ZÜRCHER HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN
SCHOOL OF MANAGEMENT AND LAW

Masterthesis

Die Blockchain Technologie: Eine Methode zur Identifikation von Anwendungsfällen

Wirtschaftsinformatik

Autor

Anand Paul Mooken

Zürich, Schweiz

Matrikelnummer: 08-263-386

Erster Begutachter / Betreuer

Dr. Hans-Dieter Zimmermann

FHSG, Fachhochschule St. Gallen

Zweitbegutachter

Dr. Matthias Baldauf

FHSG, Fachhochschule St. Gallen

Vorgelegt am 26. Mai 2017

Abstract

Längst hat die Blockchain seit der Einführung der Kryptowährung Bitcoin im Jahr 2009 Forscher und auch Experten aus der Privatwirtschaft in ihren Bann gezogen. Waren es anfangs zunächst vor allem Anwendungsfälle aus der Finanzbranche, haben sich diese mit der Blockchain weiterentwickelt. Das Potenzial der Technologie ist heute unbestritten gross, doch nur langsam entwickeln sich Initiativen in anderen Bereichen ausserhalb des Finanzsektors.

Das Ziel dieser Masterarbeit ist es, mittels einer selbst erarbeiteten Methode Anwendungsfälle zu identifizieren, welche sich für die Blockchain eignen. Dabei sollte die Methode branchenübergreifend verwendbar sein. Um dies zu erreichen, wurde in einem theoretischen Teil zunächst der aktuelle Stand der Blockchain Technologie erfasst. In einem aufbauenden Teil wurden Anwendungsfelder der Technologie betrachtet und analysiert. Durch Nutzung von explorativen Forschungsmethoden wurden weitere potenzielle Anwendungsfelder miteinbezogen. Mittels qualitativen Experteninterviews wurde der Status Quo der Blockchain vertieft und die Stärken und Schwächen sowie die Implikationen durch eine SWOT-Analyse klassifiziert und erfasst. Aus all diesen Teilen wurden Parameter abgeleitet, welche in der erarbeiteten Methode zur Anwendung kommen. Die Verifikation der Methode erfolgte durch theoretische Anwendung sowie der Evaluation mit Experten.

Die Erkenntnis des Status Quo der Blockchain zeigt auf, dass die Technologie insgesamt ihren disruptiven Attributen gerecht wird, insbesondere in Hinblick auf die Anwendungsfälle. Die Experten sind sich jedoch einig, dass die wahren Anwendungsfälle für die Blockchain erst noch entwickelt werden müssen und dabei auch die Kombination von Thematiken wie das Internet der Dinge und die künstliche Intelligenz das Anwendungsspektrum enorm erweitern. Die Methode zur Identifikation kann hierbei erste Indikationen dazu liefern, ob ein angedachter Fall mittels Blockchain zielführend umgesetzt werden kann.

Vorwort

Die folgende Arbeit «Die Blockchain Technologie: Eine Methode zur Identifikation von Anwendungsfeldern» entstand im Rahmen des Masterstudiengangs in Wirtschaftsinformatik an der ZHAW School of Management and Law.

Mein erster Dank gebührt meinem Gutachter, Dr. Hans-Dieter Zimmermann, für die Einräumung grosser Freiräume bei der Ausarbeitung meiner Masterarbeit und die fachliche Unterstützung sowie die vielen expliziten wie auch impliziten Anregungen; Stichwort Twitter.

Weiter möchte ich mich bei allen Fachexperten herzlichst bedanken, welche sich die Zeit nahmen, um mit viel Passion und steter Freundlichkeit bereitwillig über die Blockchain und meine Methode zu diskutieren. Auch die zahlreichen kritischen Anregungen haben zu neuen Sichtweisen geführt, welche ich als wichtige positive Anreicherung der entstandenen Methode erachte. Insbesondere möchte ich hier Frau Dr. Karin Frick vom Gottlieb Duttweiler Institut danken für die Einladung an die Blockchain Valley Conference 2017.

Daneben gilt mein Dank auch den akademischen Institutionen der ETH Zürich, der UZH sowie der Zentralbibliothek Zürich, die mir den Zugang auf ein grosses physisches Repertoire an qualitativ hochstehender Literatur ermöglicht haben.

Zuletzt möchte ich auch meinem privaten Umfeld danken. Insbesondere meiner Familie und Partnerin, die mir die Ausbildung meiner Wahl ermöglicht haben und mir in dieser intensiven Zeit immer zur Seite gestanden sind.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AML	Anti-Money Laundry
BaaS	Blockchain as a Service
BC	Blockchain
BTC	Bitcoin (auch als informeller Währungscode genutzt)
DAPP	Decentralized Application
DoS	Denial of Service
DSRM	Design Science Research Methodology
E2E	End to End
FinTech	Finanztechnologie
ICO	Initial Coin Offering
IoT	Internet of Things / Internet der Dinge
KYB	Know your Business
KYC	Know your Client
P2P	Peer to Peer
PoF	Point of Failure
PoS	Proof of Stake
PoW	Proof of Work
SEC	United States Securities and Exchange Commission, die US-Börsenaufsichtsbehörde
TEE	Trusted Execution Environment
USD	US Dollar
WM	Wealth Management
Y2K	Year 2000 – Jahr 2000

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

«Blockchains sind so bedeutend wie das Internet»

- Andreas Hirstein, Redaktion NZZ am Sonntag Wissen

Seit mehreren Jahrzehnten vollzieht sich eine neue industrielle Revolution, in der die Digitalisierung eine tragende Rolle einnimmt (Kohlmann, 2015, p. 2f.). So wird geschätzt, dass bereits im Jahr 2007 94 Prozent der gesamten Informationskapazität weltweit digital verfügbar war (Hilbert & López, 2011). Die Digitalisierung treibt die Transformation ganzer Branchen massiv voran. Unternehmen aus den verschiedensten Wirtschaftssektoren haben sich den veränderten Gegebenheiten angepasst und bieten sowohl ergänzende als auch vollkommen neue Dienstleistungen an. Daneben betraten im Zuge der Digitalisierung neue bzw. branchenfremde Wettbewerber den Markt, welche, zunächst von der Industrie belächelt, über die Zeit zu gewichtigen Konkurrenten angewachsen sind. Prominentes Beispiel dafür ist der Online-Versandhändler Amazon. 1994 als Online-Buchhandlung im US-Bundesstaat Washington gegründet, konnte das Unternehmen laut Forbes im Jahr 2013 allein in Nordamerika mit dem Vertrieb von Büchern einen Umsatz von 5,25 Milliarden US-Dollar verzeichnen (Bercovici, 2014). Im gleichen Jahr reduzierte sich die Anzahl der unabhängigen Buchhandlungen in Amerika von 4‘000 um mehr als 50 Prozent auf nun knapp 2‘000 (Bercovici, 2014). Das Beispiel zeigt deutlich, dass die digitale Revolution eine ernsthafte Gefahr für traditionelle Unternehmen darstellen kann; doch birgt sie auch ein grosses Potenzial für jene, die wissen, wie man ihre Vorteile für sich nutzen kann.

Die Blockchain ist dabei eines der oft genannten Schlagwörter im aktuellen Diskurs um die Digitalisierung und wird als einer der vielversprechendsten Technologien überhaupt diskutiert (Bühler, et al., 2015), (Courtneidge & Buelli, 2015), (McLean, 2016) (Tapscott & Tapscott, 2016). Im aktuellsten «Gartner Hype Cycle for Emerging Technologies» Report befindet sich der Begriff demnach auch nahe dem «Peak of Inflated Expectations», dem Gipfel der überzogenen Erwartungen, mit einer von Gartner eingeschätzten Zeitspanne von fünf bis zehn Jahren bis zum produktiven Einsatz - years to mainstream adaption (Gartner Research, 2016). Ausgelöst durch den ersten Anwendungsfall – der Kryptowährung Bitcoin – sind es vermehrt Exponenten der Finanzbranche aber auch zahlreiche Start-ups - in der Finanzbranche als Fintechs bezeichnet – welche nun vorpreschen und versuchen, die Vorteile der Technologie mit einem messbaren Mehrwert für das eigene Geschäftsmodell zu verwerten. Entsprechend stammen die meisten White Papers sowie praktischen Anwendungsfälle aus diesem Bereich. Doch ganz im Sinne des einleitenden Zitats von Andreas Hirstein soll sich das Konzept von Blockchain nicht

nur auf eine spezifische Branche reduzieren; das Potenzial kann so bedeutend sein wie es das Internet vor mehr als 20 Jahren einst bot und noch immer bietet.

1.1 Ausgangslage

Technisch vereinfacht ausgedrückt handelt es sich bei der Blockchain um ein digitales Journal für Transaktionen zwischen zwei oder mehreren Rechnern. Jede Veränderung wird hierbei erfasst und dezentral transparent auf allen im System teilnehmenden Rechnern im P2P (Peer-to-Peer) Netzwerk abgespeichert.

Die Blockchain wurde erstmals im Whitepaper von Satoshi Nakamoto im Jahr 2008 beschrieben (vgl. Kapitel 2.1). Seither hat nicht nur die darauf aufbauende Kryptowährung Bitcoin viel Wirbel in Forscherkreisen ausgelöst. Während die Bitcoin als Währung mitunter viele negative Schlagzeilen behauptete, wie beispielsweise der Skandal um die illegale Plattform Silkroad, welche mitunter mit Drogen und Kinderpornografie im Darknet handelte und Bitcoin als Bezahlwährung nutzte (Roy, 2013) ebenso wie kürzlich der Erpresservirus «Wanna Cry», so hat das Konzept der Blockchain als Basistechnologie der Bitcoin vermehrt seriöse Akteure der Informatik und Wirtschaft aufmerksam gemacht. Die Blockchain wird von vielen Experten aus Forschung und Praxis denn auch als Grundstein für einen Paradigmenwechsel der Informationsgesellschaft angesehen und entsprechend als disruptive Technologie bezeichnet. Dabei wird der Technologie attestiert, dass sie das Potenzial birgt, unsere Gesellschaft nachhaltig zu verändern (Swan, 2015), indem traditionelle Geschäftsmodelle durch die Blockchain effizienter gestaltet werden (Morabito, 2017), aber auch ganz entfallen könnten (Tapscott, 2016).

Abbildung 1: Interesse der Blockchain weltweit im zeitlichen Verlauf (Google Trends, 2017)

Die obige Abbildung zeigt das implizite Interesse der Blockchain auf der Suchmaschine Google. Deutlich zu sehen ist, dass sich ein signifikanter Anstieg der Suchhäufigkeit zum Begriff in den letzten zwei Jahren ergeben hat. Diese Indikation lässt sich durch die Anzahl von Konferenzen zur Technologie sowie den neu gegründeten Start-ups zur Blockchain stützen. Entsprechend findet die Blockchain, wie bereits einleitend erläutert, auf dem Gartner Hype Cycle für neuaufkommende Technologien nahe dem Gipfel der überzogenen Erwartungen (vgl. Abb. 2).

Abbildung 2: Gartner's Hype Cycle for Emerging Technologies 2016 (Gartner Research, 2016)

Es sind längst nicht mehr die Start-ups, welche sich aktiv mit der Technologie beschäftigen, sondern seit wenigen Jahren auch grosse Konzerne und traditionelle Unternehmen. Dabei befindet sich die Technologie in der kritischen Entwicklungsphase. Die jetzt entwickelten Anwendungsfälle entscheiden, wie die Blockchain zukünftig in unserem Alltag Verwendung findet – oder nicht (Morabito, 2017).

1.2 Problemstellung

Ausschlaggebend für die Durchsetzung der Blockchain ist, wie Unternehmen die Technologie adaptieren und ihr Geschäftsmodell ausrichten, um das volle Potenzial der Blockchain auszuschöpfen (Morabito, 2017). Doch seit dem Aufkommen der Blockchain sind es primär Unternehmen und Start-ups aus der Finanzbranche, welche sich mit dem Konzept auseinandersetzen und mit häufigen Publikationen zum Thema die allgemeine Wahrnehmung dominieren. Dies lässt sich auch darauf zurückführen, dass die Blockchain erstmalig für eine Anwendung im Bereich der Finanzindustrie genutzt wurde; dem Zahlungsverkehr mit Bitcoin (Taylor, 2015).

Eine Wahrnehmungsanalyse mit IBM Watson bestätigt dieses Bild. Als Input der Untersuchung wurden wissenschaftliche Publikationen aber auch Nachrichtenartikel sowie soziale Netzwerke wie Facebook und Twitter analysiert. Dabei hat sich folgende Tag Cloud ergeben:

Abbildung 3: IBM Watson Analyse zum Begriff Blockchain (IBM Watson, 2017)

Wie initial festgestellt, zeigt sich auch hier erneut die starke Konnotation der Blockchain mit der Finanzindustrie. Aufgrund dieser starken Assoziation fokussiert diese Arbeit auf die Problemstellung der fehlenden Sichtbarkeit von Anwendungsfeldern der Blockchain ausserhalb des Finanzsektors. Durch die Parametrisierung der Blockchain Technologie sollen Kriterien zusammengefasst werden, mit welcher sich ein jeder Anwendungsfall unabhängig von der Branche auf die Eignung für die Blockchain Technologie identifizieren lassen soll.

1.3 Zielsetzung

Das initiale Ziel dieser Arbeit ist die Blockchain Technologie und ihren aktuellen Entwicklungsstand aufzuzeigen. Mit einem Fokus auf aktuelle Anwendungsfälle sollen die mit der Blockchain einhergehenden Implikationen der Technologie aufgezeigt werden. Angereichert mit wissenschaftlichen und explorativen Elementen aus der Literaturrecherche und der Analyse von Expertenaussagen sollen als weiteres Ziel potenzielle Anwendungsfelder der Blockchain Technologie ermittelt werden. Auf dieser Grundlage soll festgestellt werden, ob sich aus den gesammelten Daten ein Muster herleiten lässt, mit welchem es möglich wird, beliebige Anwendungsfälle auf die Eignung für die Blockchain Technologie zu prüfen und so zu identifizieren.

Grundsätzlich lassen sich die Ziele dieser Arbeit entsprechend in den folgenden drei Punkte zusammenfassen:

- Aufzeigen der Blockchain Technologie und ihren aktuellen Entwicklungsstand
- Systematische Aggregation von aktuellen und potenziellen Anwendungsfeldern zu verwertbaren Kriterien
- Erarbeitung einer Methode zur Identifikation von Anwendungsfällen, welche sich für die Blockchain Technologie eignen

1.4 Forschungsfrage

Die Forschungsfrage leitet sich hauptsächlich durch die Problemstellung und der damit verbundenen Zielsetzung ab. Mit dieser Arbeit soll der aktuelle Entwicklungsstand der Blockchain Technologie wiedergeben werden. Entsprechend simpel lässt sich die erste Forschungsfrage definieren:

Primäre Forschungsfrage

Was ist der Status Quo der Blockchain Technologie?

Um die primäre Forschungsfrage zu beantworten, bedarf es untergeordneter Forschungsfragen, welche sich im Detail mit der Thematik befassen:

1. & 2. untergeordnete Forschungsfrage

Wo liegen aktuell die Anwendungsfelder der Technologie?

Was sind mögliche Implikationen der Anwendung der Blockchain Technologie?

Die gewonnenen Erkenntnisse obiger Forschungsfragen dienen als Grundlage zur Erarbeitung sowie Verifikation einer Methode, mit welcher sich die Eignung der Blockchain Technologie auf diverse Anwendungsbereiche mittels parametrisierten Eingaben ermitteln lässt. Somit ergibt sich die finale Forschungsfrage:

3. Forschungsfrage

Wie können potenzielle Anwendungsfelder für die Blockchain Technologie systematisch identifiziert werden?

1.5 Forschungsdesign

Als Grundlage zur Erreichung der Zielsetzung und zur Beantwortung der Forschungsfragen definieren die folgenden Unterkapitel das zu verwendende Forschungsdesign.

1.5.1 Forschungsansatz

Der in dieser Arbeit verwendete Forschungsansatz verbindet ein induktives mit einem deduktiven Vorgehen. Laut Saunders et al. (2012, S.127ff.) ergibt eine Kombination der Ansätze ein verbessertes Resultat, sofern dies vom Forschungsgegenstand bzw. dem Setting ermöglicht wird. Des Weiteren bietet die Verwendung beider Vorgehensweisen die Möglichkeit, erarbeitete Thesen direkt zu verifizieren (Saunders et al., 2012, S. 124-128).

Im Kontext dieser Arbeit ist der durch die Induktion verursachte Bias insbesondere durch die von Experten gemachten Aussagen zu den erarbeiteten (Zwischen-)Resultaten möglich. Ihr Input dient zur Verifikation sowie Verfeinerung der getroffenen Aussagen. Deduktion führt andererseits zu einer zu starken Verallgemeinerung was zu einer abstrakten Lösung führen kann, die das Problem nicht mehr lösen kann. Entsprechend werden die zwei Vorgehensweisen wie folgt angewandt:

- Induktives Vorgehen: Erarbeitung der Kriterien / Thesen
- Deduktives Vorgehen: Evaluation der erarbeiteten Kriterien / Thesen

1.5.2 Forschungsprozess

Dem Forschungsprozess dieser Arbeit unterliegt das Design Science Research Methodology (DSRM) Prozessmodell von Peffers, et al. (2008) und Hevner & Chatterjee (2010). Die Methodologie eignet sich für die Herleitung von Artefakten sowie Verifikation dieser und lässt sich in folgendes Modell einordnen.

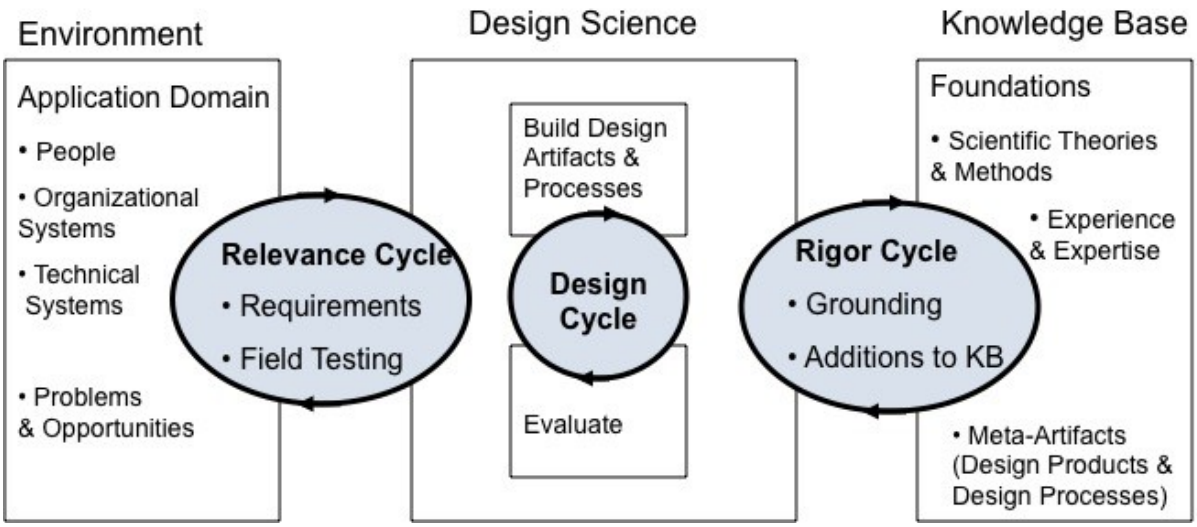


Abbildung 4: Design Science Research Methodology Process Model (Peffers, et al. 2008)

Der DSRM Prozess besteht aus sechs Schritten (Hevner & Chatterjee, 2010, p. 28ff.):

- **Problemidentifikation und –motivation**
  - Beschreibung des Problems und des Nutzens einer Lösung
- **Beschreibung für eine Ziellösung**
  - Herleitung von Zielen aufgrund der Problemstellung unter Sicherstellung der Machbarkeit und Möglichkeit
- **Design und Entwicklung**
  - Erstellen eines Artefakts; Artefakten sind Konstrukte, Modelle, Methoden oder Umschreibungen (Hevner, et al., 2004, pp. 75-105)
- **Demonstration**
  - Demonstration des neuen Artefakts und deren Lösungsfähigkeit
- **Evaluation**
  - Evaluation des neuen Artefakts unter Berücksichtigung der Problemstellung
- **Kommunikation**
  - Publizieren der neuen Lösung über Kommunikation.

Für diese Arbeit werden die sechs Prozessschritten in folgenden Kontext gebracht:

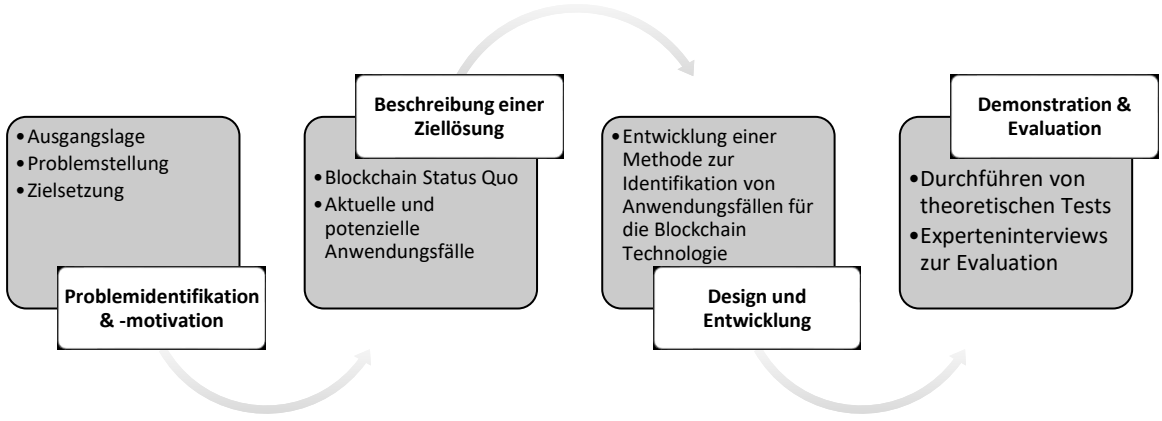


Abbildung 5: Kontextualisierung des DSRM Prozesses auf die Masterarbeit, (Eigene Darstellung in Anlehnung an Hevner & Chatterjee, 2017)

Der finale Prozessschritt der Kommunikation stellt die Wiedergabe der Entwicklung und der Methode in dieser Masterarbeit dar.

Als Artefakt wird in dieser Arbeit die zu erarbeitende Methode zur Identifikation von Anwendungsfällen für Blockchain betrachtet. Durch die Analyse der Umwelt (Environment, vgl. Abbildung 4) soll das

Artefakt verbessert werden. Die identifizierten Parameter sowie die Resultate aus der Analyse der Blockchain Technologie sollen als neugewonnenes bzw. verifiziertes Wissen in die Knowledge Base einfliessen, um die Grundlage für weitere Forschung zur Blockchain zu begünstigen.

Die Forschung kombiniert die Attribute einer deduktiven sowie induktiven Vorgehensweise. Hierbei ist die Erarbeitung des Status Quo der Blockchain sowie die Evaluation der Methode zur Identifikation von Anwendungsfällen für die Blockchain deduktiver Natur und die Gestaltung dieser Methode induktiv getrieben.

1.5.3 Forschungsmethoden

Die verwendeten Forschungsmethoden dieser Arbeit lassen sich dem Forschungsframework von Hevner et al. (2008) zuordnen (vgl. Abbildung 4). Nachfolgend werden die einzelnen Bestandteile der Arbeit mit den jeweils genutzten Forschungsmethoden aufgeführt und zusätzlich den Bereichen des «Information System Research Framework» zugeordnet.

Forschungsmethode	Bestandteil der Arbeit	Zuordnung im «Information System Research Framework»
Literaturrecherche	- Blockchain Status Quo - Methode zur Identifikation von Anwendungsfällen für Blockchain	Knowledge Base – Fundations
Experteninterviews	- Grundlagen – Basis - Methode zur Identifikation von Anwendungsfällen für Blockchain	Environment – People
Qualitative Nutzwertanalyse	- Analyse der Blockchain Technologie	Knowledge Base – Methodologies
Sekundäranalyse & Explorative Forschung	- Identifikation von aktuellen und potenziellen Anwendungsfeldern	Knowledge Base – Fundations

Tabelle 1: Forschungsmethoden in Relation zur Forschungsarbeit und dem IS Research Framework (Eigene Darstellung, 2017)

Die Nutzung von Forschungsmethoden, welcher der Knowledge Base des Forschungsframeworks von Hevner et al. (2004) zugeordnet werden können (Literaturrecherche, qualitative Nutzwertanalyse, Sekundäranalyse) fundiert die Rigorosität der Forschungsergebnisse. Die Identifikation von potenziellen Anwendungsfeldern wird durch eine explorative Forschung erweitert. Die Praxistauglichkeit wird zusätzlich durch die Durchführung theoretischer Tests sowie Experteninterviews dargelegt. Die Evaluation der Ergebnisse soll insbesondere durch Experteninterviews vorgenommen werden. Attribute bzw.

Anforderungen an Gutachter werden hierfür initial definiert, um die Selektion von qualifizierten Experten für diesen Schritt zu ermöglichen sowie nachvollziehbar zu machen. Der Interviewleitfaden wurde abgeleitet aus den Forschungsfragen der Arbeit und nach den heuristischen Methoden der Themenanalyse sowie Codierung von Froschauer und Lueger (2003, p. 82) interpretiert. Hierbei wurde das Konzept der Rückkopplung verwendet, welches vorgibt, die Erkenntnisse jedes Interviews in den Interviewleitfaden des nachfolgenden Interviews einzubauen. Somit ergibt sich ein dynamischer Fragekatalog, welcher die erhobenen Daten mit jeder Iteration vertiefter erfassen lässt (Froschauer & Lueger, 2003, p. 76).

1.6 Vorgehensweise

Die Arbeit startet mit der initialen Erfassung des aktuellen Entwicklungsstands der Blockchain Technologie. Hierzu werden die derzeit dominierenden wissenschaftlichen Ansätze sowie produktive Fallbeispiele systematisch gesammelt und analysiert. Daraus sollen konkrete sowie potenzielle Implikationen der Technologie abgeleitet und aggregiert werden. Die damit erhaltene Datengrundlage soll im finalen Schritt zu generalisierbaren Parametern für die zu erarbeitende Methode zusammengeführt werden. Durch die rationelle Verknüpfung der einzelnen Parameter soll so die Methode zur Identifikation von Anwendungsfällen, welche sich für die Blockchain Technologie eignen, erarbeitet werden.

