dass der neue Block auch tatsächlich von der bisherigen Blockchain abgeleitet ist. Diese annähernd sofortige Verifizierbarkeit, welche von allen Teilnehmern des Bitcoin-Netzwerks im Eigeninteresse durchgeführt wird, ist einer von zwei Hauptaspekten des Sicherheitskonzepts. Auf Grund der Abhängigkeiten von Blöcken untereinander, sowie der Tatsache, dass Transaktionen nicht vorhersehbar sind, können Blöcke auch nicht vorberechnet werden.

Der zweite integrale Teil des Blockchain-Sicherheitskonzepts ist die Antwort auf die Frage nach der Motivation neue Blöcke zu erstellen. Da enorme Rechenleistung aufgebracht werden muss, um einen Block erstellen zu können, entstehen bei jedem Versuch einen Block zu berechnen Kosten (Elektrizität, Wartung, möglicherweise muss defekte Hardware ersetzt werden, …). Außerdem wird die Schwierigkeit des zu Grunde liegenden kryptografischen Problems an die Gesamtrechenleistung des Netzwerks angepasst, weshalb es mittlerweile nur mehr mit spezieller, kostspieliger Hardware realistisch ist, einen Block erstellen zu können. Diese Anpassung wird wie viele andere Aktivitäten auch von jedem Teilnehmer individuell durchgeführt. Nur Blöcke, deren Erstellung ein gewisses Mindestmaß an Rechenleistung erfordert hat, werden somit als gültig akzeptiert.[8]

Die erfolgreiche Erstellung eines neuen Blocks wird direkt belohnt, weshalb sich innerhalb des Bitcoin-Netzwerks ein sehr aktiver Wettbewerb entwickelt hat: Jeder neu erstellte Block enthält frisches Kapital in Form neu erstellter UTXO, welche an den Ersteller ausgeschüttet werden. Aus technischer Sicht wird dies durch eine spezielle Transaktion, die *Coinbase*-Transaktion, bewerkstelligt, welche zu Gunsten des Miners Outputs ohne Inputs erzeugt. Die Coinbase-Transaktion ist immer die erste Transaktion in einem Block. Anfangs wurden BTC 50 pro Block ausgeschüttet. Dieser Betrag halbiert sich alle 210000 Blöcke. Ende 2012 kam es zur ersten Halbierung auf BTC 25. Im Juli 2016 kam es zur nächsten Halbierung auf BTC 12,5. Die nächste Halbierung wird für Juli 2020 erwartet [18]. Im Jahr 2140 werden alle Bitcoins im Umlauf sein [19]. Danach fällt diese Einnahmequelle für Miner weg.

Zusätzlich oder alternativ dazu erhält ein erfolgreicher Miner 100% der Gebühren aller Transaktionen, die in den neuen Block aufgenommen wurden. Hier ergeben sich erste Konflikte, wenn man versucht, dieses System direkt auf traditionelle Zahlungs– und Währungssysteme anzuwenden: Die Gesamtmenge an Währungseinheiten ist bei Bitcoin auf 20999999,9769 limitiert [20], was in einem deflationären Wirtschaftssystem resultiert. Diese Deflation ist laut Experten jedoch zwingend erforderlich, da sich Investitionen in spezielle Mining-Hardware im Rahmen eines inflationären Währungssystems nicht lohnen würden [21].

Nachdem der Weg jeder Währungseinheit von deren Entstehung an lückenlos nachvollziehbar ist, ist auch *double spending* (das mehrfache Bezahlen mit ein und derselben Währungseinheit) nicht möglich. Im Rahmen einer Transaktion kann vom Empfänger überprüft werden ob die ihm zugesicherten Währungseinheiten auch tatsächlich am Konto des Senders vorhanden sind, und nicht bereits ausgegeben wurden: Nachdem Miner nur gültige Transaktionen in Blöcke aufnehmen, und gültige Transaktionen double spending ausschließen, reicht das Vorhandensein der UTXO in der Blockchain als Sicherheit. Tatsächlich wird diese Überprüfung automatisiert von einer Wallet-Applikation ausgeführt. Dies kann je doch im Zweifelsfall (auch durch eigenen Code) nachgeprüft werden, sollte man der Wallet nicht ausreichend vertrauen. Dienste wie *Blockchain.info* [22] bieten interaktive Blockchain-Suchen an, um weitere Informationen über Transaktionsverläufe zu erhalten. Generell ist die Performance solcher Abfragen nach einmaligem Preprocessing kein Problem, daher können derartige Services auch Unabhängig von Drittanbietern in Wallet-Applikationen umgesetzt werden. Abgesehen davon ist der Quellcode nahezu aller Wallet-Implementierungen frei verfügbar,

[8] Generell ist es nicht profitabel sich nicht korrekt zu verhalten, da man sich als einzelner gegenüber einer Masse sich anders verhaltender Individuen nicht durchsetzen kann. In dieser einfachen Tatsache liegen viele Sicherheitsprinzipien von Kryptowährungen begründet; die Mehrheit gibt die Richtung vor. Wer gegen den Konsens verstößt wird ausgeschlossen, bzw. ignoriert. Das gilt sowohl für Miner als auch für einfache Nutzer.

wodurch dessen Korrektheit überprüft werden kann. Weitere technische Grundlagen des Konzepts werden im folgenden Abschnitt behandelt.

3.2. Sicherheitskonzepte der Blockchain

Im Kern des Blockchaindesigns steht eine bestimmte Klasse von Einwegfunktionen: Kryptografische Hashfunktionen, welche Daten beliebiger Größe auf ein Datum fixer Größe (den *Hash*) abbilden (welcher üblicherweise als Hexadezimalzahl dargestellt wird). Eine Hashfunktion kann nicht invertiert werden, wodurch eine Rückberechnung der Daten, welche auf einen gegebenen Hash abbilden unmöglich ist. Generell ist es im Idealfall nicht möglich zu einem vorgegebenen Hash passende Daten zu finden, die auf diesen abbilden, da dies im Widerspruch zur Einwegcharakteristik kryptografischer Hashfunktionen stünde. Tatsächlich ist eine solche Berechnung sehr wohl möglich, allerdings ist der damit verbundene Rechenaufwand je nach Hashfunktion so hoch, dass dies de-facto unmöglich ist. Weitere Details zu Hashfunktionen sind Abschnitt A.1 zu entnehmen. Wenn eine Hashfunktion entsprechend aufgebaut ist, führen (wie in Abschnitt A.1 beschrieben) bereits kleinste Änderungen in den Eingangsdaten zu weitreichenden Änderungen im resultierenden Hash. Dadurch werden auch Ähnlichkeiten in den Eingangsdaten im resultierenden Hash verschleiert. Die Integrität der Blockchain basiert auf den eben skizzierten Eigenschaften von Hashfunktionen. Details hierzu werden in diesem Abschnitt erläutert. Zu Beginn soll jedoch die Struktur eines Blocks und die Verkettung von Blöcken zu einer Blockchain illustriert werden.

Ein Block besteht abgesehen von Transaktionsdaten (inklusive Coinbase-Transaktion) auch noch aus dem Hash des vorhergehenden Blocks und einem weiteren Feld – in diesem Zusammenhang als *Nonce* bezeichnet – dessen Wert frei wählbar ist. Folglich basiert der Hash eines Blocks (durch den Einbezug des Hashs des Vorgängerblocks) auf allen vorherigen Blöcken. Eine Änderung in einem Block resultiert in einer Änderung des Hashwertes dieses Blocks. Da ein Hash nicht vorherberechnet werden kann, ist auch nicht vorhersehbar, wie sich Änderungen auf den Hash eines Blocks auswirken. Da jedoch der Hash des Vorgängerblocks auch Teil eines jeden Blocks ist, wirken sich Änderungen eines Blocks über die daraus folgende Änderung im Hash dieses Blocks auch auf alle nachfolgenden Blöcke aus. Folglich können einmal verkettete Blöcke dadurch auch nicht neu arrangiert werden. Daraus ergibt sich eine eindeutige Blocksequenz, wie in Abbildung 3 dargestellt.

