Hochschule Wismar

Fakultät für Ingenieurwissenschaften

Bereich Elektrotechnik und Informatik

Master-Thesis

Vergleich von Kryptowährungen anhand von Transparenz, Anonymität, Disruption, Dezentralität und Sicherheit

Eingereicht am: 04.Oktober 2019

von: Marc Krüger

Aufgabenstellung

In der vorliegenden Master-Thesis wird untersucht, welche der Faktoren Transparenz, Anonymität, Disruption, Dezentralität und Sicherheit entscheidend für den Erfolg und die Durchsetzung von Kryptowährungen sind. Im Rahmen dieser Untersuchung sollen zusätzlich zu dieser zentralen Forschungsfrage folgende weitere Fragestellungen beantwortet werden:

→ Welche Organisationen, Unternehmen und Behörden sind von Kryptowährungen und der dahinterstehenden Blockchain-Technologie betroffen?

→ Wie können am Markt bestehende Organisationen, Unternehmen und Behörden die Wahrscheinlichkeit einer Disruption durch die Entwicklung von Warnsystemen verringern?

→ Wie können Organisationen, Unternehmen und Behörden die aktuellen Abläufe an neue Geschäftsprozesse adaptieren?

Zur Veranschaulichung insbesondere der letztgenannten Fragestellung wird der Import der Bitcoin-Blockchain in eine Neo4J-Datenbank realisiert.

Kurzreferat

Diese Masterarbeit beleuchtet die verschiedenen Kryptowährungen in Bezug auf Transparenz, Anonymität, Disruption, Dezentralität und Sicherheit. Dabei werden vorzugsweise Kryptowährungen betrachtet, die eine hohe Bekanntheit und Marktkapitalisierung aufweisen. Zudem wird darauf geachtet, Kryptowährungen auszuwählen, die unterschiedliche Ansätze verfolgen, um Vor- und Nachteile insbesondere auch in Bezug auf den Faktor Sicherheit herauszuarbeiten. Ein praktisches Beispiel zeigt, wie Daten aus einer Blockchain wie bei der Kryptowährung Bitcoin weiterverarbeitet werden und in eine Graphdatenbank überführt werden. Abgerundet wird die Masterarbeit durch eine von einem Bankunternehmen durchgeführte Zukunftsstudie zu Kryptowährungen.

Um die Forschungsfrage zu beantworten, wird ein qualitativer Vergleich von Kryptowährungen erarbeitet. Die Ergebnisse zeigen, dass lediglich bei den zwei Kryptowährungen Litecoin und LIBRA die Bewertung neutral ausfällt. Die restlichen Kryptowährung werden durchweg positiv bewertet.

Auf dieser Grundlage ist es empfehlenswert, dass Organisationen, Unternehmen und Behörden sich mit dem Thema Kryptowährungen auseinandersetzen müssen und neue Geschäftsprozesse durch den Einsatz von Prototypen zu entwickeln sind. Insbesondere sind Steigerungspotentiale der Effizienz durch den Einsatz von Kryptowährungen zu erwarten.

Abstract

The master thesis highlights the different crypto currencies in terms of transparency, anonymity, disruption, decentralization and security. It selects those crypto currencies that have a high profile and market capitalization. In addition, care is taken to select crypto currencies in such a way that they pursue a different approach in order to work out advantages and disadvantages, especially with regard to security. A practical example shows how blockchain data continues to be processed as in Bitcoin and converted into a graph database. The master's thesis is rounded off by a future study on cryptocurrencies conducted by a banking company.

To answer the research question, a qualitative comparison of cryptocurrencies is developed. The results show that only in the two cryptocurrencies Litecoin and LIBRA the rating is neutral. The remaining cryptocurrency are rated positive.

On this basis, it is recommended that organizations, businesses and government agencies deal with cryptocurrency issues and develop new business processes through the use of prototypes. In particular, potential for improvement in efficiency can be expected through the use of cryptocurrencies.

Inhaltsverzeichnis

1 Einführung in Kryptowährungen....8
1.1 Forschungsfrage und Zielsetzung....9
1.2 Struktur der Masterarbeit....10
1.3 Auswahl der Literaturquellen....11
1.3 Auswahl der Literaturquellen....11
1.4 Geschichtlicher Hintergrund....11
1.5 Das bestehende Geldsystem....12
1.5.1 Die Geldschöpfung aus dem „Nichts“....12
1.5.2 Die Einordnung der Geldarten....14
2 Kryptowährung als Geldeinheit....15
2.1 Entwicklung des Geldsystems....16
2.2 Zahlungsarten....16
2.2.1 Nicht elektronische Zahlungsarten....16
2.2.2 Elektronische Zahlungsarten....17
2.3 Einführung in den monetären theoretischen Hintergrund....20
2.4 Kryptowährung als Geld und Tauscheinheit....21
2.4.1 Nutzen von Kryptowährung als Tauschmittel....21
2.4.2 Nutzen von Kryptowährung als Wertspeicher....22
2.4.3 Nutzen von Kryptowährung als Recheneinheit....22
3 Technologie von Kryptowährungen....23
3.1 Kryptografie....23
3.1.1 Kryptografische Hashfunktionen....24
3.1.2 Elliptic-Curve-Verfahren....25
3.1.3 SHA-256....31
3.1.4 Keccak....36
3.1.5 Troika....38
3.1.6 BLAKE....42
3.1.7 X11....42

3.1.8 Scrypt....43
3.2 Bewertung der kryptografischen Hashfunktionen....44
3.3 Kryptoagilität....47
3.4 Entstehung von Kryptowährungseinheiten....47
3.5 Verwalten von Kryptowährungseinheiten....49
3.5.1 Konsensfindung mittels Proof-of-Work (POW)....49
3.5.2 Konsensfindung mittels Proof-of-Stake (POS)....53
3.5.3 Konsensfindung mittels Proof-of-Activity (POA)....54
3.5.4 Konsensfindung mittels Proof-of-Capacity (POC)....55
3.5.5 Konsensfindung mittels Proof-of-Importance (POI)....55
3.6 Typen von Blockchains....55
3.6.1 Öffentliche Blockchains....56
3.6.2 Private Blockchains und konsortiale Blockchains....57
3.7 Kryptowährungen....57
3.7.1 Bitcoin....58
3.7.2 Ethereum....59
3.7.3 Ripple....62
3.7.4 Dash....64
3.7.5 Monero....67
3.7.6 IOTA....70
3.7.7 LIBRA....72
4 Applikationen mit Kryptowährungskontext....74
4.1 Klassifizierung der Kryptotoken....74
4.1.1 Smart Property....75
4.1.2 Kryptoasset....75
4.2 Dezentrales Nachweisverfahren....76
5 Proof of Concept anhand verschiedener Faktoren....77
5.1 Programmierung und API-Anbindung....77
5.1.1 BitcoinJ....77
5.1.2 EthereumJ und Solidity....78
5.2 Übersicht der APIs und Protokollrealisierung....79
5.3 Import der Blockchain in Graphdatenbanken....81

5.3.1 Vorhandene Benchmarks bei Graphdatenbanken....82
5.3.2 Import der Bitcoin-Blockchain....83
5.4 Recherchemöglichkeiten für Strafverfolgungsbehörden....85
5.4.1 Maltego....85
5.4.2 Online-Services....86
5.5 Empirische Untersuchungen von Kryptowährungen....86
5.6 Disruption bei Unternehmen, Organisationen und Behörden....89
5.6.1 Disruptive Geschäftsmodell durch die Blockchain....90
5.6.2 Zukunftsaussichten bei Kryptowährungen....91
6 Fazit....96
Literaturverzeichnis....100
Bilderverzeichnis....118
Tabellenverzeichnis....119
Verzeichnis der Abkürzungen....120
Anlagenverzeichnis....121
Thesen....123

1 Einführung in Kryptowährungen

Mit der fortschreitenden Digitalisierung beeinflussen und verändern zunehmend neue Trends die verschiedenen Bereiche des Wirtschafts- und Privatlebens. Eine dieser großen Innovationen wurde von Satoshi Nakamoto im Jahre 2008 in einem Aufsatz veröffentlicht [1]. Mit dem Erscheinen der ersten Kryptowährung Bitcoin wurden die bestehenden Zahlungsmöglichkeiten erweitert. Zudem wurden durch die hinter dem Bitcoin-System stehende Blockchain-Technologie andere Wirtschaftsbereiche außerhalb der Finanzbranche dazu inspiriert, neue disruptive Geschäftsmodelle zu entwickeln [2]. Gründerteams mit Geschäftsideen entdeckten die Blockchain-Technologie, um neue Geschäftsprozesse zu modellieren [3]. Etablierte Unternehmen müssen sich den neuen Herausforderungen, die mit der Blockchain-Technologie einhergehen, stellen [4]. Dabei zeigt sich, dass Kryptowährungen mehr als nur reine Bezahlarten sind. Websites wie ‚Coinmarketcap' führen neben den reinen Bezahlkryptowährungen auch Kryptoeinheiten auf, die noch andere Funktionalitäten beinhalten. So werden Kryptowährungen wie Monero auch dafür verwendet, kriminelle Aktivitäten im Internet zu verschleiern. Für die Bearbeitung von Ermittlungsvorgängen muss daher technisches Know-how über die verwendeten Kryptowährungen vermittelt werden. Dazu werden ausgewählte Kryptowährungen qualitativ nach Faktoren bewertet. Durch ein Praxisbeispiel wird gezeigt, wie Kryptowährungen in eine eigene Datenhaltung überführt werden.

1.1 Forschungsfrage und Zielsetzung

Ziel dieser Arbeit ist, bekannte Kryptowährungen qualitativ zu untersuchen und diese zu bewerten. In der vorliegenden Master Thesis werden dazu bekannte Kryptowährungen hinsichtlich der Faktoren Transparenz, Anonymität, Disruption, Dezentralität und Sicherheit untersucht und vorgestellt. Dabei wird analysiert, welche dieser Faktoren entscheidend zum Erfolg der Kryptowährungen beitragen. Es soll somit die folgende für die vorliegende Master Thesis relevante zentrale Forschungsfrage beantwortet werden:

→ Welcher der genannten Faktoren Transparenz, Anonymität, Disruption, Dezentralität und Sicherheit sind entscheidend für den Erfolg und die Durchsetzung von Kryptowährungen?

Zudem ergeben sich folgende weitere Fragestellungen, die sich von der zentralen Forschungsfrage ableiten:

→ Welche Organisationen, Unternehmen und Behörden sind von Kryptowährungen und der dahinterstehenden Blockchain-Technologie betroffen?

→ Wie können am Markt bestehende Organisationen, Unternehmen und Behörden die Wahrscheinlichkeit einer Disruption durch die Entwicklung von Warnsystemen verringern?

→ Wie können Organisationen, Unternehmen und Behörden die aktuellen Abläufe an neue Geschäftsprozesse adaptieren?

Die Beantwortung der Forschungsfragen ist auch für Strafverfolgungsbehörden relevant, um auf die zukünftigen Entwicklungen vorbereitet zu sein.

1.2 Struktur der Masterarbeit

In Bild 1 wird die Vorgehensweise und Struktur der Master Thesis dargestellt.

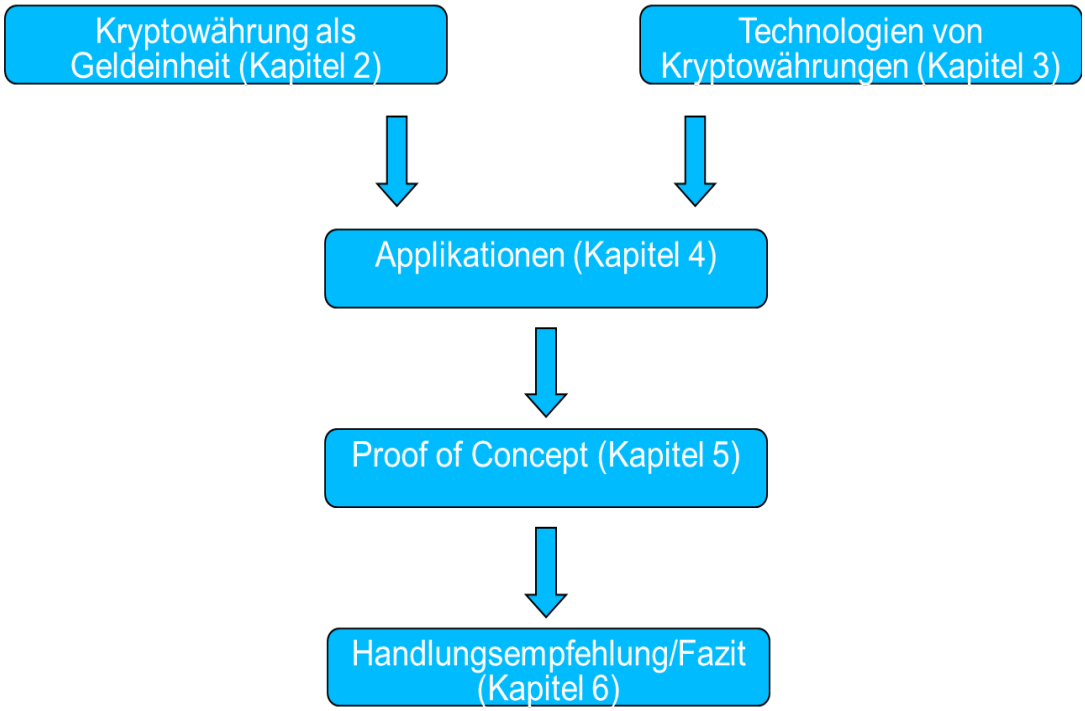

Bild 1: Vorgehensweise

So zeigen das zweite und dritte Kapitel die Grundlagen für theoretische Überlegungen auf. Dabei wird im zweiten Kapitel auf bestehende Zahlungsmodelle eingegangen. Danach werden Kryptowährungen analysiert, inwieweit diese die Funktion als Wertspeicher, Kalkulationseinheit und Tauschmittel übernehmen können. Das dritte Kapitel widmet sich den Technologien von Kryptowährungen, erläutert und vergleicht diese miteinander. Am Ende des dritten Kapitel wird eine Bewertung der Technologien vorgenommen. Kapitel 4 stellt Einsatzfelder für Kryptowährungen, Kryptoassets und dezentrale Nachweisverfahren vor. Im fünften Kapitel werden in Form eines „Proof of Concept“ Möglichkeiten zur API-Anbindung von Kryptowährungen praktisch angewendet. Ebenfalls wird ein mögliches Mining

von Kryptowährungen gezeigt. Der Schluss des fünften Kapitels demonstriert Anwendungen, um Recherchemöglichkeiten für Strafverfolgungsbehörden zu ermöglichen. Das sechste Kapitel schließt mit dem Fazit der Master Thesis ab.

1.3 Auswahl der Literaturquellen

Der Themenbereich der Kryptowährungen ist noch jung. Klassische Literaturquellen in Form von Print-Publikationen wurden daher noch nicht in der Vielzahl veröffentlicht, wie dies in anderen Wissensgebieten üblich ist. Aktuelles Wissen wird überwiegend über Forschungsartikel vermittelt. So veröffentlichen einschlägige Magazine wie Kryptomagazine[1] Artikel zu den Themen Blockchain und Kryptowährungen. Die Themenstellung der Master Thesis selbst umfasst auch weitere Themenbereiche. Die Selektion der Literaturquellen erfolgt unter der Prämisse, eine möglichst breite Wissensbasis zu bilden, um anhand dieser die in der vorliegenden Master Thesis genannten Forschungsfragen zu beantworten

1.4 Geschichtlicher Hintergrund

Während der weltweiten Finanzkrise im Jahre 2008 veröffentlichte Satoshi Nakamoto [1] ein neuartiges monetäres Peer-to-Peer-System. Im darauffolgenden Jahr empfahl Nakamoto eine beispielhafte Referenzimplementierung der Kryptowährung Bitcoin. Seitdem hat der Bitcoin eine weltweite Bekanntheit erlangt. Im Jahr 2014 wurde die 1.000-Euro-Marke pro Bitcoin an den Handelsplätzen überschritten.

[1] Vgl. www.krypto-magazin.de

1.5 Das bestehende Geldsystem

Im bestehenden Geldsystem erschaffen die konventionellen Banken neues Geld durch die Vergabe von Krediten. Dies schließt auch die Nutzung von Kreditkarten ein. Die Entstehung neuen Geldes wird dem Bereich der Geldschöpfung zugeordnet. Geld selbst repräsentiert physisch oder virtuell einen entsprechenden Wert. Zudem wird Geld mittels Transaktionen an andere Besitzer weitergereicht. Dieser Transfer kann über eine zentrale Instanz erfolgen oder wird über einen Mechanismus dezentral abgewickelt.

1.5.1 Die Geldschöpfung aus dem „Nichts“

Eine Wertsteigerung des Geldes erfolgt durch die Verringerung der Menge an Geld. Dies geschieht sowohl in zentralen als auch in dezentralen Geldsystemen. Liegt ein dezentrales Geldsystem vor, so können neue Geldeinheiten durch jeden Akteur im Geldsystem neu erschaffen werden. Dabei beobachtet der Akteur, ob die Erstellungskosten unter den Werterträgen der Geldeinheiten liegen (siehe Bild 2).

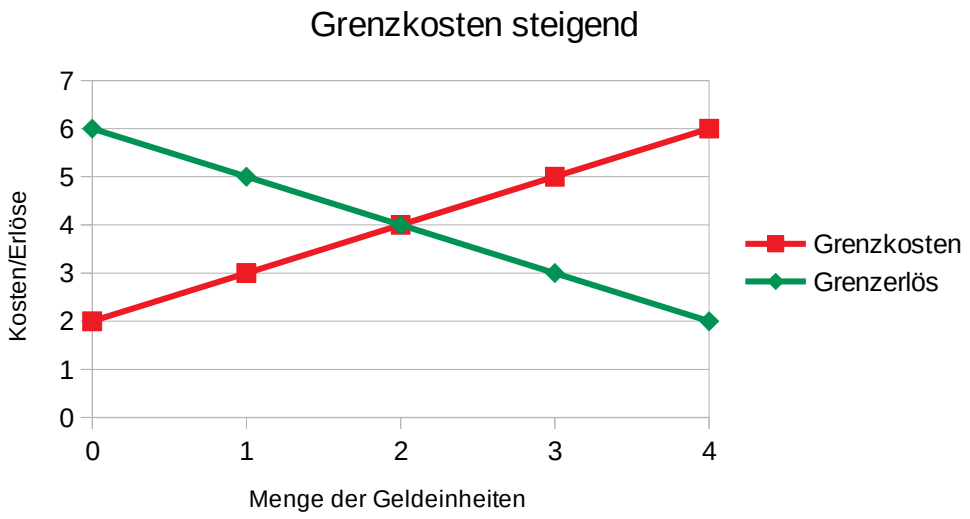

Bild 2: Grenzkosten steigend

Befinden sich die Akteure in einem von einer zentralen Instanz gesteuerten Geldsystem, so werden die Kosten der Entstehung neuer Geldeinheiten ignoriert (siehe Bild 3).

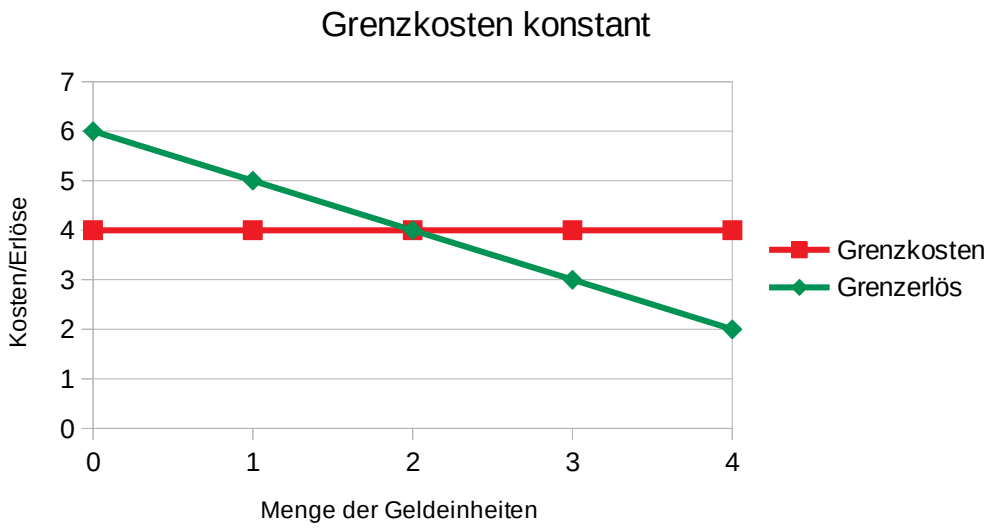

Bild 3: Grenzkosten konstant

1.5.2 Die Einordnung der Geldarten

Mit dem Begriff der Kryptowährung wie dem Bitcoin wird ein System beschrieben, das weit mehr als nur die eigentlichen Geldeinheiten darstellt. So stellt sich die Frage, wie und in welcher Form das Geld repräsentiert wird. Ebenfalls kann Geld auf unterschiedliche Art erschaffen werden. Zu guter Letzt muss dargelegt werden, wie Geldeinheiten den Besitzer wechseln und wer diese Transaktionen initiiert. Aus diesem Grund werden in Tabelle 1 die einzelnen Geldarten mithilfe der Kategorien zentrale/dezentrale Transaktion, physische/virtuelle Repräsentation und monopolistische/wettbewerbsmäßige Geldschöpfung beschrieben.

	Transaktionen		Repräsentation		Geldschöpfung	
	Dezentral	Zentral	Physisch	Virtuell	Monopol	Wettbewerb
Kryptowährung	Hoch	-	-	Hoch	-	Hoch
Bargeld	Hoch	-	Hoch	-	Hoch	-
Giralgeld	-	Mittel	-	Hoch	Mittel	Mittel
Warengeld	Hoch	-	Hoch	-	-	Hoch
Zentralbankreserven	Hoch	Hoch	-	Hoch	Hoch	-

Tabelle 1: Eigenschaften der Geldarten

2 Kryptowährung als Geldeinheit

Im 20. Jahrhundert basierte das weltweite Geldsystem zunächst auf dem Bretton-Woods-Abkommen [5], ehe US-Präsident Richard Nixon 1971 den Goldstandard auflöste und damit den Übergang zum Schuldgeldsystem ermöglichte [6]. Mit jeder Kreditaufnahme wird fortan neues Geld ex nihilo erschaffen [7]. Geld selbst speichert Informationen darüber ab, dass Menschen sich gegenseitig einen Gefallen schulden, ohne gleich in Gegenleistung getreten zu sein [8]. Diese Gefallen werden überall und zu jeder Zeit ausgeübt. Dabei speichern die Teilnehmer bewusst oder unbewusst diese Gefallen in einer eigenen Buchhaltung. Ein starkes Ungleichgewicht dieser gegenseitigen Schuldverhältnisse, bei denen ein Teilnehmer ständig einen Gefallen erledigt und ein anderer einseitig davon profitiert, wird zu Verwerfungen in der Beziehung führen. Es muss daher ein Mechanismus in den gegenseitigen Beziehungen eingeführt werden, der die Möglichkeit zur Findung eines von allen akzeptierten Konsens bietet. Je größer der Teilnehmerkreis einer gemeinsamen Gruppe wird, desto schwieriger wird es, einen Konsens der Teilnehmer herzustellen. In der Regel kennen sich die Teilnehmer immer weniger, je größer die Gruppe zur Konsensfindung wird. Die Gefälligkeiten werden daher in großen Gesellschaftsgruppen durch Geld ersetzt. Geld erfüllt damit eine Gedächtnisfunktion und ermöglicht es, Buch über geleistete Gefälligkeiten innerhalb einer Gruppe zu führen. Damit Geldtransaktionen in einem System funktionieren, werden Regeln zur Herstellung, der Repräsentanz und der Transaktionsdurchführung aufgestellt.

Die Funktionsweise des Geldsystems wird in den folgenden Kapiteln anhand der verschiedenen Bezahlarten erläutert.

2.1 Entwicklung des Geldsystems

Bei Betrachtung des Geldsystems fällt der Blick auf die klassischen physischen Münzen und Banknoten. Das Bargeld repräsentiert auch klar geregelte Eigentumsverhältnisse bezüglich des Bargeldes. Beim Kauf eines Gutes wechselt das Bargeld den Eigentümer. Dubletten oder eine mehrfache parallele Nutzung des Geldes ist ausgeschlossen. Die Einschaltung einer dritten Instanz, die den Kaufvorgang bezüglich des Eigentümers des Bargeldes überprüft, entfällt.

2.2 Zahlungsarten

Bei der Betrachtung eines Kaufs von Waren oder Dienstleistungen wird erkennbar, dass die Zahlungsarten in elektronische und nicht elektronische eingeteilt werden können.

2.2.1 Nicht elektronische Zahlungsarten

Unter die Klasse der nicht elektronischen Zahlungsarten fallen alle diejenigen, die nicht über oder mit dem Internet realisiert werden und in der Regel entweder einen Besuch in einer Bank erfordern oder physisch abgewickelt werden. Dazu zählen unter anderem die Zahlungsarten Lastschrift, Vorkasse, Nachnahme, Bargeld und Überweisung [9]:

- Bargeld: Das Bargeld ersetzte den reinen Warentausch im Zuge des stetig wachsenden Handels. Wurden zunächst Münzen als Universalgut als Ersatz für den reinen Warenaustausch eingesetzt, so setzte sich immer mehr das

Papiergeld durch.