2 Blockchain – Status Quo

Die Blockchain ist ein digitaler Ledger (zu Deutsch: Hauptbuch), welcher alle Transaktionen, welche jemals getätigt wurden, erfasst und ablegt. Im Anwendungsfall der Bitcoin werden alle zehn Minuten alle Transaktionen bis zur letzten Erfassung gesammelt und in der Blockchain als Block abgelegt. Dieser neue Block wird der Blockchain angehängt, wodurch sich eine lineare und chronologische Abfolge von Blöcken ergibt. Hierbei beinhaltet der neue Block jeweils eine Referenz zum vorhergehenden Block, womit sich der Begriff Blockchain, also Kette von Blöcken, erklären lässt. Jeder Full Node, also jeder Computer, welcher eine Mining Applikation installiert hat und selbst über genügend Rechenleistung zum Mining von Blöcken verfügt, kann so einen Block generieren. Mining umschreibt in diesem Fall die Aktivität der Generierung eines neuen Blocks (vgl. Kapitel 2.2 – Aufbau einer Blockchain). Jeder Benutzer, der sich mit seinem Full Node dem entsprechenden Blockchain Netzwerk anschliesst, lädt automatisch die komplette Blockchain auf seinen lokalen Rechner und kann somit alle Transaktionen bis zum ersten Block, bezeichnet als Genesis Block, zurückverfolgen.

Eine Vielfalt von Quellen beschäftigen sich mit der Funktionsweise der Blockchain und viele Definitionen eröffnen verschiedene Ansichten auf die Technologie. Die Arbeit orientiert sich an der Theorie der Versionierung der Blockchain nach Swan (2015, S. ix) sowie der begrifflichen Differenzierung nach Burgwinkel (2016, S. 5). Die beiden Ansätze lassen sich gut kombinieren. Sie sind in folgender Abbildung kontextualisiert.

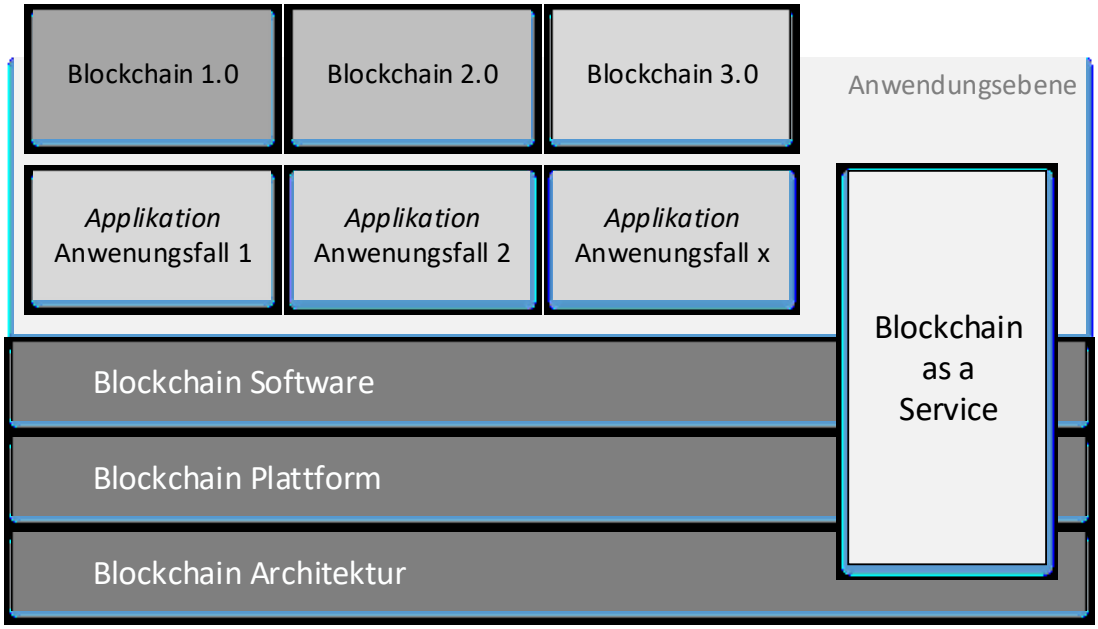


Abbildung 6: Verwendete Grundlage dieser Arbeit (Eigene Darstellung in Anlehnung an Swan, 2015 und Burgwinkel, 2016)

Blockchain als technische Architektur

Die Kombination von technischen Methoden, wie der SHA256 Verschlüsselung, der digitalen Signatur und weiteren Technologien, welche seit mehr als 30 Jahren bekannt sind.

Blockchain-Plattformen

Das verteilte Netz, in der die Blockchain Software agiert bzw. angeboten wird.

Blockchain Software

Die Ebene, in welcher den Programmcode bereitstellt – im Jahr 2016 sind mehr als 20 verschiedene kommerzielle als auch Open-Source Software Produkte verfügbar (Burgwinkel, 2016, p. 67). Darunter zählen Ethereum und die Bitcoin Software.

Blockchain-Applikation

Basierend auf der Blockchain Software bzw. Plattform angebotene Applikationen, welche einen konkreten Anwendungsfall realisieren. Konkret lässt sich Bitcoin als Applikation nennen. Auf der Ethereum Software gibt es zahlreiche Applikationen, welche verschiedene Anwendungsfälle abbilden, wie beispielsweise Etheria (eine Blockchain Version des populären Spiels Minecraft), KYC-Chain (eine Applikation zur Kundenidentifikation nach der KYC Gesetzgebung) oder Eth-Tweet (ein Blockchain-basiertes Twitter).

Blockchain-as-a-Service

Die Realisierung eines Blockchain Dienstes in der Cloud unter Verwendung aller Ebenen als E2E-Konzept.

Blockchain 1.0: Die Währung

Die Anwendung der Blockchain für die Entwicklung von Kryptowährungen in Bezug auf den Zahlungsverkehr.

Blockchain 2.0: Die Verträge

Die Anwendung der Blockchain für die Entwicklung von wirtschaftlichen, handelsgetriebenen und finanziellen Vorgängen, welche komplexer sind als der reine Zahlungsverkehr im Sinne einer Geldüberweisung.

Blockchain 3.0: Die nächste Evolution

Die Anwendung der Blockchain auf weitere Felder wie der Wissenschaft, den Behörden, des Gesundheitswesens und vielen weiteren Gebieten.

Nachfolgend wird zunächst auf die geschichtliche Entstehung der Blockchain eingegangen, bevor dann auf den Aufbau samt wichtigsten Begriffsdefinitionen detailliert eingegangen wird.

2.1 Historie

Die Blockchain hat ihren ersten bekanntgewordenen Einsatz und somit Ursprung in der darauf aufbauenden dezentralen Kryptowährung Bitcoin. Bis heute ist unklar, wer genau Bitcoin und somit die Blockchain als Technologie erfunden hat. Unter dem Pseudonym Satoshi Nakamoto wurde das Konzept samt der Technologie in einem Whitepaper namens Bitcoin-Whitepaper im November 2008 über eine verschlüsselte E-Mail-Adresse veröffentlicht. Viele Personen haben seither den Anspruch erhoben, das Whitepaper verfasst zu haben. Zuletzt war dies der australische Computerfachmann und Unternehmer Craig Steven Wright. Evidenzen, die diesen Anspruch bestätigen, wurden bis heute nicht geliefert (Safi, 2016). 2011 wurde jedoch festgestellt, dass das Erfinderteam rund um Satoshi Nakamoto sich aus der Community rund um Bitcoin zurückgezogen hat.

Im Jahr 2009 wurde der erste Bitcoin-Client veröffentlicht und seither kontinuierlich über die eigens eingerichtete Bitcoin-Community weiterentwickelt. Mit der Feststellung «Ich werde mich fortan anderen Dingen widmen.» beendete der oder die Erfinder im Frühjahr 2011 das Engagement und überliess die Weiterentwicklung der Open-Source Gemeinschaft. Auch wenn im Whitepaper von Satoshi Nakomoto die Blockchain als Technologie mit keinem Wort erwähnt wird (Nakamoto, 2008), so hat sich die beschriebene Technologie zu einem verbreiteten Schlagwort gewandelt.

2.2 Prinzipien einer Blockchain

Die Blockchain Technologie stützt sich auf Prinzipien, welche bereits im Paper von Satoshi definiert wurden und noch heute in unterschiedlicher Ausprägung bestehen (Nakamoto, 2008, p. 5ff.), (Mougayar, 2016, p. 3f.), (Tapscott & Tapscott, 2016, p. 16), (Tanenbaum & Van Steen, 2007, p. 4ff.).

- Ein verteiltes Netzwerk, welches eine direkte Interaktion der Teilnehmer ermöglicht und ein offenes System darstellt – *distributed power and resources - decentralisation, openness, transparency, integrity, scalability*
- Keine Drittpartei notwendig – *no trusted third party, zero-trust*
- Eine Transaktionskette, die nicht veränderbar ist – *immutability*
- Sicherheit durch Verwendung von kryptographischen Algorithmen – s*ecurity, anonymity*

Diese Prinzipien entsprechen der Entwicklungsstufe Blockchain 1.0. Mit der Weiterentwicklung zur Blockchain 2.0 sind weitere Eigenschaften hinzugekommen (Swan, 2015, p. 9):

- Automatisierung durch codierte Verträge – *automatization*
- Variable Anzahl an Verarbeitungsschritten einer Transaktion - *Interaction*

Mougayar (2016) unterscheidet zudem zwischen den einzelnen Dimensionen der Blockchain, welche von dieser Arbeit ebenfalls aufgriffen wird und eine weitere Gruppe von Parametern für das zu erarbeitende Modell ausmachen:

Technisch: Backend Datenbank, welche einen digitalen Ledger offen verwaltet

Business: Ein Netzwerk zum Austausch von Werten zwischen den Teilnehmern

Legal: Ein Mechanismus zur Validierung von Transaktionen ohne Drittpartei

In den folgenden Kapiteln wird darauf eingegangen, wie die Blockchain Technologie es ermöglicht, die zuvor genannten Prinzipien abzubilden. Dabei wird jeweils immer auf das erfüllte Prinzip referenziert.

2.3 Aufbau einer Blockchain

Die nachfolgende Definition zum Aufbau einer Blockchain zeigt auf, dass es sich hierbei um eine raffinierte Kombination von bereits bestehenden Einzelkomponenten handelt. Dabei vereint die Blockchain zum ersten Mal mehrere Technologien wie Hashing, ein Peer-to-Peer Netzwerk, die Theorie des Merkle Trees und weitere technische Elemente zu einem in sich kohärenten Ansatz.

2.3.1 Die kryptographische Hash-Funktion

Ein erstes Konzept zum Verständnis der Blockchain bildet die kryptographische Hash-Funktion. Ein Hash ist dabei ein digitaler Fingerabdruck von Daten. Jede Menge an Daten egal welcher Form kann in so einen Hash Wert übersetzt werden. Dabei hat dieser Hash Wert entgegen der beinhaltenden Daten immer die gleiche vordefinierte Länge unabhängig davon, ob es sich bei den ursprünglichen Daten um einen einzelnen Namen oder aber ein ganzes Lexikon handelt[1]. Ebenso verhaltet es sich bei einem leeren Input, sprich, keinen Daten. Die Blockchain verwendet hierbei aktuell den bekannten Secure

[1] Die Grösse des Inputs x kann je nach gewähltem Algorithmus Standard auf eine fixe Bitgrösse limitiert sein, so bei einer AES Verschlüsselung. Diese von Blockchain nicht verwendete Verschlüsselungsformen nennt man Blockchiffre (National Institute of Standards and Technology, 2001).

Hash Algorithm *SHA-256* wobei die Zahl 256 des Hash-Algorithmus dafürsteht, dass der zu generierende Hash Wert jeweils immer 256 Bit gross ist. Der Verschlüsselungsalgorithmus gilt dabei zum heutigen Zeitpunkt als sehr sicher (Paar & Pelzl, 2009, p. 313). Die Blockchain nutzt die nachfolgenden Eigenschaften der weitverbreiteten Verschlüsselungsfunktion (Bonneau et al., 2016, S. 2ff.):

Hash Collision Resistance

Die Kollisionsresistenz ist ein wichtiges Argument für die Blockchain. Mathematisch wird eine Kollision wie folgt ausgedrückt:

$$x_1 \neq x_2, \qquad H(x_1) = H(x_2)$$

Die Funktion besagt, dass die Werte x_1 und x_2 als unabhängige Werte in der Hash-Funktion $H()$ zu einem gleichen Wert führen. Dies beschreibt eine Kollision (Paar & Pelzl, 2009, p. 301). Als kollisionsresistent kann eine Hash-Funktion bezeichnet werden, wenn es *unmöglich* ist, zwei Werte, x_1 und x_2, zu finden, sodass $x_1 \neq x_2$ aber $H(x_1) = H(x_2)$ sind (Bonneau et al., 2016, S. 2). Auch wenn es theoretisch bei jedem Hash Alogrithmus zu einer Kollision kommen kann, so würde es es im Falle der 256-bit Verschlüsselung mit einem Computer, welcher 10'000 Hash Werte pro Sekunde berechnen kann, mehr als eine Oktillion (10^{27}) Jahre benötigen, um nur die Hälfte aller möglichen Kombinationen auf eine mögliche Kollision hin zu prüfen (Paar & Pelzl, 2009, p. 314).

Hiding

Eine weitere Eigenschaft der kryptographischen Hash-Funktion, wessen sich die Blockchain bedient, bildet das sogenannte *Hiding*. Dies bezeichnet die Tatsache, dass bei einer Hash-Funktion $y = H(x)$ der Wert des Input Parameter x nicht ermittelt werden kann. Um dies zu bewerkstelligen, wird der Input Parameter x mit einem geheimen, zufälligen Wert r konkateniert:

$$H(r \| x)$$

Diese geheime und zufällige Variable r wird als *Nonce* bezeichnet. Nonce wird in der Kryptographie als willkürliche Zahl definiert, welche nur einmal genutzt werden darf (Needham & Schroeder, 1978). In der von Blockchain genutzten SHA256 Verschlüsselung handelt es sich hierbei um einen zufälligen 256-bit Wert. Der mit der Nonce konkatenierte Wert x kann nun nicht mehr ohne Weiteres ermittelt werden.

Bonneau et al. (2016, S. 6) unterscheiden dabei zwischen *Hiding* und *Binding*. Die komplementäre Sicherheitseigenschaft *Binding* beschreibt die Unmöglichkeit,

zwei Paare (x, r) und (x', r') zu finden, bei welcher $x \neq x'$

aber $H(r \| x) == H(r' \| x')$

Verifikation

Durch die oben genannten Eigenschaften *Hiding* und *Binding* lässt sich der Parameter x durch eine erneute Konkatenation mit dem Nonce r durch eine andere Partei verifizieren. Indem die Hash-Funktion H mit dem Wert $r||x$ ausgeführt wird, sollte der exakt gleiche Hash Wert berechnet werden, wie dies vom Erzeuger des Hash Werts ausgegeben wurde. Dabei wird das *Binding* durch die zuvor erwähnte Eigenschaft der Kollisionsresistenz gestützt, womit es nur eine einzige Konstellation von x und r geben kann, die zum gleichen Hash Wert führt.

Puzzle Friendliness

Die letzte Eigenschaft eines Hash-Algorithmus, welcher von der Blockchain genutzt wird, ist die Puzzle Friendliness. Vereinfacht ausgedrückt handelt es sich hierbei um den Umstand, dass der *Nonce* Wert r in der Funktion $H(r||x) = y$, für jeden möglichen n-bit Output y der Funktion H nicht unterhalb des Zeitaufwandes 2^n gefunden werden kann. Wenn eine Hash-Funktion puzzle friendly ist, dann gibt es keine bessere Lösungsstrategie, als das Durchrechnen der Funktion mit allen zufälligen Werten für r bis der passende Wert für r gefunden ist (Bonneau et al., 2016, S. 9). Diese Eigenschaft wird insbesondere für das Mining der Blockchain – explizit für den «Proof of Work» Mechanismus - verwendet, auf die in einem späteren Kapitel eingegangen wird.

Die Hash Funktionen sind bereits seit mehreren Jahren in verschiedenen Anwendungen im Einsatz. Das Konzept bietet verschiedene Eigenschaften (Matusiewicz et al., 2016), welche nicht alle für die Blockchain notwendig sind. Die aufgeführten vier Eigenschaften sind essentiell für die Gestaltung einer Blockchain und dienen zum Verständnis der Technologie. Weitere Eigenschaften von kryptographischen Hash-Funktionen werden innerhalb dieser Arbeit nicht weiterverfolgt. Nachfolgend wird ein zusätzliches Verfahren erläutert, die thematisch noch zur kryptographischen Hash-Funktion gehört, jedoch überleitend das Konzept der Blockchain als Kette von Blöcken veranschaulicht.

Merkle-Damgård Verfahren

Die kryptographische Hash-Funktion gibt als Ergebnis einen Hash Wert aus. Die Funktion konvertiert dabei jeweils einen beliebig langen Input zu einem 256-bit langen Hash Wert. Sollte der Input grösser sein als der Output, so bedient sich die SHA-256 Funktion des *Merkle-Damgård Verfahrens*.

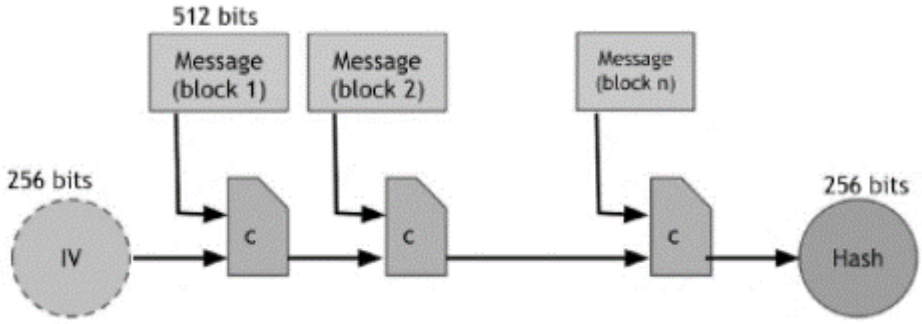


Abbildung 7: Vereinfachte Darstellung einer SHA-256 Verschlüsselung unter Verwendung des Merkle-Damgård Verfahrens (Bonneau et al., 2016)

Dieses bricht den Input anhand eines vordefinierten Initialisierungsvektors (häufig 0) auf und verknüpfen die einzelnen 256-bit langen Hash Werte so, dass sie zusammengefasst wieder den Input konstruieren können, wie auf nachfolgender Abbildung illustriert wird. Dabei wird der Input Wert, sprich die zu verschlüsselnde Nachricht, immer auf ein Vielfaches der Blockgrösse von 256-bit erweitert – bekannt als das *Paddingverfahren*.

Die Verknüpfung der einzelnen Datensätze, die aus diesem Verfahren erstellt werden, führt zur technischen Definition der Blockchain. Es unterstützt die folgenden Prinzipien der Blockchain: *Security, Integrity*.

2.3.2 Digitale Signatur

Ein weiterer technischer Bestandteil der Blockchain bildet die digitale Signatur. Die seit 1994 standardisierte Technik ermöglicht die elektronische Signatur von Daten (Boneh, 2011, p. 347). Dokumente können so signieren werden, wobei die Signatur jeweils *persönlich* ist und nur vom dazugehörigen Subjekt erstellt werden kann, jedoch *von allen eingesehen* und verifiziert werden. Zusätzlich ist sie exklusiv auf nur jenen Dokumenten, die vom Subjekt willentlich unterzeichnet wurden und soll nicht ungewollt auf andere Dokumente repliziert werden können (Bonneau, et al., 2016, p. 16). Eine Fälschung kann so also *nicht erzwungen* werden. Dies umschreibt bereits die zwei Eigenschaften einer digitalen Signatur, die auch für die Blockchain genutzt werden.

Eine zusätzliche Eigenschaft der digitalen Signatur ist jene der digitalen Identität. Mit dem Konzept des Private und Public Key lassen sich Aussagen personalisieren und gegenüber Dritte identifizieren. Dies führt zum ***dezentralisierten Identitätsmanagement***, eine Eigenschaft, welche dem Blockchain Prinzip der Dezentralisation durch Distribution folgt und den *Proof-of-Ownership* gewährleistet. Eine digitale Identität lässt sich ohne weiteres erstellen, in dem ein neues Paar aus privatem und öffentlichem

Schlüssel als digitale Signatur erstellt wird. Dies ist der Mechanismus, wie in einem Bitcoin Netzwerk die Identität festgelegt und geprüft wird.

Die Blockchain nutzt technisch die gegebenen Methoden der bewährten digitalen Signatur, weshalb an dieser Stelle nicht weiter auf die Funktionsweise eingegangen wird.

Wallet

Die Wallet bildet eine Art Portemonnaie in einem Blockchain Netzwerk. Es handelt sich hierbei vereinfacht ausgedrückt um eine Applikation, welche die eigenen digitalen Signaturen der Blockchain bestehend aus jeweils einem Public Key und einem Private Key ablegt. Der öffentliche Schlüssel bildet im Netzwerk die Adresse des Portemonnaies während der private Schlüssel genutzt werden muss, um Transaktionen tätigen (Antonopoulos, 2014, p. 7). Verschiedene Anbieter bieten solch eine Wallet für unterschiedliche Blockchain Applikationen und Softwares an. Darunter zählen Bitcoin Wallet, Coinomi, Copay oder Green Address (Bitcoin.org, 2017).

Die digitale Signatur unterstützt die folgenden Prinzipien der Blockchain: *Decentralisation, Transparency, Integrity, Openness, Immutability, Zero-Trust*

Anstelle der Signierung der Nachricht und somit dem Klartext eines Blocks, wird bei einer Blockchain der Hash-Pointer von jedem Block signiert. Dies ist bereits Teil der Datenstruktur einer Blockchain und wird im nächsten Kapitel erörtert.

2.3.3 Datenstruktur einer Blockchain

Nachdem eine Nachricht mittels der zuvor erwähnten kryptographischen Hash-Funktion verschlüsselt wurde, müssen diese Daten strukturiert abgelegt werden. Das Merkle-Damgård Verfahren gewährleistet eine Verarbeitung von beliebig langen Input Werten zu einem verschlüsselten 256-bit langen Hash-Wert, bestimmt jedoch nicht die Struktur des Outputs. Zudem fehlt noch die Signatur, welche wie zuvor erwähnt aus Effizienzgründen nicht auf der Nachrichtenebene passiert. Die Struktur der Daten und deren Umsetzung ist der namensgebende Teil der Blockchain. Und hierbei arbeitet eine Blockchain mit sogenannten *Hash-Pointern*.

Hash-Pointer

Für jeden neuen Block wird ein Hash-Pointer generiert, welcher nicht nur eine Referenz auf den davorliegenden Block beinhaltet, sondern die verschlüsselten Daten davon in der Berechnung des Hash-Pointers miteinbezieht. So ergibt sich schematisch das folgende Abbild:

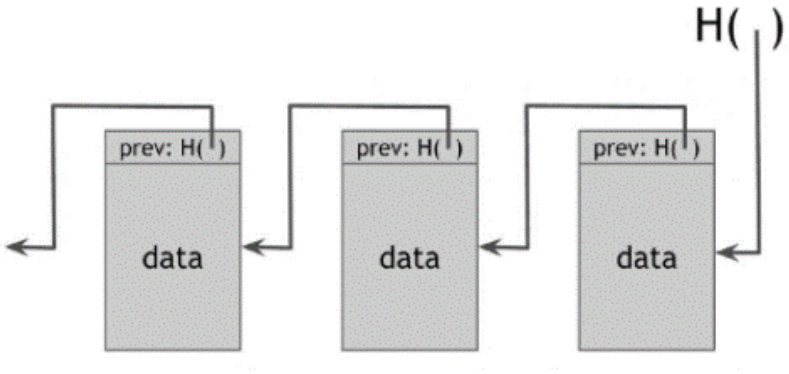


Abbildung 8: Hash-Pointer einer Blockchain (Bonneau et al., 2016)

Jeder Block führt eine eigene Hash-Funktion aus, welche als Input den Hash-Wert des vorhergehenden Blocks sowie der im eigentlichen Block abgelegten Daten verwendet. Die so verknüpften Blöcke sind somit ***fälschungssicher*** - *immutable*. Wird versucht, innerhalb einer Kette ein Block zu modifizieren, so verlieren die nachfolgenden Hash-Pointer ihre Gültigkeit, da sie auf den 'alten' Hash-Wert des manipulierten Blocks aufbauen.

Merkle Tree

Eine weitere Datenstruktur, welche sich mit den Hash-Pointern umsetzen lässt, ist der Merkle Tree. Benannt nach seinem Erfinder Ralph Merkle ist die Form wie der Name bereits sagt, ein Baum, welcher aus einzelnen miteinander verbundenen Blöcken besteht (Buchmann et al., 2007). Ein Merkle Tree ist eine Datenstruktur, welche genutzt wird, um effizient grosse Mengen an Daten zusammenzufassen, zu verfiizieren und die Integrität zu prüfen. Nachfolgend wird ein solcher Merkle Tree abgebildet.

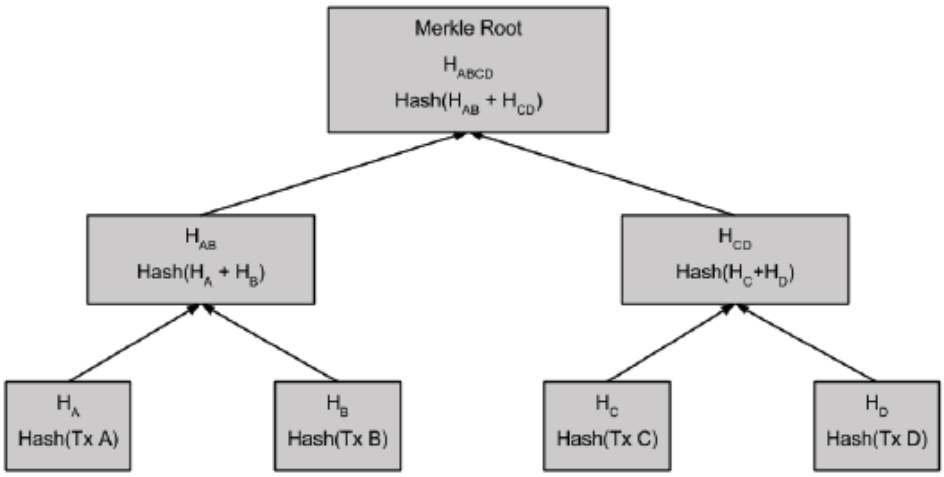


Abbildung 9: Merkle Tree in einer Blockchain (Antonopoulos, 2014, p. 171)

Wie die Abbildung zeigt, werden die Blöcke jeweils zu Paaren gruppiert und für jedes Paar existiert eine Datenstruktur, die zwei Hash-Pointer beinhaltet – im Abbild wäre dies H_A und H_B. Zusammengefasst definieren sie die nächste Ebene des Baums – $Hash(H_A + H_B) = H_{AB}$. In einer weiteren Iteration gelangt man in diesem Beispiel zum obersten Block der Blockchain, welche im Kontext des Merkle Tree als Merkle Root bezeichnet wird. Wie bereits die verknüpften *Hash-Pointer* eine ***Fälschungssicherheit*** bieten, so ist auch hier das gleiche Prinzip angewendet. So fallen Manipulationen innerhalb eines Merkle Trees sofort auf, da die höher angeordneten Hash-Werte nicht mehr korrekt sind. Jeder Versuch einer Manipulation kann erkannt werden, in dem nur der *oberste Hash-Wert* H_{ABCD} des Merkle Root bekannt ist – was zu einer ***schnellen Validierung*** einer Blockchain führt.