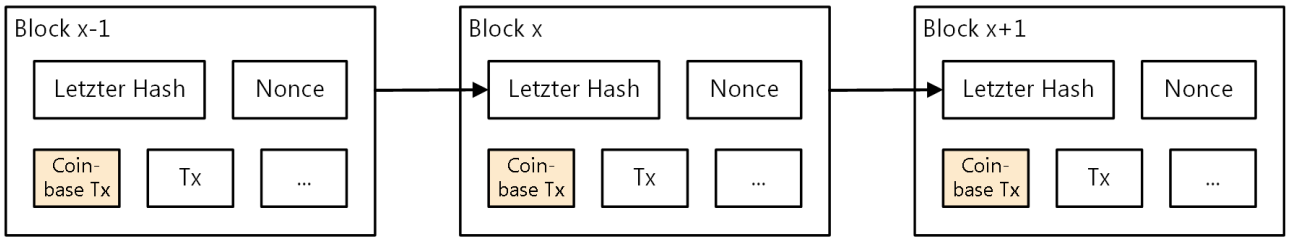

Abbildung 3: Blockchain - Kette bestehend aus mehreren Blöcken

Ein neu erstellter Block ist gültig, wenn er auf einen Hash mit vorgegebenem Präfix abbildet und alle enthaltenen Transaktionen gültig sind. Um dieses Ziel zu erreichen werden die in einen Block aufzunehmenden (gültigen) Transaktionsdaten gesammelt, ein Wert für den Nonce gewählt und der Hash des Blocks berechnet. Wenn der resultierende Hash nicht über das vorgegebene Präfix verfügt, wird der Wert des Nonce geändert und die Berechnung wiederholt. Der Wert des Nonce wird so oft geändert, bis der resultierende Hash mit dem gewünschten Präfix beginnt. Da ein Hash nicht vorhersehbar ist, führen oft erst mehrere Trillionen oder Trillarden Versuche zum Erfolg[9]. Dieses eben beschriebene Konzept wird als *Proof of Work* bezeichnet. Derjenige Miner, welcher einen gültigen Block erstellt hat, beweist durch den Hash des Blocks, dass er ein gewisses Maß an Arbeit verrichtet hat. Der Beweis liegt im Aufwand begründet, welcher aufgebracht werden muss, um einen Block zu erstellen, dessen Hash mit dem gewünschten Präfix beginnt. Genau darin besteht die Überwindung der Einwegcharakteristik der verwendeten Hashfunktion. Andere Teilnehmer des Netzwerks können die Gültigkeit eines neuen Blocks leicht verifizieren, indem sie den Hash des Blocks berechnen und überprüfen, ob dieser tatsächlich mit dem vorgegebenen Präfix beginnt. Der

[9] Mitte September 2016 liegt die Hash-Rate des gesamten Netzwerkes bei ca. 1,7 Trillionen Hashes/s. Quelle: [37]

Aufwand hierfür ist gering und kann daher von jedem Teilnehmer individuell aufgebracht werden. Somit wird keine vertrauenswürdige Instanz benötigt, welche die Integrität und Validität eines Blocks und der im Block gesammelten Transaktionsdaten garantiert. Folglich erübrigt sich die Notwendigkeit einer zentralen Instanz. Gültige Daten sprechen sozusagen für sich selbst und sind inhärent integer und valide. Zusammengefasst arbeiten alle Teilnehmer unabhängig voneinander auf ein gemeinsames Ziel hin, ohne einander vertrauen zu müssen.

Durch die verteilte Struktur von Kryptowährungsnetzwerken und die dezentrale Erzeugung und unabhängige Validierung von Blöcken ergibt sich automatisch auch ein Schutz gegenüber Zensurmaßnahmen. Da Miner unabhängig voneinander Blöcke erstellen, ist es nicht möglich, einzelne Transaktionen zu zensieren bzw. deren Aufnahme in die Blockchain zu verhindern. Selbst wenn tausende Miner daran gehindert werden könnten, eine Transaktion in einen Block aufzunehmen, gibt es immer noch zehntausende andere Miner, welche nicht behindert wurden und weiterhin Blöcke erstellen. Folglich wird eine ordnungsgemäß erstellte Transaktion, welche auch Transaktionsgebühren abwirft, früher oder später in einen Block aufgenommen werden. Nachdem keine zentrale Instanz existiert und jeder Teilnehmer die Gültigkeit von Blöcken überprüfen kann, verbreiten sich auch dann noch alle Informationen erfolgreich im Netzwerk, wenn Teile davon ausfallen, oder bewusst gestört werden. Es müsste also das gesamte Netzwerk einer Kryptowährung vom Netz genommen werden, um die Verarbeitung von Transaktionen effektiv verhindern zu können.

Eine besondere Stärke der Blockchain ist auch die Unveränderbarkeit einmal in der Vergangenheit validierter Daten als direkte Konsequenz aus der Unumkehrbarkeit der verwendeten Hashfunktion. Der Aufwand einen manipulierten Block mit dem Hash eines bereits gültigen Blocks zu erzeugen ist um ein Vielfaches höher als einen Hash mit einem bestimmten Präfix zu erzeugen. Da nur Teile des Hashs (das Präfix) eines gültigen Blocks im Zuge dessen Erstellung festgelegt sind, ist hierfür auch weit weniger Rechenleistung notwendig, als man aufbringen müsste um einen Block zu erzeugen, dessen vollständiger Hash im Vorhinein fixiert ist. Genau das wäre jedoch nötig um einen Block in eine bestehende Blockchain einzufügen oder einen bestehenden zu modifizieren. Schließlich wirken sich Änderungen eines Blocks über dessen Hash auch auf alle nachfolgenden Blöcke aus. Ein viel effizienterer Angriffsweg wäre, einen Block mit korrektem Präfix zu generieren und alle darauffolgenden Blöcke ebenfalls neu zu erstellen um auf diese Weise nachträglich Transaktionsdaten zu manipulieren. Allerdings ist selbst hierfür der Aufwand dermaßen hoch, dass auch Manipulationen dieser Art praktisch ausgeschlossen werden können.
An der Spitze der Blockchain sind zumindest Mehrdeutigkeiten denkbar: Es kann theoretisch vorkommen, dass zwei Blöcke mit einem gültigen Präfix erstellt werden, welche unterschiedliche Transaktionsdaten enthalten. Nachdem es noch keine Nachfolgeblöcke gibt, deren Hash auf einem dieser Blöcke aufbaut, ist es in diesem Fall nicht notwendig, dass zwei Blöcke den exakt gleichen Hashwert haben, um gültig zu sein. Lediglich das Präfix muss deckungsgleich sein. Allerdings ergibt sich aus der verketteten Struktur direkt ein Abwehrmechanismus, der Mehrdeutigkeiten und Widersprüche verhindert: Nachfolgende Blöcke können nur auf einem der möglichen Blöcke basieren. Wenn tatsächlich der Fall eintritt, dass es mehrere Spitzen einer Blockchain gibt, wird ein deterministisches Verfahren angewandt um zu entscheiden auf welchem Block zukünftige Berechnungen basieren. Konkret wird der Block ausgewählt, dessen Hash als Zahl interpretiert dem kleinsten Wert entspricht. Allerdings besteht durch die dezentrale Struktur der Blockchain die Möglichkeit, dass sich Informationen nicht gleichmäßig innerhalb des Netzwerks verbreiten. Dadurch kann es vorkommen, dass einem Teil des Netzwerks die Existenz einer von mehreren Spitzen vorenthalten wird. Folglich kann es zu Gabelungen (sogenannten *Forks*) in der Blockchain kommen. Dies hat zur Folge, dass die Blockchain an verschiedenen Stellen im Netzwerk auf unterschiedlichen Spitzen fortgeführt wird. Das erwähnte deterministische Auswahlverfahren, auf dessen Basis Mehrdeutigkeiten eliminiert werden, bezieht jedoch nicht nur den aktuellen Block, sondern auch alle vorhergehenden Blöcke ein. Sollte tatsächlich der Fall eintreten, dass sich ausgehend von einer Gabelung mehrere Zweige der Blockchain weiterentwickeln, kann auch dieses Problem gelöst werden. Als gültig wird immer die Kette erachtet, die zusammen den größten Proof-of-Work aufweist. Vereinfacht ausgedrückt ist das jene Kette, welche sich aus Blöcken zusammensetzt, deren als Zahl interpretierte Hashwerte in Summe am kleinsten sind. Blöcke in anderen Zweigen verlieren nach kurzer Zeit ihre Bedeutung, sobald alle Teilnehmer um alle Ketten Bescheid wissen. Da auch die

Selektion einer gültigen Kette von allen Teilnehmern individuell durchgeführt wird, reicht schlichtweg das Wissen um alle Ketten aus, um dieselbe Kette als gültig zu erachten wie alle andern Teilnehmer, denen diese Kette bekannt ist. Die in ungültigen Ketten enthaltenen Transaktionen werden ebenfalls als ungültig betrachtet.