- Lastschrift: Beim Verfahren mittels Lastschrift erteilt eine Person einer anderen Person oder einem Unternehmen die Erlaubnis, Geld von seinem Bankkonto direkt abzubuchen. Das Lastschriftverfahren findet oftmals dann Anwendung, wenn periodische Bezahlvorgänge wie Mietzahlungen abgewickelt werden.

- Nachnahme: Beim Bezahlvorgang mittels Nachnahme wird bei Auslieferung der Ware direkt beim Postzusteller oder Postschalter bezahlt. Zusätzlich zum Warenpreis wird vom Paketdienst die Gebühr für den Nachnahmeservice eingefordert.

- Überweisung: Die Überweisung findet zwischen verschiedenen Konten einer oder mehrerer Banken statt, indem ein bestimmter Geldbetrag von einem Konto auf ein anderes Konto überschrieben wird. In der Regel werden dazu Überweisungsträger auf Papier ausgefüllt und am Bankschalter abgegeben.

- Vorkasse: Die Bezahlung mittels Vorkasse sieht vor, dass ein Käufer oder Servicenutzer einer Dienstleistung einen Geldbetrag im Voraus bezahlt, noch bevor dieser die Gegenleistung dafür erhält. Der Geldbetrag kann bar oder unbar zum Beispiel über eine Überweisung transferiert werden.

2.2.2 Elektronische Zahlungsarten

In die Klasse der elektronischen Zahlungsarten fallen all jene, die über das Internet und an Geldgeräten realisiert werden. Dazu zählen die Sofortüberweisung, Paypal, die elektronische Überweisung und die Kreditkartenzahlung.

- Sofortüberweisung: Das Web-Bezahlsystem Sofortüberweisung wird von der Firma Sofort GmbH betrieben. Dabei handelt es sich um ein bargeldloses Vorkassensystem, bei dem der Verkäufer einer Ware eine Bestätigung über die durchgeführte Bezahlung des Käufers erhält. Damit weiß der Verkäufer, dass die Ware freigegeben oder versendet werden kann. Die eigentliche Bezahlung durch einen Käufer erfolgt durch die Eingabe von Benutzerkennung und Passwort des Bankkontos. Anschließend muss noch die Übermittlung einer Transaktionsnummer für den eigentlichen Transfer des Geldes an den Verkäufer erfolgen. Für jede durchgeführte Transaktion muss vom Verkäufer eine Gebühr gezahlt werden.

- Paypal: Paypal ist ein mittlerweile etabliertes Unternehmen, das Bezahldienste im Internet anbietet. Bei einem Bezahlvorgang werden Beträge von einem Paypal-Konto auf ein anderes übertragen. Es besteht die Möglichkeit, das Paypal-Guthaben an ein Konto einer Bank zu transferieren, um dieses zum Beispiel später an einem Geldautomat abzuheben. Ebenfalls sind Bezahlvorgänge auch ohne eigenes Paypal-Guthaben möglich. Dazu kann ein Bankkonto für die Lastschrift eingetragen werden. Eine weitere Möglichkeit ist die Verknüpfung mit einer Kreditkarte. Wird nun ein Bezahlvorgang gestartet, so erfolgt im Rahmen dieses Vorgangs eine Weiterleitung auf die Paypal-Website. Der Benutzer gibt dann seinen Benutzernamen und das dazugehörige Passwort ein und meldet sich bei Paypal an. Danach wird die Transaktion angezeigt und muss vom angemeldeten Benutzer bestätigt werden. Nach Abschluss der Bezahlung wird der Benutzer wieder zur Händlerseite zurückgeleitet. Eine Besonderheit bei Paypal ist der sogenannte Käuferschutz. Bei betrügerischen Transaktionen wird der Kaufpreis auf Kosten von Paypal zurückerstattet.

- Kreditkarte: Die Bezahlung von Waren oder Dienstleistungen kann mithilfe

einer Kreditkarte vorgenommen werden. Kreditkartenunternehmen wie zum Beispiel Visa, Mastercard oder American Express geben die Karten an ihre Kunden aus. Für die Nutzung einer Kreditkarte fallen verschiedene Gebühren an. Nach Nutzung der Kreditkarte für die Bezahlung von Waren oder Dienstleistungen erfolgt nach einigen Wochen die Abbuchung der Geldbeträge vom angegebenen Girokonto. Neben den konventionellen Kreditkarten sind am Markt auch sogenannte Debit-Karten erhältlich. Diese werden in der Regel von den bekannten Kreditkartenunternehmen angeboten, sind allerdings Karten, die rein auf Basis von Guthaben genutzt werden können [10].

- elektronische Überweisung: Unter einer elektronischen Überweisung werden in der Regel Überweisungen verstanden, die mittels Website oder Terminal durchgeführt werden [11]. Um als Kunde einer Bank an dem Verfahren teilzunehmen, werden diesem seitens der Bank sowohl eine persönliche Identifikationsnummer (PIN) als auch Transaktionsnummern (TAN) zur Verfügung gestellt. Dazu loggt der Kunde sich online auf der Bank-Website mit seinem Benutzernamen und der dazugehörigen PIN ein. Für die Überweisung wird in der Regel eine spezielle vorbereitete Webseite bereitgestellt. Dort kann der Kunde Pflichtfelder wie die internationale Bankkontonummer (englisch International Bank Account Number IBAN) und den Verwendungszweck ausfüllen. Im nächsten Schritt wird vom System eine spezielle TAN abgefragt, die der Kunde zur Legitimation der Transaktion angeben muss.

2.3 Einführung in den monetären theoretischen Hintergrund

In den Jahren der weltweiten Finanz- und Wirtschaftskrise geriet das internationale Finanzsystem in große Schwierigkeiten, die sich auch auf die vorab beschriebenen Zahlungsarten auswirkten. Zeitgleich erschien am 1. November 2008 ein Artikel von Satoshi Nakamoto, in dem ein Peer-to-Peer-Bezahlsystem vorgestellt und beschrieben wurde. Ein Jahr später stellte Nakamoto in einer weiteren Veröffentlichung die erste Referenzimplementierung des Bitcoin-Systems vor. Seitdem wird die Weiterentwicklung des Bitcoin-Systems von einer großen Gemeinschaft im Internet vorangetrieben. Die Software selbst ist Open Source und somit für jeden Nutzer frei verfügbar. Bis heute ist nicht geklärt, wer sich hinter dem Pseudonym Nakamoto verbirgt. Seit der Veröffentlichung von Nakamoto hat sich das Bitcoin-System stetig weiterentwickelt. Entsprechend wuchs auch das Interesse am Bitcoin, so dass im Jahr 2014 für einen Bitcoin mehr als 1.000 Euro bezahlt wurden. Im Jahr 2018 überstieg der Preis die 15.000-Euro-Marke, fiel jedoch im Folgejahr auf rund 3.000 Euro ab. Das starke Interesse an der Kryptowährung Bitcoin beruht darauf, dass bei deren Entwicklung folgende drei Hauptziele beachtet wurden [12]:

- Dezentrales Geld [13]

- Transparenz

- Pseudonym

Bei einem dezentralen Geld entfällt der Intermediär in Form einer Zentralbank. Die Transparenz ermöglicht das Nachvollziehen von durchgeführten Transaktionen und erhöht dadurch das Vertrauen. Die Transaktionen werden

durch ein Pseudonym durchgeführt und schützen damit die Identität der beteiligten Transaktionspartner.

2.4 Kryptowährung als Geld und Tauscheinheit

Um eine Einordnung von Kryptowährungen in das bestehende Geldsystem vorzunehmen, müssen zunächst die Rollen der Geschäfts- und Notenbanken betrachtet werden. Im derzeitigen Zentralbankensystem verfügen die Noten- und Geschäftsbanken über das Geldschöpfungsrecht, indem diese neue Kredite an die Wirtschaft, Privatpersonen oder staatliche Institutionen ausgeben [14]. Dabei unterliegt die Repräsentation, Transaktion und Geldschöpfung bestimmten Kontrollmechanismen. Die Geldschöpfung beschreibt einen Prozess, bei dem neues Geld erzeugt wird. Dieses neu erzeugte Geld wird zudem im Geldkreislauf in Umlauf gebracht. Dabei werden Seiteneffekte wie Inflation oder Deflation erzeugt, so dass die im Umlauf befindliche Menge an Geldeinheiten gesteuert werden muss. Geld wird durch physische Geldeinheiten wie Metallmünzen oder Banknoten repräsentiert, kann aber auch rein virtuell sein. Werden die Transaktionen von Geldeinheiten betrachtet, so werden diese über eine zentrale oder dezentrale Instanz abgewickelt.

2.4.1 Nutzen von Kryptowährung als Tauschmittel

Allgemein hat Geld sich in arbeitsteiligen und spezialisierten Gesellschaften behauptet, da dort keine Selbstversorgungen der Menschen und autarkes Leben möglich ist. Vielmehr sind Menschen in den Gesellschaften mit Arbeitsteilung gezwungen, nicht vorhandene Waren gegen im Besitz befindliche

Waren zu tauschen.

2.4.2 Nutzen von Kryptowährung als Wertspeicher

Das Geld wird als komfortable Möglichkeit zur Wertspeicherung verwendet. Sobald Güter erworben werden sollen, wird dieses als Gegenwert entsprechend genutzt. Gleichzeitig werden auch Reserve angelegt, was wiederum die Liquidität erhöht. Wird die Anzahl verfügbarer Einheit wie bei der Kryptowährung Bitcoin auf 21 Millionen begrenzt, so ist langfristig von einer deflationären Entwicklung des Bitcoins gegenüber dem Fiat-Geld wie Euro oder US-Dollar auszugehen. In Studien wird zudem gezeigt, dass weltweit nur 1,2 Millionen Bitcoin besitzen [15]. Trotz der dezentralen Eigenschaft von Bitcoin hat sich in den letzten Jahren eine Konzentration der Bitcoin nur auf wenigen Wallets eingestellt. Der dezentrale Gedanke wird dadurch konterkariert [16].

2.4.3 Nutzen von Kryptowährung als Recheneinheit

Geld wird als Intermediär zwischen Waren und Dienstleistungen eingesetzt. Dadurch wird die Anzahl an Tauschpartnern der Waren und Dienstleistungen deutlich erhöht und entfällt das aufwändige Suchen. Kryptowährungen wie Bitcoin verfügen zudem über die Eigenschaft, dass kleine Stückelungen einer Einheit bis zur achten Nachkommastelle verwendet werden können. Ein Bitcoin kann in zehn Deci-Bitcoins umgerechnet werden, während 100 Centi-Bitcoin einen Bitcoin ergeben.

3 Technologie von Kryptowährungen

Im dritten Kapitel werden die verschiedenen technologischen Ansätze von Kryptowährungen vorgestellt. Die Kryptowährungen werden derzeit in eine erste, zweite und dritte Generation unterteilt [17]. Zunächst wird das Bitcoin-System erläutert. Der Bitcoin zählt neben dem Litecoin, Dogecoin, Dash und Monero zur ersten Generation. Ethereum und Ripple werden zur zweiten Generation gezählt. Der dritten Generation wird das IOTA zugerechnet, da die Technologie sich eklatant von den Kryptowährungen der ersten und zweiten Generation unterscheidet.

3.1 Kryptografie

In der Kryptografie werden symmetrische und asymmetrische Verschlüsselungsverfahren verwendet [18]. Bei den symmetrischen Verschlüsselungsverfahren müssen die an einer Kommunikation beteiligten Partner über den gleichen Schlüssel zur Ver- und Entschlüsselung von Nachrichten verfügen. Diese Verfügbarkeit des gleichen Schlüssels ist problematisch, da beide Parteien sich auf einen gemeinsamen Schlüssel einigen und schließlich diesen auch über einen sicheren Kanal austauschen müssen. Ansonsten besteht die Gefahr, dass dieser Schlüssel von Dritten abgefangen wird und so verschlüsselte Nachrichten dechiffriert und mitgelesen werden können. Um die Nachteile der symmetrischen Verschlüsselungsverfahren aufzuheben, wurden alsbald asymmetrische Verschlüsselungsverfahren entwickelt, die als Publik-Key-Verfahren bezeichnet werden [19]. Bei den asymmetrischen Verfahren wird ein öffentlicher und ein

privater Schlüssel verwendet. Der öffentliche Schlüssel dient zur Verschlüsselung einer Nachricht, die mit dem privaten Schlüssel wieder entschlüsselt wird. Der öffentliche Schlüssel wird dabei veröffentlicht, während der private Schlüssel beim Eigentümer verbleibt und ansonsten niemandem zur Verfügung gestellt werden darf. Eine Nachricht kann mit dem öffentlichen Schlüssel nicht entschlüsselt werden. Auch kann ein privater Schlüssel nicht aus dem öffentlichen Schlüssel abgeleitet werden. Umgekehrt ist allerdings eine Herleitung eines öffentlichen Schlüssels aus dem privaten Schlüssel möglich. Damit können digitale Signaturen von Nachrichten realisiert werden, indem der Besitzer eines privaten Schlüssels die Nachricht mit eben diesem signiert und die anschließende Überprüfung durch den öffentlichen Schlüssel erfolgt. Zum einen kann damit die Unverfälschbarkeit der Nachricht nachgewiesen werden. Zum anderen wird damit auch gezeigt, dass eine Nachricht von einer bestimmten Person stammt. Bei Kryptowährungen werden digitale Signaturen zur Beweisführung von Transaktionen verwendet.

3.1.1 Kryptografische Hashfunktionen

Die meisten Kryptowährungen verwenden zur Verschlüsselung, Integrität und Authentizität kryptografische Hashfunktionen [20]. Die Hashfunktionen weisen drei typische Eigenschaften auf:

- Der Eingabewert kann beliebig groß sein.

- Die Hashfunktion erzeugt schnell einen Ausgabewert mit einer vorab festgelegten Größe und ist dabei deterministisch.

- Die Berechnung eines Ausgabewerts aus einem gegebenen Eingabewert

ist verhältnismäßig einfach. Damit ist es möglich, aus einem Eingabewert einen Ausgabewert fester Größe zu erzeugen. Gleichzeitig ist die Umkehrfunktion auch unter großem technischen und zeitlichen Aufwand praktisch nicht berechenbar.

Damit eine Hashfunktion als kryptografisch gilt, müssen noch drei weitere Eigenschaften erfüllt werden:

- Kollisionsresistenz: Eine Kollision liegt vor, wenn mindestens zwei verschiedene Eingabewerte den gleichen Ausgabewert erzeugen. Solange keine Kollision gefunden wird, gilt eine Hashfunktion als kollisionsfrei.

- Kleine Änderungen mit großer Wirkung: Bereits eine kleine Änderung des Eingabewertes führt zu einem stark veränderten Ausgabehashwert.

- Puzzlefreundlichkeit [21]: Eine Hashfunktion H gilt als puzzlefreundlich, wenn für den Ausgabewert y nicht möglich ist, x der folgenden Funktion in weniger als 2^n der Zeit zu ermitteln:

$$H(k \| x) = y \tag{3.1}$$

3.1.2 Elliptic-Curve-Verfahren

Das Elliptic-Curve-Verfahren (Elliptic Curve Cryptography – ECC) ist ein asymmetrisches Verschlüsselungsverfahren, das bei zahlreichen Kryptowährungen wie Bitcoin und Ethereum angewendet wird [22]. Elliptic Curve nutzt einen kleineren Schlüssel wie RSA (benannt nach Rivest, Shamir, Adleman), ist jedoch deutlich sicherer. Durch die verkürzten Schlüssel wird sowohl Speicherplatz als auch Berechnungszeit bei der Ver- und Entschlüsselung eingespart. Beim ECC-Verfahren werden, wie der Name

bereits verrät, elliptische Kurven für die Berechnungen verwendet [23]. Generell lautet die Formel einer elliptischen Kurve wie folgt:

$$y^2 = x^3 + ax + b \tag{3.2}$$

Um ein bestimmtes Verhalten wie Singularitäten oder Überschneidungen der Kurve auszuschließen, wird zu der genannten Formel noch eine Abgrenzung in der folgenden Form vorgenommen:

$$4a^3 + 27b^2 \neq 0 \tag{3.3}$$

Wie in Bild 4 dargestellt, werden die Punkte der Kurve spiegelsymmetrisch zur Abzisse gezeichnet [24].

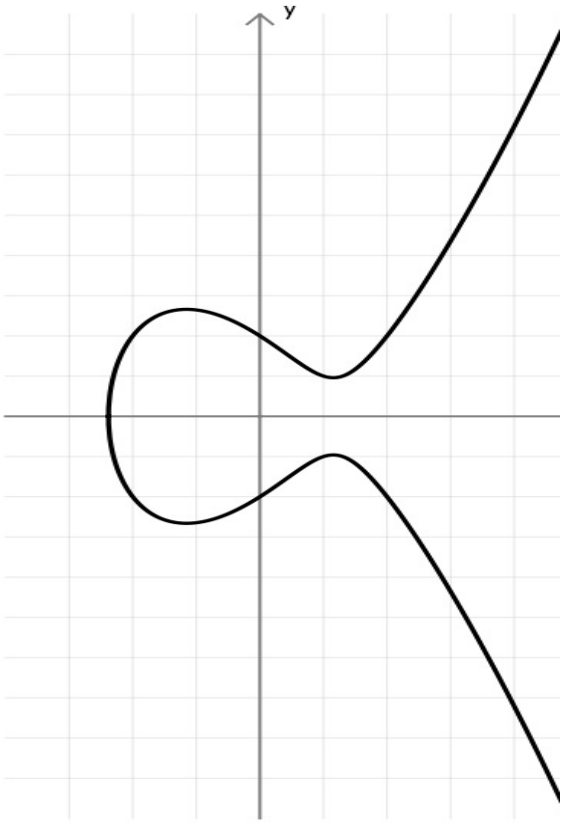

Bild 4: Beispiel einer elliptischen Kurve

Es ist zudem erkennbar, dass eine zur Ordinate nicht parallel gezeichnete Gerade einen oder drei Schnittpunkte mit der elliptischen Kurve aufweist. Dieses Verhalten der Geraden mit der elliptischen Kurve kann für bestimmte Operationen genutzt werden. Die grundlegende Addition von zwei Punkten P und Q auf der elliptischen Kurve erfolgt in der Weise, dass zunächst eine Gerade durch die beiden Punkte gezogen wird. Dabei entsteht ein dritter Schnittpunkt R, der nun an der Abszisse gespiegelt wird. Dazu wird der Y-Wert des Punktes R negiert. Das Ergebnis der Addition ist ein Punkt -R. Beim ECC-Verfahren steht allerdings nur ein Punkt zur Verfügung. Der Basispunkt P wird zunächst mit sich selbst addiert. Dabei ist wieder eine Gerade von Punkt P zu Punkt P zu ziehen, so dass als Ergebnis unendlich viele Möglichkeiten entstehen. Um ein Ergebnis zu erhalten, wird eine lineare Näherungsfunktion in Form der Tangente von Punkt A gewählt. Die Tangente berührt sowohl Punkt P als auch einen Punkt Q, wobei beide Punkte auf der elliptischen Kurve liegen. Das Ergebnis der Addition wird berechnet, indem der Punkt Q an der Abszisse gespielt wird. Dabei entsteht der Punkt -Q, der auch als 2*P bezeichnet werden kann. Bei bestimmten Kryptowährungen wie Bitcoin und Ethereum wird eine besondere Form der elliptischen Kurve mit dem Namen SECP256K1 und der folgenden Gleichung:

$$y^2 = x^3 + 7 \tag{3.4}$$

Grafisch betrachtet ergibt sich dabei folgendes Bild 5:

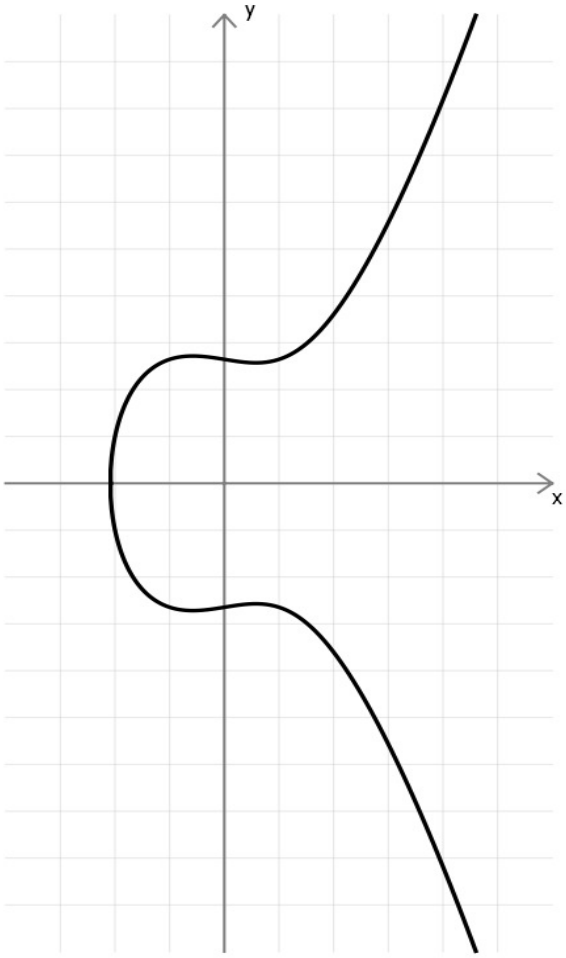

Bild 5: Elliptische Kurve bei Bitcoin und Ethereum

Die Besonderheit ist hier, dass der Ausgangspunkt P bereits festgelegt ist. Diese Festlegung des Ausgangspunktes P erleichtert die mathematischen Operationen auf der elliptischen Kurve SECP256K1 erheblich. So liefert zum Beispiel die Addition von Punkt P mit dem Punkt 2*P den neuen Punkt 3*P.

Dieses als skalare Multiplikation bezeichnete Vorgehen ermöglicht schnelle Kalkulationen von Punkten auf der elliptischen Kurve und verwendet dabei die allgemeine Formel:

$$n \cdot P + r \cdot P = (n + r) \cdot P \tag{3.5}$$

Die Kryptowährungen nutzen große Punktkoordinaten im ECC-Verfahren. Dies würde dazu führen, dass die Berechnungswerte ins Unendliche anwachsen können. Zur Begrenzung wird daher im Verfahren selbst ein begrenztes Feld festgelegt, bei dem nur ganzzahlige Integer-Werte mit einem bestimmten Maximalwert von 256 Bit erlaubt sind. Die operative Umsetzung erfolgt mittels einer geeigneten Modulo-Operation auf die Funktion der elliptischen Kurve. Innerhalb der Funktion begrenzt damit der Divisor der Modulo-Operation den Wertebereich der Funktion, wobei die höchste Primzahl vor dem Maximalwert gewählt wird. Dadurch entsteht eine Primkurve mit optimalen Eigenschaften der Kryptografie, um die mathematischen Operationen wie Addition und Multiplikation zurückberechnen zu können. Bei Anwendung der Modulo-Operation wird ein endliches Feld zurückgeliefert, das dieselben spiegelsymmetrischen Attribute aufweist. Die Anwendung der mathematischen Operationen innerhalb des endlichen Feldes verläuft analog zur elliptischen Kurve. Die Addition von zwei Punkten erfolgt damit ebenso wie bei der elliptischen Kurve. Eine Besonderheit tritt dann ein, wenn die Tangente das endliche Feld verlassen sollte. Hier sorgt der Modulo-Operator dafür, dass die Tangente wieder auf der anderen Seite des endlichen Feldes eintritt. Das ECC-Verfahren selbst findet im sogenannten Elliptic Curve Digital Signature Algorithm (ECDSA) Verwendung. Zunächst wird ein privater Schlüssel erzeugt. Um anschließend einen passenden öffentlichen Schlüssel zu erzeugen, muss der private Schlüssel entsprechend oft auf der elliptischen Kurve des ECDSA

addiert werden, bis der gewünschte öffentliche Schlüssel errechnet wird [26]. Bei Anwendung der Algorithmen Add- und Double kann aus dem privaten Schlüssel vergleichsweise schnell der öffentliche Schlüssel zurückgeliefert werden. Die Anwendung der Umkehrfunktion, bei der aus dem öffentlichen Schlüssel der private Schlüssel mittels Elliptic Curve Discrete Logarithm errechnet wird, führt zu langen Berechnungen mit nicht akzeptablen Zeiträumen. Die elliptische Kurve SECP256K1 verwendet Schlüsselgrößen von 256 Bit.

Digitale Signaturen

Um die Authentizität und Integrität einer Transaktion von Kryptowährungseinheiten zu beweisen, werden bei den Kryptowährungen digitale Signaturen verwendet [27]. Die Signierung einer Transaktion im ECDSA-Algorithmus erfolgt durch die Beweiserbringung von einem zugehörigen privaten Schlüssel x zu einem öffentlichen Schlüssel X. Dabei darf der private Schlüssel x nicht der Öffentlichkeit bekannt werden. Die Signaturerstellung zu einer zu versendenden Nachricht m erfolgt, indem der Versender der Nachricht m eine Zufallszahl r mit 256 Bit Länge generiert. Die Addition der Zufallszahl r mit einem beliebig gewählten Punkt P führt zu einem neuen Punkt R [28]. Entsprechend besteht nun die Möglichkeit, die Kalkulation der digitalen Signatur mittels der nachfolgenden Formel durchzuführen:

$$s = hash(m, R) \cdot x + r \tag{3.6}$$

Zwar könnte die Formel nach dem privaten Schlüssel in der folgenden Form umgestellt werden:

$$x = \frac{s - r}{hash(m, R)} \tag{3.7}$$

Diese Umstellung führt jedoch zu einer Gleichung von zwei unbekannten Variablen x und r, da der Wert für r ebenfalls geheim ist. Wird die Transaktion durchgeführt, so beinhaltet diese die beiden Teile der Nachricht m und die Signatur (s,R). Der Nachrichtenempfänger kann damit auf den öffentlichen Schlüssel X, die Signatur (s,R) und die eigentliche Nachricht m zugreifen. Der Empfänger wird nun die Nachricht auf ihre Authentizität prüfen, indem die Signatur überprüft wird. Dadurch wird die folgende Formel mit gelieferten Werten möglich:

$$S = hash(m, R) \cdot X + R \tag{3.8}$$

Das Ergebnis von S wird verglichen mit dem Produkt aus dem Punkt P und der Signatur s:

$$S = s \cdot P \tag{3.9}$$

Bei Korrektheit der Gleichung kann die Echtheit der Transaktion bestätigt werden.