Ebenfalls ist die Verifikation eines Blocks mit einer Teilmenge des gesamten Merkle Trees möglich. Denn ein neu hinzugefügter Block muss nur den Pfad zum Merkle Root errechnen und somit nicht alle Blöcke berücksichtigen, wie dies in der Abbildung 8 mit aneinander geordneten Blöcken der Fall wäre. Durch diesen Fakt lässt sich die sogenannte **Proof of Membership –** die Prüfung, ob ein Block und dessen Erzeuger zur Blockchain gehört - schnell umsetzen.

Es unterstützt die folgenden Prinzipien der Blockchain: *Immutability*, *Integrity*, *Security, zero-trust*

2.3.4 Netztopologie

Eine weitere Komponente der Blockchain Technologie ist ihr verteiltes Netz. Dabei handelt es sich um eine Form des Peer-to-Peer Netzwerk. Oram et al. (2011, p. 21) gibt eine grundlegende Definition für den Begriff:

> [a Peer-to-Peer system is] *a self-organizing system of equal, autonomous entities (peers)* [which] *aims fort he shared usage of distributed resources in a network environment avoiding central services.*

Die Ähnlichkeiten zu den Grundprinzipien der Blockchain sind dabei sehr auffällig. Das Konzept ist bereits seit 2005 bekannt und lässt sich folgendermassen charakterisieren (Steinmetz & Wehrle, 2005, p. 10ff.) – wobei pro Attribut direkt ein Vergleich mit der Blockchain gezogen wird:

- *Peers weisen eine hohe Heterogenität bezüglich der Bandbreite, Rechenkraft, Online-Zeit, […] auf.*
  Dieses Attribut trifft ebenfalls auf die Blockchain zu, auch wenn für die Peers Limitationen bezüglich Bandbreite und Rechenkraft bestehen (nach unten).
- *Die Verfügbarkeit und Verbindungsqualität der Peers kann nicht vorausgesetzt werden.*
  Ebenfalls ein Attribut, welches auf die Blockchain zutrifft.

- *Peers bieten Dienste und Ressourcen an und nehmen Dienste anderer Peers in Anspruch (Client-Server-Funktionalität).*
  Ein Attribut, welches zumindest in der heutigen Umsetzung der Blockchain nicht ganz zutrifft. Als Dienst exisitert in einer Blockchain das Mining. Dies ist jedoch nicht in einer Client-Server-Funktionalität umgesetzt. Auch aufbauende Konzepte wie die Smart Contracts entsprechen nicht dieser Charakterisierung.
- *Dienste und Ressourcen können zwischen allen teilnehmenden Peers ausgetauscht werden.*
  Die Blockchain erweitert um das Konzept der Smart Contracts (beschrieben in einem späteren Kapitel) entspricht diesem Attribut. Dabei können die Daten als Ressource nicht nur ausgetauscht werden, sie müssen.
- *Peers bilden ein Overlay-Netzwerk und stellen damit zusätzliche Such-Funktionen zur Verfügung.*
  Das Blockchain Netzwerk kann als Overlay-Netzwerk bezeichnet werden, bietet jedoch in seiner puren Form keine Such-Funktion an – da alle Daten lokal bei jedem Peer verfügbar sind.
- *Peers haben eine signifikante Autonomie (über die Ressourcenbereitstellung).*
  Dieses Attribut trifft wieder auf die Blockchain als verteiltes Netzwerk zu, welches den Teilnehmer freistellt, wie er sich im Netzwerk involvieren möchte.
- *Das P2P-System ist selbstorganisierend.*
  Auch dieses Attribut trifft sehr gut auf die Blockchain zu, sind die Prozesse selbstorganisierend – Stichwort Konsens (beschreieben in einem späteren Kapitel)

(nach Steinmetz & Wehrle, 2005)

Die Verwendung eines P2P-Netzwerks stützt das Prinzip der Blockchain einer Immutability – nicht Veränderbarkeit. In der gängigen Fachliteratur spricht man deshalb auch von einer Distributed Blockchain (Burgwinkel, 2016, p. 67) also der verteilten Blockchain als Synonym zur Blockchain. Im Gegensatz zu einem reinen P2P-Netzwerk unterscheidet sich die Distributed Blockchain jedoch durch einen wichtigen Aspekt. Die Dezentralisierung ist durch eine komplette Kopie aller Daten – der Blockchain – bewerkstelligt. Hierbei ist die Blockchain nicht zentral auf nur einem Rechner gespeichert und auch nicht wie bei einem P2P-Netzwerk in Fragmenten auf verschiedenen Rechnern, sondern komplett auf vielen gleichzeitig. Somit haben mehrere sogenannte Peers eine exakte Kopie der Blockchain. Wird auf einem Rechner nun eine Manipulation vorgenommen, so kann die Blockchain auf diesem einen Rechner wohl einen gültigen Hash Wert beinhalten, dieser wird jedoch nicht mehr mit jenen Hash Werten übereinstimmen, die sich auf den anderen Rechnern / Peers befinden. Die nachfolgende Abbildung verdeutlicht die Unterschiede zwischen einer zentralisierten, einer dezentralisierten (P2P-Netzwerk) und einer verteilten Architektur.

Abbildung 10: Vergleich von zentralem, dezentralem und verteiltem Netz (Swanson, 2015)

Die Distributed Blockchain – ab jetzt wieder als Synonym für Blockchain genutzt – bietet im Vergleich zu einem zentralisierten und dezentralisierten Netzwerk analog der obigen Abbildung die folgenden Attribute, welche aus verschiedenen Literaturquellen zusammengestellt:

	ZENTRALISIERT	**DEZENTRALISIERT**	**VERTEILT**
FAULT TOLERANCE / STABILITÄT	Sehr anfällig, da nur eine zentrale Einheit exisitert – kompletter Systemausfall	Anfällig, da der Ausfall von Directory Peers Teile unbrauchbar macht – beschränkter Systemausfall	Sehr stabil, da jeder Peer das gesamte System stützen kann – kein Systemausfall
POINT OF FAILURE (POF) / MAINTENANCE	Einfach zu warten, da nur eine zentrale Einheit berücksichtigt werden muss	Erschwert zu warten, da mehrere PoF berücksichtigt werden müssen	Schwierig zu warten, da jeder Peer berücksichtigt werden muss
SKALIERBARKEIT	Tiefe Skalierbarkeit	Mittlere Skalierbarkeit	Unbeschränkte Skalierbarkeit
ENTWICKLUNG	Schnell, zentral abgestimmt	Langsam, Standards müssen zuerst festgelegt werden	Langsam, Standards müssen zuerst festgelegt werden
HIERARCHIE / ENTSCHEIDUNG	Zentral	Gleichberechtigt basierend auf lokalen Daten	autonom und global koordiniert

EVOLUTION / DIVERSITÄT	Langsam, ein zentrales Framework	Schnell, da hohe Diversität die Evolution begünstigt	Schnell, da hohe Diversität die Evolution begünstigt
LATENZZEIT	Tief - Abhängig von der Performance der zentralen Einheit	Mittel - Abhängig vom angesprochenen Peer	Tief – Verarbeitung kann über jeden Peer erfolgen

Tabelle 2: Attribute von zentralen, dezentralen und verteilten Netzwerken

Diese Eigenschaften führen nicht nur zur erwähnten *Immutability* der Blockchain, sondern unterstützen die folgenden Prinzipien einer Blockchain (Tanenbaum & Van Steen, 2007, p. 4ff.):

Immutability, distributed power and resources - decentralisation, transparency, openness, scalability, no-trust

Die Skalierbarkeit ist ein Prinzip der Blockchain, welche je nach Form mittels Incentivierung erreicht wird. Ähnlich verhält es sich bei der Transparenz und der Offenheit, welche je nach Form der Blockchain unterschiedlich gewichtet werden (vgl. 2.3.7 Formen einer Blockchain). Zum Verständnis dessen wird zunächst auf den Aufbau eines einzelnen Blocks einer Blockchain eingegangen.

2.3.5 Aufbau eines Blocks

Eine Blockchain besteht aus einer chronologischen Kette von nummerierten Blöcken die zusätzlich jeweils den Hash Wert des vorhergehenden Blockes enthalten (vgl. Abbildung 8). Ein Block ist ein strukturiertes Datengefäss, welches getätigte Transaktionen einer Blockchain Anwendung für die Blockchain ablegt.

Block vs. Coin vs. Token

Zum besseren Verständnis sollen zunächst die Terminologien definiert werden. So verwenden insbesondere Online Quellen die Begriffe Block, Coin und Token als Synonyme. In dieser Arbeit wird differenziert zwischen den drei Begriffen wie folgt (Swan, 2015, p. 71):

Coins bezeichnet einen simplen Träger von Wert, beispielswiese einen Bitcoin. Dieser Wert ist fix vergeben und verhaltet sich entsprechend statisch.

Token sind ebenfalls Träger von Wert, jedoch können diesem Wert komplexe mehrschichtige Informationen mitgegeben werden. Es handelt sich um eine Weiterentwicklung der einfachen Coin. Ein gutes

Beispiel dafür ist ein Smart Contract, welcher ausführbaren Code enthält und somit ein mehrdimensionales Objekt darstellt. Insbesondere bei Permissioned Blockchains (vgl. 2.3.7 Formen einer Blockchain) sind diese Token nicht als Währung zu sehen, sondern eher als verifizierbare kryptographische Belege zwischen den Teilnehmern als Beleg für Audit Zwecke (Swanson, 2015, p. 13).

In der Fachliteratur wird auch der Begriff *Digital tokenized asset* verwendet, was verallgemeinert für Beides steht (Christidis & Devetsikiotis, 2016, p. 2295).

Ein *Block* ist hierbei ein Speicher der Transaktionen mit diesen Elementen (Antonopoulos, 2014). Es bildet das Gefäss, welches dann auf der Blockchain abgelegt wird, wobei die explizite Verwendung von Coins oder Token von der aufliegenden Blockchain Software bzw. Applikation (vgl. Abbildung 6) vorgegeben wird.Abbildung 6: Verwendete Grundlage dieser Arbeit (Eigene Darstellung in Anlehnung an Swan, 2015 und Burgwinkel, 2016)

Block Header

Der Block besteht aus einem Header und einem Datenbereich, welcher eine Liste von Transaktionen beinhaltet. Der Header legt Metainformationen wie die Referenz zum letzten Block ab wie auch den Hash-Wert des Merkle Root. Zusätzlich sind hier je nach Konsensmechanismus (vgl. 2.3.6 Distribuierter Konsens) Informationen dazu abgelegt. Die folgenden ein Beispiel von Attributen, die in den Header abgelegt werden (Antonopoulos, 2014):

Header Hash: Der Hash-Wert des Blocks

Previous Block Header Hash: Die Referenz zum vorhergehenden Block als dessen Hash-Wert

Timestamp: Der Zeitstempel, welcher aussagt, wann der Block erstellt wurde

Difficulty: Ein Wert, der auf die Schwierigkeit der Konsensfindung hinweist.

Nonce: Der Nonce Wert (vgl. 2.3.1 Die kryptographische Hash-Funktion), welcher der Hash-Funktion zugewiesen wurde

Merkle Root: Der Hash-Wert des Merkle Root, dem obersten Block des Merkle Trees

Transaktionen / Datenbereich

Gefolgt wird dieser Header durch den Datenteil, den Transaktionien, welche durch diesen Block erfasst werden. Transaktionen beschreiben einen Transfer von Tokens oder Coins von einem Teilnehmer zu einem anderen. Dabei unterscheidet man bei Kryptowährungen (vgl. 2.4.1 Kryptowährungen) drei unterschiedliche Arten von Transaktionen (Antonopoulos, 2014, pp. 21-22). Die Standard-Transaktion, welche wie bereits beschrieben, eine 1:1 Relation zwischen Sender und Empfänger aufweist. Daneben

gibt es die aggregierte Transaktion, welche eine n:1 Relation aufweist. Mehrere Sender schicken Tokens oder aber Coins an einen einzigen Empfänger. Zuletzt gibt es die gegensätzliche Form, genannt Verteilungstransaktion, bei welcher ein Sender mehreren Empfängern einen Token bzw. Coin schickt; eine 1:n Relation. Abgeleitet handelt es sich um drei Attribute plus einen oder mehrere Hash-Pointer als Transaktions-ID, welche bei Kryptowährungen eine Transaktion ausmachen. Dieser Hash-Pointer zeigt auf vergangene Transaktionen, welche mit diesem eindeutigen Token bzw. Coin gemacht wurden. So löst Bitcoin das Problem des Double Spending[2]. Ethereum, was in dieser Arbeit als Vertreter der Blockchain 2.0 – Smart Contracts - betrachtet wird, kennt zusätzlich Attribute (Ethereum Homestead, 2017): Eine Signatur zur Identifikation des Senders (nur für den Empfänger), ein optionales Datenfeld als Befehl für den Smart Contract und Felder zur Verhandlung von Transaktions- bzw. Ausführungskosten, welcher ein Smart Contract generiert und vom Sender gedeckt werden müssen (vgl. 2.4.2 Smart Contracts).

Block Size

Der Datenteil macht den grössten Teil eines Blocks aus, welcher je nach Anwendung eine bestimmte Grösse nicht überschreiten darf. Der Header ist 80 Byte gross, während der Datenteil mindestens eine Grösse von 250 Byte aufweist und durchschnittlich mehr als 500 Transaktionen beinhaltet (Antonopoulos, 2014, p. 209). Die folgende Tabelle gibt ein allgemeines Bild über den Aufbau eines Blocks.

GRÖSSE	ATTRIBUT	BESCHREIBUNG
4 BYTES	Block Size	The size of the block, in bytes, following this field
80 BYTES	Block Header	Several fields form the block header
1-9 BYTES (VAR INT)	Transaction Counter	How many transactions follow
VARIABLE	Transactions	The transactions recorded in this block

Tabelle 3: Aufbau eines Blocks (Antonopoulos, 2014, p. 209)

Arten von Blöcke

Der erste Block hat keinen Vorgänger, weshalb der Vorgängerwert einen Nullwert enthält.

Genesis Block	Der erste Block einer Blockchain

[2] Die Double-Spending Attacke beschreibt das Problem der Mehrfachausgabe des gleichen digitalen Tokens (Bonneau, et al., 2016, p. 34)

Stale Block	Ein Block, welcher zwar erfolgreich errechnet (mined) wurde und so auch akzeptiert wäre, jedoch durch einen gleichzeitig erzeugten Block nicht Teil der Blockchain wurde
Orphan Block	Ein Block, dessen vorhergehender Block noch nicht durch den Rechner des Teilnehmers verarbeitet / abgelegt wurde. Somit kann der Orphan Block noch nicht fertiggestellt werden.
Uncle Block	Ein Block des Ethereum Derivats der Blockchain, welcher implizit in der Blockchain ist, jedoch inhaltlich 1:1 dem integrierten Block gleicht

Tabelle 4: Arten von Blöcken in einer Blockchain

Die aufgeführten Arten lassen sich folgendermassen visualisieren. Grün gekennzeichnet ist der Genesis Block, schwarz die integrierten Blöcke einer Blockchain und violett Uncle Blöcke. Stalled Blocks, blau, gehören nicht zur Blockchain und sind nicht mit dieser verbunden.

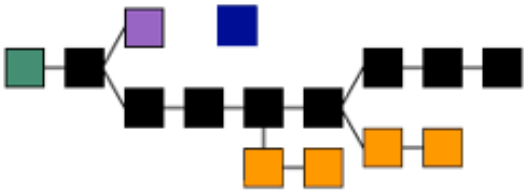


Abbildung 11: Darstellung einer Blockchain (Eigene Darstellung in Anlehnung an Theymos, 2015)

(Hard) Fork

Die orangen Blöcke auf oberer Abbildung zeigen einen sogenannten Fork (zu Deutsch: Gabel). Dabei handelt es sich um eine Abspaltung gewisser Blöcke von der eigentlichen Blockchain. Dazu kann es kommen, wenn zwei Miner zeitgleich einen Block erzeugen und der Blockchain anfügen wollen, dabei weisen die Blöcke unterschiedliche Versionen bzw. Informationen auf. Die Uncle Blöcke von Ethereum gehören einer einfachen Fork an. Die Unstimmigkeiten werden dabei jedoch schnell gelöst, indem neue Blöcke jeweils nur an der längsten gültigen Kette angehängt werden (Bergmann, 2015). Wie bereits erwähnt, ist eine Manipulation einer Transaktion in einem Block verbunden mit der Neuberechnung der ganzen Blockchain gesehen vom zu manipulierenden Block. Somit können die Teilnehmer sich sicher sein, dass es sich bei der längsten Kette um die valide Kette handelt (DeMartino, 2016, p. 187) und alle weiteren Forks ignorieren.

Daneben gibt es jedoch den Hard Fork. Dies ist ein erzwungenes Ereignis, welches sich durch eine Änderung an der Blockchain Software ergibt. Als Beispiel kann die Veränderung der bei Bitcoin zurzeit auf

1MB limitierten Block Size betrachtet werden. Sollte man diese vergrössern, so verstehen ältere Teilnehmer des Netzwerks die neuen Blöcke nicht mehr, sollten sie sich nicht zu den Anpassungen bekennen.

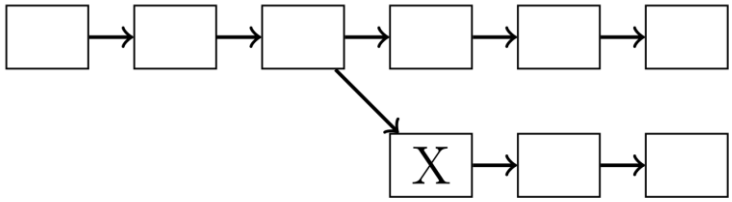


Abbildung 12: Darstellung eines Hard Forks (Bergmann, 2015)

Der Block X in obiger Abbildung bildet so einen nach neuem Protokoll erzeugten Block. Ältere Teilnehmer werden diesen ignorieren und weiterhin die 'alte' Blockchain nutzen. Neuere Teilnehmer, welche die Anpassung akzeptiert haben, werden jedoch ab Block X weitermachen. So entstehen parallel zwei Blockchains mit unterschiedlicher Kompabilität (Bergmann, 2015). Dieses Verhalten kann auch zu Problematiken führen, was später in der Arbeit analysiert wird.

Der beschriebene Aufbau eines Blocks unterstützt die folgenden Prinzipien der Blockchain: *Integrity*, *Immutability, Security*

2.3.6 Distribuierter Konsens

Da die Blockchain auf einem verteilten Netzwerk basiert, gibt es viele Teilnehmer, welche gleichzeitig an der Erstellung eines neuen Blocks arbeiten. Der absehbare Konflikt liegt in der Mehrzahl an möglichen Blöcken, die der Blockchain hinzugefügt werden könnten. Daneben kann es dazu kommen, dass Teilnehmer mit negativen Absichten gefälschte Blöcke generieren und so zu ihren eigenen Gunsten manipulieren. Um dies zu vermeiden, muss das Netz sich einigen darauf, welcher Block valid ist und der Blockchain hinzugefügt wird. Es muss ein Konsens gefunden werden, ohne dass sich die anonymen Teilnehmer im Netz gegenseitig vertrauen müssen (Bonneau, et al., 2016, p. 29). Ebenfalls muss dieser Konsens gefunden werden, wenn die Teilnehmer selbst zum Zeitpunkt der Transaktion nicht aktiv im Netz sind (Zepf, 2016, p. 12).

Ein Konsensmechanismus ist hierbei der Prozess, in welchem eine Mehrheit (in gewissen Fällen alle Teilnehmer) zu einer Übereinkunft des Status der Blockchain kommen. Es handelt sich hierbei um Regeln und vordefinierten Abläufen, welche eine konsistente Datenhaltung zwischen mehreren Teilnehmern ermöglicht (Bonneau, et al., 2016, p. 29). Um dies zu bewerkstelligen, gibt es verschiedene An-

sätze welche über die letzten drei Jahrzehnte für verteilte Systeme entwickelt wurden, um Fehlertoleranzen in diesen Systemen zu verwalten. Dabei unterstützt der distribuierte Konsens die folgenden Prinzipien der Blockchain: *decentralisation, integrity, scalability, zero-trust, immutability, security* und *anonymity*.

Die Blockchain greift die folgenden Ansätze auf.

2.3.6.1 Proof of Work

Mit der Vorstellung der Blockchain mit Bitcoin wurde ein Konzept des Konsenses implementiert, welches sich Proof of Work (PoW) nennt. Es verfolgt das Prinzip, das die Wahrscheinlichkeit einer Sybil-Attacke[3] durch die Auswahl eines zufälligen Node ausgeschlossen werden kann. In diesem Ansatz des impliziten Konsenses können zunächst folgende Schritte differenziert werden (Bonneau, et al., 2016, p. 34):

1. Neue Transaktionen werden allen Teilnehmern (Nodes) des Netzwerks mitgeteilt (Broadcast)
2. Jeder Node sammelt neue Transaktionen in einem Block
3. In jeder Iteration kann ein zufällig gewählter Node seinen so erstellten Block an alle anderen Teilnehmer mitteilen (Broadcast)
4. Die anderen Teilnehmer akzeptieren den Block nur, wenn alle Transaktionen valide sind
5. Die Teilnehmer zeigen ihre Akzeptanz, in dem sie den Hash-Wert des neuen Blocks in ihre neuen Blöcke inkludieren

Zwischen dem dritten und vierten Schritt verbirgt sich der Proof of Work. Die bei Bitcoin und zurzeit auch bei Ethereum angewendete Methode sichert ab, dass der neue Block *schwierig* (bezogen auf Zeit und Auslastung der Ressourcen) in der Erstellung war. Wie in dieser Arbeit bereits aufgezeigt, beinhaltet ein Block einen Hash-Wert bestehend aus dem Datenteil / Transaktionen und dem Hash-Wert des vorhergehenden Blocks. Der Proof of Work gibt einen Zielwert für diesen zu generierenden Hash-Wert vor, genannt *Target Value.* Dieser bestimmt, wie hoch der zu generierende Hash-Wert maximal sein kann und somit, wie schwierig es ist, einen Hash-Wert unterhalb dieses *Target Value* zu berechnen. Folgende Abbildung verdeutlicht den Ablauf in der Praxis:

[3] Eine Sybil-Attacke bezeichnet eine Attacke auf ein P2P-Netzwerk durch einen Identitätsbetrug und kann Entscheide und Abläufe in solchen P2P-Netzwerken manipulieren, verlangsamen oder abhören (Douceur, 2002).

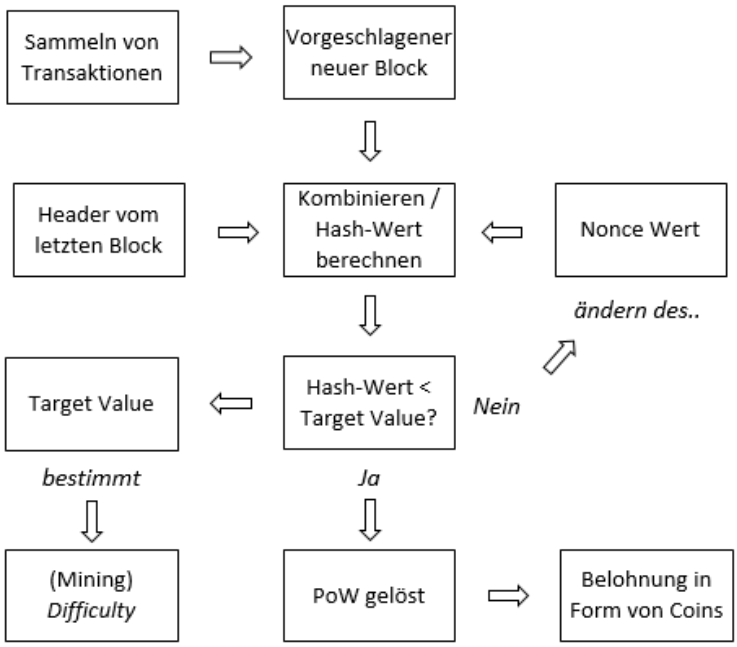


Abbildung 13: Proof of Work Methode (Eigene Darstellung in Anlehnung an Bitcoin Mining, 2015)

Hier kommt die im Kapitel 2.3.1 Die kryptographische Hash-Funktion beschriebene Eigenschaft der Puzzle Friendliness einer kryptographischen Hash-Funktion zum Tragen. Der *Nonce* Wert muss so gewählt werden, dass der generierte Hash-Wert kleiner als der *Target Value* ist. Die *(Mining) Difficulty* ist hierbei eine Messgrösse, wie schwierig es ist, einen Hash-Wert unterhalb des *Target Value* zu finden. Je tiefer der *Target Value* gewählt wird, desto mehr Zeit braucht es, den passenden *Nonce* Wert zu finden und desto höher ist somit die *(Mining) Difficulty*. Die Belohnung für das Lösen des Rätsels wird im Kapitel 2.4.1.1 Funktionsweise (Mining beschrieben.

PoW ist ein Teil des Mining. Durch die Beteiligung aller Teilnehmer an diesem Mining Prozess mit PoW entsteht ein Wettlauf um die Erzeugung eines neuen Blocks. Dabei werden enorme Rechenleistungen gefordert, was zu einem hohen Stromverbrauch führt. Da nur der Block des ersten Miners verwendet wird, wird ein Grossteil der aufgebrachten Rechenleistung als unnütz verworfen. Die Nachhaltigkeit dieses Ansatzes kann deshalb in Frage gestellt werden.