So lange nicht ein Miner über mehr als 51% der Rechenleistung des gesamten Netzwerks verfügt, ist davon auszugehen, dass Blöcke die mehr als drei Generationen in der Vergangenheit liegen, „in Stein gemeißelt“ sind. Je mehr Rechenleistung ein Miner aufbringen kann, umso schneller kann dieser auch neue, gültige Blöcke erstellen, da in kürzerer Zeit mehr Versuche unternommen werden können, einen gültigen Block zu erstellen. Die Problematik bei einer 51%-Ungleichverteilung besteht darin, dass ein so mächtiger Miner über genug Rechenleistung verfügt, um schneller neue Blöcke erzeugen zu können, als alle restlichen Miner zusammen. Ein Angriffsszenario könnte wie folgt aussehen:

1. Ein übermächtiger Miner gibt Währungseinheiten für Waren oder Konsumgüter aus, indem er eine Transaktion in Auftrag gibt.
2. Diese wird von einem beliebigen anderen Miner in einen neuen Block aufgenommen und somit vom gesamten Netzwerk als gültig betrachtet.
3. Der übermächtige Miner wird vom Händler die Waren (oder das Konsumgut) erhalten, da die Transaktion nachweislich gültig ist.
4. Der Miner erstellt einen Block, der auf demselben Vorgängerblock aufbaut wie der eben erstellte, gültige Block, nimmt jedoch die zuvor getätigte Transaktion nicht in diesen auf. Stattdessen erstellt und nimmt er eine neue Transaktion auf, die dieselben UTXO an eine seiner Adressen transferiert.
5. Da der Miner schneller neue Blöcke erstellen kann, als alle anderen Miner zusammen, wird er auch schneller weitere Blöcke erstellen, können, welche auf dem neuen Block ohne der ursprünglichen Transaktion aufbauen.
6. Die Folge daraus ist, dass die gezielt erstellten Blöcke einen höheren Proof-of-Work aufweisen, als jene Kette, welche die ursprüngliche Transaktion des Miners enthält.
7. Da der Proof-of-Work der gezielt erzeugten Kette am größten ist, wird diese Kette vom gesamten Netzwerk als gültig anerkannt.
8. Der Miner kann somit nachträglich bereits ausgegebene Währungseinheiten zurückgewinnen, indem er die betreffenden Transaktionen über den eben beschriebenen Weg an sich selbst überweist. Dadurch verliert die zuvor ausgestellte, an sich gültige Transaktion ihre Gültigkeit, da es sich um *double spending* handeln würde.

Wenn sich die mit der ursprünglichen Transaktion bezahlten Waren bereits am Transportweg befinden, oder es sich um Verbrauchsgut handelt, welches schon konsumiert wurde, wird der Händler um die Bezahlung geprellt.

Eine derart grobe Ungleichverteilung der Rechenleistung wird jedoch durch die Belohnung in Form von frischem Kapital und Transaktionsgebühren für erfolgreiches Mining verhindert, da hierdurch ein lebendiger Wettbewerb aufrechterhalten wird. Durch die Aussicht auf Profit werden neue Miner angelockt und bestehende Miner dazu veranlasst, einen Teil ihrer Einnahmen in bessere Hardware mit erhöhter Rechenleistung zu investieren, um ihre eigenen Erfolgschancen zu erhöhen. Auch wenn es immer wieder Verschiebungen der verfügbaren Rechenleistung innerhalb des Netzwerks gibt, sind besorgniserregende Ungleichverteilungen und daraus resultierende Betrugsfälle ausgeblieben. Wenn die Gesamtrechenleistung des Netzwerks jedoch nicht ausreicht, um zu verhindern, dass einzelne Teilnehmer (oder neu hinzustoßende Teilnehmer) über mehr als 51% der Gesamtrechenleistung verfügen, kann dies den Untergang einer blockchainbasierten Kryptowährung bedeuten. Ein solcher Niedergang einer Kryptowährung ist unter [23] näher ausgeführt. Auf Grund der beschriebenen Sicherheitsvoraussetzungen blockchainbasierter Kryptowährungen können die Sicherheitskonzepte des Blockchain-Designs nicht direkt auf kleinere (möglicherweise geschlossene) Systeme angewendet werden.

Die Eigenschaften des Blockchain-Designs machen die Technologie jedoch ungeachtet dessen auch außerhalb von Kryptowährungen attraktiv. Auf Grund der Konzeption als zentrale Datenbank innerhalb eines vollständig dezentralisierten Systems bietet sich eine Anwendung als Datenbank in verteilten Systemen auch abseits von Kryptowährungen an. Besonders private Blockchains, welche im Gegensatz zu Kryptowährungssystemen abgeschottet von der Öffentlichkeit betrieben werden können, bieten potentiell neue Möglichkeiten. Das Prinzip der im folgenden Kapitel ebenfalls beschriebenen partiellen Transaktionen sowie Multi-Signatur-Transaktionen sind auch auf Szenarien abseits von Kryptowährungen anwendbar.

4. Anwendungsmöglichkeiten der Blockchain-Technologie

Auch abseits von Kryptowährungen bietet die Blockchain-Technologie viele Anwendungsmöglichkeiten. Beispiele dafür sind *Colored Coins* [24], *Smart Property* [25], *Namecoin* [26] und *Smart Contracts*. Einige dieser Konzepte sind jedoch nach wie vor eher als Experiment zu betrachten, jedoch unterstreichen sie die vielseitigen Anwendungsmöglichkeiten der Blockchain-Technologie. *Colored Coins* haben beispielsweise das Ziel reale Vermögenswerte wie Währungen oder andere Finanzinstrumente in der Bitcoin-Blockchain abzubilden und zu verwalten. Unter *Smart Property* versteht man Eigentum, welches über die Bitcoin-Blockchain mittels Verträgen kontrolliert wird. *Namecoin* hat als Ziel ein dezentralisiertes Open Source Informationsregistrierungs- und Transfersystem. Mittels Namecoin wurde beispielsweise ein zensurbeständiges, verteiltes, alternatives Domain Name System (DNS) umgesetzt. Dies veranschaulicht, dass die Blockchain-Technologie auch als Stütze kritischer Infrastruktur eingesetzt werden kann. *Smart Contracts* haben das Ziel, digitale Güter mittels Programmcode, welcher beliebige Regeln umsetzt, zu kontrollieren. Neben diesen Anwendungsbeispielen kann die Blockchain auch als Datenbanksystem oder als private Blockchain für den internen Betrieb genutzt werden. In jedem Fall handelt es sich um Blockchain-Implementierungen, welche sich von der Bitcoin-Blockchain unterscheiden und auch entsprechend angepasste Endbenutzersoftware verwenden. Beispielsweise werde andere kryptografische Funktionen eingesetzt um die Integrität der Daten zu garantieren. Unabhängig davon werden Blockchainanwendungen, welche nicht auf Kryptowährungen und Transaktionen abzielen, auch andere Informationen in der Blockchain protokollieren. Folglich ist der Ausdruck „Wallet“ für zugehörige Endbenutzersoftware nicht mehr zutreffend, da diese andere Aufgaben erfüllt. Im Rahmen dieses Abschnitts wird auf einige der eben beschriebenen Anwendungsmöglichkeiten der Blockchain-Technologie abseits von Kryptowährungen näher eingegangen.

4.1. Private Blockchain

Anders als in öffentlichen Systemen wie Kryptowährungen, ist ein Proof-of-Work innerhalb privater Netzwerke nicht notwendigerweise im selben Ausmaß notwendig, um die Integrität der in einer Blockchain gespeicherten Daten zu garantieren. Schließlich können Zugangskontrollen sicherstellen, dass nur ausgewählte Teilnehmer einem geschlossenen System beitreten können. Denkbar sind Szenarien mit definierten, vertrauenswürdigen Minern. Dadurch würde es sich zwar nicht mehr um voneinander unabhängige Miner handeln, der dezentrale Charakter, aber auch die Unveränderbarkeit aller in der Blockchain gespeicherten Daten blieben bestehen. Durch die gezielte Wahl des Aufwandes, welcher für die Erstellung neuer Blöcke benötigt wird, ließen sich neue Blöcke in nahezu beliebig kurzen oder langen Intervallen generieren. Die Frage nach der Sicherheit bzw. Integrität der in die Blockchain aufgenommen Daten ist in solchen Fällen im Gegensatz zu einer öffentlichen Blockchain von weit weniger technischer Natur. Wenn Miner nicht unabhängig voneinander operieren, lassen sich auch bestehende Sicherheitsmodelle für blockchainbasierte Kryptowährungen nicht auf diese Art privater Netzwerke anwenden. Dies ist jedoch in solchen Fällen auch nicht notwendig. Vielmehr würden rechtlich bindende Garantien teilweise an die Stelle mathematischer Beweise treten. Zusammenfassend können derartige Ansätze als hybride Blockchain-Systeme mit zentralen Zugangsregeln und (je nach Bedarf) leichter zu berechnenden Hashes charakterisiert werden.