Angriffsmöglichkeiten

In [29] werden Angriffsmöglichkeiten unter anderem gegen ECDSA aufgezeigt. Insbesondere wird ein Angriff gegen den geheimen Schlüssel d demonstriert, der allerdings eher theoretischer Natur ist.

3.1.3 SHA-256

Die Hashfunktion SHA ist eine Abkürzung für Secure Hash Algorithm. SHA-256 liefert als Ausgabewert Hashwerte mit einer Länge von 256 Bit. Als Eingabewerte werden Blöcke mit einer Größe von 512 Bit verwendet. Die

kryptografische Hashfunktion Sha-256 wird in insgesamt 64 Durchläufen berechnet [30]. Dabei findet eine Verarbeitung von jeweils acht gleich großen Wortwerten statt, die mit einem konstanten 32 Bit-Wert eines Blocks verknüpft werden. Damit verschieben sich die Datenblöcke um eine Stelle nach rechts. So kann gewährleistet werden, dass eine Vermischung der berechneten Werte durchgeführt wird (siehe Bild 6).

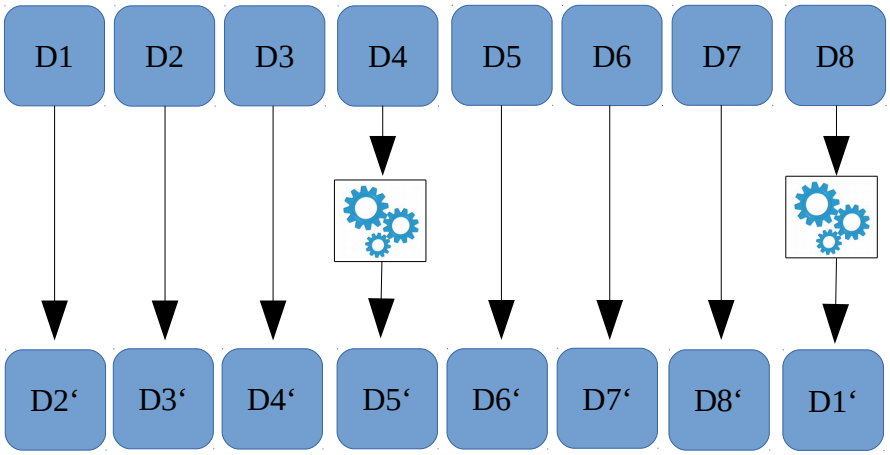

Bild 6: SHA-Algorithmus

Die Berechnung der Werte D4‘ und D7‘ erfolgt noch auf eine differenziertere Weise, indem die Eingabewerte in den Mechanismus mit integriert werden (siehe Bild 7).

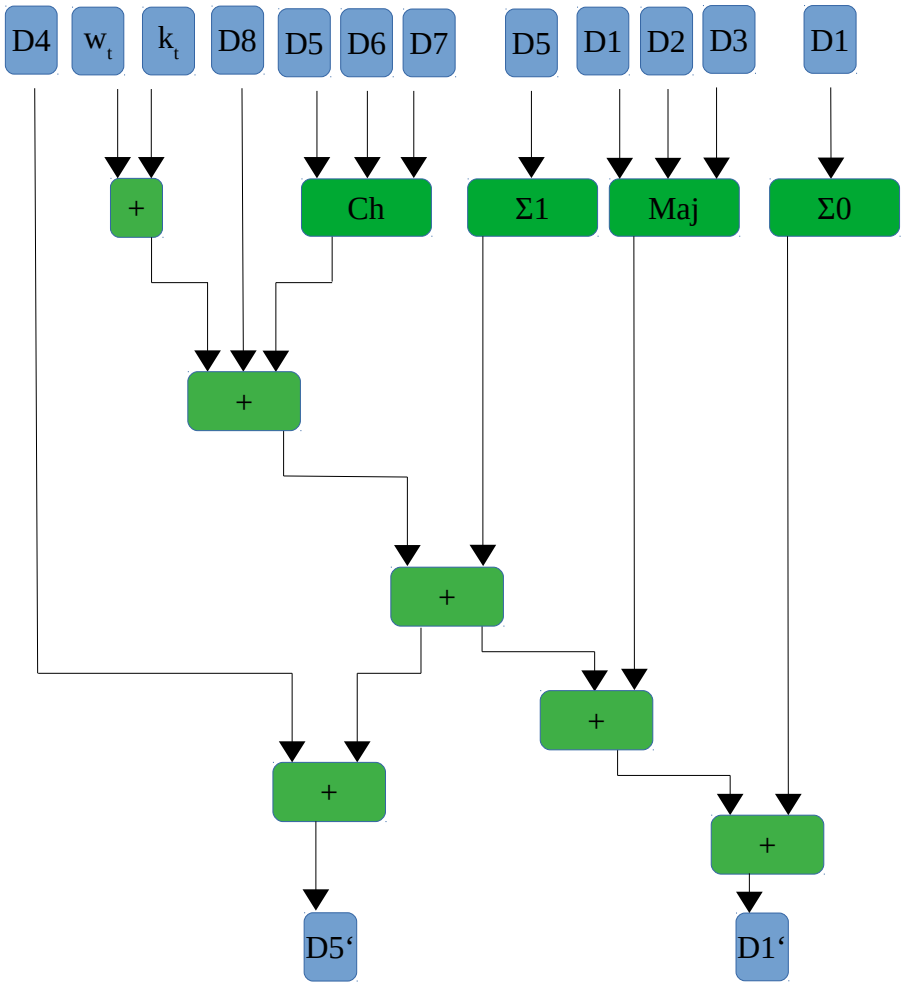

Bild 7: Berechnungen bei SHA

Der SHA-Algorithmus setzt bei der Berechnung auf die Funktionen ‚Choose‘, Σ0, Σ1 und Majority. Zunächst erhält die Choose-Funktion die Zeichenketten von D5, D6 und D7 als Binärwerte übergeben. Die Choose-Funktion führt nun eine Vermischung der drei Binärmuster nach folgendem Schema durch:

1.) Ansehen des ersten Bits von D5.

2.) Falls das erste Bit von D5 eine Eins darstellt, dann erhält die erste Stelle der Ausgabe das erste Bit von D6.

3.) Falls das erste Bit von D5 eine Null enthält, dann erhält die erste Stelle der Ausgabe das erste Bit von D7.

4.) Die anschließende Bearbeitung erfolgt nun analog für jedes Bit einzeln.

Der Algorithmus von Σ1 wird so durchgeführt, dass D5 als Eingabewert dient. Der Eingabewert wird danach dreimal einer Rotation unterzogen. Dies geschieht, indem der Eingabewert einer Rechtsverschiebung um sechs Stellen unterzogen wird. Im nächsten Schritt wird eine Rechtsverschiebung um elf Stellen durchgeführt. Im dritten Schritt findet noch eine Rechtsverschiebung um 25 Stellen statt. Die so berechneten drei Teilergebnisse dienen im nächsten Schritt dazu, eine Überprüfung der ersten Bit-Stelle eines jeden Teilergebnisses zu veranlassen. Bei einer ungeraden Anzahl von Einsen wird an erster Stelle des Ausgabewertes eine Eins ausgegeben. Ergibt das Resultat eine gerade Anzahl an Einsen, so wird eine Null an die erste Stelle des Ausgabewertes gesetzt. Analog verhält es sich mit der weiteren Abarbeitung der übrigen Stellen. Die gleiche Berechnungsmethode gilt für die Σ0-Funktion. Dabei wird D1 als Eingabewert verwendet und finden entsprechende Rechtsverschiebungen um 22, 13 und 2 Bit statt. Bei der Majority(Maj)-Funktion werden die Eingabewerte von D1, D2 und D3 benutzt. Um eine Eins an der ersten Stelle des Ergebnisses zu erhalten, müssen bei den drei Eingabewerten mehr Einsen an der ersten Stelle stehen. Die Berechnung der weiteren Ausgabewerte erfolgt stellenweise analog. Die Resultate fließen direkt in 32-Bit-Operationen. Dabei findet zunächst eine Addition von D8, dem Resultat der Ch-Funktion und der Summe von w_t und k_t statt. w_t ist eine Variable, deren Inhalte vorab in 64 Teile mit einer Größe von je 8 Bit aufgeteilt wurden. k_t symbolisiert eine Konstante. Das Resultat der Addition dieser drei Größen fließt in eine Addition mit dem Ergebnis der Σ1-Funktion. Anschließend wird eine Addition mit dieser neu berechneten Summe und D4 durchgeführt. Ebenfalls wird zu dieser neu berechneten Summe die Summe der Majority-

Funktion hinzuaddiert. Das neu entstandene Resultat wird dem Ergebnis von Σ0 addiert, um daraus den Wert für D1‘ abzuleiten. Die acht so gebildeten Ausgabewerte D1‘ bis D8‘ fließen in einer weiteren Runde als Eingabewerte D1 bis D8 ein. In Summe werden 64 Runden abgearbeitet. Ist die Berechnungsvorschrift 64-mal durchgelaufen, so werden die acht Datenblöcke zu einem 256-Bit-Ausgabebithashwert zusammengefasst.

Angriffsmöglichkeiten

Es wurden bereits wissenschaftliche Versuche unternommen, Urbild- oder Kollisionsangriffe gegenüber der SHA-2-Familie beziehungsweise SHA-256 durchzuführen [31]. So führte [32] bei SHA-256 erfolgreich einen deterministischen Kollisionsangriff in reduzierter Rundenzahl durch. Dabei kann zu einem bekannten Klartext und einem verschlüsselten Text der Schlüssel in 24 Runden ermittelt werden. In [33] wird gezeigt, dass ein Urbildangriff bei 42 durchgeführten Runden zum Erfolg führt. Zudem wird in [34] ein weiterer Meet-in-the-Middle-Urbildangriff vorgestellt. Das SHA-256-Verfahren wird hier in 43 statt 64 Runden durchgeführt, so dass der Angriff erfolgreich verläuft. In [35] wird gezeigt, dass bei 46 Runden eine differentielle Kryptoanalyse durchgeführt werden kann. Die Biclique-Angriffsmethode wird bei maximal 52 durchgeführten Runden zum Erfolg führen [36]. Es sei darauf hingewiesen, dass SHA-256 für einen Durchlauf 64 Runden benötigt, bislang kein erfolgreicher Urbild- oder Kollisions-Angriff über die volle Rundenzahl von 64 bekannt ist und damit das Verfahren mit einer hohen Wahrscheinlichkeit als sicher eingestuft wird [37].

3.1.4 Keccak

Die Hashfunktion Keccak gewann 2012 einen von dem National Institute of Standards and Technology (NIST) durchgeführten Wettkampf und trägt daher den Name SHA-3. Die NIST hat in den Jahren danach kleine Änderungen des Algorithmus realisiert. Im Ethereum-Projekt wird dennoch am Ursprungsalgorithmus von 2012 festgehalten, da das Team um Ethereum versteckte Hintertüren des US-Geheimdienstes National Security Agency (NSA) befürchtete [38]. Keccak selbst wird in der Form eines „Schwammes“ realisiert [39]. Die Eingabewerte repräsentieren dabei die aufzusaugenden Inhalte und der Hashwert wird vom Algorithmus ausgedrückt. Keccak-256 führt zunächst die Definition eines internen 1.600 Bit großen Zustandes durch. Dieser 1.600 Bit große Zustand besteht aus der Kapazität und der Bitrate, wobei die Kapazität doppelt so groß ist wie der Ausgabehashwert. Bei Keccak-256 ist wie der Name bereits sagt der Ausgabehashwert 256 Bit groß, entsprechend weist die Kapazität eine Größe von 512 Bit auf. Die Kapazitätsbits sind verborgen, so dass eine Hashentnahme verhindert wird. Von den 1.600 Bits müssen die 512 Bits subtrahiert werden, um die verfügbare Bitrate von 1.088 Bits für den Hashwert zu ermitteln. Der Zustandsraum besteht aus Quader mit einer Länge von fünf, einer Breite von 64 und einer Höhe von fünf Blöcken. Grafisch entsteht so ein Quader, dessen Bits im Anfangszustand mit null festgelegt werden. Zunächst werden bei Start des Keccak-Algorithmus die 1.088 Nachrichtenblöcke gebildet. Falls eine Division der Nachricht durch 1.088 keine ganzzahlige Zahl zurückliefert, so füllt Keccak die Nachricht mit Werten passend auf. Zudem passt ein Block exakt zur entsprechenden Bitrate. Hierzu wird ein Block mit 17 64-Bit-Worten gebildet. Ein Ablegen der Worte ist nun deutlich vereinfacht, da der Block eine Länge von 64 Bit aufweist. Die

Durchführung sieht dabei vor, dass als erstes eine exklusives Oder-Verknüpfung (XOR) der Bits der Worte aus dem ersten Block mit den Bits des Quaders berechnet wird. Hier bleiben allerdings die Bits der Kapazität unberücksichtigt. Als Ergebnis wird ein Quader mit einem bestimmten Anfangszustand gebildet. Im nächsten Schritt wird das Hashing gestartet, indem dieses für die Keccak-Berechnung der Zustandsquader verwendet wird. Die Schwammfunktion von Keccak selbst wird in 24 Runden durchlaufen. Dabei wird pro Runde eine fünffache Permutation durchgeführt. Die θ-Permutation ist für die Invertierung eines jeden Bits des Zustandsquaders zuständig. Hierbei wird betrachtet, ob eine gerade oder ungerade Anzahl von Bits aus der Addition einer Spalte mit der jeweils vorherigen bzw. nachfolgenden Scheibe entsteht. Dabei stellt eine Scheibe ein 5x5 Bit großes Feld aus dem Quader dar. Die ρ-Rotation sorgt dafür, dass die sogenannten Bahnen nach einem bestimmten Ablauf durchlaufen werden. Damit wird eine Veränderung der Scheiben des Quaders erreicht. Eine Bahn entspricht 64 Bit in der Breite der erscheinenden Reihen des Quaders. Die π-Permutation führt einen Wechsel der Bahnen durch. Die innere Bahn bleibt davon unberührt. Sowohl die ρ- als auch die π-Rotation sind lineare Permutationen. Bei der χ-Permutation wird für jedes Einzelbit eine XOR-Operation auf die UND-Verknüpfung von a und b der jeweiligen Quaderzeile durchgeführt. Die Quaderzeile entspricht dabei einer 5 Bit großen längs verlaufenden Reihe des Quaders. Die τ-Funktion erfüllt insgesamt eine besondere Aufgabe, da diese die Symmetrien löscht. Es wird dazu eine Addition von 7 Bits mit einer 7 Bit großen Konstanten durchgeführt. Dieser Vorgang wird insgesamt 24-mal wiederholt.

Angriffsmöglichkeiten

Vom Keccak-Team werden auf der eigenen Website bekannte Angriffsmöglichkeiten angegeben. So wird aus dem Jahr 2019 ein Angriff in [40] gelistet, der bei lediglich vier durchlaufenden Runden der Schwammfunktion f als Urbildangriff durchführbar ist. Ein Kollisionsangriff aus dem gleichen Jahr wird in [41] aufgeführt, bei dem nach sechs durchgeführten Runden ein Kollisionsangriff simuliert werden kann. In [42] wird an den Ergebnissen des eigenen Keccak-Wettbewerbs zum Brechen des Algorithmus festgehalten. Dabei wird festgestellt, dass die beste Urbildangriffs-Lösung aus vier Runden besteht. Der beste Kollisionsangriff kann nach sechs durchgeführten Runden erfolgen. Auch hier ist erkennbar, dass es zwar theoretische Angriffsvektoren gibt, diese aber praktisch keine Bedeutung haben, wenn die Schwammfunktion wie vorgesehen 24-mal durchlaufen wird.

3.1.5 Troika

Mit der Entwicklung von Troika werden bestimmte Designziele verfolgt. So wird die folgende kryptografische auf SHA3-Keccak basierende Hashfunktion

$$h : F_3^* \rightarrow F_3^{243} \tag{3.10}$$

verwendet. Es handelt sich dabei um eine ternäre Hashfunktion, da die IOTA-Foundation zukünftig ternäre Prozessoren herstellen möchte. Auch hier handelt es sich um eine Schwammkonstruktion.

Dabei werden Eingabewerte beliebiger Länge auf Ausgabehashwerte von 243 Trits abgebildet. Ein Trit wird im Ternärsystem verwendet und stellt ein

Stellwertsystem zur Basis 3 dar. In einem herkömmlichen Ternärsystem kann ein Trit die Werte 0,1 oder 2 annehmen. Das IOTA-System wird als ein ausgeglichenes Ternärsystem verwendet, bei dem die Werte -, 0 und + als Digitalzeichen vorkommen. Ein Tryte besteht aus 3 Trits und kann entsprechend 27 verschiedene Zustände annehmen. Troika selbst wird als Schwammkonstruktion mit einer Rate von 243 und einer Kapazität von 286 Trits realisiert. Dabei werden die drei folgenden Sicherheitsaspekte berücksichtigt:

Urbild-Widerstand: Für einen gegebenen Ausgabewert y darf es nicht möglich sein, eine Umkehrfunktion zu finden, die zu den Eingabewerten x‘ führt. Es gilt damit y=h(x‘)

Zweiter Urbild-Widerstand: Für ein x mit der Funktion y=h(x) muss es unmöglich sein, x‘!=x zu finden und damit die Zuweisung h(x‘)=y zu ermitteln.

Kollisionen-Widerstand: Es darf nicht möglich sein, zwei verschiedene Eingabewerte x und x‘ zu finden, so dass h(x)=h(x‘) gilt.

Status Layout

Die Hashfunktion Troika arbeitet auf $x \in F_3^{9x3x27}$ Zuständen. Dabei ist ebenfalls folgende Festlegung für F erfolgt:

$$F_3 = \{0,1,2\} = \{0,1,-1\} \tag{3.11}$$

Angriffsmöglichkeiten

Wird die Troika-Hashfunktion mit einer Kapazität von ‚c‘ Trits instanziiert und einer zufälligen Permutation bei einer Ausgabelänge von $n = \frac{c}{2}$ Trits, so ergeben sich folgende Eigenschaften:

- Kollisionsangriff: Geringe Erfolgsaussichten für das Auffinden von Kollisionen, wenn weniger als $3^{n/2}$ Abfragen durchgeführt werden.

- Urbild-Angriff: Geringe Erfolgsaussichten, wenn weniger als 3^n Abfragen gestellt werden.

Dabei wird für n=243 festgelegt.

Werden die Eigenschaften der S-Boxen betrachtet, so ergibt sich eine differentielle Gleichförmigkeit von $\Delta s=3$. Damit beträgt die Möglichkeit einer differentiellen Kryptoanalyse bei den s-Boxen $\delta_s=3^{-2}\approx 2^{(-3,17)}$. Zudem führt ein Vergleich von zufälligen 3-Trits-S-Boxen zu dem Ergebnis, dass 10^7 solcher S-Boxen lediglich bei nur $\simeq 0{,}05\%$ die gleiche differentielle Uniformität von 3 besitzen. Es tritt keine S-Box mit einer differentiellen Uniformität von 2 auf. Vielmehr liegt der Durchschnitt der differentiellen Uniformität zwischen 5 und 6. Werden die Eigenschaften der Diffusionsschicht betrachtet, so ergeben sich bei einem dreidimensionalen Zustand von 9x3x27 Trits folgende eindimensionale Zustände von 729 Trits:

$$\bar{x}=[x_{0,0,0},\ldots,x_{8,0,0},\ldots,x_{8,1,0},\ldots,x_{8,2,26}]^T \tag{3.12}$$

Troika verwendet zur Vermischung der Spaltenparität einen entsprechenden Mixer:

$$\theta(A)=A+1_m^m AZ \tag{3.13}$$

1_m^m entspricht dabei einer $m\times m$ Matrix, wobei alle Elemente gleich 1 sind. Der Spaltenparitätsmixer θ stellt eine lineare Abbildung definiert durch eine quadratische Paritätsfaltungsmatrix Z dar. Es wird dabei der θ -Effekt von der Matrix Z auf eine Matrix A addiert. Im nächsten Schritt kann die Spaltenparität

als eine Art Spaltenparitätsmixer durch Ableiten der Paritätsfaltungsmatrix Z ausgedrückt werden:

$$Z = Z_{i,j}, Z_{i,j} \in F_3^{27\,x27}, 0 \leq i, j < 27 \tag{3.14}$$

Für $Z_{i,j}$ gilt dabei:

$$Z_{i,j} \begin{cases} Z_1 \, for \, i = j \\ Z_1^T \, for \, i \equiv (j-1) \, mod \, 27 \\ 0^{27\,x\,27} \, ansonsten \end{cases} \tag{3.15}$$

Bedingt durch die Struktur von Z ergibt sich damit die Matrix Z‘ wie folgt:

$$Z' = -Z \tag{3.16}$$

Die Matrix Z‘ stellt zwar die Paritätsfaltungsmatrix vom Spaltenparitätsmixer^{-1} dar, diese ist jedoch nicht die Inverse der Matrix Z. Der Grund liegt darin, dass die Matrix Z nicht von vollem Rank ist und daher nicht umkehrbar ist. Der Spaltenparitätsmixer^{-1} wird mittels der folgenden umkehrbaren Transformationsmatrix ausgedrückt:

$$M^{-1} = Z' + I \tag{3.17}$$

Angriffsmöglichkeiten auf den Tangle

Bekannte Angriffsszenarien zielen bei Kryptowährungen darauf ab, einen Double-Spend-Angriff durchzuführen. Dabei wird im Netzwerk zweimal die gleiche Transaktion versendet. Beim Waste-Money-Angriff zahlt ein Einzahler auf ein mit einem anderen Bundle kollidierendes Bundle ein. Dieses Bundle wird nicht angenommen, so dass die Kryptowährungseinheit verloren ist. Der Large-Weight-Angriff zielt darauf ab, eine große Rechenleistung im Netz einzusetzen. Im Fall von Troika wird $n = 243$ gesetzt.

3.1.6 BLAKE

Die kryptografische Hashfunktion BLAKE war ein Finalist des SHA-3-Verfahrens und findet Verwendung bei der Hashfunktion X11. BLAKE beinhaltet verschiedene Variationen für die Hashwerte von 224, 256, 384 und 512 Bits. Dabei wird auf Blockgrößen von 32 Bits für BLAKE-224 und BLAKE-256 und 64 Bits für BLAKE-384 und BLAKE-512 zurückgegriffen. Der Datenblock ist dabei 16 Wörter groß. Eine Nachricht erhält zusätzlich noch ein Abschlussbyte als Erweiterung. Diese erweiterte Nachricht wird in Blockgrößen von 512 bis 1024 Bits aufgeteilt. Blake gilt als sehr sicher und wurde lediglich mit deutlich reduzierter Rundenzahl angegriffen [45].

3.1.7 X11

Der X11-Hashalgorithmus gehört zu den Proof-of-Work-Hashfunktionen. Ziel bei der Entwicklung von X11 ist es, der speziellen Application Specific Integrated Circuit-Hardware (ASIC) zum Minen von Kryptowährungseinheiten den Prozess deutlich zu erschweren, so dass der Einsatz dieser Hardware nicht mehr lohnenswert ist. Gleichzeitig soll Benutzern das Schürfen von Kryptowährungseinheiten mittels Zentralprozessor (englisch Central Processing Unit CPU) und Grafikkarte (englisch Graphics Processing Unit GPU) ermöglicht werden. X11 kombiniert elf verschiedene Hashfunktionen in einem Algorithmus. Folgende Hashfunktionen werden in X11 verwendet: BLAKE, BLUE MIDNIGHT WISH (BMW), Grøstl, JH, Keccak, Skein, Luffa, CubeHash, SHAvite-3, SIMD und ECHO.