2.3.6.2 Proof of Stake

Aufgrund der Problematik der Nachhaltigkeit von PoW ist der Ansatz des Proof of Stake entstanden. Hierbei steht nicht die pure Rechenleistung im Vordergrund, sondern die proportionale Beteiligung – *Stake* – am Gesamtvolumen der Token bzw. Coins. Adaptiert auf die Kryptowährung Bitcoin würde dies bedeuten, dass der Erzeuger von Blöcken mit einem Besitz von einem Prozent aller Bitcoins ein Prozent der Blöcke erzeugen darf. Der Grundgedanke ist, dass ein selbst beteiligter Nutzer ein entspre-

chend grösseres Interesse an einer sicheren Blockchain hat, da er auch explizit von Angriffen und Manipulationen des Systems betroffen ist. Potenzielle Angreifer müssten zudem im Vergleich zum PoW nicht über eine grosse Rechenleistung verfügen, sondern über einen erheblichen Anteil der Tokens bzw. Coins. Solch ein Vorhaben lohnt sich finanziell nicht. Im Vergleich zum PoW exisitert im PoS kein Mining, alle Token bzw. Coins sind mit dem Genesis Block verfügbar. Entsprechend werden auch keine Belohnungen durch die Generierung neuer Coins ausbezahlt. Die Motivation zur Teilnahme an solch einer Blockchain wird rein über eine Transaktionsgebühr generiert. Durch den Fokus weg von Rechenleistung und PoW kommen kürzere Blockzyklen zustande was zu einer schnelleren Transaktionsverarbeitung führt.

Auch wenn PoS die Kritik der Nachhaltigkeit an PoW lösen kann, so haben sich neue Probleme ergeben. Diskutiert wird hier insbesondere die Nothing-at-Stake Attacke. Hierbei wird bei einem möglichen Fork an allen Strängen weitergearbeitet, womit sich keine eindeutig gültige Kette ergeben kann.

2.3.6.3 Weitere Formen des Konsenses

Proof of Activity

Bei diesem Ansatz handelt es sich um die Kombination von PoW und PoS. Der Mining Prozess startet analog dem PoW, womit ein Rennen um die Erzeugung des ersten Blocks entsteht. Nachdem der Block erzeugt wird, wird geprüft, ob der Teilnehmer, welcher den Block erzeugt hat, über einer entsprechenden Stake im Netzwerk verfügt (coindesk, 2017). Die Nachteile der beiden Ansätze PoW und PoS werden hierbei ebenfalls kombiniert.

Proof of elapsed Time

Der von Intel erfundene Konsens arbeitet mit einer zentralisierten vertrauten Ausführungsumgebung – TEE / Trusted execution evironment. Der Ansatz ist vergleichbar mit dem PoW, jedoch wird kein kryptographisches Rätsel gelöst, sondern die TEE vergibt den Auftrag zur Erzeugung eines Blocks in Form einer Lotterie. Im Vergleich zum PoW führt dies zu einer erheblichen Einsparung von Energie, doch der Nachteil ist, dass es sich hierbei um eine zentralisierte Instanz handelt.

Die Form des Konsenses kann abhängig zur Form einer Blockchain aufwändiger sein (PoW, PoS) oder einfacher. Die bestimmende Variable ist das Vertrauen, das bereits innerhalb eines Netzwerks herrscht oder eben nicht. Deshalb werden im Folgenden die verschiedenen Formen einer Blockchain vorgestellt.

2.3.7 Formen einer Blockchain

Auch wenn mit der Blockchain 1.0 nur eine Form der Blockchain bekannt ist, so kann man heute zwischen vier verschiedenen Formen unterscheiden.

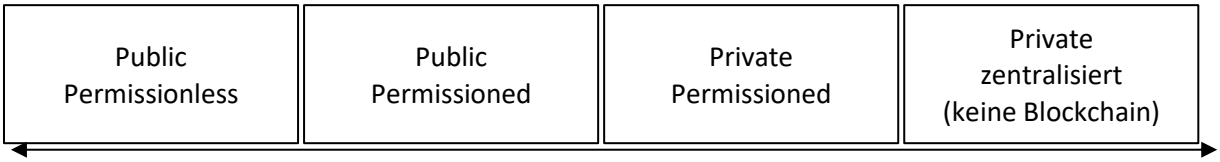


Abbildung 14: Formen einer Blockchain (Eigene Darstellung in Anlehnung an Walport, 2015, p. 35)

Public vs. Private Blockchain

Die öffentliche bzw. public Blockchain ist offen für alle Teilnehmer. Als prominentestes Derivat zählt Bitcoin, mit welcher die Blockchain 1.0 vorgestellt wurde. In dieser Form der Blockchain gibt es keine Beschränkungen auf die Teilnehmer, welche die Daten auslesen und Transaktionsvorschläge einreichen darf. Dabei sind die Daten durch kryptographische Funktionen und digitalen Signaturen dennoch verschlüsselt. Teilnehmer können die spezifischen Daten zwar immer noch lesen, jedoch nicht unbedingt verstehen. Ist die Blockchain für die Verwendung nur durch gewisse Teilnehmer wie eine Organisation oder einem Konsortium beschränkt, so ist die Blockchain privat (Peters & Panayi, 2015).

Permissionless vs. Permissioned Blockchains

Eine weitere Dimension der Form einer Blockchain ist die Berechtigungen auf Rollen im Netzwerk. Bei Bitcoin handelt es sich dabei beispielsweise um die Berechtigung zum Erzeugen von Blöcken. Bei einer permissionless Blockchain kann jeder Teilnehmer jede Rolle einnehmen während bei einer permissioned Blockchain die Berechtigung für verschiedene Rollen im Netzwerk zentral vorher vergeben wurden oder durch eine vordefinierte Liste, genannt Whitelist, gewährt wurde. Die Identität der Teilnehmer wird geprüft und je nach Ausprägung muss der Teilnehmer verschiedenen Richtlinien durch KYC oder KYB Prozesse genügen, um am Netzwerk zu partizipieren. Im Gegensatz zu öffentlichen Blockchains ist die Identität der Teilnehmer oder zumindest dessen Vertrauenswürdigkeit somit bekannt (Swanson, 2015). Bekannte Derivate, welche eine permissioned Blockchain nutzen, sind Ripple (Kryptowährung) und Hyperledger (Smart Contracts). Durch das bereits vorhandene Vertrauen können zeitaufwändige Konsensmechanismen einfacher umgesetzt werden. Die geschlossene Blockchain bietet entsprechend eine höhere Geschwindigkeit der Prozessierung im Vergleich zu einer öffentlichen Blockchain. Hierbei handelt es sich jedoch um eine Blockchain mit Restriktionen mit welchen sie von den Kernprinzipien

der originalen Blockchain abweicht, wie *decentralisation* und *no-trust* – die Teilnehmer kennen und vertrauen sich hier bereits.

Hybrid

Neben den öffentlichen und privaten sowie permissionless und permissioned Blockchains existieren hybride Formen, welche verschiedene Eigenschaften der vier Formen kombinieren und somit verschiedenen Ansprüchen gerecht werden. So nutzen Unternehmen, welche regulatorische Rahmenbedingungen einhalten müssen, private, permissioned Blockchains ein.

2.4 Aufbauende Konzepte

Entsprechend der Literatur unterscheidet auch diese Arbeit zwischen drei wesentlichen Hauptkategorien von Blockchain Applikationen (Swan, 2015, p. ix ff.):

- **Blockchain 1.0: Die Währung**
  Die Anwendung der Blockchain für die Entwicklung von Kryptowährungen in Bezug auf den Zahlungsverkehr.
- **Blockchain 2.0: Die Verträge**
  Die Anwendung der Blockchain für die Entwicklung von wirtschaftlichen, handelsgetriebenen und finanziellen Vorgängen, welche komplexer sind als der reine Zahlungsverkehr im Sinne einer Geldüberweisung.
- Blockchain 3.0: Die nächste Evolution
  Die Anwendung der Blockchain auf weitere Felder wie der Wissenschaft, der Behörden, des Gesundheitswesens und vielen weiteren Gebieten.

In den nachfolgenden Unterkapiteln werden die Konzepte der Blockchain 1.0 und 2.0 erläutert. Hierzu wird für die Blockchain 1.0 *Bitcoin* als bekanntestes Derivat näher betrachtet. Für die Blockchain 2.0 wurde *Ethereum* als derzeit erfolgreichstes Vorhaben (Müller & Hasic, 2016, p. 16) gewählt. Auch wenn sich die folgenden Konzepte basierend auf der Blockchain Technologie bereits als Anwendungsfelder klassifizieren lassen, werden diese grundlegenden Anwendungsfälle bewusst nicht als aktuelle Anwendungsfälle eingeordnet. Dies deshalb, da die Konzepte den Funktionsumfang der Blockchain bestimmen bzw. erweitert haben und somit nach Sicht des Autors fest mit der Blockchain Technologie verbunden sind. Unter Blockchain 3.0 verstehen sich dann aber die potenziellen Anwendungsfelder der Technologie.

2.4.1 Kryptowährungen

Kryptowährungen bilden den ersten Anwendungsfall einer Blockchain überhaupt. Namentlich ist es Bitcoin, welche das Erfindersyndikat um Satoshi Nakamoto auf Basis der Blockchain umgesetzt hat. Da die Blockchain eigens für die Kryptowährung konzipiert wurde, nutzte dieser Anwendungsfall das gesamte Potenzial, welches die Blockchain anfangs zu bieten hatte. Die Währungen sind dabei effektiv nichts weiter als Hash-Werte in ihrem jeweiligen System (Müller & Hasic, 2016).

Kryptowährungen gab es schon vor bereits 20 Jahren, bevor die erste Blockchain-basierte Kryptowährung – Bitcoin – eingeführt wurde. Im Gegensatz zu dieser verliessen sich diese auf dritte Parteien, welche die Währung verwalteten und ausgaben. Diese Abhängigkeit bot jedoch einen Angriffspunkt, was schliesslich zu ihrem Scheitern führte (Forte, et al., 2015). Die Blockchain vermeidet solch eine Abhängigkeit.

Während des letzten Jahrzehnts haben sich neben Bitcoin weitere digitale Währungen wie LiteCoin, PeerCoin, AuroraCoin, DogeCoin und Ripple entwickelt, welche alle auf die einst für Bitcoin entwickelte Technologie basieren. Dies nur die bekannteren Blockchain Applikationen. Insgesamt sollen es bis zum heutigen Zeitpunkt mehr als 3’000 Kryptowährungen basierend auf Blockchain sein, wovon mindestens hundert einen täglichen Handelsumsatz von jeweils über 1'000 US Dollar erreichen (Vigna & Casey, 2016). Eine Studie des World Economic Forum (2015) prognostiziert, dass in den nächsten elf Jahren Transaktionen im Umfang von 10% des globalen Bruttoinlandsprodukts über die Blockchain gespeichert werden. Wenn immer eine Kryptowährung neu emittiert wird, spricht man auch von einem ICO – Initial Coin Offering. Der Erfolg der Bitcoin ist der Beachtenswerteste unter all jenen Kryptowährungen; besonders in Bezug auf die eindrückliche Preisentwicklung. Erst im März 2017 stellte die Währung einen neuen Rekord auf: Erstmals übertraf der Wert des digitalen Geldes den Preis einer Unze Feingold mit 1'235 US Dollar (Nestler, 2017). Zwischenzeitlich hat sich der Wert der Bitcoin weiter gesteigert und hat im Mai 2017 die Marke von 2'500 US Dollar deutlich überschritten.

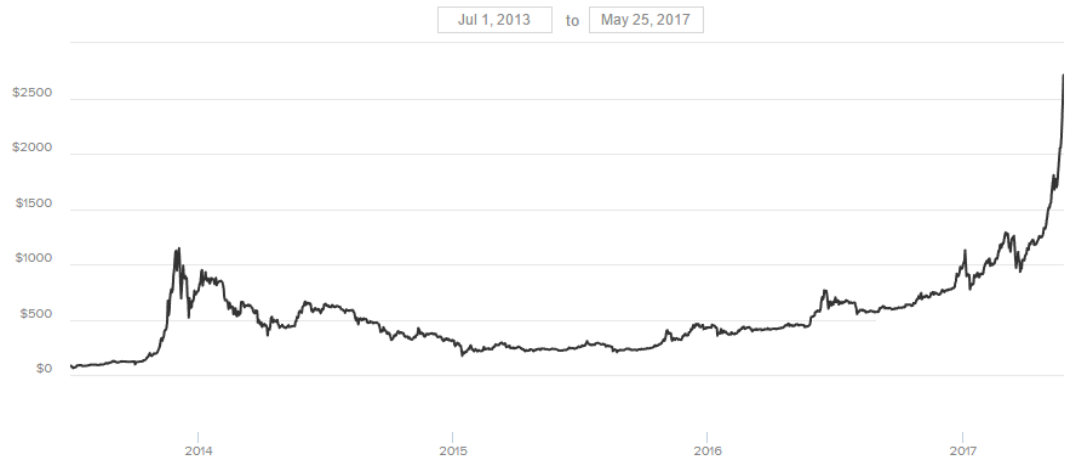


Abbildung 15: Kursentwicklung der Bitcoin seit deren Bestehen (Coindesk, 2017)

Die obere Abbildung zeigt die Entwicklung des Kurses der Bitcoin zum US Dollar. Ebenso eindrücklich wie die Preisentwicklung ist die Preisvolatilität der digitalen Währung (Ciaian et al., 2016).

Der Erfolg der Kryptowährung wird umso beachtlicher, wenn man die vorhergehenden, gescheiterten Versuche zur Konstruktion einer elektronischen Währung hinzuzieht. Dazu gehört CyberCash, welches bereits kurz vor der Jahrtausendwende auf den Markt kam und durch den Y2K Bug[4] grosse Verluste verursacht hat und bereits im Jahr 2001 wieder vom Markt verschwand (Bonneau et al., 2016, S. XIII). Der vom World Wide Web Consortium (W3C) Mitte der Neunzigerjahre verabschiedete Standard zum Zahlungsverkehr im Web, genannt «Standard Secure Electronic Transactions», kurz SET, auf welchem auch CyberCash und viele weitere Versuche von elektronischen Währungen basierten, hatte eine fundamentale Schwachstelle: Zertifikate. Durch die Pflicht, dass Händler und gar Kunden ein eigenes Zertifikat besorgen mussten, war die Nutzerakzeptanz von Anfang an gering (Bonneau et al., 2016, S. XIII). 2015 hat das W3C jedoch bekannt gegeben, einen neuen Versuch zur Standardisierung zu initiieren, wobei man Bitcoin gleich miteinbezieht und auf dessen bewährtes Konzept der Kryptowährungen bei der Ausdefinierung des überarbeiteten Standards zurückgreift (Myers, 2015).

Die Euro Banking Association (2015) sieht drei Verwendungszwecke, an welche sich Kryptowährungen richten: Online Handel, Wertabsicherung und Spekulation.

[4] Der Y2K Bug, auch als Jahr-2000-Problem bezeichnet, ist ein Problem von Informatiksystemen, welche die Behandlung von Jahreszahlen als zweistellige Angabe nutzten und dadurch beim Jahreswechsel 1999/2000 keine logisch korrekten Datensätze mehr generieren können (Branigin, 1998)

2.4.1.1 Funktionsweise (Mining)

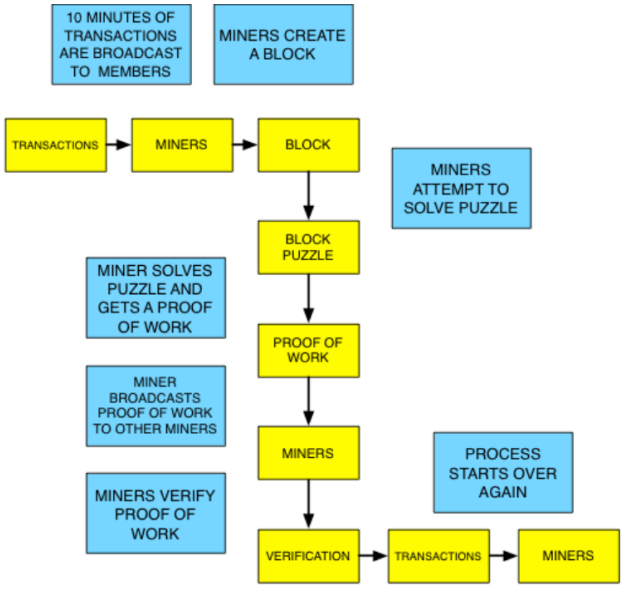


Abbildung 16: Funktionsweise von Bitcoin (Napkin Finance, 2016)

Die obere Abbildung zeigt die Funktionsweise im Kontext der Bitcoin vom Senden der Transaktion bis zur Verifikation und die Archivierung in der Blockchain. Eine Transaktion sieht dabei folgendermassen aus:

LEDGER

ACCOUNT TYPE	CASH				
TRANSACTION DATE	TRANSACTION DETAIL	REFERENCE	DEBIT	CREDIT	BALANCE
1/1/16	Expenses for Jan	Ref#1	$100.00		$100.00
2/1/16	Tax withheld	Ref#2		$110.00	($10.00)

Tabelle 5: Beispiel eines Blocks einer Kryptowährung (IBM Research, 2017)

Wichtig ist, dass eine Transaktion erst gültig ist, sobald diese innerhalb eines Blocks in der Blockchain abgelegt und somit von allen Teilnehmern im Netz gesehen werden kann. Hierzu bedarf es dem Prozess des Mining.

Mining

Der Begriff Mining, zu Deutsch schürfen, ist bekannt aus der Goldgewinnung. Im Kontext der Bitcoin wird dem Begriff eine ähnliche Bedeutung zugewiesen. Anstelle von Gold werden hier jedoch digitale Token und die damit verbundene Kryptowährung geschürft. Hierbei kann bei Kryptowährungen das

Gesamtvolumen im Kontext einer public Blockchain (vgl. 2.3.7 Formen einer Blockchain) nur durch das Mining erhöht werden. Das Mining bei Bitcoin dient den folgenden zwei Zwecken (Coindesk, 2014):

- Erzeugen von Coins (Bitcoins)
- Verifikation und Bestätigung von Transaktionen

Dabei gilt, dass eine Transaktion erst gültig ist, wenn sie durch den Mining Prozess erfolgreich verifiziert und damit der Blockchain hinzugefügt wurde (Antonopoulos, 2014, pp. 26-29). Zusätzlich ist das Gesamtvolumen bei Bitcoin limitiert auf insgesamt 21 Millionen Bitcoins. Dies ist fest im Protokoll verankert (Antonopoulos, 2014, p. 177).

Der Prozess des Mining kann in folgende Schritte eingeteilt werden (Coindesk, 2014):

- Verifikation der Transaktion
- Sammeln von Transaktionen in einen Block
- Selektion des Headers des aktuellsten Blocks und Übernahme als Hash-Wert in den neu zu erzeugenden Block
- Lösen des PoW Rätsel
- Hinzufügen des Blocks an die lokal gespeicherte Kopie der Blockchain
- Propagieren der Änderung ins Blockchain Netzwerk

Dabei gilt, je mehr Miner ein Netzwerk hat, desto sicherer wird es. Der Mining Prozess wird immer dann gestartet, nachdem ein neuer Block aus dem letzten Mining Prozess erfolgreich der Blockchain hinzugefügt wurde. Im Beispiel der Bitcoin wurde der Soll-Durchschnitt der Mining Dauer – sprich der Generierung eines neuen Blocks – auf zehn Minuten festgelegt. Um diesen Wert trotz der steigenden Anzahl von Teilnehmern mit stärkerer Rechenleistung beizubehalten, wird die *Mining Difficulty* des PoW kontinuierlich erhöht. Hierbei wird alle 2'016 Blöcke – entspricht ca. zwei Wochen - der *Target Value* neu berechnet, um die durchschnittliche Zeit zum Minen eines Blocks bei zehn Minuten zu halten.

Mining Pools sind hierbei Zusammenschlüsse von einzelnen Computern, welche gemeinsam mehr Rechenleistung erbringen.

Incentive

Wie der Abbildung 13 zu entnehmen ist, führt ein gelöstes PoW Rätsel zu einer Belohnung – *Incentive.* Mit jedem neuen Block erhält der Erzeuger somit eine Belohnung in Form von Coins. Bei Bitcoin sind dies zurzeit 12.5 Bitcoins pro Block. Dieses Incentive halbiert sich alle 210'000 Blöcke um die Hälfte.

Bei einem maximalen Volumen von 21 Millionen Bitcoins lässt sich dies in einer mathematischen Funktion fassen:

$$\frac{\sum_{i=0}^{32} 210000 \lfloor \frac{50.10^8}{2^i} \rfloor}{10^8}$$

Die nächste Halbierung wird im Juni 2020 erwartet (Bitcoinblockhalf, 2017). Daneben gibt es einen zweiten des Incentives; die Transaktionsgebühr.

Jeder Sender einer Transaktion kann selbst bestimmen, wie viel von seinem zu überweisenden Betrag als Transaktionsgebühr ausbezahlt wird. Ein Miner bekommt hierbei die Gebühren aller Transaktionen, welche er in einem Block gesammelt hat (Bonneau, et al., 2016, p. 40). Auch wenn es sich um eine freiwillige Gebühr handelt, kommt diese Art des Incentives zum Tragen, sobald alle Bitcoins – 21 Millionen – geschürft sind. Denn mit diesem Moment entfällt die erstgenannte Belohnung und die Miner werden ausschliesslich über die Transaktionsgebühr zur Verifikation von Transaktionen motiviert (Nakamoto, 2008).

2.4.1.2 Vorteile

Keine zentrale Abhängigkeit

Im Gegensatz zu den bereits erfolglosen digitalen Währungen vor Bitcoin ist diese nicht abhängig von Drittparteien. Durch die Dezentralisierung erfolgt die Verifikation und Erzeugung der Währung voll automatisiert und stets mit vollster Sicherheit (Morabito, 2017).

Double-Spending Attacke

Die Double-Spending Attacke beschreibt das Problem der Mehrfachausgabe des gleichen digitalen Tokens. Dabei unterliegt es der Theorie, dass jedes digitale Objekt sich sehr leicht vervielfachen lässt, der Unterschied zum Original jedoch nicht auszumachen ist. Dies bedeutet, dass ein Benutzer beispielsweise den Bitcoin in einer Transaktion gleichzeitig an mehrere Personen überweist. Gleichermassen fallen unter der Double-Spending Attacke Transaktionen mit Token, welche gar nie dem Sender gehört haben. Die Lösung dieser Problematik lässt sich ganz einfach umschreiben: Blockchain. Durch die folgenden Eigenschaften verhindert die Technologie eine unrechtmässige Double-Spending Attacke:

- Die gesamte Transaktionshistorie eines jeden Bitcoins ist für jeden sichtbar und zu jederzeit verfügbar
- Die Blockchain besteht aus einer nummerierten Transaktionskette, bei der nur Transaktionen bzw. Blöcke hinzugefügt werden können, jedoch nicht nachträglich mutiert oder gar gelöscht
- Die digitale Signatur beweist die Eigentümerschaft des jeweiligen Bitcoins

- Jeder Bitcoin ist eindeutig identifizierbar über eine Seriennummer

Unmöglichkeit der Fälschung – Immutability

Wie es auch der Vorteil der Blockchain ist, so können die Kryptowährungen basierend auf dieser Technologie und deren Transaktionen nicht gefälscht werden (Morabito, 2017).

2.4.1.3 Nachteile

Konsensmechanismus

Der häufig bei Kryptowährungen angewendete PoW-Ansatz ist ein kontroverser Ansatz zur Erreichung des Konsenses innerhalb des Netzwerks (vgl. 2.3.6.1 Proof of Work).

Funktionalität

Die Blockchain 1.0 verfügt über einen limitierten Funktionsumfang. So können vereinfacht gesagt nur Transaktionen ausgeführt werden, wobei ein Sender einen Betrag an einen Empfänger überweist. Bedingungen oder andere komplexere Funktionen lassen sich dabei nicht umsetzen. Zusätzlich entstehen Probleme hinsichtlich des Konsumentenschutzes, da Transaktionen irreversibel sind (Morabito, 2017).

Die Pseudoanonymität

Auch wenn innerhalb des Bitcoin Netzwerks anonyme Identitäten durch die Erzeugung neuer digitaler Signaturen erstellt werden können, so impliziert dies nicht automatisch eine absolute Anonymität. Durch die Transaktionen, welche über diese 'Identität' getätigt werden, lassen sich Verhaltensmuster generieren. Durch den Fakt, dass die gesamte Transaktionshistorie – sprich die Blockchain an sich - öffentlich ist, können so Analysen getätigt werden und möglicherweise Rückschlüsse über die Person getroffen werden (Spagnuolo, et al., 2014, p. 457ff.). Deshalb reden Wissenschaftler von einer Pseudoanonymität oder kurz Pseudonymity von Kryptowährungen. Auch wenn dazu noch ein grosser Aufwand betrieben werden müsste, so lässt sich die Pseudoanonymität nicht verleugnen (Spagnuolo, et al., 2014, p. 458).

Die Pseudodezentralisierung

Als Begrifflichkeit abgeleitet von der Pseudoanonymität kritisieren viele Wissenschaftler die propagierte Dezentralisierung von Kryptowährungen (Bonneau, et al., 2016, p. 129ff.). Das Paradoxon erschliesst sich durch folgende Überlegungen. Es gibt zunächst eine zunehmende regionale Zentralisierung der Mining Pools in Asien, explizit in China. Gegeben durch günstige Strompreise (staatlich oder durch Korruption) ist es wesentlich günstiger, Mining Pools dort zu betreiben. Neben diesem stark

diskutierten Thema gibt es aber auch Wallet Anbieter oder Bitcoin Börsen, welche genau genommen zentral agieren oder nur schwach dezentralisiert sind.

Preisvolatilität

Die Ungewissheit der Preisentwicklung ist ein generelles Problem der Kryptowährungen. Durch die unkontrollierte Entwicklung ist es schwer, die derzeitig in der Finanzpolitik umgesetzten Massnahmen auf eine Kryptowährung anzuwenden. Als Beispiel ist der enorme Wertzuwachs der letzten Tage im Mai 2017 zu betrachten. Ein solcher Wertzuwachs würde einer gigantischen Deflation gleichkommen, welche schlimmer wäre als jene, die durch die Weltwirtschaftskrise der USA in den Dreissigerjahren des zwanzigsten Jahrhunderts verursacht wurde (Meier, 2017). Bitcoin stellt somit keine gute Option für den Ersatz von traditionellen Währungen dar.

Transaktionsgebühr

Die Transaktionsgebühr, welche aus den Kosten des Mining bestehen, sind abhängig von den Daten (Anzahl Transaktionen) und nicht dem Betrag, der überwiesen wird. Die Transaktionsgebühren wurden initial als Vorteil aufgeführt. Doch durch diese Abhängigkeit von Gebühr und Daten kann es dazu führen, dass bei kleinen Beträgen die Transaktionsgebühr höher ausfallen kann als der zu überweisende Betrag.

Begünstigung illegaler Aktivitäten

Aufgrund von der häufigen Nutzung von Bitcoins im Kontext illegaler Aktivitäten sowie der Anonymität, unter welchem Deckmantel solche Geschäfte agieren, werden Kryptowährungen von keiner Bank in der Schweiz angenommen, denn sie fallen in der Schweiz durch die FINMA geregelt unter die Geldwäschereiverordnung (FINMA, 2015). Auch in vielen anderen Ländern wie die USA sind solche Verordnungen zu Ungunsten der Kryptowährungen vorhanden.