Eine weitere (wenn auch sehr abstrakte) Möglichkeit ergibt sich durch die Schaffung eines Anreizsystems, welches im Rahmen einer privaten Blockchain auf die Ausschüttung von frischem Kapital verzichten kann. In solchen Fällen ist eine gezielte Auswahl vertrauenswürdiger Miner nicht

notwendig. Wenn die Aufrechterhaltung des fehlerfreien Betriebs eines geschlossenen Systems Anreiz genug für alle Beteiligten ist, sich korrekt bzw. ehrlich zu verhalten, kann eine funktionierende private Blockchain ohne die Koppelung an irgendeine Form von Kapital aufrechterhalten werden. Das Blockchain-Modell lässt sich jedoch auch allgemeiner als generisches verteiltes Datenbanksystem an Stelle traditioneller (relationaler) Datenbanken einsetzen.

4.2. Blockchain als verteiltes Datenbanksystem

Das Blockchain-Design ist nicht auf die Nutzung als Transaktionsregister festgelegt. Daher sind beliebige Anwendungsfälle denkbar, in denen bisher auf traditionelle Datenbanksysteme gesetzt wurde. Traditionelle Zahlungssysteme (sowohl global gesehen als auch das dem Durchschnittsverbraucher bekannte Endkundengeschäft) sind vom technischen Standpunkt aus betrachtet verteilte, heterogene Datenbanksysteme: Kassenterminals, Bankomaten, und viele weitere Systeme arbeiten auf Datensätzen, welche mit unterschiedlichen Datenbanken abgeglichen werden müssen. Hierbei ist es besonders wichtig, dass Transaktionen entweder ganz oder gar nicht durchgeführt werden. Alle abgefragten Daten müssen auch konsistent sein. Dabei ist es wichtig, dass Daten wie z.B. Kontostand immer und überall möglichst aktuell abrufbar sind. Im Idealfall sollte es auch zu möglichst keinen Verzögerungen kommen und Änderungen des Kontostandes daher auch überall sofort korrekt widergegeben. Dabei handelt es sich offenkundig um ein komplexes Gesamtsystem mit vielen internen Abhängigkeiten. Die hierarchische Struktur der aktuellen Bankensystems trägt zusätzlich zu dieser Komplexität bei. Blockchainbasierte Systeme arbeiten global auf einer einzigen Ebene. Durch den Wegfall aller Hierarchien lassen sich viele Abläufe vereinfachen. Das Abgleichen miteinander verknüpfter Datenbanken würde beispielsweise völlig wegfallen. Besonders unter Einbezug der im Finanzbereich verarbeiteten (Transaktions-)Daten kommen die Stärken des Blockchain-Designs als verteilte Datenbank, welche zu jedem Zeitpunkt konsistente Daten liefen muss, zum Tragen [27]. Wenn die Gültigkeit von in einer Blockchain zu speichernden Datensätzen mittels automatisiert auswertbarer Regeln sichergestellt werden kann, zeigt sich ein Alleinstellungsmerkmal der Blockchain: Da alle Teilnehmer die von ihnen verarbeiteten Datensätze individuell und automatisiert unabhängig voneinander prüfen, können beliebig viele Teilnehmer gleichzeitig auf Datensätzen arbeiten, ohne dass diese sich untereinander abstimmen müssen [28].

Ein anschauliches Beispiel hierfür liefern Kryptowährungen wie Bitcoin: Nachdem jede UTXO als Input nur einer nachfolgenden Transaktion verwendet werden kann, und Transaktionen von jedem einzelnen Teilnehmer unabhängig validiert werden, propagieren ungültige Transaktionen nicht durch das Netzwerk. Weiters werden sie auch nicht in neue Blöcke aufgenommen, da Miner nur von gültigen Transaktionen durch Transaktionsgebühren profitieren. Wenn der Fall eintritt, dass eine UTXO für mehrere Transaktionen verwendet wird, wird daher garantiert nur einer dieser Transaktionen in einen neuen Block aufgenommen. Andere Transaktionen, welche diese UTXO als Input referenzieren werden dadurch nachweislich ungültig. Transaktionen stellen somit atomare Operationen auf einer verteilten Datenbank dar. Zusammengefasst lassen sich mit Hilfe der Blockchain-Technologie beliebige Delivery-Versus-Payment-Systeme umsetzen (wobei im Falle privater Blockchains eben ein angepasstes Anreizsystem für Miner zum Einsatz kommen muss).

4.3. Multi-Signatur-Transaktionen

Bedingt durch die Freiheiten bezüglich Freigabebedingungen von Transaktionen ergeben sich auch Möglichkeiten etablierte Geschäftspraktiken direkt innerhalb blockchainbasierter Systeme abzubilden. Das Szenario eines Firmenkontos mit mehreren Zeichnungsberechtigten wird beispielsweise direkt von Bitcoin unterstützt, lässt sich jedoch auch entkoppelt von Kryptowährungen unverändert umsetzen: Abgesehen von „regulären“ Adressen, die dem öffentlichen Teil eines public/private key pair entsprechen, können auch Adressen generiert werden, welche an mehrere private Schlüssel gebunden sind. Einerseits ergibt sich damit die Möglichkeit, dass mehrere Personen (jede mittels ihres eigenen privaten Schlüssels) Transaktionen ausgehend von einer geteilten Adresse autorisieren. Andererseits lässt sich mit derartigen Adressen auch erwirken, dass eine Transaktion von mehreren Personen (mehreren privaten Schlüsseln) autorisiert werden muss. Die verwendete Applikation muss diese Adressen unterstützen. Im Fall von Bitcoin wurde diese Funktionalität erst Nachträglich eingeführt, weshalb nur aktuelle Wallets mit entsprechenden Adressen umgehen können [29]. Die genaue Konfiguration einer solchen geteilten Adresse wird bei

deren Erstellung festgelegt und kann nachträglich nicht verändert werden. Dabei kommen keine speziellen kryptografischen Verfahren zum Einsatz, sondern die Adresse hat ein im Protokoll definiertes Format, welches mehrere öffentliche Schlüssel enthält.

Abgesehen vom letztbeschriebenen Fall ergibt sich auch auf eine weitere Art ein zusätzliches Maß an Sicherheit. Sollte ein privater Schlüssel verloren gehen, können weiterhin Transaktionen in Auftrag gegeben werden, so lange es noch genügend weitere Schlüssel gibt, welche ausgehende Zahlungen autorisieren können. Die Blockchain-Technologie erlaubt durch noch flexibler gestaltbare Freigabebedingungen jedoch weitere Szenarien losgelöst von Kryptowährungen ausgehend von partiellen Transaktionen bis hin zu sogenannten *Smart Contracts*, wie sie in den folgenden Abschnitten beschrieben sind.

4.4. Partielle Transaktionen

Das Konzept der *partiellen Transaktionen* erlaubt es Transaktionen zu definieren, welche im Gegensatz zu fix vorgebebenem Input und Output (und somit auch fix vorgegebenen Sender- und Empfängeradressen) eine Seite offen lassen. Angenommen eine Partei verfügt über einen gewissen Betrag in Euro und möchte diesen in britische Pfund wechseln. Augenscheinlich spielt es (im einfachsten Fall) keine Rolle, wer im Besitz der gewünschten Menge an Devisen ist. Führt man diesen Ansatz weiter, ist es auch irrelevant, wie viele Parteien in einen derartigen Handel involviert sind. Im ersten Schritt definiert eine Partei eine partielle Transaktion, welche nicht ausgeglichen ist. Es wird lediglich ein Angebot veröffentlicht eine bestimme Menge Devisen zu veräußern. Sobald sich ein Käufer findet, welcher bereit ist den vorgeschlagenen Preis zu bezahlen wird die Transaktion abgewickelt. Ab diesem Zeitpunkt ist es irrelevant wer dieser Käufer ist, oder wie viele Käufer gemeinsam den vorgeschlagenen Kaufpreis aufbringen.