3.1.8 Scrypt

Scrypt wurde im Jahr 2010 veröffentlicht und gilt als Nachfolger der als unsicher eingestuften Verschlüsselungsfunktionen bcrypt und PBKDF2. PBKDF2 und bcrypt erwiesen sich bei Wörterbuchangriffen wie Brute-Force oder Rainbow-Tables als unzureichend. Der Grund ist, dass oftmals Schlüssel als Passwort verwendet werden, um daraus einen Hash-Ausgabewert zu erzeugen. Die Umkehrung der Hashfunktion ist zwar praktisch nicht durchführbar, jedoch können mittels Rainbow-Tables Eingabewerte zu Hashwerten gefunden werden. Um das Ermitteln der Hashwerte zu erschweren, werden zusätzlich sogenannte Salt-Werte in der Berechnung der Hash-Ausgabewerte berücksichtigt. Dazu werden diese Salt-Werte einfach an den Eingabewert angehängt. Der Salt muss der Entschlüsselungsfunktion ebenso bekannt sein. Scrypt berücksichtigt neben der reinen algorithmischen Rechenzeit ebenfalls die spezielle verwendete Hardware für das Brechen der Passwörter und erhöht den Aufwand entsprechend. Zwar können die Hashfunktionen bcrypt und PBKDF2 die Berechnungen verlangsamen, jedoch wird dieser Effekt durch die Parallelisierung der Berechnungen wieder kompensiert. Scrypt verfolgt hier einen anderen Ansatz. Dazu wird der Arbeitsspeicher der Rechner berücksichtigt, indem Scrypt einen Vektor von 16 Megabyte Größe verlangt. Scrypt wird daher auch als sequentiell speicherintensiv bezeichnet.

3.2 Bewertung der kryptografischen Hashfunktionen

Die Bewertung von kryptografischen Hashfunktionen wird durch die beiden folgenden Eigenschaften Urbildangriff und Kollisionsangriff bestimmt. Bei einem sogenannten Urbild(Preimage)-Angriff wird die verwendete kryptografische Hashfunktion angegriffen, indem zu einem Hashwert ein weiterer Eingabewert gesucht wird, der denselben Ausgabehashwert erzeugt. Ein Kollisionsangriff greift ebenfalls die Hashfunktion an, indem zu einem festgelegten Hashwert zwei verschiedene Eingabewerte gesucht werden. Die gewählten Eingabewerte sind vom Angreifer frei wählbar [46]. In der folgenden Tabelle 2 wird die Bewertung der kryptografischen Hashfunktionen, die beim Mining zum Einsatz kommen, dargestellt:

Hashfunktion	Sicherheitsanalyse	Bewertung
SHA-256	- Bis 2023 Anwendung empfohlen [46]. - Komplexität des besten Angriffs liegt bei 2^{128}. - Größe des Hashwertes liegt bei 256 Bit. - Findet Verwendung bei Kryptowährungen wie Bitcoin. - Folgt der Merkle-Damgård-Konstruktion.	+

Keccak-256	- Urbild-Angriff: Bester Angriff nach vier Runden realisiert mit folgenden Parameterwerten: r=1440, c=160, 4 Runden [48] - Kollisions-Angriff: Angriff nach sechs Runden erfolgreich mit den folgenden Parameterwerten: r=1440, c=160, 6 Runden [49]. - Findet Verwendung bei Kryptowährungen wie Ethereum. - Kleinere Versionen und Varianten von Keccak-256 sind deutlich schwerer zu brechen. Diese verfügen zwar über einen kleinen Zustandsraum, weisen aber gleichzeitig einen deutlich reduzierten Freiheitsgrad in Bezug auf die Kapazität auf. - Folgt der Schwammkonstruktion.	++

Scrypt	- Ein theoretischer Seitenkanalangriff ist bekannt [46]. - Je nach Passwort entstehen verschiedene Zugriffszeiten beim Vektor auf den Speicher. Das anschließende Hochzählen kann theoretisch für ein Passwort-Sieb verwendet werden. - Bei niedrigen Parametern ist Scrypt offenbar besser angreifbar als andere Hashfunktionen [50].	+
CryptoNight [51]	- Ist ein vergleichsweise neuer Hashing-Algorithmus aus dem Jahr 2013. - Nach eigenem Review keine großen Probleme erkannt. - Noch keine öffentlichen Wettbewerbe zum Brechen des Algorithmus gestartet. - Sehr große Schlüssel werden verwendet.	o
X11	- Verwendet elf verschiedene Hashfunktionen - Wird allgemein als sicherste kryptografische Hashfunktion klassifiziert. - Mining ist nur über Grafikkarte und CPU möglich	++

Blake-256	- War Finalist des SHA-3 Auswahlverfahrens. - Wurde sehr gut von verschiedenen Forschergruppen analysiert [52][53]. - Erfolgreiche Kryptoanalyse bei angesetzten acht Runden mit einer Komplexität von 2^{232} bewiesen.	+

Tabelle 2: Bewertung der kryptografischen Hashfunktionen

Neben den Hashfunktionen, die in verschiedenen Kryptowährungen verwendet werden, ist die Entstehung von Kryptowährungseinheiten von Bedeutung.

3.3 Kryptoagilität

Die Kryptoagilität bezeichnet einen Vorgang, bei dem von einem alten auf ein neues Verschlüsselungsverfahren umgestellt wird, indem das aktuelle eingesetzte Verschlüsselungsverfahren durch ein neues ersetzt wird [54][55]. Kryptoagilität kann mittels Hardfork der Kryptowährungen realisiert werden.

3.4 Entstehung von Kryptowährungseinheiten

Um in den Besitz von Kryptowährungseinheiten zu gelangen, können diese neben einem Kauf über Handelsplattformen mittels eines ‚Mining'-Prozesses hergestellt werden [56]. Es existiert keine zentrale Instanz, die neue Einheiten an ihre Teilnehmer ausgibt. Die Bezeichnung ‚Mining' entstammt dem Bergbau, da das Schürfen von Gold mit dem Erzeugen und Berechnen von

Kryptowährungseinheiten vergleichbar ist. Das Mining bei Kryptowährungen bezeichnet einen Prozess, bei dem die innerhalb des Netzwerkes entstandenen Transaktionen von Kryptowährungseinheiten von den Sende- an die Empfangsadressen verarbeitet werden. Um einen besseren Durchsatz der Transaktionen und die Last im Netzwerk zu reduzieren, werden die Transaktionen in Blöcke zusammengefasst. Diese Blöcke müssen abschließend vom Netzwerk bestätigt und an das komplette Netzwerk versendet werden. Auf dem dezentralen Knoten wird die Blockchain anschließend um den neu bestätigten Block erweitert. Die Blockchain selbst stellt damit auch ein historisches Register aller jemals durchgeführten Transaktionen innerhalb des Netzwerkes dar. Je nach Kryptowährung wird das Erstellen von Blöcken innerhalb von mehreren Sekunden bis Minuten erledigt [57]. Nach dem Speichern einer Transaktion in einem Block erfolgt eine Bestätigung darüber. Danach ist eine Rückabwicklung der durchgeführten Transaktion nicht mehr möglich. Mittels der Einführung von freiwilligen Transaktionsgebühren wird die Bestätigung von Transaktionen im Netzwerk bevorzugt behandelt. Die Transaktionsgebühren müssen die Mining-Betreiber der Infrastruktur des Netzwerkes bezahlen [58]. In der Blockchain der jeweiligen Kryptowährung werden alle Transaktionen gespeichert. Die Blockchain selbst stellt eine dezentrale Datenbank dar und wird auf allen Rechner der Netzwerkteilnehmer abgelegt. Damit keine einzelnen Teilnehmer des Netzwerkes versuchen, diese zu manipulieren, wird ein Schutzmechanismus während des Minings angewendet. Ein Teilnehmerrechner des Netzwerkes, der sich am Mining mittels spezieller Software beteiligt, muss eine vom Netzwerk mathematisch gestellte Aufgabe auf Basis der letzten Transaktion lösen [59]. Erst wenn dieser Teilnehmerrechner als Erster im Netzwerk die Aufgabe gelöst hat, werden diesem neue Kryptowährungseinheiten als Belohnung zugeteilt. Dazu

verwendet der Rechner einen Algorithmus, um daraus einen Schlüssel in Darstellung eines Hashwertes zu finden. Dieser Hashwert selbst wird aus der Liste der letzten Transaktionen und dem Hashwert des letzten hinzugefügten Blocks in der Blockchain erzeugt. Jedem neu generierten Block wird der Hashwert des Vorgängerblocks hinzugefügt. Damit ergibt sich eine Block-Kette, bei der die Hashwerte der Blöcke sich aus den Vorgängerblöcken berechnet haben [60]. Das Mining selbst legt fest, welche der gemeldeten Transaktionen in einen neuen Block und damit in die Blockchain übernommen werden. Manipulierte Transaktionen werden abgelehnt. Die Blockchain erfährt dagegen in einem bestimmten Rhythmus eine Aktualisierung in Form von neuen Blöcken, denen die Transaktionen zugewiesen sind.

3.5 Verwalten von Kryptowährungseinheiten

Eine öffentliche Blockchain bietet allen Teilnehmern im Netzwerk die Möglichkeit, jede durchgeführte Transaktion von anderen Teilnehmern einzusehen und durch die eigenen Miner zu bestätigen. Die Blockchain wächst durch die steigende Anzahl der Transaktionen stetig weiter. War es früher notwendig, die komplette Blockchain auf dem Rechner gespeichert zu haben, so existieren nun Lösungen, um die Transaktionen auch ohne Herunterladen der Blockchain zu ermöglichen [61]. Halten nicht genügend Teilnehmer die Blockchain dezentral auf ihrem Rechner, so wird das Netzwerk instabil. Zur Lösung des Problems werden bei einem Teil der Kryptowährungen sogenannte Masternodes verwendet, auf die an anderer Stelle noch eingegangen wird. In dezentralen Dateien wird die Blockchain verwahrt. Die Netzwerkteilnehmer müssen sich einig sein, welche Inhalte in der Blockchain abgelegt werden.

Dabei wird die Steuerung und Kontrolle der Inhalte der Blockchain nicht zentral durch eine autoritäre Instanz ausgeübt. Vielmehr wird in einem dezentralen Kollektiv entschieden, welche Daten in der Blockchain abgelegt werden. Dazu wird ein Konsens im Netzwerk gefunden, der die Parameter im Bereich der Sicherheit und Wirtschaftlichkeit einer Blockchain prägt. Im Bereich der Kryptowährungen existieren fünf verschiedene Konsensmechanismen.

3.5.1 Konsensfindung mittels Proof-of-Work (POW)

Die erste bekannte Kryptowährung Bitcoin verwendet zur Konsensfindung das Proof-of-Work-Verfahren [62]. Zahlreiche andere nachfolgende Kryptowährungen haben sich zur Beweisfindung ebenfalls für das Proof-Work-Verfahren entschieden [63]. Das Verfahren POW besagt, dass zur Zuteilung einer Belohnung vorher eine Arbeitsleistung erbracht werden muss. Dieser Arbeitsnachweis erfolgt bei den meisten Kryptowährungen über den Vergleich von Hashwerten. Dabei muss der ermittelte Hashwert einer vom Netzwerk vorgegebenen bestimmten Schwierigkeitsstufe entsprechen. Die Schwierigkeitsstufe wird über die Anzahl von Nullen links beginnend des Hashwertes dargestellt. Die Ermittlung des Wertes durch die Netzwerkteilnehmer erfolgt in ‚Trial and Error'-Versuchen. Dabei werden zahlreiche Hashwerte berechnet, die sich bei einem möglichen Einfügen in den neu zu erstellenden Block unter einem gewählten Hashwert befinden. Die übrigen Teilnehmer prüfen, ob der gewählte Hashwert sich unterhalb des Schwellwertes befindet [64]. Je mehr Rechnerleistung im Netzwerk zur Verfügung steht, desto schneller kann der ermittelte Wert überprüft werden. Damit geht die Tatsache einher, dass beim Bereitstellen von Rechenleistung

durch eine große Anzahl an Teilnehmern die neuen Blöcke für die Blockchain ebenfalls zügig erstellt werden. Nachteilig wirkt sich aus, dass die Blöcke der Blockchain schnell errechnet wären. Um dies zu verhindern, wird ein dynamischer Schwierigkeitsgrad in die Software integriert. Dieser Schwierigkeitsgrad passt sich automatisch an die aktuelle Rechenleistung des Netzwerkes an. Dazu werden von der Software an den Anfang des Hash-Schwellwertes Nullen gesetzt. Je mehr Nullen sich am Anfang befinden, desto schwieriger wird die Kalkulation des Hashwertes für den neuen Block. Entsprechend steigt der Aufwand für die Generierung von zahlreichen Hashwerten, um einen Treffer unterhalb des Hash-Schwellwertes zu erhalten [65]. Wird mittels des Schwierigkeitsgrades vorgegeben, dass der neu zu errechnende Hashwert mit Null beginnen muss, so existiert eine Lösung mit null und neun falschen Antworten, die am Anfang Zahlen von eins bis neun enthalten. Wird der Grad der Schwierigkeit auf zwei Nullen am Anfang des Hashwertes angehoben, so existiert wieder nur eine Lösung mit einer Doppelnull. Dagegen sind bereits 99 falsche Möglichkeiten denkbar. Eine Rückberechnung auf den Ursprungshashwert ist nicht vorhanden, so dass die neuen Hashwerte nur mittels „Trial-and-Error“ gefunden werden können. Allen Kryptowährungen ist gemeinsam, dass diese über einen Schwierigkeitsgrad verfügen. Dieser wird je nach Kryptowährung unterschiedlich berechnet und angepasst. Das Bitcoin-System passt seinen Schwierigkeitsgrad an alle 2016 Blöcke an [66]. Dies entspricht einem Zeitraum von 14 Tagen. Bei anderen Kryptowährungen ist dieses Intervall oftmals kürzer [67]. Bei der richtigen Aufgabenlösung zur Berechnung eines validen Blocks wird diesem Block eine erste Transaktion mit der Belohnungsauszahlung in Form von Kryptowährungseinheiten zugewiesen. Die Belohnung in Form von Kryptowährungseinheiten wird dem Rechner mit der richtigen Lösung

zugewiesen. Damit wird deutlich, dass sich das Geldschöpfungssystem grundlegend von einem von der Zentralbank gesteuerten System unterscheidet [68]. Das Datenregister in Form der Blockchain und der dezentrale Aufbau des Peer-to-Peer-Netzwerkes substituieren die Zentralbank. Die Anwendung von asymmetrischen Verschlüsselungssystemen, bei denen der private Schlüssel im Besitz des Teilnehmers verbleibt und dieser gleichzeitig seinen öffentlichen Schlüssel mit den übrigen Teilnehmern teilt, gewährleistet die Anonymität der Teilnehmer [69]. Gleichzeitig sind deren durchgeführte Transaktionen von jedem einsehbar, ohne dabei allerdings die wahre Identität der Transaktionsteilnehmer zu kennen. Eine Gefahr für das Kryptowährungsnetzwerk besteht bei einer 51-prozentigen Bereitstellung von Rechnerleistungen aus einer Hand. Derjenige Teilnehmer könnte damit die Blöcke selbst berechnen und als gültig an die Blockchain hängen [70]. Dieses Risiko kann derzeit als gering angesehen werden, da die Kosten mit zunehmender Verbreitung von Miner-Hardware erheblich sind. Als Maßeinheit für die Rechnerkapazität wird ‚Hashes pro Sekunde' verwendet. Typische Schreibweise dafür ist ‚Hashwerte pro Sekunde (H/s)' [71]. Mit zunehmenden Zahlen von Teilnehmern steigert sich die Rechenleistung im Netzwerk der Kryptowährung. Reichen anfangs noch die CPU eines Computersystems aus, so werden zunehmend je nach Berechnungsmethode Grafikkarten oder spezielle ASIC-Chipsätze verwendet [72][73]. Durch die deutlich gesteigerte Leistung nimmt auch der Stromverbrauch drastisch zu. Das Bitcoin-Netzwerk verbrauchte 2018 rund 72 Terrawattstunden an Strom, was vergleichbar mit dem Energiebedarf von Chile ist [74]. Die erste Kryptowährung Bitcoin verwendet als Verschlüsselung den Secure Hash Algorithmus 256 (SHA256) [75]. Dabei handelt es sich um eine Einwegfunktion. Weisen zwei Nachrichten denselben Prüfwert auf, so sind die Nachrichten identisch. Zwei unterschiedliche Nachrichten erzeugen auch

unterschiedliche Prüfwerte. Zur SHA2-Familie gehören SHA224, SHA256, SHA384 und der SHA512 [76]. Die Bit-Länge des Hashwertes wird über die entsprechenden Zahlen nach dem Wort SHA dargestellt. Während Kryptowährungen wie Bitcoin auf den SHA-Algorithmus setzen, hat sich parallel dazu der Scrypt-Algorithmus entwickelt. Dieser wird zum Beispiel bei der Kryprowährung Litecoin verwendet. Der Scrypt-Algorithmus erschwert die Nutzung von spezieller Hardware wie die ASIC-Miner, indem die Rechenoperationen in den verhältnismäßig teuren Arbeitsspeicher verlagert werden [77]. Eine Weiterentwicklung von Scrypt ist der ScryptN-Algorithmus [78]. Dieser verfügt über einen anpassbaren N-Faktor, der im Laufe der Zeit ständig größer wird. Der N-Faktor stellt den Teil des RAM-Arbeitsspeichers dar, der für das Berechnen der Hashoperationen benötigt wird. Steigert sich der N-Faktor, so wird das Mining mittels Hardware wie ASIC-Miner oder Grafikkarten zunehmend ineffizient. Ein anderer Algorithmus ist das X11-Verfahren [79]. Bei diesem Algorithmus werden elf Hashfunktionen miteinander verbunden, so dass infolge ein Mining über die Grafikkarte oder CPU effizienter ist als über die spezielle ASIC-Hardware. Im Laufe der Zeit stieg der Schwierigkeitsgrad für das Mining besonders im Bitcoin-Netzwerk deutlich an. Grund war, dass die Anzahl der Miner ebenfalls stetig schnell wuchsen. Damit wurde das ‚Solo-Mining' unattraktiv, denn ein einzelner Akteur würde Jahre benötigen, um zumindest einmal die richtig Lösung für das gestellte Problem zu finden. Entsprechend haben sich Akteure zu sogenannten Mining-Pools zusammengeschlossen, um die einzelnen Hardwarekapazitäten zu bündeln [80]. Wird die Lösung des Mining-Pools gefunden, so teilen sich die an dem Pool beteiligten Akteure die Belohnung anteilsmäßig entsprechend ihrer zur Verfügung gestellten Hardwarekapazitäten.

3.5.2 Konsensfindung mittels Proof-of-Stake (POS)

Die meisten Kryptowährungen verwenden zur Lösung des gestellten Problems das bereits erwähnte Proof-of-Work-Verfahren.Kryptowährungen wie der Peercoin verwendet den Proof-of-Stake-Algorithmus [81]. Bei diesem Verfahren wird das Halten einer bestimmten Menge von Kryptowährungseinheiten in der eigenen Wallet über eine bestimmte Zeitspanne in Form von neuen Kryptowährungseinheiten belohnt. Ein Mix der beiden Berechnungsverfahren POS und POW verwendet die Kryptowährung Deutsche Elektronische Mark (DEM). Sobald sich ein Akteur mit der eigenen Wallet mit dem POS-Kryptowährungsnetzwerk verbunden hat, nimmt dieser am ‚Belohnungssystem' teil. Nach Erzeugen eines neuen Blocks wird an die Teilnehmer eine coinstake-Transaktion durchgeführt [82]. Dabei werden die vorhandenen Einheiten an die eigene Hashadresse versendet, erhöht um die Menge der neuen Belohnungseinheiten. Wie erkennbar ist, werden keine besonderen hohen Rechnerkapazitäten benötigt, um neue Einheiten zu generieren. Der Prozess zur Generierung neuer Einheiten wird im Proof-of-Stake als ‚Minting' bezeichnet [83]. Vom POS-Verfahren wurde der sogenannte Delegated Proof-of-Stake (DPoS) abgeleitet [84]. Beim DPoS vertrauen sich Benutzer gegenseitig, indem Transaktionen von diesen bestätigt werden. Dadurch werden diese als Zeugen bezeichneten Teilnehmer als besonders vertrauenswürdig eingeschätzt. Entsprechend erhalten diese die Belohnungszahlungen in Form von Kryptowährungseinheiten.

3.5.3 Konsensfindung mittels Proof-of-Activity (POA)

Im Proof-of-Activity (POA)-Verfahren veranlasst zunächst der Proof-of-Work eine Bestätigung eines Blocks durch eine festgelegte Anzahl von Teilnehmern mit einem entsprechenden Guthaben in ihrer Wallet im Kryptowährungsnetzwerk [85]. Durch diese Kombination von Proof-of-Work und Proof-of-Stake werden die bereitgestellten Rechnerkapazitäten als auch das in der Wallet vorhandene Kryptowährungsvermögen belohnt. Manipulationsversuche werden damit erschwert. Ein Beispiel einer Kryptowährung ist die Deutsche Elektronische Mark (DEM), die das Proof-of-Activity-Verfahren anwendet

3.5.4 Konsensfindung mittels Proof-of-Capacity (POC)

Beim Proof-of-Capacity(POC)-Verfahren werden die von den Minern bereitgestellten Festplattenspeicher berücksichtigt [86]. Der Speicher wird dabei in Plots berechnet und dem Mining-Netzwerk zur freien Verwendung übertragen. Je nach bereitgestelltem Speicherplatz für das Netzwerk erfolgt entsprechend die Belohnungsbezahlung. Das POC-Verfahren findet in der im Jahr 2014 gegründeten Kryptowährung Burstcoin Anwendung. Verwendungsmöglichkeiten außerhalb von Kryptowährungen finden sich in der Abwehr von Spam-Nachrichten und der Verteidigung gegen DDoS-Angriffe.

3.5.5 Konsensfindung mittels Proof-of-Importance (POI)

Die Kryptowährung NEM verwendet als Nachweisverfahren für die Blockberechnung den Proof-of-Importance(POI)-Algorithmus [87]. Teilnehmer müssen einen Minimalbetrag in ihrer Wallet halten, um damit als Node im

Netzwerk wahrgenommen zu werden. Damit nehmen die Teilnehmer am Verfahren teil, um den nächsten neuen Block zu bestätigen. Mittels Wahrscheinlichkeitsberechnung wird dabei der Teilnehmer ausgewählt, der den nächsten Block berechnet und damit die Belohnung in Form von Kryptowährungseinheiten erhält. In die Wahrscheinlichkeitsberechnung fließen neben der Anzahl der im Node hinterlegten Kryptowährungseinheiten auch die Transaktionen der letzten 30 Tage ein

3.6 Typen von Blockchains

Die beschriebenen Sicherheitsaspekte insbesondere durch eine damit einhergehende höhere Latenz und der große Energieaufwand zur Berechnung der Blöcke führen damit zu generellen Fragestellungen bezüglich einer Kategorisierung der Blockchain-Netzwerke [88].

Es kann eine Klassifikation der Blockchains nach privat, konsortial und öffentlich vorgenommen werden [89]. Insbesondere übernehmen in öffentlichen Blockchains die Miner die Aufgabe der Validierung von neuen Blöcken und deren Transaktionen. Blockchains im privaten bzw. konsortialem Umfeld verfügen über eine vorab ausgewählte Instanz, die einen neuen Block prüft und diesen entweder an die Blockchain anhängt oder ablehnt.

3.6.1 Öffentliche Blockchains

Derzeit richtet sich der Fokus bei der Betrachtung von Blockchains insbesondere auf monetäre Systeme. Lediglich das Ethereum-Netzwerk bietet mittels der Entwicklungssprache Solidity die Möglichkeit, auch sogenannte

Smart-Contract-Anwendungen zu entwickeln. Jedem Teilnehmer steht es frei, sich an öffentlichen Blockchains in Form von Transaktionen zu beteiligen [90]. Dabei sind die öffentlichen Blockchains in einem Peer-to-Peer-Netzwerk dezentral organisiert. Damit einhergehend hält jeder Knoten und Teilnehmer eine identische Kopie der Blockchain, die alle per Konsens-Algorithmus berechneten Transaktionen enthält. Die Berechnung der Transaktionen erfolgt mittels sogenannter Miner, die damit auch die Architektur im Netzwerk darstellen. Der kostenintensive Betrieb der Miner wird mittels eines Belohnungssystems attraktiv gestaltet. So wird für das Finden eines gültigen Blocks eine Belohnung im Fall des Bitcoin-Netzwerks in Form von Bitcoins ausgezahlt. Es können lediglich neue Transaktionen gebündelt in einem neuen Block an die Blockchain gehängt werden, eine Veränderung von alten Blöcken ist nicht möglich. Die Transaktionen selbst werden mittels des eigenen privaten Schlüssels signiert, so dass die Herkunft nachgewiesen wird. Über den Konsens-Mechanismus überprüfen sich die Teilnehmer in einem öffentlichen Blockchain-Netzwerk gegenseitig.

3.6.2 Private Blockchains und konsortiale Blockchains

In privaten und konsortialen Blockchain-Netzwerken ist eine Korrektur bereits erfolgter Transaktionen erlaubt [91]. Dazu werden bestimmte in einem privaten Blockchain-Netzwerk festgelegte Implementierungen und Regelungen realisiert und eingeführt. Eine vertrauenswürdige Instanz darf bei entsprechendem Bedarf die Korrektur vornehmen oder ermöglicht die Realisierung von Implementierungen zur Korrektur bestehender Blockchains. Der Zugang zum privaten Blockchain-Netzwerk ist zulassungsbeschränkt. Die am Markt erhältlichen Kryptowährungen weisen überwiegend öffentliche Blockchains auf.

Daneben drängen auch immer mehr Kryptowährungen wie LIBRA auf den Markt, dessen Blockchain-Zugang durch eine Instanz überwacht wird. Auf die bedeutendsten Kryptowährungen wird im Folgenden eingegangen.

3.7 Kryptowährungen

In den nachfolgenden Unterkapiteln werden die am stärksten kapitalisierten Kryptowährungen vorgestellt.