Die Incentivierung

Insbesondere beim PoW Mechanismus fallen Transaktionskosten an. Diese dienen als Incentivierung der Miner für ihre Rechenleistung. Bitcoin gibt vor, dass der Betrag alle vier Jahre um die Hälfte reduziert wird. Dies aufgrund der Erwartungshaltung, dass sich in dieser Zeit mehr und mehr Teilnehmer dem Netzwerk anschliessen. Diese Erwartungshaltung lässt sich jedoch nicht verifizieren.

2.4.2 Smart Contracts

Die Smart Contracts im Kontext der Blockchain werden als dessen Weiterentwicklung gesehen und setzen auf die Vorteile dieser auf (Swan, 2015, p. 9). Schon 1997 wurde das Konzept der Smart

Contracts von Nick Szabo folgendermassen als computerbasiertes Transaktionsprotokoll definiert, das die Bedingungen eines Vertrags inkludiert (Szabo, 1997).

Diese Dimension der Blockchain befindet sich noch immer in der Entwicklung und es gibt keine Standarddefinitionen. Daher gibt es neben den eigentlichen Smart Contracts weitere Blockchain Softwares und Applikationen, die zu den Blockchain 2.0 Applikationen gehören. Darunter unter anderem Bitcoin 2.0, Smart Properties, dezentrale Applikationen (DAPP), dezentrale, autonome Organisationen (DAO) und dezentrale, autonome Unternehmen (DAC) (Swan, 2015, p. 9). Allen gemein ist deren Erweiterung der initialen Prinzipien der Blockchain 1.0 um *Automatization* und *Interaction*. Diese Arbeit fokussiert auf die Smart Contracts und deren verwendete Systemkomponenten als bekanntesten Vertreter der Blockchain 2.0. Smart Contracts im Kontext der Blockchain basieren grundlegend auf der Definition von Szabo (1997). Unter den vielen Definitionen ist folgende am prägnantesten:

> *"A smart-contract is an event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger"* (Brown, 2015)

Es handelt sich dabei vereinfacht gesagt um kleine Computerprogramme, die Entscheidungen basierend auf bestimmten Bedingungen treffen können (Kôlvart, et al., 2016). Smart Contracts bilden den Input von *dezentralisierten Applikationen* (DAPP), bei welchen es sich um dezentral laufende Applikationen handelt, welche von der Ethereum Blockchain und der dazugehörigen Ethereum Virtual Machine unter Zunahme des Smart Contracts ausgeführt werden können. Die Smart Contracts beinhalten einen Wert (Token oder Coins) und ein Regelwerk um diesen Wert, welches aus Bedingungen besteht.

Die grundlegende Idee dahinter ist, dass die Bedingungen (im Kontext von Vertragsbedingungen) zur Transaktion eines Werts durch dieses Regelwerk innerhalb der Blockchain ohne eine weiteren Intermediär verifizierbar wird (Mougayar, 2016). Dafür können durch die Smart Contracts externe Informationen verarbeitet werden, um mittels der vordefinierten Regeln und Bedingungen, welche in der Blockchain abgelegt sind, einen bestimmten Vorgang auszulösen. Smart properties sind hierbei Werte (digital oder physikal durch Asset Tokenization digitalisiert), welche einen Eigentümer in der Blockchain verlinkt haben und somit einen klar definierten Eigentümer aufweisen (Mougayar, 2016).

2.4.2.1 Funktionsweise

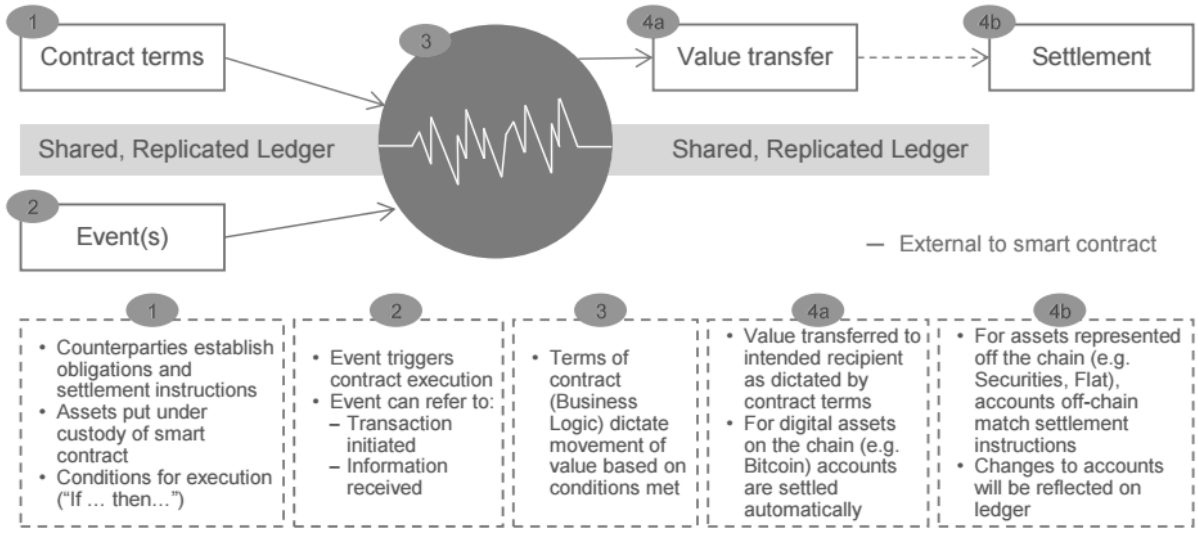


Abbildung 17: Funktionsweise eines Smart Contracts (Tuesta, et al., 2015)

Die obige Abbildung zeigt die Funktionsweise eines Smart Contracts. In dieser Arbeit wird der aktuell bekannteste Vertreter von Smart Contracts als Blockchain Software betrachtet; Ethereum basiert auf der von Swan (2015) definierten Blockchain 2.0. Es handelt sich hierbei um eine Erweiterung des mit Bitcoin eingeführten Blockchain. Wie Bitcoin kann auch Ethereum auf der Ebene der Applikationen digitales Geld genutzt werden. Doch im Gegensatz zu Bitcoin und allen Kryptowährungen, welche auf der Blockchain 1.0 basieren und eindimensionale Transaktionen erlauben, sind weitere Anwendungsfälle möglich (Grassegger, 2015, p. 16). Ethereum als Vertreter der Blockchain 2.0 in dieser Arbeit ist im hohen Grad programmierbar. Es wurde so gestaltet, dass komplexe Anwendungen darin umgesetzt werden können. Solche Blockchain Softwares erstellen Token (Bitcoin nur Coins).

Die Ethereum Fundation ist eine Organisation mit Sitz in Baar im Kanton Zug. Das vom Russen Vitalik Buterin gegründete Unternehmen beschäftigt sich mit Smart Contracts und nutzt eine eigene Kryptowährung namens Ether. Dabei handelt es sich um eine open-source Blockcain, welches allen Teilnehmern ermöglicht, dezentrale Anwendungen auf der Blockchain auszuführen.

Ethereum Virtual Machine

Die Ethereum Virtual Machine läuft bei jedem Teilnehmer im Netzwerk und ermöglicht Anwendern, beliebig komplexe DAPPs auszuführen und mittels den Smart Contracts zu steuern. Dabei sind diese virtuellen Maschinen vergleichbar mit bestehenden wie die Java Virtual Machine. Sie bilden eine Umgebung, in welcher DAPPs mittels Smart Contracts ausgeführt werden können. Dabei können hierbei verschiedene Programmiersprachen zur Erstellung von Smart Contracts genutzt werden (Solidity – die Ethereum-eigene Programmiersprache, Javascript oder Python) (Ethereum Homestead, 2016).

Ether & Gas

Auch Ethereum hat im Kontext der Smart Contracts eine Kryptowährung implementiert, welche die Bezahlung innerhalb des Netzwerks ermöglicht. Sie lautet Ether und ist ebenfalls für jeden im Tausch durch traditionelle Währungen erwerbbar. Daneben exisitert jedoch eine andere Messgrösse, die sich bei Ethereum Gas nennt. Diese wird innerhalb von Ethereum als Grundlage zur Berechnung der Transaktionsgebühr verwendet. So wird die Transaktion zwar in Ether bezahlt, jedoch wird die Transaktion durch Gas multipliziert. Gas bildet den Arbeitsaufwand, welcher benötigt wird, um die Transaktion auszuführen. Dabei kommt dieser Transaktionsgebühr eine besondere Funktion zur Absicherung des Netzwerks gegen DoS-Attacken – sprich der Überflutung des Netzwerks mit in diesem Fall vielen Smart Contract Transaktionen - zu. Denn durch diese Transaktionsgebühr wird abgesichert, dass sinnlose Transaktionen sehr kostspielig sind. Als weiteren Vorteil zählt die gesteigerte Code Effizienz durch diesen Ansatz. Denn je effizienter dieser ist, desto weniger Rechenleistung wird zu deren Ausführung benötigt was zu einer niedrigeren Gas Wert und somit zu einer niedrigeren Transaktionsgebühr führt.

Erweiterter Gebrauch des Merkle Trees

Zwar führt die Verwendung des Merkle Trees bei Bitcoin zu einer schnellen Verifikation von gemachten Transaktionen, doch bietet die einfache Merkle Tree keinen Status zu gemachten Transaktionen. Bei Ethereum kommen deshalb mehrere Merkle Trees zum Einsatz, um die Dimensionen Transaktion, Belege (Effekt einer Transaktion) und den Status ebenfalls abzulegen (Buterin, 2015).

Folgende Abfragen können mittels dieser Verwendung von mehreren Merkle Trees gemacht werden:

- Ausgabe aller Instanzen eines Events *x*, die durch eine Adresse *y* im Zeitraum *z* emittiert wurden
- Existenz des Accounts
- Aktueller Kontostand
- Simulation der Durchführung einer Transaktion auf einem Smart Contract und der entsprechende Output

Ausführung eines Smart Contracts

Die Funktionsweise eines Smart Contracts in Ethereum kann wie folgt aufgezeigt werden. Hierzu wird der Prozess eines Kaufs eines Musiktitels als Beispiel genommen. Dieser hat drei verschiedene Funktionen: Kaufen, Kauf verifizieren und Album herunterladen. Für einen Kauf schickt ein Teilnehmer einen Betrag (Ether) an die DAPP des Verkäufers. Die DAPP prüft den Betrag und fügt die Adresse (Hash-Wert) des Käufers sowie einen Status in die Käuferliste. Um den Musiktitel zu beziehen, ruft der Käufer die Funktion Album herunterladen auf. Die DAPP prüft die Käuferliste nach der Adresse des Käufers

und gibt aufgrund dessen den Download frei. Mit der Funktion Kauf verifizieren können Käufer beweisen, dass sie den Musiktitel gekauft haben, in dem sie nur ihre Adresse mitteilen. Die DAPP kann damit erneut prüfen, ob die Person in der Käuferliste vorhanden ist. In der folgenden Abbildung sind die einzelnen Schritte visuell dargestellt.

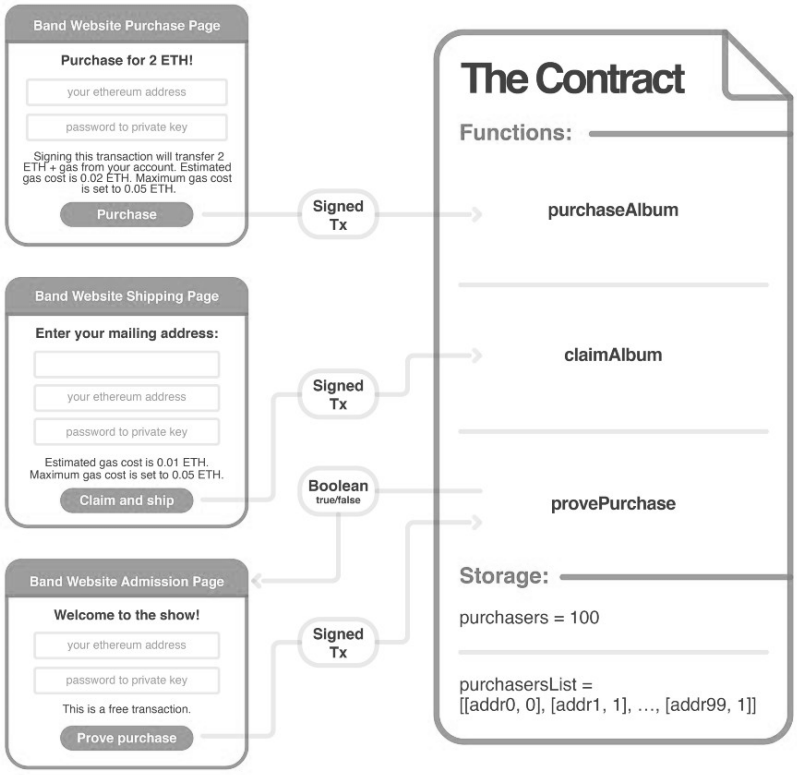


Abbildung 18: Smart Contract Interaktionen (Goldin, 2017)

2.4.2.2 Anwendungsbeispiele

Eth-Tweet ist ein verteilter Dienst, welcher die Funktionalitäten von Twitter auf einem verteilten Netzwerk anbietet. Dabei gibt es auch keine zentrale Autorität, welche die Nachrichten löschen könnte. Dies kann nur der Ersteller selbst. Des Weiteren können Teilnehmer Spenden in Ether erhalten. Dies soll laut den Machern die Motivation liefern, sich aktiv am Netzwerk zu beteiligen (github, 2016).

WeiFund nutzt Ethereum als Crowdfunding Applikation. Über einen Browser mit Ethereum Unterstützung wie Ethereum Mist kann die Seite aufgerufen und Crowdfunding Projekte unterstützt werden. Im Vergleich zu bekannten Crowdfunding Seiten wie Kickstarter nutzt WeiFund Smart Contracts. Dadurch können Zahlungen von Supportern mit komplexen Bedingungen verknüpft werden. So ergibt sich ein weiteres Feld an Möglichkeiten, wie Investitionen gesteuert werden können (Palmer, 2016).

2.4.2.3 Vorteile

Die folgenden Vorteile sind ergänzend zu den Vorteilen der Blockchain 1.0.

Automatisierung und Echtzeitausführung

Die Umsetzung von Smart Contracts erlaubt die automatisierte Ausführung von vorbestimmten Bedingungen. Durch die Automatisierung braucht es keinen Intermediär, welche die Transaktion und deren Bedingungen überprüfen muss, womit störende Eingriffe dritter Parteien in die Ausführung entsprechend nicht notwendig bzw. möglich sind (Juels, et al., 2015). Die Vertragsausführung erfolgt dabei in Echtzeit.

Kostenersparnis

Durch die Reduzierung von Intermediären im Prozess der Vertragsausführung reduzieren sich die Kosten für Vertrag, Durchsetzung und Compliance (Walport, 2015). Die Interaktionen zwischen den Vertragsparteien reduziert sich dadurch ebenfalls, was zu einer weiteren Effizienzsteigerung und deshalb Kostensenkung führt (Juels, et al., 2015).

Inkludierung von externen Faktoren

Durch die Smart Contracts können externe Faktoren in der Ausführung der Regeln inkludiert werden (Juels, et al., 2015). Dadurch erweitert sich das Spektrum von potenziellen Anwendungsfällen massiv, da meist eine Kondition eines Vertrags durch einen externen Faktor beeinflusst wird.

2.4.2.4 Nachteile

Exakte Ausführung / Flexibilität

Der Smart Contract wird exakt so ausgeführt, wie er implementiert wurde. Dies führt zu einem Ausschluss des Rückzugs einzelner Vertragsparteien. Dies kann jedoch auch als Vorteil gesehen werden (Juels, et al., 2015). Jedoch bedeutet dies auch, dass die Verträge bei der Implementierung exakt definiert werden müssen, was in gewissen Anwendungsfällen sehr viel Aufwand bedeutet. Dass dies zu desaströsen Ausmassen führen kann, zeigt ein Exploit eines Smart Contracts in Ethereum (Daian, 2016). Hierbei wurde eine Schwachstelle in einem Smart Contract ausgenutzt und ein Verlust von 150 Millionen USD erzeugt. Dabei handelte es sich um die finanziellen Mittel von Ethereum als Unternehmen. Das Unternehmen musste reagieren und hat deshalb einen Hard Fork initiieren, um den Verlust rückgängig zu machen. Dies wiederspricht jedoch eindeutig dem Prinzip der Immutability, weshalb der Schritt zu kontroversen Diskussionen unter den Experten führte und immer noch als Schwäche der

Blockchain betrachtet wird (Daian, 2016). Für Ethereum hätte kein Hard Fork jedoch zum Bankrott geführt.

Abbildung der realen Welt

Smart Contracts können zwar externe Faktoren bei der Ausführung von Bedingungen inkludieren, doch der reale Status eines Gegenstands liefert keine Daten (ausgenommen IoT Geräte). Somit zeigen sich hier erste Limitationen bezogen auf Anwendungsfällen (Tuesta, et al., 2015).

Zusätzlich ist es zum heutigen Zeitpunkt nicht klar, in wie weit ein Smart Contract eine rechtliche Basis hat. So fehlt die Option, seine Rechte basierend auf geltendem Recht durchzusetzen (Brown, 2015).

Wie bereits in vorhergehendem Nachteil erwähnt, muss ein Smart Contract zudem initial korrekt implementiert werden. Für die korrekte Abbildung von Verträgen und Regulatorien bedarf es zumindest initial einen grossen Aufwand (Tuesta, et al., 2015).

Beschränkung durch Daten

Hierbei ist nicht die Datengrösse gemeint, sondern der Fakt, dass jede Interaktion durch Daten in Form von Programmiercode ausgedrückt werden muss, um sie in einem Smart Contract zu bearbeiten (Peters & Panayi, 2015).

2.5 Anbieter und Anwendungsfelder

Insgesamt zählt im Januar 2017 die Organisation Venture Scanner (2017) knapp 900 Firmen, welche in irgendeiner Form mit der Blockchain arbeiten oder dieses als Grundpfeiler ihres Geschäftsmodells einsetzen. Dabei nutzt die Mehrzahl dieser Unternehmen die Anwendungsform der Kryptowährung der Blockchain. Reine Blockchain Unternehmen (im Venture Scanner Report als Blockchain Innovators bezeichnet), sind noch klein in der Zahl und in ihrer Grösse, werden jedoch von Investoren stark unterstützt. Knapp 855 Millionen USD von insgesamt 1,9 Milliarden USD an Venture Capital für Blockchain und Bitcoin wurden seit 2015 in diese Unternehmen investiert. Im Venture Scanner Innovation Quadrant (2017) wurden diese Unternehmen als Disruptors eingeordnet – also Unternehmen, welche ein stark disruptives Geschäftsmodell betreiben.

Abbildung 19: Blockchain / Bitcoin Unternehmen (Venture Scanner, 2017)

Die schiere Zahl an Anbieter führt in dieser Arbeit zur Koppelung dieser mit den Anwendungsfeldern. So werden nachfolgend zunächst die Anwendungsfelder beleuchtet und danach die Anbieter mit ihren Anwendungsfällen betrachtet.

Anwendungsfelder

Im Oktober 2014 wurde die erste Heirat in der Blockchain notariell beurkundet, welche einer Eintragung in einem behördlich geführten Personenstandsregister entspricht (Alexander, 2014). Die Universität Nicosia zertifiziert die Zeugnisse ihrer Studenten in Form von Transaktionen in der Blockchain und lässt die Bezahlung der Semestergebühren über Bitcoins zu (University of Nicosia, 2015). Im Juni 2016 fand in der Ukraine nach dreimonatiger Vorbereitungszeit die weltweit erste Blockchain-basierte Auktion statt, bei dem staatlich ausgestellte Lizenzen verkauft wurden (Kaltofen, 2016). Die britische Regierung erforscht den Nutzen der Blockchain innerhalb von öffentlichen Prozessen (UK Government Office for Science, 2016). Die Isle of Man (Land unter der britischen Krone) betreibt ein Handelsregister für Unternehmen basierend auf der Blockchain und hat diverse Reformen zugunsten der Blockchain und Bitcoin erwirkt (Coindesk, 2017). Deloitte arbeitet mit Blockchain-Technologie, um grösseres Vertrauen in die Bücher von Firmen zu schaffen und Prüfungen zu automatisieren (Allison, 2015). IBM arbeitet an diversen Initiativen zur Koppelung von IoT Geräten mit der Blockchain sowie einer standardisierten Identität für die Blockchain (Jai & Carmichael, 2017).

Nachfolgend werden aktuelle und potenzielle Anwendungsfelder von Blockchain betrachtet. Bereits seit der Vorstellung der Bitcoin und der darunterliegenden Blockchain Technologie haben Forscher damit begonnen, neue Anwendungsfelder für die innovative Technologie zu suchen (Müller & Hasic, 2016). Zwischenzeitlich haben sich konkrete Anwendungsformen der Blockchain Technologie ergeben. Aufgrund der Vielzahl an aktuellen Anwendungsfällen sollen die nach Meinung des Autors interessantesten und vielversprechendsten Anwendungsfelder samt ihren Anbietern betrachtet werden. Diese Auswahl stützt sich auf die getätigte qualitative Literaturrecherche sowie einer zusätzlichen Analyse der Suchaktivität zum jeweiligen Anwendungsfeld mittels Google Trends (Google Trends, 2017) und dem IBM Analytics Tool Watson. Die nachstehende Tabelle zeigt mögliche Anwendungsfälle und Beispiele der Blockchain 2.0 nach Swan (2015, S. 10).

Klasse	*Beispiele*
Generell	Hinterlegungstransaktionen, verzinsliche Wertpapiere, Schiedsgericht, mehrfach Signierung Transaktionen
Finanztransaktionen	Aktien, Private Equity, Crowdfunding, Bonds crowdfunding, bonds, Anlage Fonds, Derivate, Renten und Pensionen
Öffentliche Register	Land und Besitztum Ansprüche, Fahrzeugregistrierung, Geschäftslizenzen, Heiratsurkunde und Todesurkunde
Identifikation	Fahrausweis, Identifikationskarte, Pass oder Wählerregister
Private Register	Schuldscheine, Darlehen und Kredite, Verträge, Wetten, Unterschriften, Testamente, Trust und Übertragungsurkunden
Beglaubigungen	Versicherungsnachweise, Eigentumsnachweise und notariell beglaubigte Urkunden
Physikalische Asset Schlüssel	Das Zuhause, Hotelzimmer, Mietautos oder der Zugang zum Auto
Immaterielle Assets	Patente, Marken, Urheberrechte, Reservationen und

Tabelle 6: Beispiele für Blockchain 2.0 Anwendungen (Swan, 2015, p.10)

Zunächst wird auf die derzeit bekanntesten Anwendungsfelder eingegangen.

Schadprogramme

Ein sehr aktuelles Anwendungsfeld ist der Einsatz der Blockchain Technologie bei Schadprogrammen. Dabei handelt es sich um eine implizite Problematik von Bitcoin und potenziell auch anderen Kryptowährungen mit ähnlichen Eigenschaften. So stellen diverse Wissenschaftler fest, dass es eine positive Korrelation zwischen Suchbegriffen um Softwareentwicklung, illegalen Aktivitäten und Bitcoin gibt

(Yelowitz & Wilson, 2015). Dabei wird die Kryptowährung nicht direkt als Bedrohung genutzt, sondern als anonymes Bezahlmittel wie es davor die anonyme Transaktion über Zahlungsdienstleister wie Western Union geboten haben.

RANG	LAND	SUCHBEGRIFF WERT
1	Nigeria	100
2	Ghana	73
3	Estland	51
4	Slowenien	46
5	Südafrika	42

Tabelle 7: "Bitcoin" - Interesse nach Region (Google Trends, 2017)

Die Auswertung von Google Trends zeigt, dass der Begriff „Bitcoin“ in der aktuellen Momentaufnahme vom 10. Mai insbesondere in den afrikanischen Ländern eine hohe Beliebtheit aufweist. Aufgrund der aktuell umhergreifenden Schadsoftware «WannaCry», welche Benutzer- und Systemdateien von Windows Rechnern verschlüsselt und den Nutzer als Ransomeware für eine Entschlüsselung der Daten auffordert, einen unterschiedlich hohen Betrag in der Kryptowährung Bitcoin zu zahlen, verwundert diese Auswertung nicht. Hier sollte jedoch angemerkt werden, dass auch schon vor der Einführung von Bitcoin solche Angriffe stattfanden und somit Bitcoin nur eine Alternative zur Überweisung von Zahlungen darstellt. Dabei aber eine sehr viel leichtere als die traditionellen Optionen.

Finanzbranche

Aus der Literaturrecherche geht hervor, dass die Finanzbranche zurzeit die grössten Anstrengungen im Kontext der Blockchain betreiben. Entsprechend wird für die Betrachtung der aktuellen Anwendungsfelder die Anwendungsfelder dieser Branche gewählt. Trotz des Fakts, dass die Blockchain Technologie Finanzintermediäre theoretisch ersetzen könnte (Condos, et al., 2016, p. 18), argumentiert die Euro Banking Association (2015), dass auch diese Intermediäre durch den Einsatz der Technologie entscheidende Effizienzsteigerungen erzielen können. Eine Analyse von Santander InnoVentures (2015) zeigt unter anderem, dass die Infrastrukturkosten von Banken durch die Blockchain bis ins Jahr 2022 um bis zu 20 Millionen USD pro Jahr reduziert werden könnten (Belinky, et al., 2015).