Partei	Output	Input
A	€ 10,00	£7,88

Unausgeglichene partielle Transaktion

Partei	Output	Input
A	€ 10,00	£ 7,88
B	£ 7,88	€ 10,00

Ausgeglichene Zwei-Parteien-Transaktion

Partei	Output	Input
A	€ 10,00	£ 7,88
B	£ 1,80	€ 2,28
C	£ 6,08	€ 7,72

Ausgeglichene Drei-Parteien-Transaktion

Tabelle 2: Partielle Transaktionen

Das Prinzip des eben beschriebenen Beispiels lässt sich auf Börsen aller Art umlegen und somit beispielsweise auch auf den Aktienmarkt anwenden. Angebote können von beliebig vielen Parteien unabhängig voneinander bedient werden und werden vom System (von den Clients unabhängig voneinander) automatisiert abgewickelt, sobald die im System definierten Bedingungen erfüllt sind. Die naheliegendste Bedingung wäre auch hier, dass Input und Output einer Transaktion ausgeglichen sein müssen. Der in Abschnitt 4.7 beschriebene verteilte Handelsplatz *Ripple* ist ein Beispiel für die Umsetzung des eben beschriebenen Konzepts und enthält weitere Details, bezogen auf eine konkrete Umsetzung dieses Konzepts.
In Prinzip lassen sich jedoch beliebig komplexe Bedingungen definieren, welche beispielsweise Regelungen betreffend Transaktionsgebühren beinhalten. Blockchainbasierte Systeme erlauben jedoch weitaus vielfältigere, allgemeinere Anwendungen, welche als *Smart Contracts* bezeichnet werden. Diese sind im folgenden Abschnitt näher beschreiben.

4.5. Smart Contracts

Unter einem Smart Contract versteht man ein Stück Code, welches digitale Güter basierend auf Regeln kontrolliert. Im Rahmen von Bitcoin wurde die Skriptsprache *Script* entwickelt, welche benutzt werden kann um Smart Contracts im Rahmen des Bitcoin-Systems zu programmieren [30]. Multi-Signatur-Transaktionen können als Beispiel für einen Smart Contract gesehen werden; Smart Contracts werden sozusagen als Teil von Transaktionen (z.B. deren Freigabebedingungen) in der Blockchain gespeichert. Es wird hier „Contract“ als ein Computerprogramm verstanden, das die technische Umsetzung von sonst in Verträgen üblichen Phasen wie Verhandlung und Umsetzung unterstützt. Es können hier Elemente des Rechtemanagements, die Bindung an Bedingungen oder Auktionen über die kryptografischen Methoden der Blockchain gesichert werden.

Script wurde bewusst einfach gehalten, wodurch sich einige Vorteile aber auch Nachteile ergeben. Durch die Beschränkung der Sprache lassen sich nicht alle Operationen abbilden. Beispielsweise lassen sich keine Schleifen formulieren. Wenn nun eine Operation wiederholt ausgeführt werden soll, muss diese explizit mehrfach ausformuliert werden. Eine Konsequenz davon ist, dass die Anzahl der Wiederholungen fest vorgegeben ist, und nicht von anderen Bedingungen abhängig gemacht werden kann. Infolgedessen lassen sich nicht beliebige Abläufe in Script definieren, selbst wenn diese sehr einfach formalisierbar sind. Zusätzlich gibt es noch weitere Einschränkungen im Vergleich zu universell einsetzbaren Programmiersprachen. Diese gezielte Begrenzung der Möglichkeiten hat unter anderem den Vorteil, dass es zu keinen Endlosschleifen kommen kann. Andererseits lassen sich einige Probleme dadurch nicht oder nur sehr ineffizient abbilden. Script hat auch keinen internen Zustand, wodurch nur Ja/Nein-Verträge abgebildet werden können, aber keine komplexeren Verträge. Zudem kann mittels Script nicht auf alle Daten in der Blockchain zugegriffen werden. Beispielsweise kann der Nonce und der Hash des vorherigen Blocks nicht ausgelesen werden. Einige Applikation, wie zum Beispiel Glückspiele oder andere Anwendungen, welche eine Quelle von Zufallszahlen benötigen sind dadurch nicht umsetzbar, obwohl durch die Unvorhersehbarkeit des Hashwerts eines Blocks eine qualitativ hochwertige Quelle von Zufallszahlen eigentlich greifbar wäre. Das im folgenden Abschnitt beschriebene System Ethereum wurde entwickelt, um die Einschränkungen der Bitcoin-Blockchain und Script aufzuheben.

4.6. Ethereum

Ethereum [31] [32] wurde mit dem Ziel entwickelt, eine Blockchain mit vollwertiger Programmiersprache bereitzustellen. Mittels dieser Programmiersprache können programmierbare, intelligente Verträge, sogenannte *Smart Contracts*, erstellt werden. Bei diesen Verträgen handelt es sich um Apps, die von der Ethereum Plattform ausgeführt werden. Durch den dezentralisierten Ansatz von Ethereum können Ausfälle, Zensur und Betrug verhindert werden.
Ethereum unterscheidet zwischen zwei Arten von Konten. Die erste Art sind sogenannte extern kontrollierte Konten. Diese Konten werden durch private Schlüssel von außerhalb der Blockchain kontrolliert, ähnlich wie bei Bitcoin. Die zweite Art sind Vertragskonten, die durch den Vertragscode kontrolliert werden. Genauso wie normale Konten können auch Vertragskonten über ein Guthaben verfügen. Ein Teil dieses Guthabens wird als Entschädigung für die benötigten Ressourcen während der Ausführung bezahlt. Das Guthaben kann aber auch an andere Konten übertragen werden. Im Ethereum-System hat dieses Guthaben die Bezeichnung *Ether*.
Die von Ethereum verwendete Blockchain gleicht in vielen Aspekten der Blockchain von Bitcoin. Der Hauptunterschied zwischen den beiden Systemen ist, dass die Blockchain von Ethereum neben der Transaktionsliste auch den Zustand der Transaktionen enthält. Dadurch muss nicht von allen Nutzern die gesamte Blockchain gespeichert werden, um über den Zustand von Transaktionen Bescheid zu wissen; der letzte Block reicht aus. Ermöglicht wird dies dadurch, dass jeder Block nicht nur den Zustand der Transaktionen beinhaltet, welche in diesen Block aufgenommen wurden, sondern den Zustand aller Transaktionen. Im Weiteren werden die Fähigkeiten von Ethereum anhand von drei Beispielen demonstriert.
Das erste Beispiel ist ein Hedgegeschäft, bei dem mittels Smart Contract von den Kursschwankungen zwischen Ether und Dollar profitiert werden soll. Für solche Geschäfte wird ein „Datenkanal“-Vertrag benötigt, der von einer vertrauenswürdigen Instanz verwaltet wird. Im folgenden Beispiel könnte NASDAQ diese Rolle übernehmen. Ein solches Geschäft könnte wie folgt ablaufen:

1. Alice zahlt 1000 Ether ein.
2. Bob zahlt 1000 Ether ein.
3. Der Gegenwert von 1000 Ether in USD wird durch Abfrage des Datenkanals ermittelt und gespeichert. In diesem Beispiel handelt sich um *x* USD.
4. Nach 30 Tagen bekommt Alice den Gegenwert von *x* USD in Ether ausbezahlt. Der Gegenwert wird wieder über denselben Datenkanal ermittelt. Bob bekommt den Rest.

In diesem Beispiel würde Alice von einem fallenden Dollar-Kurs profitieren.

Als zweites Beispiel dient ein Konto. Angenommen Alice möchte ihr Guthaben sicher aufbewahren, ist aber besorgt, dass sie ihren privaten Schlüssel verlieren könnte oder, dass jemand in ihren

Computer einbricht und den Schlüssel stiehlt bzw. kopiert. Daher wendet sie sich an Bobs Bank. Alice vertraut Bob aber nicht hundertprozentig und will den durch Bob verursachbaren Schaden minimieren. Dazu kann sie folgenden Vertrag mit Bob aufsetzen:

1. Alice alleine darf maximal 10% ihres Guthabens pro Tag beheben.
2. Bob alleine darf maximal 5% ihres Guthabens pro Tag beheben, Alice kann dieses Recht jederzeit mit ihrem privaten Schlüssel annullieren.
3. Alice und Bob zusammen können beliebig viel Guthaben beheben.