3.7.1 Bitcoin

Bitcoin wird als eine Peer-to-Peer-Netzwerkarchitektur im Internet strukturiert. Dabei bezeichnet der Begriff ‚Peer-to-Peer' (P2P) eine Architektur, bei der alle am Netzwerk angeschlossenen Rechner gleichgestellt sind [92]. Diese am Netzwerk beteiligten Rechner werden Knoten genannt. Die Knoten teilen sich die Last, um Netzwerkdienste anzubieten. Die Netzwerkknotenverbindung wird dabei in einem vermaschten Netz als flache Topologie realisiert. Es existiert damit keine zentrale Serverinstanz, die die Verwaltung der Teilnehmer übernehmen würde. Alle Teilnehmer des Netzwerks sind damit gleich berechtigt. Die Peer-to-Peer-Netzwerke sind zudem elastisch, dezentralisiert und offen. Die P2P-Netzwerke stellen damit ein gutes Beispiel einer Netzwerk-Architektur wie in den Anfangsjahren des Internets in der Realisierungsform eines vermaschten Netzes dar. Die heutige Internetarchitektur ist zwar hierarchischer, aber das Internet Protokoll hat noch seine Struktur aus den Anfangsjahren behalten. Neben dem Bitcoin existieren mit Napster und

BitTorrent weitere erfolgreiche Beispiele von P2P-Netzwerken [93]. Dabei stellt die Netzwerk-Architektur P2P des Bitcoins neben der Topologienwahl auch die Grundlage für dezentrales digitales Geld dar. Der Begriff ‚Bitcoin-Netzwerk' bezieht sich auf die Sammlung von Knoten, die das P2P-Bitcoin-System realisieren. Dazu wurde extra ein P2P-Protokoll innerhalb des Bitcoin-Systems eingeführt, um diese Funktionalität zu gewährleisten. Zusätzlich zum Bitcoin-P2P-Protokoll existieren noch andere Protokolle, um das Mining zu ermöglichen und um mobile Brieftaschen verwenden zu können [94].

3.7.2 Ethereum

Ethereum ist ein Kryptotoken, der als transaktionsbasierter Zustandsautomat betrachtet wird [95]. Dabei wird ausgehend vom Genesis-Zustand der Status durch Transaktionen verändert. Ethereum verwendet zudem die Datenstruktur Modified-Merkle-Patricia-Trie (MPT), die kombiniert wird aus dem bekannten Merkle-Baum und Patricia-Tie [96]. Die Schlüssel werden im MPT in Nibbles zerlegt, die ein halbes Byte an Daten speichern. Der MPT verwaltet die drei Knoten Branch, Leaf und Extension. Mittels des Knotentypen Branch kann der Pfad innerhalb des MPT bestimmt werden. Der Leaf-Knoten ist der unterste Knoten und verfügt in der nachfolgenden Hierarchie nicht über Kinderknoten. Der Leaf-Knoten stellt den Datenspeicher dar und enthält die zu speichernden Werte. Der Extension-Knoten dient dazu, die gleichen Aufteilungen der jeweiligen Schlüssel vorzunehmen, sofern diese zu gleichen Teilen bestehen.

Sicherheit bei Ethereum

Auch die Verwendung der Blockchain als weltweiter dezentraler Speicher sämtlicher jemals durchgeführten Transaktionen macht die Formulierung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Privatsphäre erforderlich. Wie sich gezeigt hat, können diese Ziele durch die Blockchain bei den Kryptowährungen erreicht werden. Allerdings hat der Ethereum-Initiator Vitalik Buterin darauf hingewiesen, dass die Verwendung der Blockchain-Technologien nur zwei der drei Eigenschaften Skalierung, Sicherheit und Dezentralisierung entspricht [97]. Es entsteht ein Dreieck, bei dem nicht alle Eigenschaften erfüllt werden können, wobei es auf die Schwerpunktsetzung ankommt (siehe Bild 8) [98].

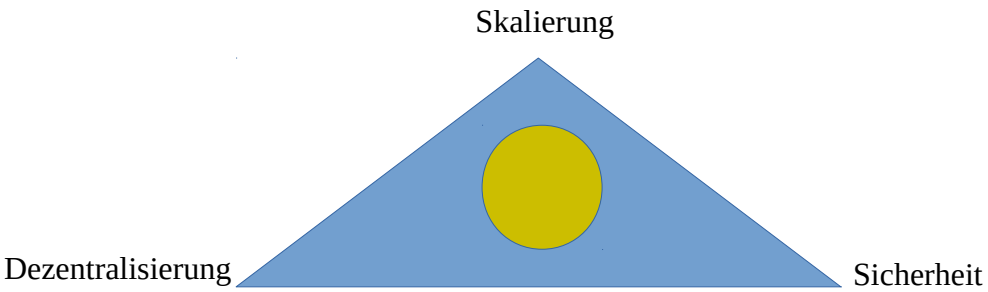

Bild 8: Trilemma

Die Blockchain-Technik hat sich seit 2009 als robust etabliert. Dennoch sind im folgenden beschriebenen Angriffsziele auf die Blockchain von Ethereum denkbar:

Dennoch sind die im folgenden beschriebenen Angriffsziele auf die Blockchain von Ethereum denkbar:

- Blockchain-Angriff: Hier versucht ein Angreifer mittels Double-Spending das Konsens-Verfahren auszutricksen [99]. So wird bei dem 51 Prozent Angriff

versucht, die Blockchain zu manipulieren. Der Angreifer kann die Transaktion rückabwickeln. Neue Blöcke anderer Teilnehmer können abgelehnt werden. Bei zwei Vorfällen wurden 51 Prozent Angriffe durchgeführt. So konnte der Mining-Pool Ghash.io mehr als 51 Prozent der Mining-Leistung im Bitcoin-Netzwerk für eine kurze Zeit bereitstellen. Im Jahr 2018 entstand bei der Kryptowährung Bitcoin Gold aufgrund des 51 Prozent Angriffs ein Schaden von rund 18 Millionen Dollar. Eine Verhinderung der 51 Prozent wird über die Umstellung des Konsens-Algorithmus Proof of Work auf Proof of Stake erzielt werden.

- Sybil-Angriff: Ein Angreifer erzeugt zahlreiche Identitäten, die dieser später kontrolliert [100]. Dabei erzeugt der Angreifer zahlreiche vollständige Knoten, die selbst aber nach außen hin unabhängig erscheinen. Mittels dieser Knoten werden andere Knoten im Netzwerk isoliert. Sybil-Angriffe sind verhältnismäßig leicht mittels Proof of Work abzuwehren, da die Kosten für die Reputation zu hoch sind. Sybil-Angriffe sind eher in kleinen Netzwerken denkbar, da die Kosten für das Erstellen der Knoten niedriger ausfallen.

- Race-Angriff: Hier startet ein Angreifer quasi zwei Transaktionen parallel. Bei jeder der beiden Transaktionen wird derselbe Output verwendet [101]. Jeder Empfänger erhält die Kryptowährungseinheit, ohne zu wissen, dass diese bereits in einer parallelen Transaktion verwendet wird. Sind die Empfänger beispielsweise Verkäufer einer Auktionsplattform, könnten diese geneigt sein, die Ware bereits an den Angreifer zu versenden. Allerdings wird sich nur eine Transaktion im Blockchain-Netzwerk durchsetzen. Einer der Empfänger wäre damit einem Warenbetrug aufgesessen. Abzuwehren ist ein Race-Angriff dadurch, dass seitens der Empfänger die Transaktion durch sechs Teilnehmer des Blockchain-Netzwerkes bestätigt wird.

- Finney-Angriff: Dieser nach dem Kryptografie-Experten Hal Finney benannte Angriff wird so durchgeführt, dass zunächst ein Miner einen Block kreiert. Diesem Block wird eine Transaktion zugewiesen [102]. Die bei der Transaktion angegebene Empfangs- und Senderadresse wird vom Angreifer kontrolliert. Der selbst erstellte Block wird nicht ans Blockchain-Netzwerk versendet, sondern vielmehr wird der Output an ein mögliches Opfer transferiert. Der Händler wird die Ware an den Täter versenden. Nun wird der Täter seinen selbst kreierten Block an das Netzwerk senden. Damit ist die Transaktion an den Händler invalide, schließlich wird der Output bereits in der Transaktion vorab verwendet. Der Täter hat damit einen Gewinn in Form einer erhaltenen Ware. Finney-Angriffe sind derzeit theoretisch, ein Empfänger eines Transaktionsbetrags kann hier ebenfalls auf die Bestätigung durch das Netzwerk warten.

- Denial-of-Service-Angriff: Die sogenannten DOS-Angriffe stellen auch bei Blockchain basierten Kryptowährungen ein großes Problem dar [103]. So kann versucht werden, Contracts-Accounts anzulegen. Das Löschen von Contract-Accounts führt zur Rücküberweisung der vorab bezahlten Gebühren. Das ständige Anlegen und Löschen von Accounts kostet dem Blockchain-Netzwerk zahlreiche Ressourcen. Aus diesem Grund werden die Größen bei neuen Blöcken limitiert. Zudem kann eine ressourcenlastige Aktion im Netzwerk auch für Nutzer entsprechend teuer sein.

- Selffish-Miner-Angriff: Bei diesem Angriff werden Proof-of-Work-Blockchains attackiert [104]. Bei diesem Angriff wird ein gefundener Block zum Beispiel in einem Mining-Pool geheim gehalten. Daraufhin wird bereits mit dem Mining des nächsten Blocks begonnen. Nach einer Weile wird dann die Kette neu erstellter Blöcke dem Blockchain-Netzwerk gemeldet.

- Sonstige Angriffe: Die Nutzer selbst können attackiert werden, indem Social Engineering eingesetzt wird, um Benutzer zu bestimmten Aktionen zu verleiten [105]. Auch Phishing-Angriff mit täuschend echt aussehenden Webseiten können Benutzer dazu verleiten, Account-Daten preiszugeben. Ein guter Schutz wird über Ledger USB Sticks erreicht, bei denen der private Schlüssel dorthin ausgelagert sind.

3.7.3 Ripple

Ripple will mit der eigenen zentralen Kryptowährung das Bank-Swift-Verfahren ablösen. Technologisch wird nicht eine dezentrale Blockchain versendet, sondern vielmehr setzt Ripple dabei auf einen Distributed Ledger [106]. Das Netzwerk von Ripple wird RippleNet genannt [107]. Mittels des RippleNets sollen die komplizierten Überweisungen zwischen verschiedenen Banken vereinfacht werden. Die Banken sollen dazu in Zukunft das Protokoll von Ripple verwenden. Ripple selbst unterhält über das eigenen Netzwerk die Kryptowährung XRP. Der Bezahlvorgang wird mittels der eigenen Schuldscheine ‚I owe u' (IOU) durchgeführt. Der Distributed Ledger führt als Register Buch über die getätigten Bezahlvorgänge.

Distributed Ledger

Die Verwaltung der Bezahlvorgänge erfolgt über einen Distributed Ledger. Der Ledger wird alle paar Sekunden aktualisiert und bleibt danach unverändert. Ist der Ledger gültig, so beinhaltet dieser den Status, eine Transaktionsliste, einen Zeitstempel und Hashwerte als Verifikation. Als Transaktionen werden Tracking-Knoten oder Validatoren versendet. Die Tracking-Knoten nehmen die Aufgabe

wahr, die Distribution der Clienttransaktionen vorzunehmen. Die Validatoren checken die Transaktionen auf Gültigkeit und kreieren eine neue valide Version von Ledger.

Ripple und Codius

Im Jahr 2014 wird in einem Whitepaper das Codius-Projekt vorgestellt. Mittels Codius sollen verschiedene Blockchains in andere Systemlandschaften integriert werden [108]. Codius-Verträge werden außerhalb einer Ethereum-Blockchain eingerichtet. Es ist auch möglich, die Contracts in verschiedenen Programmiersprachen zu entwickeln. Codius- Knoten sind billiger als zum Beispiel die Ethereum-Knoten.

3.7.4 Dash

Die Kryptowährung Dash basiert auf den Arbeiten von Satoshi Nakamoto, wobei Dash um einige Funktionen im Vergleich zum Bitcoin erweitert wird.

Masternodes bei Dash

Vollständige Knoten (Node) können als Übernahme der Serverfunktion angesehen werden. Darüber hinaus ist es möglich, Updates des kompletten Netzwerkes an die am Netzwerk angeschlossenen Parteien zu versenden. [109]. Bei Sinken dieser vollständigen Knoten laufen erhebliche Mengen an Datenverkehr und Ressourcen darüber, was enorme Kosten verursacht. Aus diesem Grund sinkt die Anzahl der Knoten innerhalb des Bitcoin-Netzwerkes. Gleichzeitig steigen die Blocklaufzeiten auf über 40 Sekunden. Es wurde ein neues Belohnungssystem und ein Anreizsystem vorgeschlagen [110]. Die Knoten dieses zweiten Netzwerkes, das auch Dash-Masternode-Netzwerk

genannt wird, gewährleisten den Zustand des Netzwerkes und führen eine Client-Synchronisierung der Netzwerkteilnehmer durch. Diese Knoten zeichnen sich durch eine hohe Verfügbarkeit aus und bieten dem Netzwerk das erforderliche Serviceniveau, um am Masternode-Belohnungsprogramm teilzunehmen. Ein wesentlicher Grund für den Rückgang der Anzahl der Knoten im Bitcoin-Netzwerk ist der fehlende Anreiz, einen Knoten zu betreiben. Mit der Zeit steigen die Kosten für den Betrieb eines vollständigen Knotens, wenn das Netzwerk mehr genutzt wird, wodurch mehr Bandbreite geschaffen wird. Wenn die Kosten steigen, konsolidieren die Betreiber ihre Dienste, um sie billiger laufen zu lassen, oder betreiben einen Light Client, der dem Netzwerk letztlich nicht hilft. Masterknoten sind wie im Bitcoin-Netzwerk vollständige Knoten, mit der Ausnahme, dass sie dem Netzwerk einen Servicelevel bereitstellen müssen und eine Sicherheitenanleihe in Form von Kryptowährungseinheiten besitzen müssen, um teilnehmen zu können. Die Sicherheiten verfallen nicht und sind während des Betriebs des Masterknotens sicher. Dies ermöglicht Masternode-Betreibern, einen Dienst für das Netzwerk bereitzustellen, die Bezahlung für ihre Dienste zu erhöhen und die Volatilität der Währung zu verringern. Um einen Masterknoten zu betreiben, muss der Betreiber die Kontrolle über 1.000 DASH nachweisen [111]. Wenn der Knoten aktiviert ist, bieten die Masterknoten den Clients im Netzwerk Dienste an und erhalten im Gegenzug eine regelmäßige Zahlung aus der Blockbelohnung. Wie beim Mining werden auch die Masterknoten aus der Blockbelohnung bezahlt. Dabei sind 45 Prozent der Blockbelohnung für die Masternode-Betreiber bestimmt. Aufgrund der Tatsache, dass das Masterknoten-Belohnungsprogramm einen festen Prozentsatz aufweist und die Nutzung des Masternode-Netzwerkes schwankt, variieren die erwarteten Masterknoten-Belohnungen entsprechend der aktuellen Gesamtanzahl der aktiven Masterknoten[112]. Zahlungen für einen Standardtag

zum Ausführen eines Masterknotens können mit der folgenden Formel berechnet werden:

$$\left(\frac{n}{t}\right)\cdot r\cdot b\cdot a \tag{3.18}$$

Die Variable n stellt dabei die Anzahl der Masternodes des Betreibers dar. Mit der Variable t wird die Gesamtzahl der Masternodes im Netzwerk ausgedrückt. Die Blockbelohnung wird mittels r (reward) präsentiert. Die Anzahl der Blocks wird über die Variable b bezeichnet. Die Variable a stellt die durchschnittliche Bezahlung für den Betrieb eines Masternodes dar. Hier liegt der Wert bei 45 Prozent der Blockbelohnung. Die mit dem Betrieb eines Masterknotens verbundenen Kosten verursachen eine harte und weiche Limitierung der aktiven Knoten im Netzwerk. Derzeit sind 8,2 Millionen DASH im Umlauf, damit können 8.200 Knoten im Netzwerk ausgeführt werden. Die weiche Limitierung wird durch den Preis für den Erwerb eines Knotens und die begrenzte Liquidität an den Börsen aufgrund der Verwendung von Dash als Währung festgelegt.

Sicherheit bei Dash

Wenn Transaktionen zusammengeführt werden, können Masterknoten möglicherweise das Guthaben der Benutzer während des Durchlaufs ermitteln. Dies stellt keine ernsthafte Einschränkung dar, da Masterknoten 1.000 DASH enthalten müssen und Benutzer zufällige Masterknoten verwenden, die sie zum Hosten ihrer Zusammenführungen auswählen [113]. Die Wahrscheinlichkeit, eine Transaktion während eines Verkettungsereignisses zu verfolgen, kann wie folgt berechnet werden:

Vom Angreifer kontrollierte Masternodes/ Gesamte	Kettentiefe	Wahrscheinlichkeit des	Benötigte

Masternodes im Netzwerk		Erfolges $(n/t)^r$	Dash
10/1.010	2	$9{,}80 \cdot 10^{-5}$	10.000
10/1.010	4	$9{,}60 \cdot 10^{-9}$	10.000
10/1.010	8	$9{,}51 \cdot 10^{-11}$	10.000
100/1.100	2	$8{,}26 \cdot 10^{-3}$	100.000
100/1.100	4	$6{,}83 \cdot 10^{-5}$	100.000
100/1.100	8	$4{,}66 \cdot 10^{-9}$	100.000

Tabelle 3: Verfolgungswahrscheinlichkeit einer Transaktion

Die Variable n speichert die Gesamtanzahl der vom Angreifer kontrollierten Knoten. Die Gesamtzahl aller Knoten wird mittels der Variable t ausgedrückt. Die Tiefe der Blockchain wird in der Variable r gespeichert. Die Auswahl der Masternodes erfolgt zufällig. Angesichts des begrenzten DASH-Angebots und der geringen verfügbaren Liquidität auf dem Markt ist es nahezu unmöglich, eine ausreichende Anzahl von Masterknoten zu kontrollieren, um bei einem solchen Angriff erfolgreich zu sein. Die Erweiterung des Masternode-Systems, die an der Transaktion beteiligten Masterknoten zu verbergen, erhöht die Sicherheit des Systems erheblich. Als Hashfunktion wird X11 verwendet [114]. Aufgrund der Komplexität und Chipgröße, die für die Erstellung eines ASIC für Mine X11 erforderlich ist, kann vermutet werden, dass dies erheblich länger dauern wird als beim Bitcoin. Dementsprechend kann eine große Anzahl von Nutzern über einen längeren Zeitraum hinweg am Mining teilnehmen. Diese Verbreitung und das Wachstum einer Kryptowährung wie Dash wird dadurch

leichter erfolgen.

3.7.5 Monero

Monero ist eine dezentrale Kryptowährung, bei der der Schwerpunkt auf privaten Transaktionen liegt [115]. Bei den meisten Kryptowährungen wie Bitcoin und Ethereum können die Transaktionen öffentlich nachvollzogen werden. Hier liegt eine Pseudonymität der beteiligten Teilnehmer vor. Um die Nachvollziehbarkeit zu vermeiden, verwendet Monero leistungsstarke kryptografische Techniken [116]. Monero ist dabei nach folgenden Prinzipien entworfen:

- Netzwerk-Dezentralisierung: Das Monero-Netzwerk und die Blockchain sind global verteilt. Es gibt keinen einzelnen Server oder keine einzelne Datenbank, die in böswilliger Absicht gehackt, kontrolliert oder zensiert werden kann. Wenn eine Regierung Monero-Knoten in ihrem Land schließen oder versuchen würde, zu begrenzen, wer Monero senden und empfangen kann, würde der Versuch vergeblich durchgeführt werden. Der Rest der Welt wird das Netzwerk unterhalten und weiterhin Transaktionen abwickeln.

- Finanzielle Sicherheit: Das Monero-Netzwerk ist durch kryptografische Mechanismen sicher, so dass ein verantwortlicher Intermediär entfällt. Jeder einzelne Monero-Teilnehmer kann die Gültigkeit des Ledgers selbst überprüfen, so dass nicht den Knotenoperatoren vertraut werden muss.

- Finanzielle Privatsphäre: Die meisten Blockchain-Systeme erreichen eine hohe Sicherheit auf Kosten der Privatsphäre. Monero legt jedoch großen Wert auf Privatsphäre ohne Sicherheitskonzessionen. Transaktionsbeträge,

Absender- und Empfängeridentität werden in der Blockchain verschleiert, so dass die getätigten Monero-Transaktionen nicht nachverfolgt werden können.

- Fungibilität: Der Begriff Fungibilität bezieht sich auf Vermögenswerte, deren Einheiten als nicht unterscheidbar und daher als austauschbar gelten [117].

Anonymisieren und Signieren bei Monero

Monero verwendet die Ringsignaturtechnologie, um die Privatsphäre des Absenders jeder Transaktion zu schützen. Eine Ringsignatur ist eine Art kryptografische Signatur, mit der ein aktiver Teilnehmer eine Nachricht im Namen einer Gruppe signieren kann [118]. Der private Schlüssel des aktiven Unterzeichners wird mit den Informationen des öffentlichen Schlüssels der anderen Mitglieder gemischt, um eine einzige Signatur zu erstellen. Jeder kann die signierte Nachricht anhand der öffentlichen Schlüssel validieren, um sicherzustellen, dass eines der Ringmitglieder die Signatur initiiert hat. Es ist jedoch nicht möglich festzustellen, von welchem Mitglied der private Schlüssel stammt. Im Kontext von Monero ist die Nachricht eine Transaktion, die durch die Ringsignatur autorisiert wird. Die Transaktion wird durch den privaten Schlüssel signiert und die öffentlichen Schlüssel von anderen Teilnehmern (von früheren Transaktionen) werden in die Signatur eingepreist. Der tatsächliche Unterzeichner und Täuschungsunterzeichner ist mathematisch gleich gültig. Die resultierende Ringsignatur kann nicht kryptografisch untersucht werden, um festzustellen, welches Mitglied die Signierung aktiv initiiert hat. Folglich kann keine externe Partei feststellen, welche der in einer Transaktion referenzierten Ausgaben tatsächlich getätigt wurden. Jede Ringsignatur erzeugt ein einzelnes Schlüsselbild, das von der tatsächlich ausgegebenen Transaktionsausgabe abgeleitet wird. Dies stellt einen kryptografisch sicheren Prozess dar. Jede

Transaktionsausgabe entspricht einem einzelnen Schlüsselbild und die Erzeugung des Schlüsselbilds lässt keine Rückschlüsse auf den ursprünglichen Unterzeichner innerhalb des Rings zu [119]. Als Beispiel für drei Ringmitglieder mit den öffentlichen Schlüsseln P1 und P3 und dem privaten eigenen Schlüssel p1 und der Nachricht M wird folgender Prozess beschrieben:

$$c_3 = H_s(M, uG, uHp(P_2)) \tag{3.19}$$

Dazu werden die Zufallszahlen s_3 und s_1 gewählt:

$$c_1 = Hs(M, s_3 G + c_3 P_{3,} s_3 Hp(P_3) + c_3 p_2 Hp(p_2)) \tag{3.20}$$

$$c_2 = Hs(M, s_{1G} + c_1 P_{1,} s_1 Hp(P_1) + c_1 p_2 Hp(P_2)) \tag{3.21}$$

$$c_3 = Hs(M, s_2 G + c_2 P_{2,} s_2 Hp(P_2) + c_2 p_2 Hp(P2)) \tag{3.22}$$

Durch die so gebildeten Ringsignaturen ist ein Rückschluss auf den echten Versender der Transaktion nicht möglich. Der Sender kennt seinen eigenen privaten Schlüssel, der durch die öffentlichen Schlüssel repräsentiert wird.

3.7.6 IOTA

Mit IOTA wurde eine neue Generation von Kryptocoin geschaffen, der skalierbar, dezentral und ein verteiltes Bestandsprotokoll beinhaltet. Ebenfalls wird die herkömmliche Blockchain durch den sogenannten Tangle abgelöst [120]. Dabei werden mittels dem Tangle die in der nachfolgenden Tabelle genannten Eigenschaften abgebildet (siehe Tabelle 4). Anders als bei der Blockchain gibt es beim Tangle keine Blöcke. Vielmehr stellt der Tangle einen quantenresistenten Direkten Azyklischen Graphen (DAG) dar. Damit wächst IOTA mittels der zunehmenden Transaktionen. Wie der Name IOTA bereits

verrät, wird IOTA für den Bereich der Kommunikation und Interaktionen von und zwischen Maschinen entwickelt (M2M). Weitere und zusätzliche Anwendungsgebiete neben dem Bereich der Mikrotransaktionen werden dargestellt:

Eigenschaft	**Beschreibung**
Modularität	Es besteht für andere Technologien die Option, sich mit IOTA zu verbinden.
Offener Quellcode	Im Internet ist der Quellcode offen einsehbar.
Keine Kosten	Die Transaktionen sind für die Nutzer von IOTA kostenlos.
Skalierbarkeit	Zahlreiche Transaktionen können pro Sekunde schnell durchgeführt werden. Das System hat durch vorhandene Skalierbarkeit keine Grenzen.
Dezentral	Auf eine zentrale Instanz und Intermediär wird verzichtet

Tabelle 4: Eigenschaften des Tangle

Transaktionsprozess bei IOTA

Der Tangle bei IOTA nimmt keine Unterscheidung von Benutzern und Validierung in Form der Miner vor. Vielmehr validieren alle Benutzer die vorliegenden Transaktionen, wie in [121] beschrieben wird. In [122] wird erläutert, wie ein automatisches System und den dazugehörigen Tangle-

Transaktionen aufgebaut werden kann.