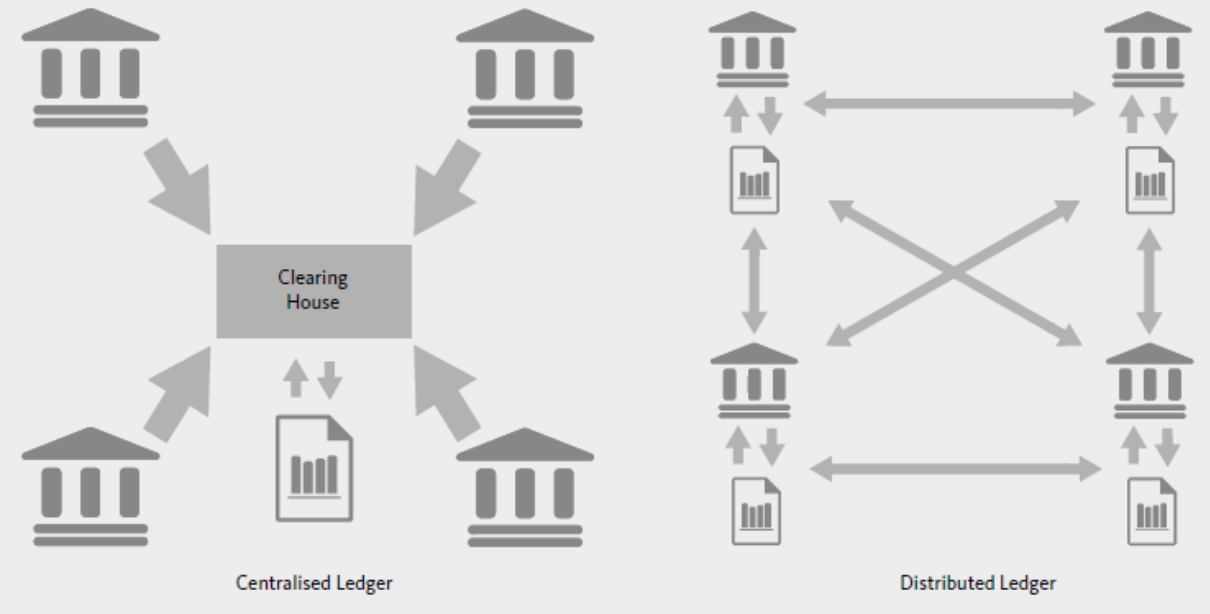


Abbildung 20: Vergleich der Abwicklungsformen mit und ohne Blockchain (Belinky, et al., 2015, p. 14)

Wie in oberer Abbildung dargestellt wird, kann der Einsatz der Blockchain durch die Dezentralisierung der Prozesse viele Schritte einsparen, in dem Intermediäre obsolet werden.

Eine Studie von PwC (2016) zeigt jedoch auf, dass bei mehr als 500 befragten Top-Managern aus der Finanzbranche nur 17% über die Blockchain gut bis sehr gut Bescheid wussten und somit 83% nur ein rudimentäres Verständnis davon hatten. In einer gemeinsamen Umfrage von Cofinpro und dem IT Finanzmagazin (2016) wurden 86 Akteure der Finanzbranche bezüglich ihrer Sicht von Blockchain befragt. Daraus konnten die folgenden Vorteile aus Sicht der Finanzunternehmen ermittelt werden:

Schnelligkeit, Kosten, Transparenz

Daneben wurden die Anwendungsfälle innerhalb des Geschäftsmodells einer Finanzinstitution gewertet mit folgendem Resultat:

Platz	*Bereich*	*Prozent*
1	Echtzeit-Überweisungen	74%
2	Krypto-Währungen	67%
3	Abwicklung von Aktien und derivative Finanzinstrumenten	64%
4	Umsetzung von Transparenzvorschriften für den Handel von Finanzinstrumenten	55%
5	Abwicklung von Bonds	43%

Tabelle 8: Anwendungsmöglichkeiten in einer Bank (Cofinpro AG, 2016)

Im Folgenden werden Anwendungsfälle betrachtet, welche durch eine Blockchain wesentliche Verbesserungen des Prozesses nachziehen.

Bereich	*Beschreibung*
Zahlungsverkehr	Der Zahlungsverkehr gehört zu einem der ersten Anwendungsfälle der Blockchain überhaupt und zwar handelt es sich um Bitcoin, welche eingehend im Kapitel 2.4.1 Kryptowährungen beschrieben wird. Die Probleme des heutigen Prozesses des Zahlungsverkehrs, welcher eine Vielzahl an Intermediären (Clearing-Stellen, Banken etc.) erfordern und eine lange Durchlaufzeit mit sich bringt, wird mittels der Blockchain und der darauf basierenden Kryptowährungen gelöst. Für Finanzinstitutionen wird insbesondere der internationale Zahlungsverkehr über die Blockchain als interessant gewertet (Euro Banking Association, 2015). Die tiefen Transaktionsgebühren sowie der durch die schnelle Verarbeitung reduzierten Wechselkursrisiken sind hierbei die ausschlaggebenden Gründe. Das Unternehmen **Ripple** mit der gleichnamigen Kryptowährung bietet genau aus diesem Grund Überweisungen mit den erwähnten Vorteilen an (RippleLabs, 2016). Aufgrund des effizienten Konsensmechanismus beträgt die Verarbeitungszeit einer Transaktion nur fünf bis 15 Sekunden – im Vergleich zu Bitcoin mit mindestens zehn Minuten (Swanson, 2015). Durch das Konzept der Tokenization können institutionelle Kunden im Ripple-Netzwerk beliebige Währungen transferiert werden. Dabei wird Währung zur Transaktion als Bitcoin gewandelt und kann nach erfolgreicher Transaktion in jede beliebige Währung umgetauscht werden (RippleLabs, 2016). Das Unternehmen **Circle** bietet einen ähnlichen Dienst auch für private Kunden an, welche mittels einer App kostengünstige und schnelle Zahlungen vornehmen können, wobei auch hier Bitcoins als intermediäre Tokens dienen (Kannenberg, 2014). Als weiterer Vorteil beschreibt Bogart und Rice (2015) eine Erhöhung der Sicherheit und Privatsphäre durch die wegfallende Pflicht, Adressen und Bankdaten bereitzustellen.
Kapitalmarkt	Auch im Devisenhandel sind mehrere Intermediäre involviert. Durch den ständigen Datenaustausch aufgrund von Kursschwankungen entstehen hier analog zum Zahlungsverkehr grosse Aufwände und entsprechend hohe Kosten.

	SETL ist ein Start-up, welches durch Deloitte finanziert wird. Durch den Einsatz der Blockchain wird das Handeln von Wertschriften sowie anderen Derivaten erleichtert. Dabei finden die Transaktionen in Echtzeit statt, wobei das System auf einer privaten, permissioned Blockchain basiert. Bereits im Jahr 2015 wurden pro Tag mehr als eine Milliarde Transaktionen durchgeführt (Setl, 2017).
Compliance	Die Compliance eignet sich sehr gut für die Blockchain, da hier ein grosser Wert auf die revisionssichere Ablegung von Datensätzen gelegt wird. Die Blockchain bietet mit ihrem Prinzip der Immutability und der Integrity der Daten die ideale Ausgangslage für einen Einsatz. Banken führen heute verschiedene Journale und haben diverse aufwändige und somit kostenintensive Mechanismen im Einsatz, um ein Fehlverhalten zu verhindern (Peters & Panayi, 2015). Dies inkludiert die Durchführung diverser interner Audits sowie die Segregation of Duties – der Verteilung der Verantwortung für die Verwaltung dieser Daten. **Balanc3** bietet als Start-up ein solches Buchhaltungssystem, welches auf Blockchain und Smart Contracts basiert und somit die Haltung von Daten mit voller Integrität, Irreversibilität der Einträge und zuverlässige Zeitstempel von Transaktionen (Peters & Panayi, 2015). Das System arbeitet dabei mit einer permissioned Blockchain. Daneben zählt die Erfüllung von diverser Gesetze und Regelungen zur Geldwäschereiprävention wie KYC und KYB – Know your client / business – zu hohen Kosten und verzögerten Transaktionen. Hier würde ein branchenweites Kundenregister basierend auf Blockchain den Aufwand für die individuelle Bank enorm reduzieren. Wenn der Prozess einmalig von einem Finanzunternehmen gemacht wurde, so können diese Informationen zum Kunden verschlüsselt in das branchenweite Kundenregister abgelegt werden und zukünftige Bankbeziehungen könnten dieses Register bei Bedarf prüfen und somit den Prozess signifikant beschleunigen. **KYC-Chain** ist eines der Start-ups, welche diesen Ansatz umgesetzt hat und teilnehmenden Banken so ein Kundenregister anbietet (KYC-Chain, 2017). Das System arbeitet dabei mit einer permissioned Blockchain.

Anbieter und Anwendungsfälle

Wie initial erwähnt, gibt es eine unübersichtlich grosse Anzahl an Anbietern, die eine fast ebenso grosse Anzahl an Anwendungsfällen bewirtschaftet. Nachfolgend sind die interessantesten Produkte beschrieben.

UNTERNEHMEN	BESCHREIBUNG
EVERLEDGER PRODUKTIV	Das hochgehandelte Start-up sieht sich als digitalen Tresor für Wertgegenstände. Diese werden mit diversen Attributen als digitales Abbild für die Blockchain erfasst (Tokenization). Ab diesem Zeitpunkt gelten die digital tokenized Assets als fälschungssicher, unveränderbar und somit vertrauenswürdig. Everledger fokussiert sich zurzeit auf Diamanten und Schmuckstücke, wo heute viele Betrugsfälle passieren. Häufig werden Zertifikate zu Diamanten dabei in Papierform erstellt, womit Versicherungsgesellschaften wie auch Behörden kein zentrales, vertrauenswürdiges Register für ihre Aktivitäten vorfinden.
ENIGMA PRODUKTIV	Enigma ist ein Start-up aus dem Massachusetts Institute of Technology, welches ermöglicht, sensitive Daten mit anderen in einem nicht-vertrauenswürdigen Netzwerk zu teilen. Hierbei nutzt das Netzwerk eine public Blockchain. Zusätzlich ist es Besitzern der sensitiven Daten möglich, diese anonym zu monetisieren. Dies erinnert den Autor dieser Arbeit jedoch auch an illegale CD Verkäufe mit sensitiven Daten, was dann noch einfacher wäre. Innovativ an der Idee ist die Analyse und Verarbeitung von Daten durch im P2P-Netzwerk verfügbare Rechenleistung, ohne dass diese 'fremden' Rechner die Daten selbst lesen können (Prisco, 2015). Als Relativierung der vom Autor getroffenen Aussage zu den CDs könnte man durch diese Funktionalität geheime Steuerdaten auf P2P-Clients in Deutschland verarbeiten, ohne, dass diese den Inhalt lesen können.
STORJ PRODUKTIV	Storj ist ein Start-up, welches ermöglicht, Daten wie auf den bekannten Cloud Speicher Anbietern wie Dropbox oder Microsoft's OneDrive abzulegen. Anstelle diese jedoch auf zentralen Servern zu speichern, werden sie in einem P2P Netzwerk bei verschiedenen Nutzern verschlüsselt abgelegt. Dabei bietet das Unternehmen dank der Blockchain Sicherheit und Privatsphäre, in dem zum einen die Daten allgemein verschlüsselt sind aber vor

	allem durch die Verwaltung dieser in der Blockchain. Damit gewährt Storj zwei Eigenschaften (Sicherheit, Privatsphäre), welche insbesondere seit der Snwoden-Affäre an Gewicht gewonnen haben (Wilkinson, et al., 2016). Die Blockchain Applikation basiert hierbei auf Ethereum und wird zudem von dessen Gründer Vitalik Buterin unterstützt und beraten (Wilkinson, et al., 2016).
DNA.BITS ENTWICKLUNG	Das Start-up DNA.Bits kombiniert die Blockchain mit der Haltung von sensitiven Patientendaten. Geplant ist, dass genetische und medizinische Daten dezentral gespeichert werden und mittels der Blockchain sicher zugreifbar sind. Dabei sieht das Konzept vor, dass eine öffentliche aber permissioned Blockchain zum Einsatz kommt, womit die Zugriffsberechtigungen klar vergeben werden können (DNA.Bits, 2015).
CONSENSYS PRODUKTIV	Unter dem Schirm von Consys existieren viele Startups, welche durch Consys in jedem Bereich unterstützt werden. Consys selbst ist ein Inkubator, welches durch Entwicklung, Ressourcenteilung und nicht zuletzt Investments Ideen aufbaut und auf den Markt bringt (consensys, 2015).
FOLDING@HOME PRODUKTIV	Ein wissenschaftliches Projekt der Stanford University, welches den akademischen Nutzen der Blockchain aufzeigt. Konkret geht es um die Simulation der Proteinfaltung (biologischer Prozess). Dieser Prozess braucht entweder sehr teure Supercomputer oder ein Netzwerk von sehr vielen zusammengeschalteten Computern, die über eine Blockchain ihre Rechenleistung dem Forschungsprojekt zur Verfügung stellen können. Dabei wird beim Mining Prozess nicht ein Hash Puzzle als Aufgabe verwendet, sondern eine Funktion zur Proteinfaltung (Stanford University, 2015).
FILAMENT ENTWICKLUNG	Das Start-up lässt seine Benutzer ein vernetztes Geschäft bauen, ohne über Kenntnisse zu Sicherheit, Skalierbarkeit oder Netzwerk Stacks zu verfügen. Über dieses können Lichter, Industriemaschinen und alle weiteren vernetzbaren Geräte gesteuert werden, ganz ohne WIFI oder Mobilnetz. Vielversprechend ist die eigentliche Vernetzung der Geräte zur Kommunikation untereinander. So können Industriemaschinen bei erhöhter Betriebstemperatur autonom die Klimaanlage aktivieren.
GUARDTIME ENTWICKLUNG	Guardtime versieht Assets wie elektronische Dokumente mit einem technischen Fingerabdruck. Dieser wird in einer permissioned Blockchain abgelegt.

	Sollten Änderungen am Dokument vorgenommen werden, so wird das durch die Blockchain erkannt.
CHRONICLED ENTWICKLUNG	Basierend auf der Blockchain Software Quorum von JP Morgan stellte das Start-up chronicled eine Blockchain Applikation und IoT Protokoll vor. Das Unternehmen setzt einen Fokus auf Gerätesicherheit und Interoperabilität zwischen verschiedenen Formen von IoT Geräten und arbeitet dabei zusammen mit 35 Herstellern von IoT Geräten zusammen. Dabei plant es einen Hardware-Chip, welcher verbaut in IoT Geräten autonomy als Teilnehmer einer Blockchain agieren kann. Mögliche Anwendungsfälle nennt das Unternehmen gleich selbst: Authentifikation von Luxusprodukten, Verfolgung von Medikamenten, Herkunftsbestimmung bei Lieferketten, Handel über LBS, militärische Anwendungen etc. **Invalid source specified.**. Dabei setzt das Unternehmen auf eine public permissioned Blockchain.
IBM PRODUKTIV	Basierend auf dem permissioned Blockchain Software Hyperledger können Benutzer IoT Daten auf der Blockchain ablegen und mittels zahlreichen Analysetools von IBM wie IBM Watson direkt auswerten (IBM Research, 2017). Der Dienst ist als Cloudservice / Blockchain as a Service (BaaS) aufgebaut und bietet einzig Hyperledger als Blockchain Software an (Förster, 2017).
MICROSOFT AZURE PRODUKTIV	In seinem Cloudsystem Azure bietet Microsoft die Blockchain as a Serivce (BaaS) an. Es ermöglicht Unternehmen ein schnelles, kostengünstiges und risikoarmes Umfeld, um Blockchain Applikationen zu entwickeln (The Hindu, 2016) Dabei bietet die Cloud die Blockchain Software von verschiedenen Partnern wie Ethereum oder Strato an.
ARCADE CITY PRODUKTIV	Arcade City ist ein Start-up, welches das Konzept der Fahrtenvermittlung – bekannt von Uber – dezentralisiert über Blockchain umsetzt. Die Plattform gehört der Community. Durch einen fairen Anteil verdienen dabei die Entwickler, die Benutzer und die Unterstützer am Modell. Dabei wird das Start-up, obwohl es noch in der Entwicklung ist, bereits als Uber-Killer bezeichnet (Hüfner, 2016).
KINNO / KOUVOLA PILOT	Das Projekt Kinno, welches unter der städtischen Regierung von Kouvola (Finnland) getrieben wird, nutzt die Blcokchain Technologie, um mit ihrem Produkt „SmartLog“ Logistikunternehmen in ihren Prozessen zu unterstützen. Es integriert mit IoT Chips ausgestattete Container in die Blockchain mit

	dem Ziel, Transportzeiten zu optimieren **Invalid source specified.**. Das Projekt befindet sich bereits in einem dreijährigen Pilotversuch bei finnischen und baltischen Logistikunternehmen. Die Stadt möchte den dort beheimateten Unternehmen die Möglichkeiten der Blockchain Technologie aufzeigen, wobei sich mittlerweile auch IBM mit USD 200 Millionen an der Entwicklung beteiligt **Invalid source specified.**.
FOLLOWMYVOTE ENTWICKLUNG	Follow My Vote ist ein Start-up, welches wie der Name wahrscheinlich bereits aussagt, ein Wählsystem über die Blockchain verwirklicht. Die Vorteile eines transparenten, anonymen, nicht modifizierbaren und sicheren Systems sind dabei von grossem Wert, sobald man die Manipulationsvorwürfe bei vielen Wahlen berücksichtigt. Das System befindet sich noch in der Entwicklung, wird jedoch voraussichtlich mit einer öffentlichen aber permissioned Blockchain arbeiten (followmyvote, 2016).
MONETAS PRODUKTIV	Monetas gehört neben Ethereum zu den wichtisten 50 Fintech Unternehmen weltweit (Burn-Callander, 2016) und hat seinen Hauptsitz in Zug. Es nutzt Bitcoin als Blockchain Software mit eigener aufgesetzter Applikation und lässt sich in der Form als permissioned aber public Blockchain einordnen. Monetas will Finanzdienstleistungen für alle Menschen erschwinglich und verfügbar machen und hat kürzlich ein Abkommen mit der tunesischen Post unterzeichnet (Monetas, 2016).
XAPO PRODUKTIV	Xapo bietet eine Wallet an welche als eigene Applikation auf der Bitcoin Software basiert. Beachtenswert ist hierbei im Unterschied zu den herkömmlichen Wallet Anbietern der Fakt, dass sie eine physische Debitkarte zum Konto mitliefern. So kann neben Online Shops auch in ganz traditionellen stationären Läden bezahlt werden und sogar Geld an allen Bankautomaten bezogen werden. Hierbei arbeitet das Start-up mit Visa zusammen (xapo, 2016). Hierzu ist jedoch im Gegensatz zu anderen Wallet Dienstleistern, wo meist nur eine E-Mail-Adresse zur Anmeldung reicht, bei xapo die Angabe und Bestätigung der Identität notwendig (Petersen, 2015). Ihren Hauptsitz hat die Firma 2015 von Palo Alto, Kalifornien in die Schweiz nach Zürich verschoben aufgrund der besser geschützten Privatsphäre und den unternehmensfreundlichen Strukturen (xapo, 2016).

BITCOIN SUISSE AG PRODUKTIV	Ebenfalls ein Schweizer Start-Up, welches vor allem mit Geldautomaten für Bitcoin in der Schweiz für Schlagzeilen gesorgt hat. Hierbei kann man mit Schweizer Franken Bitcoins am Automaten kaufen (NZZ, 2014). Daneben fokussiert sich das Unternehmen auf weitere Finanzdienstleistungen (Anon., 2017).

2.6 Internet der Dinge

Insbesondere seit der Entwicklung von Smart Contracts als selbstausführende Programme auf der Blockchain lassen sich komplexe Abläufe mit der Blockchain ausführen. Ein Vorteil der Blockchain wirkt sich dabei jedoch als Nachteil für die reale Welt aus: die vollkommen digitale Umsetzung. Reale Objekte der Welt lassen sich zwar mittels Smart Contracts und entsprechenden Attributen 'digitalisieren', jedoch ist diese Erfassung statisch. Änderungen des realen Objekts bedürfen manuelle Anpassungen.

Als Lösung sehen viele Forscher wie auch Start-ups die Vernetzung von realen Objekten durch elektronische Sensoren wie RFID Chips oder Temperaturfühler (Christidis & Devetsikiotis, 2016). Diese bereits jetzt schon sehr verbreitete Technologie erfasst den Zustand eines realen Objekts und kann es gewünschten Empfängern weiterleiten. Ebenfalls verfügen Geräte über Methoden, welche es erlauben, Funktionen auszuführen - beispielsweise das Öffnen eines Schlosses. Die Blockchain erlaubt mit dem Konzept der Smart Contracts die Automatisierung von Prozessen mit mehreren Interaktionen (Christidis & Devetsikiotis, 2016).

Gartner schätzt, dass sich die Zahl der IoT Geräte bis ins Jahr 2020 auf über 26 Milliarden erhöhen wird, im Vergleich zum Jahr 2010, als es noch knapp eine Milliarde waren (Gartner Research, 2016). Eines der grössten Probleme von IoT Geräten ist derzeit die Interoperabilität von unterschiedlichen Geräten (Vermesan, et al., 2013, p. 12). Manyika et al. (2015) haben festgestellt, dass 40% der potenziellen Wertgenerierung durch die Interoperabilität einzelner IoT Systeme ausgemacht werden, ist eine übergreifende Plattform essenziell.

IoT Gerät, Protkollo und die Cloud

Die IoT Geräte bestehen aus den Elementen des Geräts selbst, den Protokollen und der Cloud, welche als erwereiterter Speicher dient (Christidis & Devetsikiotis, 2016). Dabei umfasst der Speicher eine Datenbank, welche die Daten der IoT Geräte speichert, sowie Regelwerke und Logiken für den Betrieb des Geraäts (Porter & Heppelmann, 205). Dabei müssen sich die Geräte anmelden und registrieren, um sich zu aktivieren und nutzbar zu werden. Die Blockchain kann durch dessen Architektur diese Prozesse ersetzen. Die Geräte würden sich entsprechend untereinander authentifizieren und könnten die

Cloud durch das so entstandene P2P-Netzwerk selbst nachstellen. Insbesondere bei sehr oft günstig hergestellten, da kleinen IoT Geräten würde so einen kostenintensiveren Aufbau und die Aufrechthaltung einer Cloud Umgebung mit den zuvor genannten Diensten wegfallen. Firmeware Updates könnten auf die gleiche Weise verteilt werden und mit dem Konzept der Blockchain könnten diese sogar gegen kleine Gebühren zur Verfügung gestellt werden (Christidis & Devetsikiotis, 2016). Untere Abbildung zeigt diese Transformation durch die Blockchain.

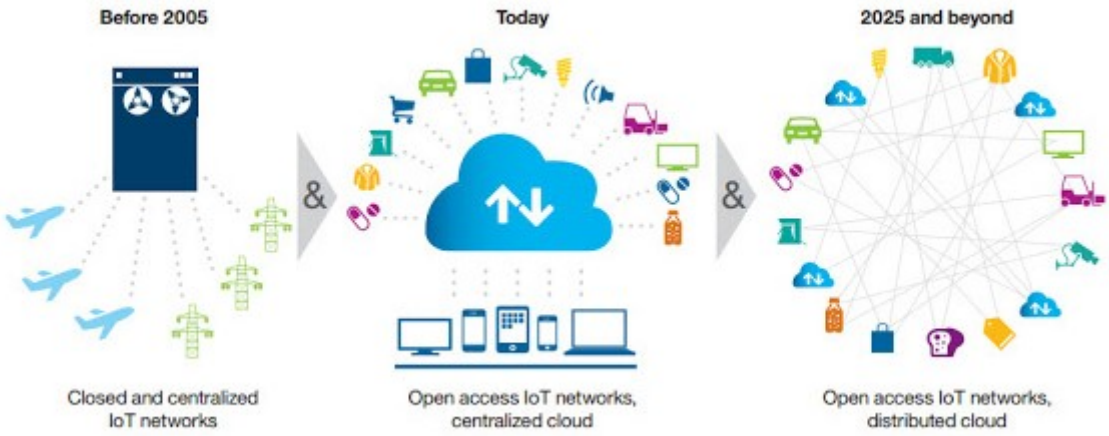


Abbildung 21: Entwicklung der IoT Architektur mit Blockchain (Christidis & Devetsikiotis, 2016)

In einer Machbarkeitsstudie haben IBM und Samsung eine Waschmaschine über die Ethereum Software angebunden (IBM, 2015). Sie war selbstständig in der Lage, Waschpulver zu bestellen, sobald keines mehr verfügbar war, den Techniker zu rufen, sobald ein Systemfehler auftrat sowie die Wäsche dann gewaschen, wenn der Strom am billigsten war. Letzteres wurde mittels eines ebenfalls entwickelten Markts für Strom innerhalb der Gemeinde umgesetzt. Die Waschmaschine konnte darüber autonom mit dem Micro-Grid der Gemeinde kommunizieren und Strom im Gegenzug von freien Waschgängen für die Verkäufer handeln (IBM, 2015).

Herausforderungen

IBM hat aus dieser Machbarkeitsstudie folgende Herausforderungen herausgeleitet und teilweise bereits durch ihr Projekt gelöst:

- P2P Kommunikation in einem trust-less Netzwerk
- Distributed file sharing
- Autonome Gerätekontrolle
- Identity

Durch die Kombination von verschiedenen Technologien ist es IBM gelungen, die Elemente von IoT Geräten zu optimieren. So findet die Kommunikation selbst über TeleHash statt, die Identifikation, Authentifizierung und Registrierung über die Blockchain (Ethereum) und die Firmeware Updates über das Bittorrent Netz (IBM, 2015).

Wie die Blockchain die Zukunft von IoT verändert

Die Blockchain ändert das heutige IoT Ökosystem basierend auf zentralen Servern zur Authentifikation und des Datenaustausches genutzt werden zu einem sicheren P2P-Netzwerk, worin IoT Geräte miteinander kommunizieren können. Mit jedem zugelassenen Gerät auf der Blockchain können sich IoT Geräte einfach identifizieren ohne die Notwendigkeit eines zentralen Servers. Und das Netzwerk ist skalierbar, so dass es Millionen von Geräten ohne Aufbringung von weiteren Ressourcen integrieren kann. Hierbei sprechen Experten von M2B - Machine-to-Blockchain Kommunikation (Christidis & Devetsikiotis, 2016). Die Integration von IoT Geräten ermöglicht aber auch für die Blockchain ganz neue Anwendungsfälle. Kombiniert mit dem Konzept der Smart Contracts können so jederzeit auch Objekte der realen Welt digital abgebildet werden und so in für die Smart Contracts wichtige Daten formuliert werden. Im folgenden Beispiel wurde so ein Logistik-Prozess ohne und mit Blockchain kombiniert mit IoT Geräten aufgezeigt. Während auf der linken Seite der Container etappenweise zum Ziel gelangt, und jeweils manuell abgefertigt werden muss, so kann der Container auf der rechten Seite autonom den Standort übermitteln und Aktionen basierend darauf auslösen.