Dieser Vertrag deckt alle Wünsche von Alice ab. Sie kann 10% ihres Guthabens pro Tag abheben und sollte sie einmal mehr benötigen, muss sie sich lediglich mit Bob abstimmen. Wenn in Ihren Computer eingebrochen wird, kann sie mit Bob zusammen ihr Guthaben auf ein neues Konto transferieren. Verliert Alice ihren Schlüssel, kann Bob ihr das Geld langfristig ausbezahlen. Sollte sich Bob als nicht vertrauenswürdig herausstellen und unberechtigterweise Guthaben abheben, kann Alice seinen Zugriff sperren, solange sie noch im Besitz ihres privaten Schlüssels ist. Der maximal mögliche Verlust beträgt mit Hilfe dieses Vertrags maximal 5% des Guthabens pro Tag.

Als drittes Beispiel dient ein Firmenkonto mit mehreren Zeichnungsberechtigten. Im Gegensatz zu Bitcoin, wo nur definiert werden kann, dass *x* aus *y* Schlüsseln benötigt werden um eine Transaktion zu autorisieren, unterstützt Ethereum eine feinere Granularität. Es kann beispielsweise definiert werden, dass fünf aus den sechs Schlüsseln zusammen das gesamte Guthaben transferieren dürfen. Vier von sechs können gemeinsam maximal 50% des Guthabens ausgeben und zwei aus sechs können zusammen nur maximal 5% ausgeben. In Ethereum sind derartige Multi-Signaturen asynchron umgesetzt. Dass bedeutet, dass die Teilnehmer ihre Signaturen der Reihe nach erstellen. Die Transaktion wird schließlich von der letzten Signatur ausgelöst.

4.7. Ripple

Ripple [33] ist ein Zahlungsnetzwerk, dessen Entwickler das Ziel verfolgen, einen vollständig dezentralisierten Handelsplatz und Devisenmarkt sowie ein Zahlungssystem basierend auf der Blockchain-Technologie aufzubauen. Handelstreibende Parteien müssen einander im Rahmen von Ripple nicht direkt vertrauen.
Die Ripple-Blockchain wird (ähnlich der Bitcoin-Blockchain) als zentrales Register eingesetzt, welches über alle Kontostände im System Buch führt, sowie auch eine Historie aller Transaktionen enthält. Zusätzlich werden auch Kauf- und Verkaufsangebote von Devisen festgehalten. Da das Ripple-Netzwerk auf denselben Prinzipien wie Bitcoin basiert, ist auch hier keine zentrale Instanz notwendig, welche den Datenbestand verwaltet und aktuell hält. Da Ripple als verteilter Handelsplatz für Devisen in bestehenden Fiat-Währungen (aber auch Güter aller Art) ausgelegt ist, bildet die Ripple-Blockchain Verbindlichkeiten (so genannte *IOUs*) zwischen Parteien ab. Somit setzt dieses Zahlungsnetzwerk ebenso wie bestehende Banken– und Börsensysteme stark auf Vertrauen zwischen einzelnen Parteien. Verbindlichkeiten werden wie bei klassischen Anleihen oder Krediten nur festgehalten. Deren Erfüllung kann jedoch mit rein technischen Mitteln nicht garantiert werden. In Gegensatz dazu können Kryptowährungen mathematische Beweise bemühen, welche eine Erfüllung von Verbindlichkeiten (so lange diese in Form von Kryptowährungen bestehen) garantieren.
Sogenannte *Ripple-Gateways* bilden ähnlich einer Wechselstube die Verbindung zwischen den im Ripple-Netzwerk gehandelten Verbindlichkeiten und den damit assoziierten Devisen und Gütern. Intern wird hierfür *XRP* als Brückenwährung verwendet: Nutzer treten an Gateways heran und wechseln z.B. einen Betrag in Euro in die entsprechende Menge XRP um, wodurch eine entsprechende Verbindlichkeit in der Ripple-Blockchain festgehalten wird. Diese Verbindlichkeit kann zu einem späteren Zeitpunkt entweder direkt eingelöst werden oder gegen IOUs anderer Währungen getauscht werden. Auf Grund der dezentral organisierten Struktur kann prinzipiell jeder Teilnehmer als informelles Gateway fungieren – sobald ein Teilnehmer Geld von einer anderen Partei annimmt und dafür IOUs ausstellt, kann dieser als Gateway angesehen werden.
Ein Vorteil dieses verteilten System ergibt sich aus dem verwendeten Vertrauensmodell, wodurch ein globaler Handel zwischen Parteien umgesetzt werden kann, welche einander nicht vertrauen: Jeder Nutzer legt fest, welchen anderen Teilnehmern er welches Maß an Vertrauen entgegenbringt. Konkret wird angegeben, welchen anderen Teilnehmern man dahingehend vertraut IOUs bis zu

einer bestimmten Höhe (und in welcher Währung) auf Verlangen einzulösen. Wenn zwei Parteien, die einander nicht kennen (und vertrauen) einen Handel eingehen möchten, kann das System diesen trotzdem automatisiert abwickeln indem Vertrauensketten gebildet werden. Ausgehend von den Handelspartnern werden so lange Vertrauensketten gebildet, bis diese sich an einem Punkt treffen und somit eine zusammenhängende Kette bilden. Innerhalb dieser Kette vertraut jeder Teilnehmer den angrenzenden Teilnehmern in einem der Höhe der Transaktion entsprechenden Maß. Sobald eine solche Kette zu Stande kommt, kann die in Auftrag gegebene Transaktion durchgeführt werden. Abbildung 4 veranschaulicht diesen Vorgang.
Obwohl dieses System einige der Eigenschaften des bestehenden Bankensystems teilt – wenn ein Institut zahlungsunfähig ist, fallen Gläubiger um ihre Verbindlichkeiten um – ergibt sich aus der dezentralen Struktur ein weiterer Vorteil: Da alle Daten dezentralisiert in einer Blockchain verwaltet werden, sind Kontostände vor Manipulationen geschützt, da diese von jedem Teilnehmer individuell (analog zu Bitcoin-Transaktionen) validiert werden. Dadurch können weder handelstreibende Parteien noch Gateways ihre Bücher fälschen. Außerdem zielt Ripple auf eine möglichst tiefgreifende Integration im Bankensektor und Kooperationen mit Geldinstituten ab. Fungiert ein Bankhaus als Ripple-Gateway, ist einerseits von einem hohen Maß an Vertrauen auszugehen, andererseits können Verbindlichkeiten auch umfassender gedeckt werden, wodurch ein zusätzliches Maß an Sicherheit entsteht.

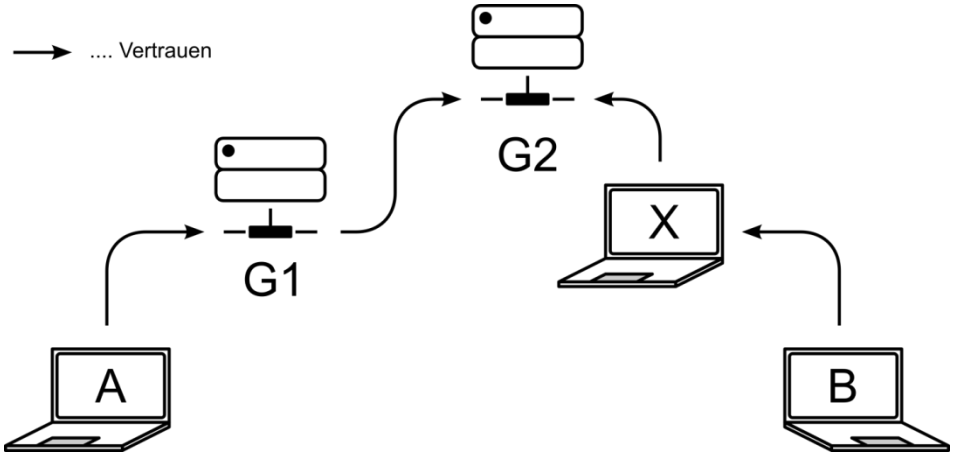

Abbildung 4: Handel ohne direktes Vertrauen:

A und B möchten miteinander handeln, vertrauen einander jedoch nicht.
A vertraut Gateway G1, G1 wiederum vertraut Gateway G2.
B vertraut Nutzer X, welcher ebenfalls Gateway G2 vertraut.
Durch die zustande gekommene durchgehende Vertrauenskette kann der Handel abgewickelt werden.