Sicherheit bei IOTA

IOTA benutzt mittels des Tangles das Winternitz One-Time Signature Scheme [123]. Darüber wird eine erhöhte Sicherheit gegenüber Quantencomputern gesehen. Jedoch zeigt [124], dass weiterführende Versuche nötig sind, um die Sicherheit des Tangles zu überprüfen.

3.7.7 LIBRA

Die von Facebook und einem angeschlossenen Konsortium aus verschiedenen Unternehmen initiierte Kryptowährung LIBRA soll im Jahre 2020 an den Markt gehen. Dabei unterscheidet sich LIBRA fundamental von den anderen Kryptowährungen wie Bitcoin oder Ethereum [125]. LIBRA ist nicht dezentral organisiert, sondern wird von einem Konsortium um Facebook gesteuert und kontrolliert. Die LIBRA-Blockchain ist eine kryptografisch authentifizierte verteilte Datenbank und basiert auf dem LIBRA-Protokoll. Die LIBRA-Blockchain wird von einem verteilten Netzwerk von Validator-Knoten verwaltet, die auch als Validatoren bezeichnet werden. Die Prüfer halten sich gemeinsam an ein Konsensprotokoll, um eine Reihenfolge der Transaktionen in der Blockchain zu vereinbaren. Der Ledger von LIBRA hat einen Status, der sich ständig aktualisiert. Clients der LIBRA-Blockchain erstellen Transaktionen und senden diese an einen Validator-Knoten [126]. Ein Validierungsknoten führt (zusammen mit anderen Validierungsknoten) ein Konsensprotokoll aus, führt

die Transaktionen aus und speichert die Transaktionen und die Ausführungsergebnisse in der Blockchain. Validator-Knoten legen fest, welche Transaktionen in welcher Reihenfolge zur Blockchain hinzugefügt werden. Bezüglich des Themas Sicherheit von LIBRA wird betont, dass es die Erhöhung von weiteren privaten Schlüsseln die Sicherheit erhöht. Es wird auch darauf hingewiesen, dass erst die praktische Arbeit mit LIBRA zeigen wird, als wie sicher das System sich erweist. Bei den zahlreichen am Konsortium beteiligten Banken ist davon auszugehen, dass das Thema Sicherheit einen hohen Stellenwert einnehmen wird.

4 Applikationen mit Kryptowährungskontext

Die Blockchain kann außer für die Abbildung von Geldtransaktionen noch für andere Applikationen verwendet werden.

4.1 Klassifizierung der Kryptotoken

Kryptowährungen sind für das Bezahlen im monetären Bereich verwendbar und stellen damit eine Sonderform der Kryptotokens dar. Mittels der Kryptotoken sind andere auf der Blockchain basierende Applikationen realisierbar. Neben der Klasse der Kryptowährung können daraus zudem die Klassen Smart Property, Smart Contracts und die Kryptoassets gebildet werden (siehe Bild 9) [127]. Technisch müssen die Felder Legitimation, Integrität und die Transaktionskonsistenz gewährleistet werden. Auf Kryptowährungen wurde in den vorherigen Kapiteln bereits ausführlich eingegangen, so dass hier die Unterklassen Smart Property, Smart Contract und Kryptoasset betrachtet werden.

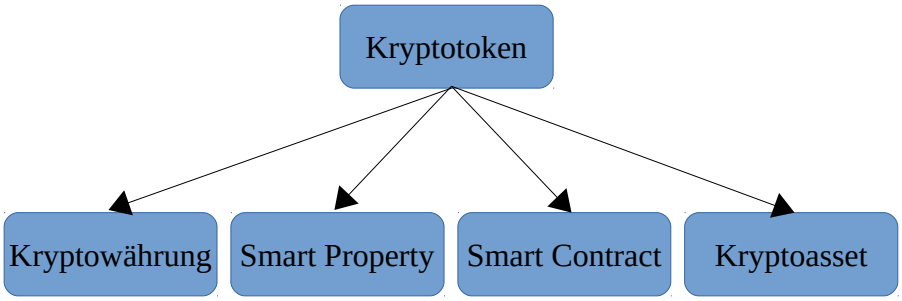

Bild 9: Klassifizierung von Kryptotokens

4.1.1 Smart Property

Mit Smart Property wird intelligentes Eigentum beschrieben, um damit bestimmte Werte in der Realwelt zu definieren und diese vertraglich festzuhalten [128]. Eine Verschiebung dieses Eigentums wird über die Blockchain dokumentiert. Als reale Objekte kommen immobile und mobile Gegenstände infrage. Smart Properties sichern mittels der Verwendung der Kryptografie auf der Blockchain jederzeit eine eindeutige Klärung der Besitzfrage zu. Hierzu gewährleistet die Rechtssicherheit in einem System diese Besitzfrage und ermöglicht den Zugang zu dem entsprechenden Objekt in der Realwelt. Prädestiniert für den Einsatz im Bereich Smart Property ist die Kryptowährung Ethereum. Mit dieser Kryptowährung kann mittels Programmiersprache eine Geschäftslogik zum Abbilden von Smart Property realisiert werden. Dabei befindet sich der Quellcode auf dezentralen Knoten im Netzwerk. Die Verwendung dieses Quellcodes schaltet den Intermediär wie zum Beispiel einen Notar bei Transfers von Immobilien aus.

4.1.2 Kryptoasset

Die Blockchains von Kryptowährungen wie dem Bitcoin dienen der Verwaltung von Finanztransaktionen [129]. Es fehlt daher eine Beziehung zu anderen Objekten, wie zum Beispiel zu Aktien. Wird ein spezieller Bereich zum Beispiel über eine Softwarelösung erzeugt, so ist die Beziehung zu dem entsprechenden Wertpapier real erschaffen. Damit geht ein Versprechen einher, dass mit der Zahlung der intrinsische Wert dem entgegensteht. Nun kann es passieren, dass eine der beteiligten Parteien den Vertrag nicht einhält. Zur Vermeidung derartiger Unstimmigkeiten werden Colored Coins eingesetzt.

Ausgewählte transaktionierte Bitcoins werden dabei besonders markiert. So werden die Besitzer von Bitcoins erkannt und kann der Vertrag über diese gefärbten Bitcoins eingehalten werden. Der kolorierte Besitzer der Bitcoin wird damit zu einem bestimmten Datum die Auszahlung erhalten. Über Ethereum können Kryptoassets leichter entworfen werden, da die Programmiersprache Solidity beliebige Geschäftsmodelle ermöglicht. Probleme können dabei insbesondere aufgrund von rechtlichen Regularien auftreten. So erweist sich beispielsweise der Ankauf von mehr als fünf Prozent aller Aktien als problematisch, da hier Meldeauflagen bestehen. Ein Verschleiern der Identität muss verhindert werden. Ebenfalls muss das Unternehmen mittels einer Gegensignatur Manipulationsversuche verhindern

4.2 Dezentrales Nachweisverfahren

Eine öffentliche Blockchain dient gleichzeitig auch dem Nachweis durchgeführter Transaktionen [130]. Eine Änderung dieses weltweiten dezentralen Registers ist nicht möglich. Wäre dies möglich, dann müssten auch die Blöcke neu berechnet werden. Aus diesem Grund sind die Transaktionen mit dem privaten Schlüssel des jeweiligen Besitzers des Schlüssels signiert. Jederzeit kann mittels öffentlichem Schlüssel die Signatur überprüft werden.

5 Proof of Concept anhand verschiedener Faktoren

Im fünften Kapitel werden Möglichkeiten vorgestellt, inwieweit im Umfeld der Kryptowährungen Anwendungen realisiert und verwendet werden können.

5.1 Programmierung und API-Anbindung

Die Nutzung der Programmierschnittstellen kann in zwei Kategorien aufgeteilt werden: Zum einen in Softwareentwicklungen, bei denen das Protokoll der jeweiligen Kryptowährungen implementiert wird. Zum anderen weisen mehrere Kryptowährungen die Möglichkeiten auf, eine eigene Geschäftslogik zu entwickeln und damit einen neuen Token zu entwerfen. Im Folgenden werden die Programmierbibliotheken für Bitcoin und Ethereum erläutert, ehe in einer Gesamtübersicht die anderen API der Kryptowährungen präsentiert werden.

5.1.1 BitcoinJ

Die BitcoinJ-Bibliothek stellte eine Implementierung des Bitcoin-Protokolls dar. Mittels dieser Bibliothek kann ein Bitcoin-Wallet verwaltet und können Transaktionen empfangen und versendet werden, ohne dabei eine Kopie vom Bitcoin Core mit der Blockchain lokal gespeichert zu haben [130]. Die Bibliothek selbst wurde in Java 7 entwickelt. Um die Bibliothek zu nutzen, kann die entsprechende Jar-Datei direkt, mittels Maven oder Gradle und über Git heruntergeladen werden. Die Verwendung der Bibliothek ist aus Java oder anderen JVM-Implementationen‘ wie zum Beispiel Python, Scala, Clojure, Kotling und Ruby möglich. Die BitcoinJ-Bibliothek verfügt über Logging- und

Assertation-Funktionen [131]. So kann beim Logging die Auswahl getroffen werden, ob zum Beispiel ein JDK-Logging oder ein Android-Logging bevorzugt wird. Innerhalb einer BitcoinJ-Anwendung werden die folgenden Klassen verwendet:

- NetworkParameters: Hier erfolgt die Festlegung, ob sich mit dem Test oder Produktion-Netzwerk verbunden wird.

- Wallet: Stellt eine Instanz zur Sicherung der ECKeys zur Verfügung. Dabei handelt es um das Interface ECKey, das einen Schlüssel aus dem elliptischen Verschlüsselungsverfahren repräsentiert.

- PeerGroup: Diese Klasse managt die Netzwerk-Verbindungen.

- BlockChain: Die Klasse BlockChain ist für die Verwaltung der verteilten weltweiten Datenstruktur verantwortlich.

- BlockStore: Bewahrt die Blockchain-Datenstruktur, wie zum Beispiel auf der Festplatte.

- WalletEventListener: Diese Klasse implementiert Wallet-Ereignisse.

Mittels BitcoinJ ist auch ein Auslesen der Blockchain möglich, um die Blöcke mit den Transaktionen beispielsweise in einer Graphdatenbank weiterzuverarbeiten (siehe Kapitel 5.3).

5.1.2 EthereumJ und Solidity

EthereumJ ist eine Java-Bibliothek, über die mit dem Ethereum-Netzwerk interagiert werden kann. EthereumJ bietet die Klasse ‚Ethereum‘ an, um mittels

dieser Facade den Zugriff auf das Ethereum-Netzwerk zu ermöglichen [132]. Der Verbindungsaufbau erfolgt über einen Node im Ethereum-Netzwerk. Dazu wird die gleichnamige Klasse ‚Node' verwendet, indem die IP-Adresse, der Port und die Nodeid verwendet wird. Ein Ethereumlistener-Adapter kann dazu implementiert werden, um Blockchain-Ereignisse abzufangen und zu verarbeiten. Die Klasse ‚Transaction' ist für das Transaktionsmanagement verantwortlich.

Die Sprache Solidity ist dafür gedacht, Geschäftsprozesse zu entwickeln und damit komplett neue Smart Contracts zu entwerfen. Dabei wird ein Skript mit dem Befehl ‚Contract' eingeleitet. Solidity selbst wird in Bytecode übersetzt. Dieser wird auf der Ethereum eigenen virtuellen Umgebung Ethereum Virtual Machine ausgeführt.

5.2 Übersicht der APIs und Protokollrealisierung

Anhand der vorgestellten Konzepte werden die Ergebnisse tabellarisch zusammengetragen (siehe Tabelle 5).

Kryptowährung / Token	Protokollrealisierung	API-Anbindung	Bewertung
Bitcoin	- BitcoinJ - Drittanbieter	- Nein, keine Möglichkeit zur Realisierung eigener Geschäftslogik im Bitcoin selbst.	+

Ethereum	- EthereumJ - Drittanbieter	- Ja, mittels Solidity kann die Geschäftslogik beliebig erweitert werden. So entsteht ein kompletter neuer Token.	++
Ripple	- Integrierte RippleAPI [133]	- Nein, keine Möglichkeit zur Realisierung eigener Geschäftslogik im Ripple selbst.	+
Dash	- Über die eigene Client-Bibliotheken DAPI.	- Nein, Dash ist für dezentrale monetäre Transaktionen vorgesehen.	+
Monero	- Mittels JSON RPC Aufrufe	- Nein, Monero ist für dezentrale monetäre Transaktionen vorgesehen.	+

IOTA	- Anbindungen für zahlreiche Programmiersprachen wie Javascript, Java, C#, Go und MAM.	- Über das Delion-Gateway sind eigene Entwicklungen unter Einbeziehung von Tangle möglich.	++
LIBRA	Mittels der eigenen Programmiersprache können transaktionsbasierte Anwendungen im LIBRA-Netzwerk entwickelt werden.	Die eigene Programmiersprache Move bietet auch Optionen, Smart-Contract-Anwendungen zu entwerfen.	++

Tabelle 5: Zusammenfassung der Kryptowährungen-APIs

5.3 Import der Blockchain in Graphdatenbanken

Die Netzwerke in der Informationstechnologie stellen Beziehungen von Sachverhalten dar. Dabei kann es sich um vermaschte Netzwerke wie das Internet, soziale Netzwerke wie Facebook oder auch Netzwerke von Transaktionen wie bei den Kryptowährungen handeln. Diese Netzwerke wachsen stetig an, so dass sich oftmals die Frage nach der effizienten Speicherung der Daten stellt. Zudem bilden sich in derartigen Netzwerken Beziehungen, die aufgrund eines gewünschten schnellen Zugriffs und der Verarbeitung der Daten ebenfalls abgespeichert werden [134]. Relationale Datenbanken speichern die entsprechenden Anwendungsdaten, die

Beziehungen werden allerdings erst während der Laufzeit über Joins gebildet, was die Leistung und Effizienz des Datenzugriffs bremst. Bei den Graphdatenbanken sind diese Relationen in der Datenbank selbst bereits vorhanden.

5.3.1 Vorhandene Benchmarks bei Graphdatenbanken

In einem Benchmark werden die drei Graphdatenbanken Neo4J, OrientDB und Titan miteinander verglichen [135][136][137]. Dabei werden vier Prozesse jeweils auf diese Datenbanken angewendet:

- Clustering: Hier wird die sogenannte Louvain-Methode angewendet [138].

- Zahlreiche Datensätze einfügen: Beim Messprozess wird die Graphdatenbank neu erstellt, die Konfiguration neu aufgesetzt, die Datensätze dazu geladen und eine Messung durchgeführt, um die Grapherstellung festzustellen.

- Einzeldatensatz einfügen: Zunächst erfolgt ein Aufsetzen der Graphdatenbank. Anschließend werden Einzeldatensätze geladen und nach jedem Einfügen eines Datensatzes mit ‚Commit' bestätigt. Dabei wird eine Zeitmessung von jedem Block durchgeführt, wobei ein Block aus 1.000 Knoten besteht.

- Abfrage: Bei diesem Test werden Abfragen über Kanten und Knoten so durchgeführt, dass anschließend der kürzeste Pfad zurückgeliefert wird.

Das Benchmark-Ergebnis wird in Tabelle 6 wiedergegeben. Dabei wird deutlich, dass das Graphdatenbanksystem Neo4J in Bezug auf große und zahlreiche Abfragen als Gewinner aus dem Benchmark hervorgeht.

Graphdatenbank/ Test	Clustering	Einfügen vieler Datensätze	Einfügen einzelner Datensätze	Abfrage	**Bewertung**
Neo4J	0	+	-	+	**+**
OrientDB	+	-	0	0	**0**
Titan	-	o	+	-	**-**

Tabelle 6: Benchmark der Graphdatenbanken

Für die Implementierung und den Import von Kryptowährungsblockchains auf das Graphdatenbankensystem wird daher auf Neo4J zurückgegriffen.

5.3.2 Import der Bitcoin-Blockchain

Die Blockchain des Bitcoins ist sequentiell gespeichert. Sämtliche Transaktionen der Vergangenheit werden in Blöcken organisiert, die chronologisch wie an einer Perlenkette miteinander verkettet sind. Suchvorgänge sind daher nach bestimmten Transaktionen mitunter nur schwer durchzuführen. Dies ist insbesondere dann der Fall, wenn Zusammenhänge von Transaktionen nachvollzogen werden sollen. Der Import der Bitcoin-Blockchain erfolgt dabei in zwei Stufen. Zum einen wird die Blockchain-Datei selbst blockweise ausgelesen. Danach können je Block die jeweiligen Transaktionen aus dem aktuell geladenen Block in den Speicher zur Weiterverarbeitung geladen werden. Die Weiterverarbeitung der jeweiligen Transaktion erfolgt, indem die Attribute der Transaktionen ausgelesen werden. Das sequentielle Abarbeiten der Blöcke erfolgt mittels der Bitcoinj-Bibliothek. Diese Bibliothek arbeitet mit dem Bitcoin-Protokoll und ist in Java realisiert [139]. Die Zugriffe auf die Datenbank werden über einen Neo4J-JDBC-Treiber

ermöglicht.

Kürzester Pfad

In Bild 10 wird die Neo4J-Datenbank mittels der Abfrage den kürzesten Weg zwischen zwei Transaktionen ermitteln und das Ergebnis an das grafische Interface der Neo4J-Datenbank zurückgegeben [140]. Dabei werden auch die dazwischenliegenden Blöcke angezeigt, woraus sich die ungefähre Zeit für die Transaktion ermitteln lässt. In dem hier vorliegenden Beispiel wurden ungefähr 30 Minuten zur Transaktionsabwicklung benötigt. Ein Block entsteht beim Bitcoin in jeder zehnten Minute. In der Farbe Grün wird jeweils eine Transaktionshashadresse abgebildet.

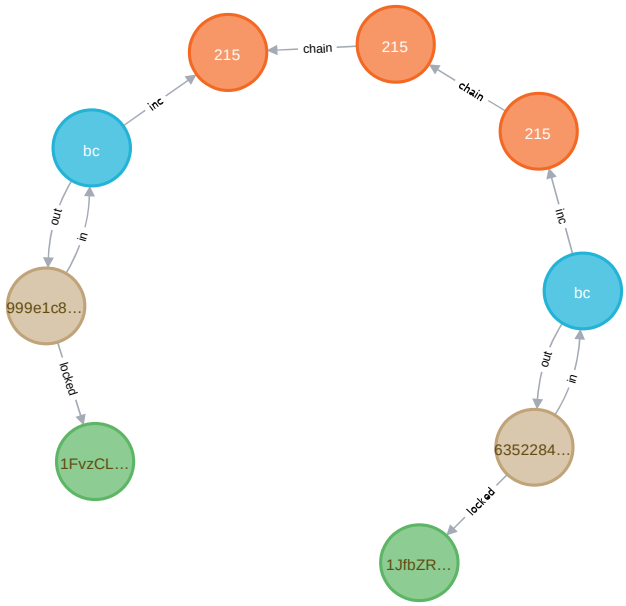

Bild 10: Kürzester Pfad

5.4 Recherchemöglichkeiten für Strafverfolgungsbehörden

Neben den selbst entwickelten Applikationen und dem Import der Blockchain von Kryptowährungen wie dem Bitcoin bietet das Internet auch eine Vielzahl an Recherchemöglichkeiten für Strafverfolgungsbehörden. Diese werden im Folgenden aufgeführt.

5.4.1 Maltego

Maltego ist eine proprietäre Software, die in den Bereichen Open Source Intelligence (OSINT) und Forensik verwendet wird [141]. Dabei hat die Entwicklungsfirma Paterva darauf geachtet, halbautomatisch Transformationen der Daten in andere Transformationen von Daten zu überführen. Der Benutzer startet mit einem Mausklick die Transformationen selbst. Diese Daten werden dabei grafisch aufbereitet und dem Ermittler angezeigt. So bietet die Software Maltego auch Transformationen für die Kryptowährungen Bitcoin und Ethereum an, die im Bereich von Ermittlungen zunehmend an Bedeutung gewinnen. In Bild 11 wird als Beispiel von der Bitcoin-Kryptowährungs-Hashadresse 1ENL6aS1oN2poUnvqUdCyb1EroPiLzG6p5 eine Transaktion durchgeführt. Die Transaktion zeigt als Empfängerhashadresse den Wert 1EgK47WCC98ifTZXaPNtf1iSkNvhJhJsfE an.

Bild 11: Bitcoin-Transaktion in Maltego

5.4.2 Online-Services

Im Internet werden verschiedene Online-Services zur Recherche angeboten. So kann auf den Seiten blockchain.info und Walletexplorer eine kostenlose Recherche gestartet werden [142]. Hier können neben Hashadressen auch gezielt Blöcke der Blockchain und zusammenhängende Transaktionen ge- und untersucht werden.

5.5 Empirische Untersuchungen von Kryptowährungen

Neben den Untersuchungen zu technischen Eigenschaften der verschiedenen Kryptowährungen bietet auch die Berücksichtigung von verfügbaren empirischen Studien Möglichkeiten, neues Wissen zu sammeln. So führte die Syracom AG im Jahr 2013 eine empirische Umfrage zu virtuellen Währungen durch [143]. Hierzu wurden Fragen an zehn Experten aus dem Finanzdienstleistungssektor gestellt. Die Experten waren in unterschiedlichen Unternehmensbereichen wie Forschung und Entwicklung oder Sicherheit tätig. Ziel der Befragung war es, insbesondere Aussagen zur Zukunftsperspektive von virtuellen Währungen, zu denen auch die Kryptowährungen gehören, zu erhalten. Im ersten Block werden Fragen zu Kenntnissen im Bereich der virtuellen Währungen gestellt. Die Fragestellungen zu virtuellen Währungen umfassen ein größeres Untersuchungsfeld, als dies bei Fragestellungen ausschließlich zu Kryptowährungen gestellt worden wären. Die Studie kategorisiert dabei folgende drei Typen:

1.) Typ 1 betrachtet die virtuellen Währungen, die lediglich im Rahmen eines bestimmten Computerspiels wie zum Beispiel World of Warcraft benutzt

werden. Eine Überführung in die reale Welt ist nicht möglich.

2.) Typ 2 stellt eine virtuelle Währung dar, die durch reale Geldvorgänge wie zum Beispiel den Wareneinkauf erzeugt wird. Diese virtuelle Währung kann nicht wieder in Realgeld umgetauscht werden.

3.) Typ 3 kategorisiert virtuelle Währungen, die in Realgeld und von Realgeld in die virtuelle Währung zurückgetauscht werden können.

Als Teilergebnis kann festgehalten werden, dass 90 Prozent der Befragten bereits über Wissen zu virtuellen Währungen verfügen. Im Vordergrund stehen bei den Befragten virtuelle Währungen, die in den verschiedenen Computerspielen verwendet werden. Die Studie hat diese Währungen bei der Befragung nicht zugelassen, sondern konzentrierte sich bei den Fragestellungen auf Kryptowährungen. Von den Befragten wird Kritik geäußert, dass die Kryptowährungen ohne jegliche Regularien am Markt erhältlich sind. Dies kann damit begründet werden, dass während der Finanzkrise viel Vertrauen in die Banken und Versicherungen verloren ging und die politische Stimmung eher zu einer stärkeren Regulierung des Bankensektors neigt. Die Befragung versucht auch, mögliche Zukunftsaussichten von Kryptowährungen zu ermitteln. Hierzu werden die Experten befragt, welchen Stellenwert die Kryptowährungen in der Finanzbranche einnehmen werden. Die befragten Experten vertreten die Ansicht, dass virtuelle Währungen sich langfristig durchsetzen werden. Zudem sind sich die Befragten der Studie sicher, dass die virtuellen Währungen erst verwendet werden, wenn durch technische und regulatorische Maßnahmen durch den Staat eine Vertrauensbasis geschaffen wird. Dabei betonen die Experten, dass Kryptowährungen durch die dezentrale Beschaffenheit verglichen mit dem Zentralbankensystem keine Stabilität

aufweisen. Bei Betrachtung der von den Fachexperten geäußerten Antworten muss das Jahr 2013 als Studienerhebung genannt werden. Unternehmen wie Paypal zeigen hohe Wachstumsraten in den letzten Jahren auf. Die Anzahl der mit Kryptowährungen durchgeführten Transaktionen steigt weltweit rasant an. Die Verwendung von Kryptowährungen hat sich vereinfacht. Es entstehen zudem zahlreiche Handels- und Tauschplätze, um Kryptowährungen zu erwerben oder zu veräußern. Kryptowährungen wie der Bitcoin zeigen an den Handelsplätzen eine große Volatilität. Je mehr Marktteilnehmer am Kryptowährungsmarkt partizipieren, desto schwächer wird diese Volatilität werden. Die Experten betonen ebenfalls, dass virtuelle Währungen im privaten Umfeld der Menschen weiter an Bedeutung gewinnen werden. Die Akzeptanz und implementierte integrierte Bezahllösungen beim Onlineshopping werden in diesem Zusammenhang als bedeutende Faktoren genannt. Die Experten sehen eine flächendeckende Verbreitung und Nutzung von virtuellen Währungen in zehn Jahren. Dabei wird eine Nutzbarkeit im Bereich von Micropayments gesehen. Als gegenwärtige Probleme sehen die Experten die verhältnismäßig hohen Hürden bei der Nutzung von virtuellen Währungen. Dazu konnten nur wenige Akzeptanzstellen ermittelt werden und zudem sind die Risiken bezüglich der Sicherheit nicht berechenbar. Seit dem Jahr der Befragung sind verschieden Sicherheitsvorfälle im Bereich von Kryptowährungen aufgetreten. So wurde die Tauschbörse MT.GOX angegriffen. Daraufhin führte Südkorea eine Regulierung für Kryptowährungen ein. Auch werden neue Lösungen im Bereich der mobilen Wallets für Kryptowährungen entwickelt. Die befragten Fachexperten betonen ebenso, dass sich neue Chancen für die Finanzbranche eröffnen. Dazu müssen die Banken die Position des vertrauensvollen Intermediär einnehmen und müssen virtuelle Währungen weiter an Bedeutung am Markt gewinnen. Gerade für kleine Finanzinstitute bieten sich Marktlücken

im Bereich von virtuellen Währungen. Die Banken sind zudem in der Lage, den neu entstehenden Markt mit frischem Kapital zu versorgen. Als Beispiel kann die Fidor-Bank angeführt werden, die erfolgreich mit der Bitcoin SE Gruppe auf der Plattform bitcoin.de zusammenarbeitet. Die befragten Experten sehen jedoch Gefahren für die Finanzbranche und benennen verschiedene Risiken. Dabei wird betont, dass das mobile Bezahlen in Kombination mit Verwendung einer virtuellen Währung erst als Risiko erkannt wird. Die Experten gehen davon aus, dass in Zukunft die Geldtransaktionen nur noch über mobile Endgeräte durchgeführt werden. Hier werden auch Geschäftsprozesse entwickelt werden, die das Bezahlen ohne Banken ermöglichen. Klassische Girokonten werden an Bedeutung verlieren, sobald sich Anbieter wie Paypal am Markt stärker behaupten werden. Ein Risiko ist es für den Finanzsektor auch, dass Non-Banks den Markt für virtuelle Währungen für sich entdecken. Die klassische Bankenwelt wird auch hier bedeutende Marktanteile verlieren.