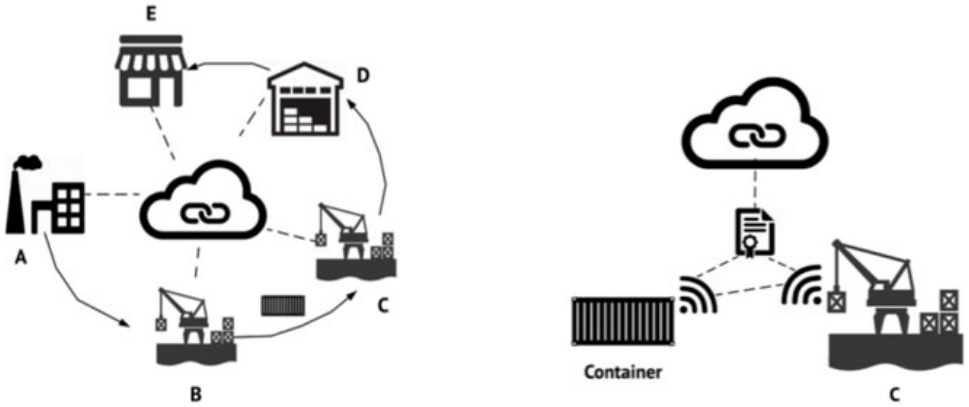


Abbildung 22: Die Phasen einer Container Lieferung (Christidis & Devetsikiotis, 2016)

Herausforderungen

Skalierung

Die pure Masse an Daten, welche durch Millionen von IoT Geräten generiert werden, müssen

Im Vergleich zu grossen Rechnern bieten IoT Geräte meist eine sehr limitierte Rechenleistung, weshalb die Art der dezentralen Konsensfindung nicht zu komplex gestaltet werden darf. Zwischen den heute

gebräuchlichen Ansätzen ist PoS entsprechend dem PoW überlegen durch den reduzierten Bedarf an Ressourcen. In einem Versuch der IBM mittels einer permissioned Blockchain, wo von 1'000 IoT Teilnehmern nur 100 als Miner berechtigt wurden, hat sich jedoch herausgestellt, dass der PoW Ansatz zumindest bezogen auf den Stromverbrauch nur sechs Prozent mehr verbraucht als der PoS Ansatz (IBM, 2015).

Kosten

Da IoT Geräte ohnehin nicht teuer sind, darf auch das unterstützende System nicht teuer sein. Dabei ist ebenfalls die Ressourcenanforderung gemeint, welche einen Chip für IoT Geräte massgeblich verteuert – je nach Leistung.

Sicherheit und Vertrauen

Ein aktuelles Problem von IoT Geräten ist die mangelhafte Sicherheit vieler Geräte aus verschiedenen Gründen. Zum einen ist der Herstellersupport nur kurzfristig und die Geräte werden nicht mehr aktualisiert, was Angriffsflächen für Schadsoftware zulässt. Zum anderen sind die Authentifizierungslösungen in vielen Geräten nicht sehr sicher aufgebaut, was auch an der Kapazität der Systeme liegt (Christidis & Devetsikiotis, 2016).

Interoperabilität

Zuletzt ist die fehlende Interoperabilität zwischen verschiedenen IoT Geräten zu erwähnen. Insbesondere durch den bereits aufgeführten Fakt, dass diese Eigenschaft gleich 40 Prozent der Wertschöpfung ausmacht (Manyika, et al., 2015).

Markt

Es gibt bereits zahlreiche Start-ups, welche sich zum heutigen Zeitpunkt mit der Blockchain in Kombination mit IoT Geräten beschäftigen. Darunter Kinno, welches die Logistik mit Smart Container revolutionieren will (vgl. Seite 53).

2.7 Künstliche Intelligenz

Die Forschung an der künstlichen Intelligenz begann schon vor einigen Jahrzehnten (Brooks, 2000, p. 291). Die Methodik des Vorgehens kann sich vereinfacht wie folgt beschreiben (McConaghy, 2017):

- Definition des fixen Datensatzes
- Gestaltung eines Algorithmus
  um die Leistung zu verbessern, beispielsweise die semantische Erkennung von verbaler Sprache anhand dieses fix definierten Datensatzes – Induktives Vorgehen

- Veröffentlichung des Algorithmus
  in einer Konferenz oder einer wissenschaftlichen Zeitschrift

Natürlich gibt es hierbei auch sehr viele weiterentwickelte Methoden in der künstlichen Intelligenz, worauf diese Arbeit jedoch nicht eingeht. Dagegen soll aus diesem sehr vereinfachten Vorgehen klar werden, dass sich aus vielen Daten Informationen ableiten lassen können. Und je mehr Daten verfügbar sind, desto akkurater können diese Informationen sein.

Möglichkeiten der Verknüpfung von Blockchain und künstlicher Intelligenz

Durch die Verknüpfung von aus der künstlichen Intelligenz stammenden Informationen können Blockchains als ausführender Bestandteil dieser Kombination erheblich grösseren Mehrwert liefern über das Prinzip der Automatisierung. Nachfolgend sollen einige Opportunitäten aus diesem Ansatz hergeleitet werden (McConaghy, 2017):

Data Sharing -> bessere oder neue Modelle

Durch die Dezentralisierung und der Transparenz der Blockchain ist es einfacher, an mehr Daten zu kommen. Diese können durch künstliche Intelligenz ausgewertet werden.

- Innerhalb eines Unternehmens können so Daten aus verschiedenen Regionen aus der Blockchain ausgelesen werden und in die strategische Planung einfliessen
- Innerhalb eines Ökosystems wie beispielsweise entlang einer Wertschöpfungskette könnte der Datenaustausch zu effizienteren Prozessen führen, die sich aus diesen Informationen generieren lassen
- Global gesehen (bei einer public Blockchain wie Bitcoin) können prädiktive Modelle zur Entwicklung in Echtzeit verarbeitet werden

Neue globale Daten -> neue globale Einsichten

Wie der letzte Punkt zu den Modellen auf globaler Ebene können auch globale Indikationen aufgrund dieser gesamtheitlichen Datenflut abgeleitet werden. Schon heute ist der Markt für solche Prognosen mit einem Milliardenbudget dotiert, wobei diverse Firmen Informationen sammeln und aufbereitet weiterverkaufen (Stichwort Bloomberg). Dies könnte mit der Umsetzung von Blockchain mit künstlicher Intelligenz von jedem Unternehmen und auch Privatperson gemacht werden bzw. deren Informationen konsumiert werden.

Audits auf Daten -> neue Sicherheitsvorkehrungen

Durch die Echtzeitanalyse von Daten innerhalb der Blockchain können bessere Sicherheitsvorkehrungen für Betrug abgeleitet werden und entsprechend weitere prädiktive Modelle entstehen, welche sich ebenfalls in Echtzeit den Umständen anpassen.

Die Kombination von Smart Contracts und künstlicher Intelligenz

Zuletzt ist der für jedermann interessanteste potenzielle Anwendungsfall zu nennen (Zarkadakis, 2017). Die Kombination von autonomen und interaktiven Smart Contracts mit dem Wissen der künstlichen Intelligenz. Während die Blockchain in diesem Kontext wie bereits beschrieben, die Daten für die Algorithmen der künstlichen Intelligenz verfügbar macht, so verarbeitet diese die Daten zu verwertbaren Informationen und Befehle, welche dann wiederum durch die Blockchain – in diesem Fall als Smart Contract – ausgeführt werden (McConaghy, 2017). Was zunächst abstrakt klingt, kann sich auf die Anwendung des persönlichen Finanzberaters abbilden. Kurz gesagt überträgt man diesem sein Vermögen und dieser legt es selbstständig erfolgsversprechend an. Konzepte von Robo Advisory Systemen in Banken beweisen heute schon, dass dies möglich ist, auch wenn die Entwicklung der künstlichen Intelligenz hierbei noch nicht soweit ist. Und hierbei gibt es einen gravierenden Unterschied zwischen des in der Bank eingesetzten Robo Advisors und dem hier beschriebenen Finanzberater. Die effiziente Informationsgewinnung mittels der Blockchain.

Da sich zum Zeitpunkt der Verfassung dieser Arbeit die Entwicklung ganz am Anfang befindet, wird neben diesem Beispiel nicht weiter auf dieses Anwendungsfeld eingegangen.

2.8 Interviews

Die durchgeführten Interviews sollen den erfassten Status Quo der Blockchain Technologie um weitere Sichtweisen erweitern. Mittels einem dafür ausgerichteten Interviewleitfaden wurden die gewählten Experten zu spezifischen Themen der Blockchain befragt.

2.8.1 Interviewleitfaden

Während der Durchführung der Interviews hat sich der Interviewleitfaden weiterentwickelt. So konnte von Interview zu Interview eine Verschärfung der Fragen erzielt werden. Dabei wurden bei jedem Interview die Erkenntnisse aus den vorherigen Interviews eingebracht sowie die Fragen an den Wissensstand sowie Tätigkeitsfeld der Interviewpartner leicht angepasst (Froschauer & Lueger, 2003, p. 76). Die spezifischen Fragen sowie das gesamte Transkript kann dem Anhang dieser Arbeit entnommen werden.

Konkret wurde auf folgende zentrale Themengebiete explizit aber auch implizit fokussiert:

- Informationsgewinnung zur Blockchain
- (Subjektive) Sichtweise auf Blockchain
- Prinzipien und Enabler der Blockchain
- Herausforderungen und Implikationen
- Kritische Punkte

2.8.2 Interviewpartner

Bei der Wahl der Interviewpartner wurde darauf geachtet, ein breites Spektrum von Blickwinkeln abzudecken. Dabei wurde versucht, den Interviewpartner zu klassifizieren (Froschauer & Lueger, 2003, p. 82ff.), in dem zu jedem Interview ein Expertenprofil erhoben wurde.

Die Experten können unter Berücksichtigung dieser Profile in folgende Kategorien eingeordnet werden:

- Technische Sichtweise [T]
- Wissenschaftliche Sichtweise [A]
- Wirtschaftliche Sichtweise [W]
- Soziale und gesellschaftliche Sichtweise [S]

Die folgende Tabelle beinhaltet alle Interviewpartner mit Kennzeichnung ihrer Sichtweisen [x] sowie die Rolle und ihre Tätigkeit, welche als Auswahlkriterium diente.

Interviewpartner	*Rolle / Unternehmen*	*Tätigkeit / Justifikation*
Andreas Hirstein [S]	Journalist NZZ am Sonntag Resort Wissen	Verfasser des Artikels «Blockchains sind so bedeutend wie das Internet»
Simon Schweri [W]	Product Manager datatrans	Aktiver Beobachter der Technologie zur möglichen Adaption für das eigene Produktportfolio
Oliver Heister [T]	Chief Technology Officer datatrans	Aktiver Beobachter der Technologie mit einem zusätzlich technischen Aspekt
Rao Jags [T] [A] [W]	Swiss Re Lab	Blockchain Workstream Lead - Reinsurance Technology Strategic Initiatives
Peter Ivankay [A] [W]	Projektleiter UBS WM Innovation Lab	Teil des Wealth Management Innovation Labs mit starkem Fokus auf die Blockchain

		inklusive Verfasser von wissenschaftlichen Arbeiten zur Blockchain
Lucas Silva *[T]*	Software Engineer ergon Informatik	Aktiver Beobachter der Blockchain Technologie mit Beteiligung am github Repository der Community
Karin Frick [A] [S]	Leiterin Research und Mitglied der Geschäftsleitung am Gottlieb Duttweiler Institut	Analysiert Trends und Gegentrends in Wirtschaft, Gesellschaft und Konsum; derzeit in Kollaboration mit IBM die Blockchain
Stipe-Mate Brkljacic [A] [W]	Programmleiter UBS, Start-up-Gründer	Mitgründer eines eigenen Start-up-Unternehmens zur Blockchain und Verfasser einer Masterarbeit zum Thema Blockchain
M.L. [W] [A]	Innovation Manager von einer der Top 4 Beratungsunternehmen	Verfasser von Blockchain Whitepapers zu zukünftigen Anwendungsfällen *[Auf Wunsch des Interviewpartners – aus Gründen der Vertraulichkeit - wurde das Transkript aus der Arbeit entfernt]*

Tabelle 9: Übersicht der Interviewpartner

3 Analyse

In der folgenden Analyse werden alle gesammelten Daten aus dem Kapitel 2 aggregiert und kategorisiert. Zunächst sollen die Erkenntnisse aus den Experteninterviews näher betrachtet werden. In einem zweiten Schritt werden diese mit den Erkenntnissen aus der Literaturrecherche verglichen. Hierbei liegt der Fokus auf die Aggregation diverser Aussagen aus den vorhergehenden Teilen der Arbeit und der Aussagen aus den Experteninterviews zu Parametern, welche in der nachfolgenden Methode zum Einsatz kommen. Abschliessend werden die kombinierten Erkenntnisse in einer SWOT Analyse strukturiert und gegenübergestellt. Der Output dieses Kapitels dient als Basis für die Erarbeitung der Methode zur Identifikation von Anwendungsfällen für die Blockchain Technologie, welche im nächsten Kapitel ausgearbeitet wird.

3.1 Auswertung der Interviews

Die qualitative Inhaltsanalyse der Interviews wird wie bereits im Forschungsdesign beschrieben, anhand der heuristischen Methode von Froschauer und Lueger (2003, p. 82) vorgenommen. Hierbei werden zunächst die durch den Interviewleitfaden vorbestimmten Schwerpunkte als Kategorien herangezogen, um danach die Aussagen aus den einzelnen Experteninterviews diesen Kategorien zuzuordnen. Dabei wurde die semantische Inhaltsanalyse mit Unterstützung der analytischen Tools von IBM (Watson) effizienter gestaltet. Mittels dieser Methode wurden zudem weitere implizite Unterkategorien identifiziert, welche in dieser Analyse inkludiert wurden.

3.1.1 Auswertung nach Kategorien

Nachfolgend werden die aus der qualitativen Inhaltsanalyse gewonnenen Thematiken in Kategorien und Unterkategorien eingeteilt. Die Unterkategorien sind dabei teils mehr als einer Kategorie zugeordnet, da der Kontext der individuellen Aussagen bei diesen Unterkategorien nicht immer der übergeordneten Kategorie entspricht, wenn die Zuordnung nur eindimensional gemacht wird.

Aussagen, die nicht unter diese Kategorien fallen, werden am Schluss der Auswertung aufgeführt.

Kategorie 1: Status Quo der Blockchain	Kategorie 2: Schwächen und Stärken der Blockchain
• Informationsgewinnung Blockchain • Einschätzung des Impacts der Blockchain • Diskussion über den Hype • Blockchain heute • Reiz einer Blockchain • Value Driver einer Blockchain	• Intermediäre • Intermediäre: Banken • Proof-of-Work / Mining • Kritische Anregungen • Positive Anregungen • Offene Entwicklung (open source) • Blockchain als Prozessoptimierer oder Solution
Kategorie 3: **Implikationen**	**Kategorie 4:** **Anwendungsfälle**
• Regulatorische Implikationen • Marktüberwachung ETF • Allgemeine Implikationen • Soziale Implikationen • Offene Entwicklung (open source)	• Bitcoin und Blockchain • Enabler der Blockchain • Technologie Unternehmen / Startups und Blockchain • Entwicklung von Anwendungsfällen • Umgang traditioneller Unternehmen mit der Blockchain • Formen der Blockchain • Blockchain als Prozessoptimierer oder Solution

Tabelle 10: Kategorien und Unterkategorien der Experteninterviews

Kategorie 1: Status Quo der Blockchain

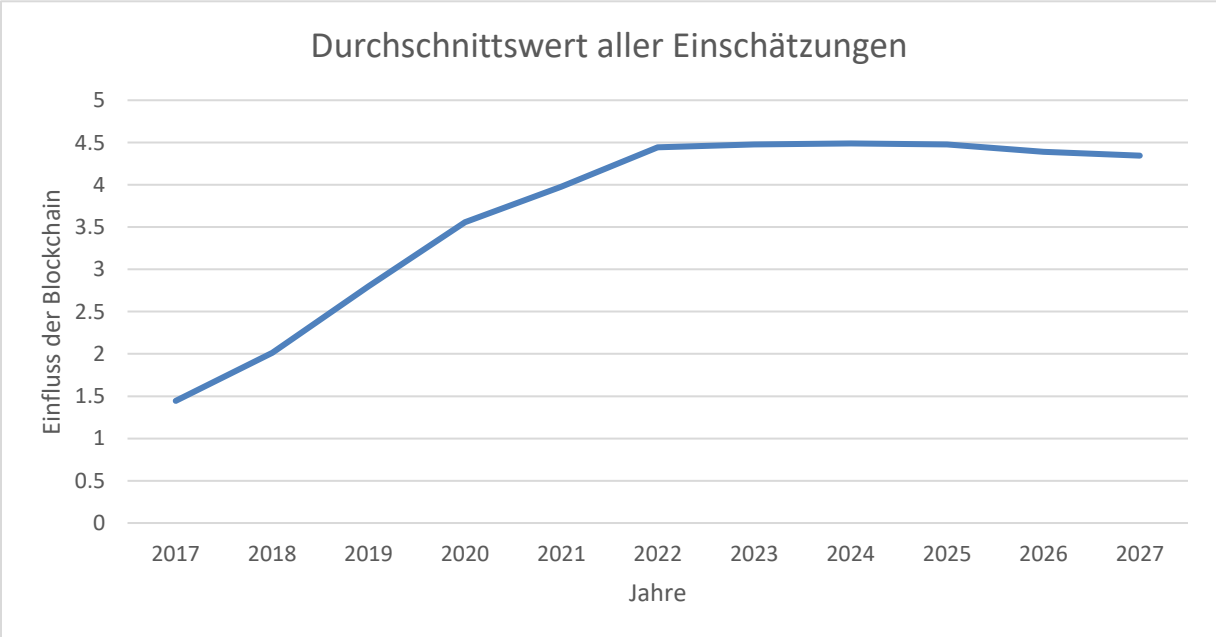
Informationsgewinnung

Als erstes wurde je nach Interviewpartner explizit aber auch implizit nach der Informationsgewinnung zur Blockchain gefragt. Hierbei stand zum einen der Fokus auf die Expertise der Interviewpartner zur Thematik aber auch das Interesse nach der Form, wie sich die verschiedenen Personen über die Entwicklung der Blockchain im Allgemeinen informieren. Zusammenfassend lässt sich hierzu sagen, dass die in Kapitel 2.8.2 bereits aufgezeigten Sichtweisen der einzelnen Interviewpartner sich auch auf die Art der Informationsgewinnung niederschlägt. Unterscheiden lassen sich hierbei zwei übergeordnete

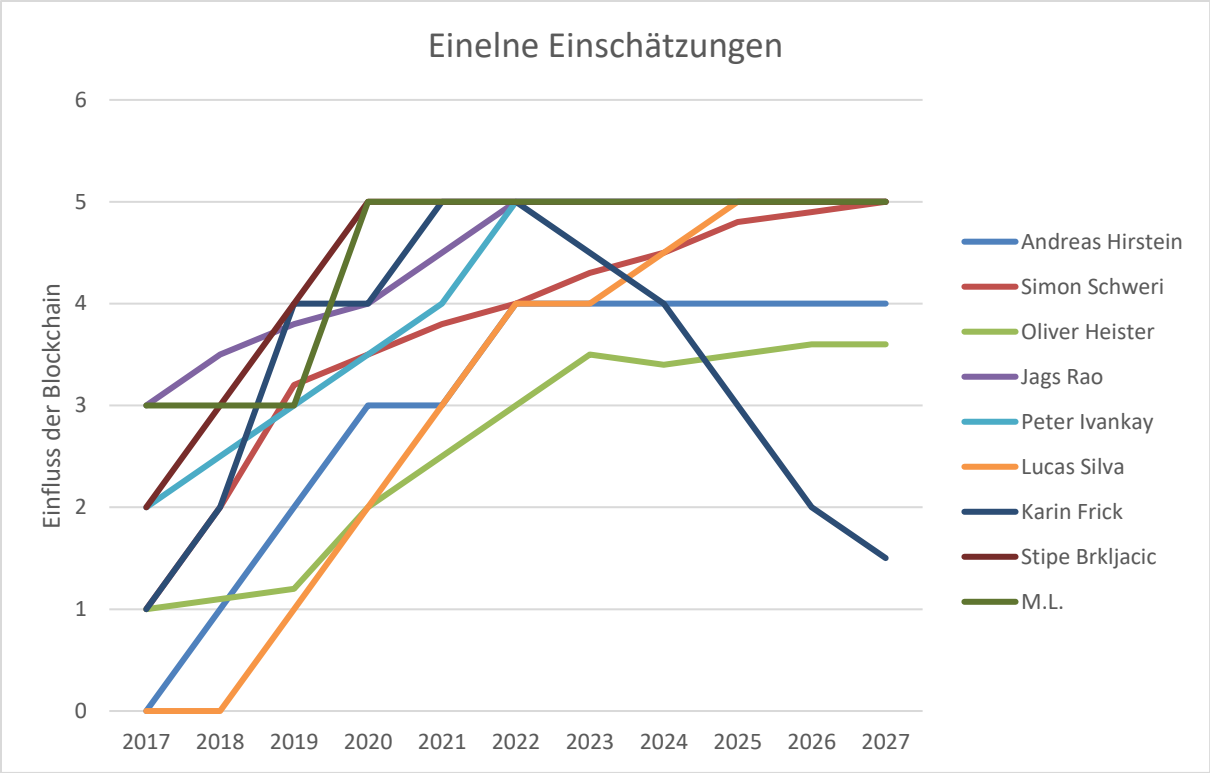
Formen; die Informationsgewinnung über wissenschaftliche Publikationen und über die Praxis. Bei ersterer Form handelt es sich dabei meist um eine passive Konsumation der Entwicklung während die Praxis auch Konferenzen umfasst, die eine aktive Auseinandersetzung mit der Technologie impliziert. In einer weiteren Unterscheidung dieser Informationsgewinnung über die Praxis lässt sich zudem feststellen, dass neben den Konferenzen vor allem eigene Projekte unter Einsatz der Blockchain Technologie die Expertise dieser Personen weiter steigert. Diese Erkenntnis ist insofern interessant, dass eine rein wissenschaftliche Betrachtung der Blockchain eine negative Korrelation zur Euphorie gegenüber der Technologie aufweist. Stark wird diese Korrelation, sobald die Person selbst über keinen wissenschaftlichen Bezug im Allgemeinen verfügt und somit selbst praxisorientiert ausgerichtet ist. Da die Selektion der Interviewpartner auch aufgrund einer zumindest minimal vorhandenen Expertise zur Blockchain getroffen wurde, müsste diese Erkenntnis mittels weiteren Personen geprüft werden. Die These wird jedoch für die zu erarbeitende Methode berücksichtigt.

Einschätzung des Impacts der Blockchain

In einem weiteren Schritt wurden die Interviewpartner gebeten, eine Einschätzung der Blockchain in ihrem Leben heute und in einem Zeitraum von fünf bis zehn Jahren zu machen. Dabei wurde eine Skala von 1 bis 5 vorgegeben; 1 als kleiner bis gar kein Impact und 5 als starker Impact. Nachfolgend sind die Aussagen aller Interviewpartner aggregiert dargestellt:



Das Bild zeigt, dass die Kurve sich über die nächsten fünf Jahre stetig steigert, um dann nur leicht abzunehmen. Generell lässt sich diese Wahrnehmung auch durch die aktuell stetig steigende Zahl von Anwendungsfällen stützen. Wenn man sich die einzelnen Einschätzungen betrachtet, so kann man jedoch einen klaren Ausreisser identifizieren:



Karin Frick, leitende Wissenschaftlerin beim Gottlieb Duttweiler Institute hat eine interessante Sichtweise auf den Einfluss der Blockchain hinsichtlich der gesellschaftlichen Dimension. So sieht sie zwar wie die anderen Interviewpartner eine klare Tendenz nach oben für die nächsten fünf Jahre, doch beschreibt daraufhin einen nachlassenden Einfluss. Auch wenn sie sich nicht direkt auf die exakten Jahreszahlen dafür festlegen will, so denkt sie, dass es nach dem Peak bald nachlassen wird. Sie begründet ihre Aussage durch das altbekannte Paradigma von neuen Technologien, welche zunächst eine grosse Wahrnehmung in der Gesellschaft finden, jedoch nach dem grössten Hype in der Phase der Produktivität wieder in den Hintergrund geraten. Implizit umschreibt sie damit auch den von Gartner definierten Lifecycle eines technologischen Hypes. Andreas Hirstein, Journalist bei der NZZ merkt hierzu an, dass es wohl für uns als Endkunden nicht relevant ist, ob es sich bei der Technologie um die Blockchain handelt oder aber um eine andere, zentral ist die gesteigerte Effizienz, die dadurch ausgelöst wird. Gleich sieht es auch M.L., einem Mitarbeiter aus einem der Top 4 Beratungsunternehmen, der sich insbesondere mit der Wahrnehmung der Blockchain Technologie bei verschiedenen Anspruchsgruppen beschäftigt hat. So teilt er die Meinung von Andreas Hirstein und fügt hinzu, dass sich Endbenutzer nicht mit der Materie selbst befassen, sondern darauf Wert legen, dass es funktioniert. Die anderen Interviewpartner sehen ihre Einschätzung denn auch eher ausgelegt auf die Sicht der Unternehmen. Auf die zusammenhängende Frage, ob die Wahrnehmung der Technologe heute noch zu gering ist, um zu diesem Zeitpunkt eine höhere Einschätzung zu erhalten, stellen die Befragten die Wahrnehmung an sich in Frage. Für die Mehrheit der Interviewpartner ist jedoch auch klar, dass heute – neben Bitcoin –

ein richtig guter praktisch umgesetzter Anwendungsfall fehlt, um die Wahrnehmung der Blockchain zu steigern.

Diskussion über den Hype

Oliver Heister und Lucas Silva, beide beruflich im Kontext der IT zu verorten, sehen den Hype als übertrieben an. Dies begründen beide entsprechend gleich mit der technischen Zusammensetzung der Blockchain. So handelt es sich wie bereits im Kapitel 2 dieser Arbeit beschrieben, nicht um gänzlich neue technische Ansätze, sondern nur um die Kombination von *bereits im Einsatz stehenden technischen Konzepten*. Ebenso skeptisch sieht der Journalist, Andreas Hirstein, den Hype um die Technologie; doch aus anderen Gründen. So sieht er als Interviewpartner mit der kleinsten technischen Expertise, doch einer stark geprägten Wahrnehmung für Trends einen unbegründeten Hype um die Blockchain. Dabei schätzt er, dass viele Personen um diesen Hype nicht wirklich verstehen, um was es sich wirklich bei der Blockchain handelt und somit der Hype übermässig befeuert wird. Simon Schweri, Produktmanager, redet ebenfalls von überzogenen Erwartungen, die möglicherweise aus dem Unverständnis der Technologie entstehen. Er gewinnt dem Hype jedoch auch etwas Positives ab; nämlich die Anziehung von vielen Unternehmen, welche sich dadurch bemüht sehen, Anwendungsfälle für ihre eigenen Geschäftsmodelle zu finden. Hiermit spricht er eine Tendenz an, welcher auch der Autor in der qualitativen und explorativen Literaturrecherche feststellen konnte. Peter Ivankay, Projektleiter für Blockchain Projekte bei der UBS – eben einem, dieser Unternehmen, welche implizit aufgrund des Hypes um die Blockchain an eben diesen Anwendungsfällen arbeitet – teilt diesen positiven Einfluss des Hypes auf die Blockchain. Seiner Meinung nach verfügt die Technologie über genügend disruptivem Potenzial, dass ausgeschöpft werden sollte. Das Ausmass des Hypes erachtet er jedoch als zu hoch. Der Grund dafür sieht er jedoch darin, dass heute noch (zu) viele Prozesse noch nicht digitalisiert bzw. automatisiert sind. Dies sieht er dann aber als übergeordneten Enabler, der die Blockchain dadurch sein könnte. Auch wenn Stipe Brkljacic, selbst Mitgründer eines Blockchain Start-ups, die Legitimation für den Hype ebenfalls als gegeben sieht, sieht er als einziger auch einen negativen Aspekt dieses Hypes. Seiner Meinung nach fokussiert der Hype zu sehr auf die wirtschaftlichen Vorteile des Konzepts und schadet zurzeit der technischen Weiterentwicklung der Blockchain. Konkret zählt er die folgenden negativen Aspekte ausgelöst durch diesen, aus seiner Sicht, wirtschaftlichen Hype auf: die langsam einsetzende Missachtung von grundsätzlichen Prinzipien der ursprünglichen Blockchain sowie die Anziehung von Massen, welche nur an einem kurzfristigen Gewinn interessiert sind; Spekulanten. Rao Jags, Blockchain Stream Leiter bei Swiss Re relativiert den Hype und sieht ihn als willkommenen Nebeneffekt, worauf er jedoch nicht primär achtet. Er gehört wie Peter Ivankay zu einem der Unternehmen, welche die Wirtschaftlichkeit und die Relevanz der Blockchain durch praktische Anwendungsfälle beweisen will.