5. Schlussfolgerungen und Ausblick

Im Rahmen dieser Studie wurden die Grundlagen moderner Kryptowährungen wie Bitcoin mit Schwerpunkt auf die daraus entstandene Blockchain-Technologie betrachtet. Auch wenn Blockchain und Bitcoin ursprünglich im Rahmen von Kryptowährungssystemen als voneinander abhängige Technologien eingesetzt wurden, ist die Blockchain auch abseits von Kryptowährungen einsetzbar.

Das grundlegende Prinzip einer Blockchain als zentrale, sequentielle Datenbank, welche dezentral verwaltet wird, bietet Vorteile gegenüber bestehenden verteilen Datenbanksystemen. Zusätzlich eröffnen sich auch neue Möglichkeiten durch die Tatsache, dass Zahlungssysteme, verteilte Handelsplätze, Devisenmärkte und Ähnliches umsetzbar sind, ohne dass handelstreibende Parteien einander Vertrauen entgegenbringen müssen. Mathematische Beweise treten an die Stelle von Vertrauensbeziehungen und rechtlich bindender Verträge. Im Rahmen von Kryptowährungen, kann dadurch unzweifelhaft garantiert, werden, dass alle Verbindlichkeiten erfüllt werden.

Die Anwendungsmöglichkeiten der Blockchain-Technologie sind jedoch viel weitreichender und nicht auf den Finanzbereich beschränkt. Mittels Smart Contracts lassen sich nahezu beliebige Prozesse abbilden.

Die vielseitigen Möglichkeiten bestehende Prozesse auf die Blockhain-Technologie zu übertragen, kombiniert mit den völlig neuartigen Anwendungen, welche erst durch die besonderen

Eigenschaften der Blockchain umsetzbar sind, und das steigende öffentliche Interesse haben mittlerweile auch Standardisierungskomitees auf den Plan gerufen. Da davon auszugehen ist, dass Blockchain-Anwendungen kontinuierlich an Relevanz gewinnen werden, ist Interoperabilität zwischen unterschiedlichen blockchainbasierten Systemen von zunehmender Wichtigkeit. Aus diesem Grund hat *Standards Australia* die Gründung einer Arbeitsgruppe zum Thema Blockchain bei der *International Organization for Standardization* angestoßen [34].

Ungeachtet des aktuell hohen Maßes an Interesse und der teils hohen Investitionen die von diversen Stellen zur Erforschung und Weiterentwicklung der Blockchain-Technologie getätigt werden, ist festzuhalten, dass es nach wie vor viele offene Fragen gibt. Bisher existieren noch keine vollständigen Modelle oder abgeschlossene Theorien, welche alle Aspekte abdecken und zufriedenstellend aufzeigen wie Blockchain konkret Einsparungen und Entwicklungssprünge im globalen Finanzmarkt oder innerhalb bestehender Zahlungssysteme ermöglichen soll. Viele konkrete Anwendungen können jedoch auch ausgehend vom aktuellen Wissensstand bereits umgesetzt werden. Die potentiellen Vorteile und eventuelle Kostenersparnisse sind jedoch, selbst wenn diese offensichtlich sind, von Fall zu Fall zu bewerten, weshalb keine allgemein gültige Aussage getroffen werden kann.

6. Referenzen

[1] Autonomous Research LLP, „BLOCKCHAIN BACK-OFFICE BLOCK-BUSTER," [Online]. Available: https://autonomous.app.box.com/s/r880n1whjrqrua9ljq9l4b7wd6zqmt67. [Zugriff am 02 05 2016].

[2] V. W. Ross, „Blockchain technology changes the future," 13 11 2014. [Online]. Available: http://www.examiner.com/article/blockchain-technology-changes-the-future. [Zugriff am 02 05 2016].

[3] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System," [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Zugriff am 03 02 2016].

[4] A. M. Antonopoulos, Mastering Bitcoin, O'Reilly, 2014.

[5] C. Bergmann, „Wie viel Strom verbrät das Bitcoin Netzwerk?," 15 Oktober 2014. [Online]. Available: https://bitcoinblog.de/2014/10/15/wie-viel-strom-verbrat-das-bitcoin-netzwerk/. [Zugriff am 20 10 2016].

[6] Allied Control, „Analysis of Large-Scale Bitcoin Mining Operations," 2014. [Online]. Available: http://www.allied-control.com/publications/Analysis_of_Large-Scale_Bitcoin_Mining_Operations.pdf. [Zugriff am 11 10 2016].

[7] K. J. O'Dwyer und D. Malone, „Bitcoin mining and its energy footprint," in *Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET*, Limerick, IET, 2014, pp. 280-285.

[8] C. Malmo, „Bitcoin hat ein großes Problem: Die Krypto-Währung ist einfach nicht nachhaltig," 10 August 2015. [Online]. Available: http://motherboard.vice.com/de/read/das-oeko-problem-von-bitcoin-darum-ist-die-krypto-waehrung-nicht-nachhaltig-3920. [Zugriff am 20 10 2016].

[9] S. Deetman, „Bitcoin Could Consume as Much Electricity as Denmark by 2020," 29 März 2016. [Online]. Available: http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020. [Zugriff am 20 10 2016].

[10] H. McCook, „http://www.coindesk.com/microscope-true-costs-banking/," 12 July 2014. [Online]. Available: http://www.coindesk.com/microscope-true-costs-banking/. [Zugriff am 26 10 2016].

[11] Bitcoin Wiki, „Talk:Scalability," 20 12 2014. [Online]. Available: https://en.bitcoin.it/wiki/Talk:Scalability. [Zugriff am 15 09 2016].

[12] amaclin, „How does the ECDSA verification algorithm work during transaction?," 2014. [Online]. Available: http://bitcoin.stackexchange.com/questions/32305/how-does-the-ecdsa-verification-algorithm-work-during-transaction.

[13] Coinbase, Inc., „Coinbase,“ 2016. [Online]. Available: https://www.coinbase.com. [Zugriff am 20 09 2016].

[14] Bitcoin Deutschland AG, „bitcoin.de Bitcoin-Marktplatz - Made in Germany,“ 2016. [Online]. Available: https://www.bitcoin.de/de. [Zugriff am 20 09 2016].

[15] Bitsquare, „Bitsquare - The decentralized bitcoin exchange,“ 2016. [Online]. Available: https://bitsquare.io/. [Zugriff am 20 09 2016].

[16] BitPay, Inc., „BitPay,“ 2016. [Online]. Available: https://bitpay.com/. [Zugriff am 20 09 2016].

[17] blockchain.info, „Blockchain-Größe,“ 2016. [Online]. Available: https://blockchain.info/de/charts/blocks-size.

[18] Bitcoin Block Reward Halving Countdown, „Bitcoin Block Reward Halving Countdown,“ [Online]. Available: http://www.bitcoinblockhalf.com/. [Zugriff am 19 10 2016].

[19] G. F. Hurlburt und I. Bojanova, „Bitcoin: Benefit or Curse?,“ in *IT Professional*, IT Professional, 2014, pp. 10-15.

[20] Bitcoin Wiki, „Controlled Supply,“ 30 07 2016. [Online]. Available: https://en.bitcoin.it/wiki/Controlled_supply. [Zugriff am 20 09 2016].

[21] M. Tillier, „Is A Blockchain Without Bitcoin Possible Or Practical?,“ NASDAQ, 03 06 2015. [Online]. Available: http://www.nasdaq.com/article/is-a-blockchain-without-bitcoin-possible-or-practical-cm482964. [Zugriff am 11 04 2016].

[22] Blockchain Luxembourg S.A., „Blockchain.info,“ 2016. [Online]. Available: https://blockchain.info/. [Zugriff am 15 09 2016].

[23] C. Bergmann, „Islands virtueller Zimbabwe-Dollar,“ 13 05 2014. [Online]. Available: http://bitcoinblog.de/2014/05/13/ein-digitaler-zimbabwe-dollar-fur-island/. [Zugriff am 14 03 2016].

[24] Bitcoin Wiki, „Colored Coins,“ [Online]. Available: https://en.bitcoin.it/wiki/Colored_Coins. [Zugriff am 09 05 2016].