5.6 Disruption bei Unternehmen, Organisationen und Behörden

Transaktionen mit Kryptowährungen werden überall in der Welt durchgeführt und weisen vergleichsweise geringe Transaktionsgebühren auf. Diese Eigenschaften stellen Unternehmen, Organisationen und Behörden vor große Herausforderungen. Entsprechend müssen Frühwarnsysteme eingerichtet werden, um eine schnelle Reaktionsfähigkeit auf die durch Kryptowährungen veränderte Transaktionsweise von Zahlungsmitteln zu gewährleisten.

5.6.1 Disruptive Geschäftsmodell durch die Blockchain

Mit dem Begriff ‚Disruption' wird das abrupte Verändern von Geschäftsmodellen bezeichnet. Fortlaufend entstehen neue Start-ups mit innovativen Ideen, die in Konkurrenz zu etablierten Unternehmen treten [144]. So sind bestimmte Innovationen derart disruptiv, dass komplette Geschäftsprozesse und Branchen sich verändern [145]. Als Beispiel können an dieser Stelle Airbnb und Uber genannt werden. Airbnb hat mit Vermittlung von Privatwohnung die Hotelbranche unter Druck gesetzt. Durch Uber steht das konventionelle Taxi-Geschäft unter Druck, da Privatfahrer selber Personen befördern und der Kontakt über die Uber-Plattform herstellt wird. Disruption ist nur von außerhalb des eigenen Geschäftsmodells möglich. Den Kryptowährungen und der dahinterstehenden Blockchain-Technologie werden disruptive Eigenschaften nachgesagt. Die Kryptowährungen bieten eine Alternative zum etablierten Finanzsystem an. Die Blockchain selbst wird Prozesse in allen Bereichen des wirtschaftlichen und behördlichen Lebens verbessern. Aus diesem Grund müssen Unternehmen, Organisationen und Behörden ein Innovations- und Technologiemanagement betreiben, um diese stattfindenden Disruptionen für sich verwendbar zu machen [146]. Zahlreiche Unternehmen der Finanzbranche haben erkannt, dass die Blockchain disruptive Attribute besitzt. Die Geschäftsprozesse der Bankenwelt werden sich durch die Blockchain-Register abrupt verändern. Smart-Contracts können die Wertpapier-Transaktionen und den Handel mit diesen abbilden. Bei den Versicherungen könnten disruptive Prozesse des Vertragsmanagements die Großversicherer zwingen, auch ihre eigenen Prozesse an die Blockchain anzupassen. Obwohl die Versicherungsbranche als eher konservativ in Bezug auf Veränderungen gilt, muss durch die zunehmende Disruption von Geschäftsprozessen auch hier

eine Verbesserung des Innovations- und Technologiemanagements einsetzen. Auch in der Strafverfolgung müssen die Prozesse an Innovationen angepasst werden. So ist es für Ermittler teilweise mit erheblichen Schwierigkeiten verbunden, entsprechende Transaktionen von Kryptowährungen nachvollziehen zu können. Hier sind entsprechende Schulungen angeraten, die auch ein Umdenken in Bezug auf das Geld- und Finanzsystem fördern. Ebenfalls wachsen die sogenannten Kryptominer, die eine neue Klasse von Malware darstellen. Die Unternehmen der Energiebranche versuchen, die Blockchain für die eigenen Geschäftsprozesse nutzbar zu machen.

5.6.2 Zukunftsaussichten bei Kryptowährungen

Das Beratungsunternehmen Deloitte führte im Jahr 2016 eine Befragung durch, welche möglichen Szenarien sich bei den Kryptowährungen ergeben können. Dabei wird von dem besten und ungünstigsten Szenario ausgegangen [147]. Zwischen diesen beiden Szenarien werden noch zwei weitere denkbare Trendszenarien aufgezeigt.

1.) Bester Fall: Das ‚Bester Fall'-Szenario beinhaltet den Erfolg der Blockchain-Technologie. Die Finanzverwaltung wird als ein allgemeines Gut betrachtet. Die Finanzbranche hat ihre Handelsplätze an öffentliche Blockchains verloren. Auch innerhalb der Contentindustrie wie Video- und Musikbranche ergeben sich große Veränderungen. Mittels einer ‚Medie-Blockchain' wird das digitale Recht von Medienerstellern gewahrt. Patientenakten werden zukünftig innerhalb einer Blockchain sicher geführt. Die durchgeführten Transaktionen von Kryptowährungseinheiten und Tokens werden sicher und zügig durchgeführt. Durch die lokale Energieerzeugung

entstehen dezentrale Energiehandelsplätze. Die Staaten der ‚Emerging Markets' partizipieren mittlerweile mittels der Blockchain und den Kryptowährungen vollständig am Welthandel. Die Blockchain hat damit eine weltweite Revolution gestartet.

Das ‚Bester Fall'-Szenario berücksichtigt, dass die Blockchain vollumfänglich in allen Bereichen des Lebens Einzug hält und die technischen Möglichkeiten der Blockchain genutzt werden. Die Blockchain-Technologie weist positive Erfolgsfaktoren auf. Dem stehen jedoch gewisse Risikofaktoren wie Volatilität, Anpassungsprobleme oder fehlende Regularien gegenüber. Für die Unternehmen, Organisationen und Behörden gilt daher, diese negative Faktoren und Risiken zu beseitigen. Nur so kann Schritt mit der technologischen Entwicklung gehalten werden.

2.) Schlechtester Fall: Im anderen ungünstigen Szenario schafft es die Blockchain-Technologie nicht, sich als eine führende Technologie zu etablieren. Die Investitionen in die Blockchain-Technologie entpuppen sich als Fehlschlag. Bitcoin selbst erlebt eine wachsende Beliebtheit. Es bestehen weiterhin die Probleme mit der Sicherheit gerade auf Handelsplätzen und bei der Skalierung von hohen Transaktionszahlen. Zudem steigt die benötigte Stromenergie weiterhin durch die Verschlüsselungstechnologien an, was auf Widerstand aufgrund der Klimawandel-Diskussion führt. Immer mehr Kriminelle entdecken Kryptowährungen zur Abwicklung ihrer Darknet-Geschäfte aufgrund fehlender staatlicher Regularien. Die Blockchain stellt damit kein geeignetes Mittel dar, um die herkömmlichen Bezahlsysteme abzulösen.

Das ‚Schlechter-Fall'-Szenario stellt die Entwicklungen bei Anhalten der Schwächen der Blockchain-Technologie dar. Eine große Community arbeitet

sehr akribisch daran, bestehende Skalierungs- und Sicherheitsprobleme von Kryptowährungen zu beseitigen. Handelsplätzen erhöhen signifikant ihre Sicherheit, um Fälle wie bei MT.Gox zu verhindern.

3.) ‚Überleben des Größten'-Szenario: Bei diesem Szenario setzt sich die Blockchain als Technologie weltweit durch. Unternehmen, Organisationen und Behörden erkennen die Blockchain-Möglichkeiten. Die Finanzbranche bleibt weiterhin am Markt und kann innovative Unternehmen im Bereich der Blockchain übernehmen. Von diesen neuen Unternehmen werden Blockchain-Softwareprodukte zu einem günstigen Preis an die Kunden gekauft. Die Unternehmen der Finanzbranche kooperieren miteinander und verabschieden gemeinsame Standards. Durch Kosteneinsparungen der Blockchain-Technologie wird die Effizienz in der Finanzbranche erhöht. In der öffentlichen Verwaltung ermöglichen Blockchain-Technologien automatische Prozesse. Im Bereich der Immobilienwirtschaft werden die Einträge im Grundbuch über ein Blockchain-Register abgebildet. Auch das Wählerregister wird mittels einer Blockchain sicher verwaltet, da die Verwendung einer Blockchain sich durch Sicherheit und Schnelligkeit auszeichnet.

Bei diesem Szenario wird deutlich, dass dieses sich aus Projekten der Finanzbranche ableitet. Bereits große Bankhäuser und Versicherungen testen die Blockchain auf ihre Verwendbarkeit im alltäglichen Geschäftsbetrieb. So wurde im Jahre 2016 ein gemeinsamen Projekt mit dem Namen ‚Blockchain Insurance Industry Initiative' von mehreren Versicherungsunternehmen ins Leben gerufen[2]. Ziel ist es, für die Versicherungsbranche weltweit Regularien und Standards für ein auf der Blockchain basiertes Vertragsmanagement festzulegen und dadurch Einsparungen in der Verwaltung zu erzielen. Im

[2] Vgl. https://b3i.tech, beteiligt u.a. Allianz, Swiss Re, Züricher Versicherung

Bankensektor arbeiten mehrere Bankunternehmen in einem gemeinsam Konsortium mit dem Namen R3 CEV zusammen. Ziel ist es hier, Zahlungstransaktionen deutliche zügiger und effizienter weltweit zu gestalten. Schätzungen gehen davon aus, dass die Verwendung der Blockchain-Technologie für die Finanzbranche ein Einsparungspotential von rund 20 Milliarden US-Dollar bedeutet (Vizepräsident und Head of Financial Services in Europa bei Infosys).

Ebenfalls führen Ermittlungsbehörden bereits Pilot-Projekte zur Identifizierung und Nachvollziehbarkeit von Zahlungsströmen der Kryptowährungen durch. Der Einsatz der Blockchain-Technologie kann Probleme mit sich bringen, an die noch gar nicht gedacht wurde. Zum einen können dies technologische Schwierigkeiten sein. Andererseits bestehen auch Risiken bezüglich staatlicher Eingriffe, die auf eine Regulierung bei den Kryptowährungen zielen.

4.) ‚Nischen'-Szenario: Im Nischen-Szenario ebbt die Hype-Stimmung bezüglich der Blockchain rasch ab. Zudem bestehen Probleme der Blockchain aufgrund von mangelnder Skalierungsmöglichkeiten. Ebenfalls vertrauen die Menschen dem Bankensystem seit der Finanzkrise nicht mehr. Der Banken- und Versicherungssektor ist dadurch stark verunsichert und radikale Änderungen müssen folgen, da die Menschen ansonsten zu Nicht-Geldinstituten und Zahlungssystemen wechseln. Die Blockchain wird daher insbesondere in Nischenbereichen eingesetzt, um damit Erträge zu erwirtschaften. Großbanken erkennen die Chancen beim Einsatz der Blockchain und können so große Teile innerhalb der Wertschöpfungskette abdecken. Am Markt etablieren sich ebenfalls Startups, die auch für die aufstrebenden Märkte den Zugang zum Kryptowährungsbereich ermöglichen.

Das Nischen-Szenario zeigt, dass die Blockchain-Technologie eine Marktnische nutzt. Es wird in diesem Szenario nur ein Teil der möglichen Applikationen durch die Blockchain substituiert oder erweitert. Derzeit haben bereits Start-ups in den aufstrebenden Märkten die Verwendung von Kryptowährungen ermöglicht. In diesen Ländern gibt es noch nicht die festen Strukturen wie in den großen Industriestaaten. Öffentliche Register können über eine Blockchain-Lösung daher leichter realisiert werden.

Die vier Szenarien zeigen, welche zukünftigen Entwicklungen im Bereich der Blockchain denkbar sind. Diese Szenarien können ebenfalls als Grundlage weiterer Prognosen für die Zukunft verwendet werden. Neben diesen qualitativen Aussagen kann es für Unternehmen lohnenswert sein, zusätzlich quantitative Prognosen durchzuführen.

6 Fazit

In dieser Master Thesis wurde ein Überblick über die einzelnen Faktoren Transparenz, Anonymität, Disruption, Dezentralität und Sicherheit in Bezug auf Kryptowährungen vermittelt. Auf Basis der Untersuchungen konnte folgendes in Tabelle 7 dargestelltes Ergebnis ermittelt werden.

	Transparenz	Anonymität	Disruption	Dezentralität	Sicherheit	Bewertung
Bitcoin	Ja	Pseudonym	Ja, mittel	Ja, hoch	Ja, hoch	+
Ethereum	Ja	Pseudonym	Ja, hoch	Ja, hoch	Ja, sehr hoch	++
Litecoin	Ja	Pseudonym	Ja, mittel	Ja, hoch	Ja, hoch	o
Ripple	Ja	Pseudonym	Ja, hoch	Nein, keine	Ja, hoch	++
Dash	Nein	Anonym	Ja, mittel	Ja, hoch	Ja, hoch	++
Monero	Nein	Anonym	Ja, mittel	Ja, hoch	Ja, hoch	+
IOTA	Ja	Pseudonym	Ja, hoch	Ja, hoch	Ja, hoch	+
LIBRA	Nein	Keine	Ja, hoch	Nein, keine	Ja, sehr hoch	o

Tabelle 7: Ergebnis nach den Faktoren

Die Kryptowährung Bitcoin hat durch eine hohe Marktkapitalisierung und Begrenzung auf maximal 21 Millionen Bitcoins eine hohe Akzeptanz bei den Benutzern von Kryptowährungen erlangt. Ethereum zeigt bereits als verhältnismäßig junge Kryptowährung, dass mit der Erweiterung über den monetären Bereich hinaus, Smart Contracts und selbst entwickelte Tokens

wirtschaftliche Prozesse stark verändern können. Der Litecoin, der gerne als Silber des Internets bezeichnet wird, befindet sich noch immer im Schatten von Bitcoin und wird es sicherlich schwer haben, eine vergleichbare Marktposition wie der Bitcoin zu erzielen. Ripple hat bereits namenhafte Investoren und Geschäftspartner an Bord und will das Swift-Verfahren durch den eigenen Ripple-Token ablösen. Dash verfügt als Proof of Work und Masternode-Kryptowährung über eine hohe Ausführungsgeschwindigkeit und geringe Kosten. Es ist daher auch hier von einer hohen Zukunftsaussicht von Dash auszugehen. Monero verwendet als Hash-Algorithmus CryptoNight, so dass im Gegensatz zum SHA-Verfahren eine speicherintensive Berechnung stattfindet. Moneros können entsprechend auf einer normalen Computerhardware über das Mining erstellt werden. Die Transaktionen werden durch die Nutzung der ‚RingCT'-Funktion verborgen. Damit wird die Akzeptanz auch von konservativen Computernutzern erhöht. IOTA wird stark in der Maschinenkommunikation zum Einsatz kommen. Zudem verfügt IOTA über eine hohe Skalierung. Die zunehmende Digitalisierung der Industrier wird die Nutzbarkeit von IOTA erhöhen. Die Kryptowährung LIBRA ist derzeit noch nicht realisiert. Die Nutzung über das soziale Medium Facebook und WhatsApp garantiert eine schnelle Verbreitung und Nutzung von LIBRA. Neben der allgemein günstigen Zukunftsaussichten der Kryptowährungen wird an dieser Stelle noch auf die anfangs erwähnten Fragestellungen eingegangen. Zunächst soll zusammenfassend beantwortet werden, welche Organisationen, Unternehmen und Behörden von Kryptowährungen und der dahinterstehenden Blockchain-Technologie betroffen sind. Dabei bleibt aufgrund der dargestellten empirischen Untersuchungen festzuhalten, dass Kryptowährungen allgemein in verschiedenen Organisationen, Branchen oder Unternehmen verwendet werden können. Hier muss allerdings in den Branchen aufgrund der Nutzung

und Akzeptanz unterschieden werden. Organisation oder Unternehmen, die hohen Wert auf soziale Interaktion legen, sind deutlich weniger für den Einsatz von Kryptowährungen geeignet als zum Beispiel die Finanzdienstleistungsbranche. Auch Behörden mit vergleichsweise starren Strukturen werden es schwer haben, Kryptowährungsprojekte zu realisieren. Auch wenn die Kryptowährungen bzw. Tokens bereits einen bemerkenswerten Erfolg verzeichnen können, so bleibt die Nutzung von digitalen Währungen nur auf einen kleinen Nutzerkreis begrenzt. Organisationen oder Unternehmen haben allerdings das Potential der Blockchain erkannt, so dass die Verbreitung von Kryptowährungen in der Zukunft zunehmen wird. Die Unternehmen erkennen Potentiale zur Steigerung der Effizienz, indem schnellere und günstige Transaktionen durchgeführt werden. Ebenfalls findet eine Automatisierung von Prozessen statt. Bei der Einsparung von Verwaltungskosten birgt die Blockchain-Technologie ein deutliches Potential. Zudem werden die Risiken im Bereich von Zahlungsausfällen und Wechselkursen reduziert. Die Anzahl der Delikte Betrug und Diebstahl werden gesenkt. Der Schutz der Daten und die Datensicherheit werden hingegen durch Kryptowährungen erhöht. Es besteht für Unternehmen und Organisationen die Gefahr, dass disruptive Geschäftsmodelle im Bereich der Kryptowährungen das alte Geschäftsmodell ablösen. Dabei steht die Technologie der Kryptowährungen und Tokens erst am Anfang. Die Gefahren von eigenen oder fremden disruptiven Geschäftsmodellen bestehen in technischen und juristischen Problemen. Entsprechend müssen bei technischen Problemen durch Neuerungen und Verbesserungen Adaptionen durchgeführt werden. Komplexer wird es bei den juristischen Problemen und Fragestellungen. Hier stellen sich Fragestellungen nach der Regulierung der Kryptowährungen durch den Staat und inwieweit diese Änderungen in die eigenen Prozesse des

Unternehmens oder der Organisation überführt werden müssen. Damit ergeben sich Empfehlungen für Unternehmen, Behörden und Organisationen, um aktuelle Abläufe an die neuen Geschäftsprozesse zu adaptieren. Im Unternehmensbereich der IT-Abteilungen muss das Thema Kryptowährungen in den Fokus gerückt werden. Die Entwicklung von Prototypen kann hier hilfreich sein. Sofern es sich dabei um eine strategische Ausrichtung handelt, so ist diese entsprechend mit hoher Priorität zu behandeln. Aus Sicht von Strafverfolgungsbehörden sind Lösungen zu entwickeln, die eine Nachverfolgbarkeit von Transaktionen der Kryptowährungen gewährleisten. Insbesondere Unternehmen sollten sich mit der Blockchain-Technologie auseinandersetzen, da dieser Technologie große Zukunftsaussichten bescheinigt werden. Smart Contracts können Unternehmensbereiche vollständig automatisieren und dem Unternehmen neue Bereiche aufzeigen. Für Behörden ergeben sich Möglichkeiten im Rahmen der Ermittlungsarbeit, diese mittels der Blockchain aufzuzeichnen und automatisiert in die Ermittlungsakte zu übernehmen. Dazu müssen die Ermittlungsbehörden in die Lage versetzt werden, Transaktionen von Kriminellen nachvollziehen zu können. Die Verwendung von APIs der Wechselbörsen für Kryptowährungen ist zu empfehlen. Es ist mit einer Softwarelösung und Identifikationsmerkmalen eines Täters realisierbar, die Transaktion einer Kryptowährung auf eine andere Kryptowährung zu verfolgen.

Literaturverzeichnis

[1] Nakamoto, Saftoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, URL: https://bitcoin.org/bitcoin.pdf, Bitcoin Foundation, November 2008, abgerufen am 1. Februar 2019.

[2] Holthusen, Jannis; Kufeld, Simon; Glatz, Florian: Vorstellung der Blockchain-Technologie, URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Vorstellung%20der%20Blockchain-Technologie.pdf, Deloitte, 2016, abgerufen am 02.Februar 2019.

[3] Leichsenring, Hansjörg: Bitcoin-Startups im Überblick, URL: https://www.der-bank-blog.de/bitcoin-startups-ueberblick/innovation/22048/, Der Bank Blog, 06.Juli 2016, abgerufen am 02.Februar 2019.

[4] Antonopoulos, Andreas M.: Mastering Bitcoin – Unlocking Digital Cryptocurrencies, O‘Reilly, 2015, S. 4f.

[5] Bordo, Michael D.: The Bretton Woods International Monetary System: An Overview. In: Michael D. Bordo, Barry Eichengreen: A Retrospective on the Bretton Woods System. The University of Chicago Press, 1993, S. 5.

[6] Irwin, Douglad A.: The Nixon shock after forty years: the import surcharge revisted. World Trade Review, 12, 2013, S.29-56.

[7] Hilton, Henry C.: Money Creation, Banks and Macroeconomic Instability, URL: https://www120.secure.griffith.edu.au/rch/file/5da3bb53-02d7-8d8b-f607-5fe161c14241/1/02Whole.pdf, S.50-52, Februar 2008, abgerufen am 07.Februar 2019.

[8] Kocherlakota : Money is memory, Federal Reserve Bank of Minneapolis, Research Staff Report, 1996, S.218.

[9] Ottersbach, T.: [Traditionelle Zahlungsverfahren, 2015]: 6.Teil: Leitfaden Ecommerce – Welche Zahlungsverfahren?, URL: https://www.ecommerce-vision.de/6-teil-leitfaden-ecommerce-zahlungsverfahren/, abgerufen am 16.Februar 2019.

[10] Braatz, Brinker, Friedrich: Zahlungsverkehr mit Karten, 1999, S. 5 und S. 85.

[11] Krüger M., Leibold K.: Internet-Zahlungen aus der Sicht der Verbraucher. In: Lammer T. (eds) Handbuch E-Money, E-Payment & M-Payment. Physica-Verlag HD, 2006.

[12] Vogel, M. (2016): Relevanz & Risiken von virtuellen Währungen am Beispiel von Bitcoin. In: Hofer akademische Schriften zur Digitalen Ökonomie. S.90-92. URL: https://opus4.kobv.de/opus4hof/files/69/HoferSchriftenDigitaleOekonomie_Bitcoin_Marion+Vogel_MM_VsfS.pdf. (Abruf am 04.08.2019).

[13] Sixt Elfriede: Vergleich zum herkömmlichen Finanzsystem. In: Bitcoins und andere dezentrale Transaktionssysteme. Springer Gabler, 2017, Wiesbaden.

[14] Europäische Zentralbank (2006): Durchführung der Geldpolitik im Euro-Währungsgebiet. Frankfurt. S. 93. URL: http://www.ecb.europa.eu/pub/pdf/other/gendoc2006de.pdf, abgerufen am 16.08.2019.

[15] Brandon, Hurst: How many people really own bitcoins – and why does it matter?. URL: https://www.businessinsider.com/heres-how-many-people-actually-own-bitcoin2014-3?IR=T, 2014, abgerufen am 27.08.2019.

[16] Rosenfeld, E. Bitcoin's 'bearwhale' and the future of cryptocurrency. URL: https://www.cnbc.com/2014/10/09/bitcoins-bearwhale-and-the-future-of-acryptocurrency.html, abgerufen am 01.07.2019-

[17] Dierksmeier, Claus; Seele, Peter. Cryptocurrencies and business ethics. Journal of Business Ethics, 2018, 152. Jg., Nr. 1, S. 1-14.

[18] Miller, Michael. Symmetrische Verschlüsselungsverfahren: Design, Entwicklung und Kryptoanalyse klassischer und moderner Chiffren. Springer-Verlag, 2013.

[19] Pommering, Klaus. Asymmetrische Verschlüsselung. URL: „http://www. staff. uni-mainz. de/pommeren/Kryptologie/Asymmetrisch/Asymm. pdf “, vom, 2009, 16. Jg.

[20] Rose, Chris. The evolution of digital currencies: Bitcoin, A cryptocurrency causing A monetary revolution. International Business & Economics Research Journal (IBER), 2015, 14. Jg., Nr. 4, S. 617-622.

[21] Douceur, John R. The sybil attack. In: International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002. S. 251-260.

[22] Menezes, Alfred J. Elliptic curve public key cryptosystems. Springer Science & Business Media, 2012.

[23] Koblitz, Neal. Elliptic curve cryptosystems. Mathematics of computation, 1987, 48. Jg., Nr. 177, S. 203-209.

[24] Laska, Michael. Punkte auf elliptischen Kurven über Q in quadratischen Zahlkörpern. Archiv der Mathematik, 1985, 44. Jg., Nr. 2, S. 159-167.

[25] Pote, Santoshi; SULE, Virendra; LANDE, B. K. Arithmetic of Koblitz Curve Secp256k1 Used in Bitcoin Cryptocurrency Based on One Variable Polynomial Division. 2019.

[26] Johnson, Don; Menezes, Alfred; Vanstone, Scott. The elliptic curve digital signature algorithm (ECDSA). International journal of information security, 2001, 1. Jg., Nr. 1, S. 36-63.

[27] Bitzer, Frank; Brisch, Klaus M. Digitale Signatur: Grundlagen, Funktion und Einsatz. Springer-Verlag, 2013.

[28] Silverman, Joseph H.: The arithmetic of elliptic curves. Springer Science & Business Media, 2009.

[29] Breitner, Joachim; Heninger, Nadia: Biased Nonce Sense: Lattice Attacks against Weak ECDSA Signatures in Cryptocurrencies, 2019, URL: https://eprint.iacr.org/2019/023.pdf, abgerufen am 17.09.2019

[30] NIST: Descriptions of SHA-256, SHA-384, and SHA-512, URL: https://web.archive.org/web/20150315061807/http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf, abgerufen a 17.09.2019.

[31] Bundesamt für Sicherheit in der Informationstechnik:Kryptographische Verfahren: Empfehlungen und Schlussellängen, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf;jsessionid=CF01D7351E4C07574024EC40A5F010C4.1_cid360?__blob=publicationFile&v=10, abgeufen am 10.09.2019.

[32] Sanadhya, Somitra K.; Sarkar, Palash: New Collision attacks Against Up To 24-step SHA-2, URL: https://eprint.iacr.org/2008/270.pdf, abgerufen am 01.07.2019.

[33] Aoki, Kazumaro, Guo, Jian, Matusiewicz, Krystian , Sasaki, Yu, Wang, Lei: Preimages for Step-Reduced SHA-2, URL: https://link.springer.com/content/pdf/10.1007%2F978-3-642-10366-7_34.pdf, abgerufen am 01.09.2019.

[34] Guo, Jian; Ling, San; Rechberger, Christian; Wang, Huaxiong: Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2, URL: https://eprint.iacr.org/2010/016.pdf, abgerufen am 15.08.2019.

[35] Lamberger, Mario, Mendel, Florian: Higher-Order Differential Attack on Reduced SHA-256, URL: https://eprint.iacr.org/2011/037.pdf, abgerufen am 01.06.2019.

[36] Khovratovich, Dmitry, Rechberger, Christian, Savelieva, Alexandra: Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family, URL: https://eprint.iacr.org/2011/286.pdf, abgerufen am 01.09.2019.

[37] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=7, abgerufen am 01.08.2019.

[38] Morawiecki, Pawel: Malicious Keccak. IACR Cryptology ePrint Archive 2015, 2015, S. 1085.

[39] Bertoni, Guido; et al. Keccak. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2013. S. 313-314.

[40] Bertoni, Guido; et al. Keccak sponge function family main document. Submission to NIST (Round 2), 2009, 3. Jg., Nr. 30.

[41] Ting, Li; SUN, Yao. Preimage Attacks on Round-Reduced Keccak-224/256 via an Allocating Approach. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2019. S. 556-584, URL: https://eprint.iacr.org/2011/037.pdf, abgerufen am 08.09.2019.

[42] Guo, Jian; et al. Practical Collision Attacks against Round-Reduced SHA-3. Journal of Cryptology, URL: https://eprint.iacr.org/2019/147.pdf, 2019, S. 1-43.

[43] Keccak-Team: The Keccak Crunchy Crypto Collision and Pre-image Contest, URL: https://keccak.team/crunchy_contest.html, abgerufen am 17.09.2019.

[44] Cybercrypt: Troika: a ternary hash function, 2018, URL: https://www.cyber-crypt.com/wp-content/uploads/2018/12/181214.iota_.troika-reference.v1.0.pdf, abgerufen am 01.09.2019.

[45] Aumasson, Jean-Philippe, Henzen, Luca, Meier, Willi, Phan, Raphael C.-W.: SHA-3 proposal BLAKE, URL: https://131002.net/blake/blake.pdf, abgerufen am 01.07.2019.

[46] Wenzel-Benner Christian; Wasserrab, Daniel: Kryptographische Hashfunktionen: Historie, Angriffe und aktuell sichere Standards, URL: https://pdfs.semanticscholar.org/b559/5b38e93d53c4db04b33066c11f3a3e81de59.pdf, abgerufen am 10.07.2019.

[47] Grembowski; Tim, et al.: Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512, URL:http://class.ece.iastate.edu/tyagi/cpre681/papers/sha-1HWISI.pdf, abgerufen am 01.08.2019.

[48] Liu, Meicheng: [CRUNCHY CONTEST] 4 rounds, width 1600, pre-image, URL:https://keccak.team/crunchy_mails/pre-r4-w1600-20161211.txt, abgerufen am 10.08.2019.

[49] Song, Ling Song; Liao, Guohong, Guo, Jian:[CRUNCHY CONTEST] 6 rounds, width 1600, collision, URL: https://keccak.team/crunchy_mails/coll-r6-w1600-20170226.txt, abgerufen am 11.08.2019.

[50] Därmuth, Markus; Kranz, Thorsten: On Password Guessing with GPUs and FPGAs, URL: https://www.mobsec.ruhr-uni-bochum.de/media/mobsec/veroeffentlichungen/2015/04/02/duermuth-2014-password-guessing.pdf, abgerufen am 04.09.2019.

[51] Noeter, Surae: REVIEW OF CRYPTONOTE WHITE PAPER, URL: https://downloads.getmonero.org/whitepaper_review.pdf, abgerufen am 05.09.2019.

[52] Guo, Jian; et al.: Analysis of BLAKE2, URL: https://eprint.iacr.org/2013/467.pdf, abgerufen am 30.08.2019.

[53] Chang, Sue-jen, et al.: Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition, URL: https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf, abgerufen am 30.08.2019.

[54] Fraunhofer Institut: Krypto-Agilität: langfristig handlungsfähig bleiben, URL: https://www.sit.fraunhofer.de/de/cryptoagility/, abgerufen am 17.09.2019.

[55] Grote, Olaf; Ahrens, Andreas; Banavente-Peces, César. A Review of Post-quantum Cryptography and Crypto-agility Strategies.

[56] Kroll, Joshua A.; Davey, Ian C.; FELTEN, Edward W. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: Proceedings of WEIS. S. 11, 2013.

[57] Mukhopadhyay, Ujan; et al. A brief survey of cryptocurrency systems. In: 2016 14th annual conference on privacy, security and trust (PST). IEEE, S. 745-752, 2016

[58] Houy, Nicolas. The Bitcoin mining game. Available at SSRN 2407834, 2014.

[59] Yuan, Yong; Wang, Fei-Yue. Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 48. Jg., Nr. 9, S. 1421-1428.

[60] Jabber, Karim; Bjorn, Pernille: Growing the Blockchain information infrastructure. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM, 2017. S. 6487-6498.

[61] Barber, Simon; et al.: Bitter to better—how to make bitcoin a better currency. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2012.

[62] Crosby, Michael; et al.: Blockchain technology: Beyond bitcoin. Applied Innovation, 2016, 2. Jg., Nr. 6-10, S. 71.

[63] Swanson, Tim: Bitcoins: made in China. Bitcoin Magazine 12. 2014.

[64] Zheng, Zibin; et al.: An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, 2017.

[64] Antonopoulos, Andreas M.: Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.", 2014.

[65] Bowden, Rory; et al.: Block arrivals in the Bitcoin blockchain, arXiv preprint arXiv:1801.07447, 2018.

[66] Gencer, Adem Efe; et al.: Decentralization in bitcoin and ethereum networks, arXiv preprint arXiv:1801.03998, 2018.

[67] Adrian, Tobias; Griffoli, Tommaso M.: The Rise of Digital Money, International Monetary Fund, 2019.

[68] Gipp, Bela; Meuschke, Norman; Gernandt, André: Decentralized trusted timestamping using the crypto currency bitcoin, arXiv preprint arXiv:1502.04015 (2015).

[69] Bradbury, Danny: The problem with Bitcoin. Computer Fraud & Security 2013.11 (2013): 5-8.

[70] O'Dwyer, Karl J.; Malone, David: Bitcoin mining and its energy footprint. 2014, S. 280-285.

[71] Taylor, Michael B.: The evolution of bitcoin hardware. Computer 50.9: 58-66, 2017.

[72] Bhaskar, Nirupama Devi; Chuen, David LEE Kuo. Bitcoin mining technology. In: Handbook of Digital Currency. Academic Press, 2015. S. 45-65.

[73] Vincent, James: Bitcoin consumes more energy than Switzerland, according to new estimate. URL: https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison, abgerufen am 22.09.2019.

[74] Vranken, Harald. Sustainability of bitcoin and blockchains. Current opinion in environmental sustainability, 2017, 28. Jg., S. 1-9.

[75] Sklavos, Nicolas; Koufopavlou, Odysseas. On the hardware implementations of the SHA-2 (256, 384, 512) hash functions. In: Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03. IEEE, 2003. S. V-V.

[76] Ertaul, Levent; Kaur, Manpreet; GUDISE, Venkata Arun Kumar R. Implementation and performance analysis of PBKDF2, Bcrypt, Scrypt algorithms. In: Proceedings of the International Conference on Wireless Networks (ICWN). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2016. S. 66.

[77] Watkins, David: Scrypt Mining with ASICs. URL: https://davidwatkinsvalls.com/files/2014_spring_SMWA.pdf, 2017, abgerufen am 30.09.2019.

[78] Narayanan, Arvind; et al: Bitcoin and cryptocurrency technologies. URL: https://pdfs.semanticscholar.org/6cab/f8bd8f6c953a8e136bf2b5834ddb883234a1.pdf, abgerufen am 30.08.2019

[79] Lewenberg, Yoad; et al.: Bitcoin mining pools: A cooperative game theoretic analysis. In: Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. International Foundation for Autonomous Agents and Multiagent Systems, 2015. S. 919-927.

[80] Mukhopadhyay, Ujan; et al: A brief survey of cryptocurrency systems. In: 2016 14th annual conference on privacy, security and trust (PST). IEEE, 2016. S. 745-752.

[81] Sprankel, Simon: Technical basis of digital currencies. Technische Universität, Darmstadt, URL: https://www.coderblog.de/wp-content/uploads/technical-basis-of-digital-currencies.pdf, 2013.

[82] Farell, Ryan. An analysis of the cryptocurrency industry. 2015.

[83] Rückeshäuser, Nadine. Do we really want blockchain-based accounting? Decentralized consensus as enabler of management override of internal controls. 2017.

[84] Bentov, Iddo, et al.: Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. IACR Cryptology ePrint Archive, 2014, 2014. Jg., S. 452.

[85] Zheng, Zibin, et al.: Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 2018, 14. Jg., Nr. 4, S. 352-375.

[86] Auer, Raphael: Beyond the Doomsday Economics of'Proof-of-Work'in Cryptocurrencies. 2019.

[87] Rieck, Sebastian: Potenzial der Blockchain–Infrastruktureller Paradigmenwechsel. In: Strategie und Transformation im digitalen Zeitalter. Springer Gabler, Wiesbaden, 2019. S. 221-236.

[88] Zheng, Zibin; et al: An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, 2017. S. 557-564.

[89] Lin, Iuon-Chang; LIAO, Tzu-Chun: A Survey of Blockchain Security Issues and Challenges. IJ Network Security, 2017, 19. Jg., Nr. 5, S. 653-659.

[90] Sankar, Lakshmi Siva; Sindhu, M.; Sethumadhavan, M. Survey of consensus protocols on blockchain applications. In: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2017. S. 1-5.

[91] Donet, Joan Antoni Donet; Perez-Sola, Cristina; Herrera-Joancomarti, Jordi: The bitcoin P2P network. In: International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014. S. 87-102.

[92] Parameswaran, Manoj; Susarla, Anjana; Whinston, Andrew B.: P2P networking: an information sharing alternative. Computer, 2001, 34. Jg., Nr. 7, S. 31-38.

[93] Nian, Lam Pak; Chuen, David Lee Kuo: Introduction to bitcoin. In: Handbook of Digital Currency. Academic Press, 2015. S. 5-30.

[94] Hölzner, Heike Marita; Blazickova, Cosima Alexandra: TOKEN ECONOMICS. URL: https://sirius-minds.com/wp-content/uploads/2019/03/01-2019_Sirius-Minds-Cases-and-Insights_Token-Economics_H%C3%B6lzner-Blazickova_final_1-2.pdf, abgerufen am 01.09.2019.

[95] Knirsch, Fabian; Unterweger, Andreas; Engel, Dominik: Implementing a blockchain from scratch: why, how, and what we learned. EURASIP Journal on Information Security, 2019, 2019. Jg., Nr. 1, S. 2.

[96] Chohan, Usman W: The Limits to Blockchain? Scaling vs. Decentralization. 2019.

[97] Hinzen, Franz J.; John, Kose; Saleh, Fahad: Proof-of-Work’s Limited Adoption Problem. NYU Stern School of Business, 2019.

[98] Karame, Ghassan O.; Androulaki, Elli; Capkun, Srdjan: Double-spending fast payments in bitcoin. In: Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012. S. 906-917.

[99] Miller, Andrew; Laviola JR, Joseph J.: Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin. Available on line: http://nakamotoinstitute. org/research/anonymous-byzantine-consensus, 2014.

[100] Tschorsch, Florian; Scheuermann, Björn: Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 2016, 18. Jg., Nr. 3, S. 2084-2123.

[101] Heilman, Ethan, et al.: Eclipse attacks on bitcoin's peer-to-peer network. In: 24th {USENIX} Security Symposium ({USENIX} Security 15). 2015. S. 129-144.

[102] Johnson, Benjamin, et al.: Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In: International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014. S. 72-86.

[103] Nayak, Kartik, et al.: Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016. S. 305-320.

[104] Guadamuz, Andres; Marsden, Christopher: Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. First Monday, 2015, 20. Jg., Nr. 12-7.

[105] Hileman, Garrick; Rauchs, Michel: Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance, 2017, 33. Jg.

[106] Moreno-Sanchez, Pedro; Zafar, Muhammad Bilal; Kate, Aniket: Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network. Proceedings on Privacy Enhancing Technologies, 2016, 2016. Jg., Nr. 4, S. 436-453.

[107] Wang, Hongwei, et al.: Knowledge graph convolutional networks for recommender systems. The World Wide Web Conference. ACM, 2019.

[108] Baliga, Arati: The blockchain landscape. Persistent Systems, 2016.

[109] Duffield, Evan; Diaz, Daniel: Dash: A privacycentric cryptocurrency. No Publisher, URL: https://pic.nanjilian.com/20180716/343445b5bc4b5e0cba45893a083b480d.pdf, 2015, abgerufen am 01.08.2019.

[110] Philipp, Andrew; Chan, Jennifer SK; Peiris, Shelton. A new look at Cryptocurrencies. Economics Letters, 2018, 163. Jg., S. 6-9.

[111] Duffield, Evan; Diaz, Daniel: Dash: A payments-focused cryptocurrency. Whitepaper, https://github.com/dashpay/dash/wiki/Whitepaper, 2018, abgerufen am 01.08.2019.

[112] Hameed, Sufian; Farooq, Sameet. The art of crypto currencies. International Journal of Advanced Computer Science and Applications, 2016, 7. Jg., Nr. 12.

[113] Lansky, Jan, et al.: Analysis of Cryptocurrencies price development. Acta Informatica Pragensia, 2016, 5. Jg., Nr. 2, S. 118-137.

[114] Osterrieder, Joerg; Lorenz, Julian; Strika, Martin: Bitcoin and cryptocurrencies-not for the faint-hearted. Available at SSRN 2867671, 2016.

[115] Noether, Shen: Ring Signature Confidential Transactions for Monero. IACR Cryptology ePrint Archive, 2015, 2015. Jg., S. 1098.

[116] Alonso, Kurt Magnus: Monero-privacy in the blockchain. 2018.

[117] Wijaya, Dimaz Ankaa; et al.: Anonymity reduction attacks to monero. In: International Conference on Information Security and Cryptology. Springer, Cham, 2018. S. 86-100.

[118] Mercer, Rebekah: Privacy on the blockchain: Unique ring signatures. arXiv preprint arXiv:1612.01188, 2016.

[119] Courtois, Nicolas T.: Stealth Address, Ring Signatures, Monero. 2016.

[120] Popov, Serguei: The tangle. cit. on, 2016, S. 131.

[121] Dinh, Tien Tuan Anh, et al.: Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 2018, 30. Jg., Nr. 7, S. 1366-1385.

[122] Strugar, Dragos, et al.: On M2M micropayments: a case study of electric autonomous vehicles. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018. S. 1697-1700.

[123] Bhattacharya, Debojyoti; Kherani, Arzad A.: Method of using ECDSA with winternitz one time signature. U.S. Patent Nr. 8,386,790, 2013.

[124] Bramas, Quentin: The Stability and the Security of the Tangle. 2018.

[125] Taskinsoy, John: Facebook’s Project Libra: Will Libra Sputter Out or Spur Central Banks to Introduce Their Own Unique Cryptocurrency Projects? Available at SSRN 3423453, 2019.

[126] Baudet, Mathieu, et al.: State machine replication in the Libra Blockchain. 2018.

[127] Oliveira, Luis, et al.: To token or not to token: Tools for understanding blockchain tokens. 2018.

[128] Buterin, Vitalik: A next-generation smart contract and decentralized application platform. white paper 3, 2014, S.37.

[129] Elendner, Hermann, et al.: The cross-section of crypto-currencies as financial assets: An overview. No. 2016-038. SFB 649 Discussion paper, 2016.

[130] Eyal, Ittay: Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. Computer 50.9, 2017, S. 38-49.

[130] Pass, Rafael: Micropayments for decentralized currencies. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.

[131] Bronleewe, David Allen: Bitcoin nfc. 2011.

[132] Li, Bin; Wang, Yijie: RZKPB: a privacy-preserving blockchain-based fair transaction method for sharing economy. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.

[133] Han, Runchao, Vincent Gramoli, and Xiwei Xu: Evaluating blockchains for iot. 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2018.

[134] Weber, Nils; Eigenstetter, Christoph; Berg, Markus M., Düsterhöft, Antje: Ontologiespeicherung in Datenbanken im Kontext natürlichsprachlicher Dialogsysteme. In Grundlagen von Datenbanken, 2009, S. 39-44.

[135] Tesoriero, Claudio: Getting Started with OrientDB. Packt Publishing Ltd, 2013.

[136] Miller, Justin J.: Graph database applications and concepts with Neo4j. Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA. Vol. 2324. No. S 36. 2013.

[137] Crossno, Patricia, et al.: Intelligence analysis using titan. 2007 IEEE Symposium on Visual Analytics Science and Technology. IEEE, 2007.

[138] De Meo, Pasquale, et al.: Generalized louvain method for community detection in large networks. 2011 11th International Conference on Intelligent Systems Design and Applications. IEEE, 2011.

[139] Bartoletti, Massimo, et al.: A general framework for blockchain analytics. Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. ACM, 2017.

[140] Miler, Mario, Damir Medak, and Dražen Odobašic: The shortest path algorithm performance comparison in graph and relational database on a transportation network. Promet-Traffic&Transportation 26.1, 2014, S. 75-82.

[141] Bradbury, Danny.: In plain view: open source intelligence, Computer Fraud & Security 2011.4, 2011, S. 5-9.

[142] Gupta, Sourav Sen.: Blockchain. John Wiley & Sons, Inc, 2017.

[143] Kurz, Hendrik: Syracom Trendstudie, 2014, S. 137 ff.

[144] Scott, Brett: How can cryptocurrency and blockchain technology Play a role in building social and solidarity finance?. No. 2016-1. UNRISD Working Paper, 2016.

[145] Raymaekers, Wim: Cryptocurrency Bitcoin: Disruption, challenges and opportunities. Journal of Payments Strategy & Systems 9.1, 2015, S. 30-46.

[146] Specht, Dieter; Martin G. Möhrle, eds.: Gabler Lexikon Technologie Management: Management von Innovationen und neuen Technologien im Unternehmen. Springer-Verlag, 2013.

[147] Deloitte Deutschland, Future of Blockchain, 2016, URL: https://www2.deloitte.com/de/de/pages/innovation/contents/blockchain-publications.html.

Bilderverzeichnis

Bild 1: Vorgehensweise.....10

Bild 2: Grenzkosten steigend.....13

Bild 3: Grenzkosten konstant.....13

Bild 4: Beispiel einer elliptischen Kurve.....26

Bild 5: Elliptische Kurve bei Bitcoin und Ethereum.....28

Bild 6: SHA-Algorithmus.....32

Bild 7: Berechnungen bei SHA.....33

Bild 8: Trilemma.....60

Bild 9: Klassifizierung von Kryptotokens.....74

Bild 10: Kürzester Pfad.....84

Bild 11: Bitcoin-Transaktion in Maltego.....85

Tabellenverzeichnis

Tabelle 1: Eigenschaften der Geldarten.....14

Tabelle 2: Bewertung der kryptografischen Hashfunktionen.....46

Tabelle 3: Verfolgungswahrscheinlichkeit einer Transaktion.....66

Tabelle 4: Eigenschaften des Tangle.....71

Tabelle 5: Zusammenfassung der Kryptowährungen-APIs.....81

Tabelle 6: Benchmark der Graphdatenbanken.....83

Tabelle 7: Ergebnis nach den Faktoren.....96

Verzeichnis der Abkürzungen

ASIC	Application Software in an Integrated Circuit
CPU	Central Processing Unit
DEM	Deutsche Elektronische Mark
ECC	Elliptic Curve Cryptography
GPU	Graphic Processing Unit
IBAN	International Bank Account Number
IOU	I owe u
M2M	Machine to Machine
MPT	Modified-Merkle-Patricia-Trie
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PIN	Personal Identification Number
POA	Proof-of-Activity
POC	Proof-of-Capacity
POI	Proof-of-Importance
POS	Proof-of-Stake
POW	Proof-of-Work
RSA	Rivest Shamir Adleman
TAN	Transaction Authentication Number
XOR	eXclusive Or

Anlagenverzeichnis

```
// Hinzufügen der Blockchain-Dateien

NetworkParameters np = new MainNetParams();

Context.getOrCreate(np);

List<File> blockchainFiles =new ArrayList<>();

blockchainFiles.add(new File("/home/btc/blockchain/blk00000.dat"));

BlockFileLoader bfl = new BlockFileLoader(np, blockchainFiles);

db = new Database();int i=0;

for(Block block : bfl) { …. }



// Zusammenfügen der Blöcke mittels Cypher

String statement="MERGE (block:block {hash:\""+block.getHashAsString()
+"\" })"+

" CREATE UNIQUE (block)-[:coinbase]->(:output:coinbase)"+

" SET "+

" block.size="+block.getMessageSize()+","+

" block.prevblock=\""+block.getPrevBlockHash()+"\","+

" block.merkleroot=\""+block.getMerkleRoot().toString()+"\","+

" block.time=" +block.getTimeSeconds()+","+

" block.nonce="+block.getNonce()+","+
```

```
" block.version="+block.getVersion()+""+

" MERGE (prevblock:block {hash:\""+block.getPrevBlockHash().toString()
+  "\"}) "+

" MERGE (block)-[:chain]->(prevblock)";

PreparedStatement ps = con.prepareStatement(statement);

ps.execute();

ps.close();
```

Thesen

These 1: Einige bereits am Markt erhältliche Kryptowährungen werden sich durchsetzen. Dazu zählen Ethereum für den Smart Contract Bereich, IOTA in der Maschinen-Kommunikation, Ripple für den Interbankentransfer von Zahlungen, Dash mit den Masternodes als gute Skalierungoption und Anonymisieren von Zahlungen, Monero wird für normalen Benutzer weiterhin interessant bleiben im Bereich des Minings, LIBRA kann schnell über die Größe von Facebook Verbreitung finden und Bitcoin wird als „Gold des Internets“ die Rolle als Referenz-Kryptowährung einnehmen.

These 2: Die Blockchain wird sämtliche Branchen erfassen und zur Disruption von Geschäftsmodellen führen. Dazu zählen insbesondere die Finanz- und Versicherungsbranche.

These 3: Die verwendeten Hashing-Funktionen sind sehr sicher. Obwohl Kollisionen bei den bestehenden Verfahren wie SHA-256 derzeit noch nicht aufgetreten sind, wird dieses Verfahren noch einige Jahre Verwendung finden. Sollten doch Kollisionen bekannt werden, so steht mit Keccak, welches bereits in einigen anderen Kryptowährungen verwendet wird, eine gute Alternative bereit.

These 4: Die zunehmende Verbreitung von Kryptowährungen im internationalen Geldtransfer wird es Strafverfolgungsbehörden enorm schwer machen, die Internet-Kriminalität zu bekämpfen. Dazu kommen Anonymisierungen von Monero und Dash, die eine Verfolgung nahezu unmöglich machen.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die hier vorliegende Arbeit selbstständig, ohne unerlaubte fremde Hilfe und nur unter Verwendung der in der Arbeit aufgeführten Hilfsmittel angefertigt habe.

Ort, Datum (Unterschrift)