[25] Bitcoin Wiki, „Smart Property,“ [Online]. Available: https://en.bitcoin.it/wiki/Smart_Property. [Zugriff am 09 05 2016].

[26] Namecoin, „Namecoin,“ [Online]. Available: https://namecoin.info/. [Zugriff am 09 05 2016].

[27] G. Greenspan, „Ending the bitcoin vs blockchain debate,“ Coin Sciences Ltd, 19 Juli 2015. [Online]. Available: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/. [Zugriff am 09 Mai 2016].

[28] G. Greenspan, „Delivery versus payment on a blockchain,“ Coin Sciences Ltd, 7 September 2015. [Online]. Available: http://www.multichain.com/blog/2015/09/delivery-versus-payment-blockchain/. [Zugriff am 10 Mai 2016].

[29] Bitcoin Wiki, „Address,“ 06 09 2016. [Online]. Available: https://en.bitcoin.it/wiki/Address#Multi-signature_addresses. [Zugriff am 15 09 2016].

[30] Bitcoin Wiki, „Script,“ [Online]. Available: https://en.bitcoin.it/wiki/Script. [Zugriff am 11 05 2016].

[31] Ethereum, „A Next-Generation Smart Contract and Decentralized Application Platform,“ [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [Zugriff am 12 05 2016].

[32] G. Wood, „ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER,“ [Online]. Available: http://gavwood.com/Paper.pdf. [Zugriff am 12 05 2016].

[33] Ripple Labs, Inc., „Welcome to Ripple,“ [Online]. Available: https://ripple.com/. [Zugriff am 11 Mai 2016].

[34] Standards Australia, „Australia proposes International Blockchain Standards,“ 14 April 2016. [Online]. Available: http://www.standards.org.au/OurOrganisation/News/Documents/Media%20Release%20-%20International%20Blockchain%20Standard%20-%2014%20April%202016.pdf. [Zugriff am 12 Mai 2016].

[35] O. Ofcorti, „16.5 Estimating the number of bitcoin miners,“ Neighbourhood Pool Watch, 29 05 2014. [Online]. Available: http://organofcorti.blogspot.co.at/2014/05/165-estimating-number-of-bitcoin-miners.html. [Zugriff am 18 05 2016].

[36] CryptoBond, „What are the Bitcoin Transaction types?,“ 29 02 2016. [Online]. Available: https://www.cryptocompare.com/coins/guides/what-are-the-bitcoin-transaction-types/.

[37] blockchain.info, „Hash Rate,“ 19 09 2016. [Online]. Available: https://blockchain.info/charts/hash-rate.

Anhang A: Relevante kryptografische Konzepte

A.1 Hashfunktionen

Eine *Hashfunktion* ist eine spezielle Form einer Einwegfunktion und bildet Werte beliebiger Größe auf Werte fixer Größe, den *Hash*, ab. Aus dieser Definition ergibt sich direkt eine gewisse Unumkehrbarkeit: Aus einem gegebenen Hash lässt sich der ursprüngliche Wert allein schon deshalb nicht ohne Weiteres berechnen, da nicht einmal die Größe des ursprünglichen Werts abgeleitet werden kann. Die Anforderungen an kryptografische Hashfunktionen umfassen diese, aber auch weitere Eigenschaften. Zusammengefasst sind dies:

- *Einwegcharakteristik (pre-image resistance)*: Es muss praktisch unmöglich sein, zu einem vorgegebenen Hash einen Eingangswert zu finden, welcher auf diesen abbildet.
- *Schwache Kollisionsresistenz (second pre-image resistance)*: Es muss praktisch unmöglich sein, zu einem gegebenen Eingangswert einen davon verschiedenen Eingangswert zu finden, welcher auf denselben Hash abbildet.
- *Starke Kollisionsresistenz (collision resistance)*: Es soll generell nicht möglich sein, zwei frei wählbare Eingangswerte zu finden, welche auf ein und denselben Hash abbilden.

Aus diesen drei Eigenschaften ergeben sich weitreichende Konsequenzen. Nachdem jegliche Form von Kollision praktisch nicht gezielt herbeigeführt werden kann, und ein gegebener Hash keinerlei Rückschlüsse auf den Eingangswert zulässt, bedeutet das im Umkehrschluss, dass bereits geringfügige Änderungen im Eingangswert zu gravierenden Änderungen im Hash führen. Wäre dies nicht der Fall, wären Korrelationen zwischen Hash und Eingangswert, und somit Rückschlüsse vom Hash auf den Eingangswert möglich. Diese Eigenschaft wird auch als Resistenz gegen *Beinahe-Kollisionen* (near-collision resistance) bezeichnet.
Auf Grund der Eigenschaften kryptografischer Hashfunktionen wird es beispielsweise unmöglich ein Dokument, dessen Hash bekannt ist, unbemerkt zu manipulieren, da ein auch nur minimal verändertes Dokument auf einen völlig anderen Hash abbildet, wodurch eine Manipulation unmittelbar festgestellt werden kann. Wie schwierig derartige Manipulationen in der Praxis sind, hängt von der Qualität der verwendeten Hashfunktion ab. Die Berechnung eines Hash ist im Regelfall sehr effizient durchführbar.

A.2 Asymmetrische Kryptografie

Asymmetrische kryptografische Verfahren beruhen auf einer speziellen Klasse von Pseudo-Einwegfunktionen, so genannten *Trapdoor*-Funktionen. Genau wie Einwegfunktionen (ähnlich wie Hashfunktionen) sind diese auch in eine Richtung einfach berechenbar, jedoch praktisch nicht invertierbar. Die Besonderheit an Trapdoor-Funktionen ist, dass eine Invertierung sehr wohl einfach durchführbar ist, wenn man über eine spezielle Information verfügt. Mittels derartiger Funktionen lassen sich kryptografische Verfahren konstruieren, welche im Gegensatz zu symmetrischen Verfahren auf den Austausch von Schlüsselmaterial verzichten – Schlüssel werden nie zwischen mehreren Parteien geteilt.
Asymmetrische kryptografische Verfahren bedienen sich der Trapdoor-Charakteristik wie folgt: Schlüssel sind zweigeteilt in einen öffentlichen und einen privaten Teil, was als *public/private key pair* bezeichnet wird. Der öffentliche Teil kann (wie der Name vermuten lässt) veröffentlich werden. Jeder im Besitz dieses öffentlichen Schlüssels kann Daten unter Zuhilfenahme dieses Schlüssels verschlüsseln. Eine Entschlüsselung ist jedoch ohne Kenntnis des privaten Schlüssels praktisch unmöglich und kann daher nur vom Besitzer des privaten Schlüssels durchgeführt werden. Eine direkte Konsequenz aus dieser Trapdoor-Eigenschaft ist die Tatsache, dass Schlüssel eindeutig einzelnen Parteien zugeordnet sind. Digitale Signaturen bauen auf ebendieser Tatsache auf.

A.3 Digitale Signaturen

Digitale Signaturen sind eine Anwendungsmöglichkeit asymmetrischer Kryptografie abseits von Datenverschlüsselung. Die in Abschnitt A.2 beschriebene Trapdoor-Charakteristik wird sozusagen verkehrt herum eingesetzt: Um ein Dokument digital zu signieren wird zuerst dessen Hash berechnet und dieser anschließend mit dem privaten Schlüssel „verschlüsselt“. Eine solche Signatur kann von jedem, dem der zugehörige öffentliche Schlüssel bekannt ist, verifiziert werden und somit dem Besitzer des privaten Schlüssels zugeordnet werden. Durch den „vertauschten“ Einsatz von

öffentlichem und privatem Schlüssel und die eindeutige Zuordnung eines Schlüssels an eine Partei, ist es im Gegensatz zu handschriftlichen Signaturen nicht möglich, im Namen einer anderen Partei eine auf deren Namen lautende Signatur zu erstellen. Daher ist beispielsweise Identitätsdiebstal nur durch Entwenden des privaten Schlüssels möglich. Gleichzeitig sind digitale Signaturen auch nicht abstreitbar, da ein einmal gültig Signiertes Dokument jederzeit mittels zugehörigem öffentlichen Schlüssel verifiziert werden kann. Auf Grund der in Abschnitt A.1 beschriebenen Eigenschaften kryptografischer Hashfunktionen ist es auch nicht möglich ein einmal digital Signiertes Dokument nachtäglich zu manipulieren ohne dass die zugehörige digitale Signatur ungültig wird.