Zusammenfassend lässt sich sagen, dass der Hype um die Blockchain analog der Einordnung im Gartner Hype Cycle überzogen ist. Der Grundtenor der Interviewpartner ist denn auch das Fehlen eines praktischen Anwendungsfalls neben der Kryptowährung, die den Hype legitimieren würde.

Blochchain heute

Die offene Frage nach der Einschätzung der Interviewpartner von der Blockchain, wie sie diese heute wahrnehmen, führte zu sehr unterschiedlichen Aussagen. Peter Ivankay knüpft an die Thematik des Hypes an und sieht die Blockchain heute noch als *Verkaufsinstrument* für Projekte. Ihm fehlen die wirtschaftlichen Kennzahlen, um einen Business Case heute schon zu legitimieren. Doch hier sieht er auch die Unternehmen in der Pflicht, welche zurzeit noch eine andere *Kostenrechnung* anwenden, als dies für die Blockchain nützlich wäre. Besonders in seinem Fachgebiet, den Banken, werden die Prozesskosten noch zu sehr vernachlässigt und der Fokus richtet sich an die Marge der Dienstleistungen. Oliver Heister fügt hinzu, dass man heute noch kein Geld mit einer Umstellung auf die Blockchain Technologie verdienen kann, wenn man berücksichtigt, welcher initiale Aufwand mit so einer Umstellung entsteht.

Gleich mehrere Interviewpartner stellen sich die Frage, ob der *Mehrwehrt* einer Blockchain ausserhalb der Kryptowährungen bereits ausreichend ist, um sie effektiv und effizient einzusetzen. Andreas Hirstein glaubt, dass sich die heutigen Prozesse über eine längere Zeit bewährt haben und entsprechend schwierig zu ersetzen sind. Stipe Brkljacic nimmt dieses Argument auf und sieht die Blockchain zunächst nicht als Ersatz bestehender Prozesse, sondern vielmehr als *Optimierer* von den heutigen Geschäftsprozessen. Ebenso sieht es der Unternehmensberater M.L. Er hat heute entsprechend vermehrt Anfragen von Unternehmen, die nicht gleich die ganze Prozesslandschaft mit Blockchain zu ersetzen versuchen, sondern vielmehr eine *Effizienzsteigerung* durch den *komplementären Einsatz* der Technologie erhoffen. Gestützt wird diese Aussage durch die Arbeiten von Rao Jags und Peter Ivankay, welche mit ihren Projekten vor allem versuchen, bestehende Prozesse zu verbessern. Lucas Silva sieht den Fokus heute noch sehr stark auf die Finanzgeschäfte.

Reiz einer Blockchain

Andreas Hirstein und Karin Frick sehen beide einen grossen Reiz der Blockchain im Hinblick auf die gesellschaftliche Auswirkung. So ist das Prinzip des Zero-Trust verknüpft mit dem Fakt, Transaktionen ganz *ohne Intermediäre* durchzuführen, als verlockenden Reiz der Blockchain an. Einen ähnlich gelagerten Reiz sieht Simon Schweri. Er sieht entsprechend die Säuberung von heute nicht korrekt laufenden Prozessen als grossen Reiz der Technologie. Konkret spricht er Prozesse an, wo *Korruption und Betrug* heute zum Alltag gehören. Dazu zählt er den Rohstoffhandel (Diamanten, Energie) aber auch behördliche Prozesse wie Wahlen und Auftragsvergaben. Einen technischen Reiz sieht Oliver Heister in der Blockchain. So geht es ihm hierbei nicht mal um die Technologie selbst, sondern um den Fakt,

dass viele Unternehmen (Partner / Kunden seines Unternehmens) noch sehr veraltete Software oder gar analoge Prozesse nutzen. Die Blockchain sieht er hier als *Mittel zum Zweck*, dass diese Unternehmen endlich eine *Aktualisierung auf eine neuere Technologie* vollziehen. Ebenfalls als Mittel zum Zweck, jedoch aus wirtschaftlicher Hinsicht, sehen Peter Ivankay und Rao Jags die Blockchain. Diese würde Unternehmen letztendlich zwingen, ihre eingespielten Prozesse wieder mal neu herauszufordern und zu optimieren. Dabei meinen jedoch beide, dass die Blockchain selbst mit ihren Prinzipien der *Immutability* und der *vollen Digitalisierung* gleich in diesem *Redesign* der Prozesse berücksichtigt werden sollte.

Value Driver einer Blockchain

Peter Ivankay, selbst Verfasser einer Diplomarbeit zum Thema Blockchain mit wirtschaftlichem Hintergrund, definiert die Value Driver der Blockchain wie folgt: Transparenz, Automatisierung, Sicherheit, Immutability, Effizienz und Geschwindigkeit bei der Auslesung der Daten. Unter dem Begriff des Mehrwerts sehen weitere Interviewpartner die Automatisierung als schlagkräftiges Argument zugunsten der Blockchain.

Kategorie 2: Schwächen und Stärken der Blockchain

Stärke: Intermediäre / Intermediär Bank – Zero Trust

Die fehlende Notwendigkeit eines Intermediär ist eines der grossen Stärken der Blockchain Technologie durch den Fakt des Zero-Trusts. Dieser Argumentation gegenüber zeigen sich die Interviewpartner geteilter Meinung. Es kann unterschieden werden von den stark an Blockchain interessierten und der Technologie euphorisch gegenüberstehenden Personen und denen, welche die Entwicklung zurzeit eher skeptisch entgegensehen. Stipe Brkljacic sieht dies sehr wohl als einer der Stärken, welche auch den grossen Hype um die Blockchain begründet. Hierbei sieht er vor allem Infrastruktur Anbieter wie die Six Group als obsolet an, sollten die Firmen ihren Zahlungsverkehr direkt über die Blockchain abwickeln. Auch Lucas Silva sieht ein gutes Potenzial dafür, dass die Technologie nicht nur im Zahlungsverkehr den Intermediär ausschalten kann. Er sieht hier vor allem die Zwischenhändler als überflüssig an. Peter Ivankay relativiert seine Aussage und sieht diese Stärke von Blockchain als langfristig gegeben, wohl aber nicht innerhalb der nächsten fünf bis gar zehn Jahren als umsetzbar. Anders sehen es der Unternehmensberater M.L., welcher nicht glaubt, dass alle Geschäftsprozesse ganz ohne Intermediär funktionieren können. Dabei erfasst es Simon Schweri am besten: Es kommt darauf an, wie man den Begriff Intermediär definiert. So glaubt er, dass es zwar Intermediäre in gewissen Anwendungsfällen geben wird, welche nicht mehr gebraucht werden durch den Einsatz der Blockchain Technologie, doch der Mehrwert, welcher diese Intermediäre der Wertschöpfungskette hinzufügen, ist allgemein sehr gering. So sind nach seiner Definition von Intermediären vor allem jene betroffen, welche keinen

oder nur einen geringen Mehrwert erbringen. Hierzu zählt beispielsweise ein Zwischenhändler, der neben seiner Marge vor allem Aktivitäten erledigt, welcher heutzutage auch ein Hersteller ohne viel Aufwand übernehmen könnte. Somit sinkt der Mehrwert des Intermediär auf Null und er wird durch die Blockchain ersetzt. Interessant sieht er jedoch, dass viele Drittanbieter als Knowhow Träger agieren. So ist es dem Hersteller wohl möglich, die Ware selbst zu verschicken, doch ein Zwischenhändler kann dies womöglich besser und günstiger machen durch sein Wissen. Im Fall von Schweris Firma ist es der Zahlungsverkehr. Viele eCommerce Kunden möchten sich nicht mit den regulatorischen und technischen Umsetzungen befassen und lagern dies aus. Auch hier sieht Simon Schweri es schwierig, dass solche Anbieter verschwinden werden durch die Blockchain Technologie. Andreas Hirstein sieht die Sachlage aus diesem Grund ein wenig differenzierter. Er glaubt eher, dass die Technologie als Optimierung der Prozesse von diesen Drittanbietern genutzt wird. Auch wenn ihn der Gedanke der Anarchie fasziniert.

Die Interviewpartner wurden in diesem Zuge mit einem konkreten Anwendungsszenario konfrontiert: Die Ablösung einer Bank durch die Blockchain. Die Mehrheit sieht dies als sehr unwahrscheinliches Szenario an. So sind es die vielgenannten Attribute des *über lange Zeit aufgebaute Vertrauen* sowie die *hohe Komplexität von vielen Prozessen* und nicht zuletzt die *regulatorischen Auflagen*, die so eine utopische Vorstellung im Keim ersticken lassen. Nur Lucas Silva glaubt, dass langfristig dieses Szenario aus technischer Sicht sehr wohl möglich ist.

Stärke: Offene Entwicklung (open source)

Gefragt wurde hierbei zwischen der offenen Entwicklung in der Community und der abgeschotteten Betrachtung von vielen kommerziell getriebenen Initiativen. Die technisch ausgerichteten Interviewpartner, Lucas Silva und Oliver Heister, sehen in der Community einen wichtigen Punkt zur Weiterentwicklung der Blockchain. Viele Erweiterungen sind aus diesem Rahmen entstanden und eine geschlossene Entwicklung führt zu proprietären Systemen, welche sich kaum durchsetzen können oder aber schlimmer, eine monopolistische Stellung einnehmen könnten. Laut Lucas Silva lassen sich zurzeit *viele Unternehmen Patente* zur Blockchain ausstellen (J.P. Morgan, Barclays) und verhindert so die freie Entwicklung zusätzlich. Dies entspricht nicht der Philosophie des oder / der Erfinderin. Hierbei sehen sie auch die Stärke der Blockchain, so wie sie jetzt ist. Es sind viele Techniker und Wissenschaftler, die über die offene Gemeinschaft ihre Ideen einbringen können und zu einer stetigen Weiterentwicklung beitragen können. Andreas Hirstein sieht die parallele Entwicklung von geschlossenen Systemen jedoch als ganz natürlich bei der Kommerzialisierung einer Technologie und drückt damit die traditionelle Sicht aus. Dem wiederspricht der Unternehmensberater M.L., er sieht eine *starke und offene Community* als grosse Stärke von jeder Bewegung. Es ist ein Erfolgsrezept, das insbesondere die Technologie stärkt. Denn der dadurch globale Diskurs führt schnell und effizient Probleme ans Licht und

Lösungen sind ebenso schnell eingeführt. Ohne diese Stärke würde die Blockchain seiner Meinung nach nicht da sein, wo sie heute ist.

Weitere Stärken

Oliver Heister und Lucas Silva sehen die zusätzlichen Prinzipien der Blockchain 2.0 als positive Entwicklung, die das Anwendungsgebiet der Blockchain enorm vergrössert. Hierbei haben sie die Smart Contracts und die dadurch ausgelöste Automatisierung und Interaktion der Blockchain im Fokus. Dies könnte ihrer Meinung nach auch Intermediären gefährlich werden, welche jetzt noch den Mehrwert durch Knowhow erbringen. Dieses Knowhow könnte mit den Smart Contracts in die Blockchain eingebracht werden. Peter Ivankey sieht die Stärke *im All-in-one Konzept* der Blockchain. So verfügt sie zum Beispiel über eine integrierte Sicherheit. Man muss sich also nicht zusätzlich um eine zusätzliche Software bemühen, welche diesen Aspekt abdeckt. Die Merkle Trees erlauben eine sehr schnelle Verifikation der Transaktionen. Genauso verhaltet es sich mit den anderen Prinzipien der Blockchain, die alle in einem Guss integriert sind. Und dabei ist alles sehr einfach. Als weitere Stärke sieht Ivankay die finale E2E Digitalisierung. Endlich können alle Prozesse vollkommen digital ausgeführt werden - physische Gegenstände können durch Asset Tokenization ebenfalls eingebunden werden. Implizit führt dies zu einem *Umdenken* bei den Unternehmen bezüglich ihrer Prozesslandschaft und langfristig zu *stark reduzierten Prozesskosten*. Die Kombination der einzelnen Technologien fasziniert auch Stipe Brkljacic. Durch die offene Entwicklung sieht er dessen Fortschritt als unberechenbar an. Als Beispiel zählt er die Speicherung von Daten analog zu heutigen Services wie Dropbox oder OneDrive in der Blockchain. Dies war vor wenigen Monaten noch gar nicht absehbar. Als Stärke sieht er deshalb auch das noch völlig unerschlossene Potenzial der Blockchain.

Schwäche: Proof-of-Work / Mining

Als klare Schwäche nennen die Interviewpartner den *Konsensmechanismus* Proof-of-Work. Insbesondere die Techniker sehen den Grundsatz des Mining initial als positiv an, sehen den PoW als zu anfällig an. Denn die Probleme sind auch breit diskutiert; die Zentralisierung von Mining Pools nach China – günstiger Strom, günstige Hardware, 66% der Hash Power kommt von vier Mining Pools in China – die Verschwendung von Ressourcen und der zeitintensive Vorgang. Stipe Brkljacic sieht hier auch grossen Verbesserungsbedarf, und betrachtet auch den PoS Ansatz als nicht ideale Lösung. Lucas Silva stellt zudem ein zukünftiges Szenario in Frage. So wird bei Bitcoin nach dem Schürfen des allerletzten Bitcoins kein weiteres Incentive mehr im PoW ausgezahlt. Er fragt sich, ob sich die Kryptowährung dann noch – nur aus den Transaktionsgebühren – halten kann. Denn diese sind selbst bestimmbar aber müssten die Miner dazu motivieren, die Transaktion zu verifizieren.

Weitere Schwächen

Simon Schweri sieht die eigentlichen Stärken der Blockchain gefährdet durch die Entwicklung der Gesellschaft. So sind bestimmende Stärken wie die Transparenz wohl nicht überall erwünscht und würden somit den Einsatz der Blockchain Technologie verhindern. Peter Ivankay ergänzt hierzu, dass die *Anonymität* der Blockchain nicht wirklich gegeben ist. Zusätzlich kritisiert er die derzeitige *Geschwindigkeit*, die für viele Anwendungsfälle nicht schnell genug ist. Oliver Heister meint zudem, dass die grossen Firmen, welche sich derzeit mit der Entwicklung der Blockchain beschäftigen, weitere kleine Blockchain Softwares und Applikationen erzeugen und sich *kein Standard* etablieren kann. Auch für Lucas Silva ist eine Standardisierung wichtig, damit man die Kraft in die Entwicklung neuer Anwendungsfälle anstelle in die Lösung von fehlender Interkompatibilität stecken muss. Lucas Silva und weitere Interviewpartner sehen eine weitere Schwäche in den vergangenen Ereignissen rund um Ethereum. Hierbei sprechen alle vom Fall des *Exploit* eines Smart Contract, welches zu einem enormen Verlust geführt hätte, hätte nicht die zentrale Organisation selbst einen Hard Fork ausgelöst. Auch wenn dies für Ethereum unumgänglich war, wurde die Glaubwürdigkeit des Prinzips des Zero-Trust untergraben. Wenn der Grundsatz gelten sollte, so müssen diese neuen Risiken akzeptiert werden und die Konsequenzen daraus getragen werden, um in neuen Entwicklungen auf diese Schwächen reagieren zu können. Lucas Silva meint zudem, dass alternative Technologien, die meist heute schon im Einsatz sind, in vielen Anwendungsfällen performanter sind, als dies die Blockchain ist.

Blockchain als Prozessoptimierer oder Solution

Abschliessend zu dieser Kategorie konnte aus der Inhaltsanalyse die folgende Erkenntnis abgeleitet werden. Die Blockchain kann in zwei Anwendungsformen eingesetzt werden. Einmal als Prozessoptimierer, als den sie von der Mehrheit der Interviewpartner kurz- und mittelfristig gesehen wird und als Solution. Hierbei ist gemeint, dass die Blockchain nicht nur als Enabler sondern als Driver des Prozesses erachtet wird. Auch hier sind sich alle Interviewpartner einig, dass es hierzu sehr viel Aufwand benötigt, um eine Prozesslandschaft eines Unternehmens umzugestalten. Man sieht diese Rolle der Blockchain somit eher als langfristiges Szenario. Nur Start-ups traut man zu, die Blockchain heute schon als Solution zu nutzen.

Kategorie 3: Implikationen

Allgemeine Implikationen

Karin Frick vergleicht die Transformation zur Blockchain als bekanntes Paradigma von der Ablösung eines alten zu einem neuen System in der Geschichte. So sind solche Erneuerungsprozesse immer von Turbulenzen begleitet. Und bei der Blockchain sieht sie hier vor allem die sozialen Implikationen (vgl. weiter unten) als gewichtig. Daneben sieht sie die Umstellung der Unternehmen als Verdrän-

gungskampf, welcher bereits eingesetzt hat und am Ende nur die effizientesten überleben. Die Blockchain beschleunigt diesen Prozess. Stipe Brkljacic impliziert aus den Stärken der Blockchain eine Demokratisierung von allem. Dies führt dazu, dass keine Monopolstellungen mehr möglich ist und alle Teilnehmer über wichtige Entscheide abstimmen können. Auch Peter Ivankay sieht dadurch eine Vereinfachung von Prozessen, da diese von allen mitgetragen werden. Generell sagt er, dass es zu einer Vereinfachung kommt, denn die Blockchain bietet mit ihrer Automatisierung eine grosse Entlastung der administrativen Tätigkeiten.

Simon Schweri sieht bei einer Einführung von Blockchain nicht nur technische Implikationen, sondern vielmehr ein Paradigma Wechsel in mehreren Bereichen. Beispielsweise kann die Stärke der Transparenz der Blockchain nur dort eingesetzt werden, wo diese erwünscht ist. Er spricht denn auch von Mächten, die deren Einsatz verhindern können, um ihre eigenen (illegalen) Profite weiterhin zu generieren. Er sieht hierdurch einen Diskurs notwendig, um diese Themen anzusprechen. Peter Ivankay ergänzt hierzu, dass die Dezentralisierung nicht überall wünschenswert ist (KYC, AML), dies jedoch durch heutige Auflagen bedingt ist.

Regulatorische Implikationen

Wie Peter Ivankay bereits erwähnt hat, sind die heutigen Regulatorien nicht ideal für den Einsatz der Blockchain. Dieser Ansicht sind auch viele anderen Interviewpartner. Entsprechend sehen sie durch den stetig wachsenden Einsatz der Blockchain Technologie eine Weiterentwicklung der Auflagen als unabdingbar und bezeichnen sie in der heutigen Form als Blocker der Technologie. Stipe Brkljacic fügt hinzu, dass bei Bitcoin derzeit das Problem besteht, dass es in vielen Ländern noch unter das Geldwäschereigesetzt fällt und die Konversion von traditionellen Währungen in die Kryptowährung und umgekehrt schwierig bis unmöglich ist, wenn man sich nicht illegal verhalten möchte.

Marktüberwachung ETF

Eine Frage im Kontext der regulatorischen Implikationen betrifft die derzeit untersuchte Kotierung von ETFs an der Börse in New York. Hierzu lassen sich zwei Erkenntnisse aus den Interviews generieren. Zum einen die Aussage, dass Blockchain als Prinzip einen Ausschluss von Drittparteien anstrebt, sich aber dann auch nicht auf Gebiete vordrängen sollte, in denen so eine Drittpartei unumgänglich ist. Zum anderen sehen es die Interviewpartner so, dass Kryptowährungen in diesem Fall nicht riskanter zu bewerten sind als die traditionellen Assets. Simon Schweri sieht in diesem Zusammenhang eine technologische Entkoppelung als Lösung der Marktüberwachung als kein gangbarer Weg. Peter Ivankay beschreibt hierzu treffend, dass sich Blockchain Applikationen nicht dorthin bewegen sollten, so sie konzeptionell nicht hingehören.

Soziale Implikationen

Karin Frick, Beobachterin vom gesellschaftlichen Wandel ausgelöst durch innovative Technologien, sieht eine sehr interessante Implikation durch die Blockchain als anstehend. Durch die Stärke des Zero-Trust und der damit wegfallenden zentralen Autorität sieht sie die Gesellschaft konfrontiert mit einem völlig ungewohnten Bild. So sind sich die Menschen gewohnt, dass sie ein hierarchisches Bild in vielen Situationen vorfinden. Sei es bei der Arbeit der Chef oder die behördliche Instanz. Die Menschen müssen sich entsprechend an ein verteiltes Netzwerk gewöhnen, bei welchem es nicht mehr eine zentrale Einheit per se gibt. Andreas Hirstein meint zu der Frage, ob durch die Digitalisierung und Blockchain als weiterer Beschleuniger dieses Prozesses die Menschen nicht mehr gebraucht werden, dass es sich um ein sehr unwahrscheinliches Szenario handelt. Er sieht aus philosophischer Sicht keinen Grund, dass technische Systeme Profit generieren, wenn kein Mensch mehr davon profitieren kann bzw. sich die so erzeugte Dienstleistung leisten kann.

Offene Entwicklung (open source)

Die offene Entwicklung der Blockchain führt dazu, dass sich die Blockchain für alle offen zeigt. Jeder kann, wenn gewollt, Einfluss in die Entwicklung nehmen. Diese Implikation stärkt das Vertrauen in die Technologie. Dabei sieht es der Grossteil der Interviewpartner als gegeben, dass sich initial die geschlossenen Systeme (private, permissioned Blockchains) in der kommerziellen Entwicklung durchsetzen werden, sprechen aber von einer parallelen Existenz beider Systeme (private und public) für unterschiedliche Anwendungsfälle.

Kategorie 4: Anwendungsfälle

Bitcoin und Blockchain

Für die Entwicklung von Anwendungsfällen ist es für alle Interviewpartner wichtig, die Differenzierung zwischen Kryptowährungen wie Bitcoin und der Blockchain zu machen. Denn die Kopplung schränkt die Sichtweise auf potenzielle Anwendungsfälle ein. Stipe Brkljacic sieht hier die Kryptowährung selbst als einen von vielen Anwendungsfeldern der Blockchain Technologie.

Enabler der Blockchain

Initial soll geklärt werden, wo die Mehrwerte einer Blockchain zu identifizieren sind, um ihren Einsatz auf potenzielle Anwendungsfälle zu fördern. Simon Schweri sagt denn auch, dass die Blockchain als Technologie eine entsprechende Effizienzsteigerung aufweisen muss, damit sie sich durchsetzen kann. Die Enabler bzw. Value Driver der Blockchain für Unternehmen werden von Peter Ivankay wie folgt zusammengefasst: Transparenz, Automatisierung, Sicherheit, Immutability, Effizienz und Geschwindigkeit beim Auslesen. In einer anderen Sichtweise auf die Enabler der Blockchain sieht Karin Frick die Kombination dieser Technologie mit IoT-Geräten und der künstlichen Intelligenz. Hieraus lässt sich der Funktionsumfang der Blockchain Technologie enorm steigern und ganz neue Anwendungsfälle werden

ermöglicht. Sie sieht die Blockchain in der jetzigen Form wie auch viele andere Experten mehrheitlich als Prozessoptimierer. Die wirklich interessanten Anwendungsfälle werden ihrer Meinung nach erst durch eine weitere Kombination der Technologien entstehen. Genauso sieht es Stipe Brkljacic, welcher hierbei eine gestaffelte Umsetzung sieht; zunächst die langsame Evolution der Unternehmen durch den Einsatz der Blockchain als Prozessoptimierer und dann der Big Bang, die Revolution durch die Technologie durch deren Einsatz als Driver, wobei auch er von der Kombination mit künstlicher Intelligenz ausgeht. Hier verweist er jedoch erneut auf die Notwendigkeit, dass sich Regulatoren dieser Entwicklung nicht entziehen und sich entsprechend den neuen Bedingungen anpassen. Ansonsten können solche Ideen nur auf dem Papier überleben.

Technologie Unternehmen / Startups und Blockchain

Die Interviewpartner sehen die Gefahr von Technologieunternehmen wie Google oder Apple als Treiber der disruptiven Entwicklung zu Ungunsten der traditionellen Unternehmen als gegeben an. Jedoch sei zu differenzieren zwischen verschiedenen Branchen. Als Erkenntnis kann aufgeführt werden, dass Bereiche, in denen eine hohe Intensität der Kontrolle durch zentrale Einrichtungen herrscht, branchenfremde Anbieter eine hohe Eintrittshemmschwelle haben. Dies sieht man auch bei Fintechs, die sich heute nur auf einen Teilbereich des Finanzgeschäfts fokussieren. Als Beispiel nennt Peter Ivankay den Zahlungsverkehr, der zwar ebenfalls reguliert ist, jedoch im Vergleich zu anderen Geschäftsfeldern einer Bank nur in einem sehr geringen Ausmass. Für die Wahrscheinlichkeit von Anwendungsfällen zur Umsetzung mit Blockchain ist demnach zunächst zu beachten, ob der Handlungsbereich zentral reguliert ist und erst dann auf mögliche Konkurrenten von technologieaffinen Industrien.

Entwicklung von Anwendungsfällen

Peter Ivankay sieht zwei verschiedene Ansätze zur Identifikation und Entwicklung von Anwendungsfällen. Zum einen gibt es die Möglichkeit, ein Konsortium zu gründen und viele Unternehmen aus einer spezifischen Branche in diesem zu bündeln. Dadurch hat ein solches Konsortium den Vorteil, über eine grosse Schlagkraft zu verfügen. Als negativ bewertet er jedoch die langwierigen Verhandlungen um Standards, die durch die vielen Teilnehmer im Konsortium verlangsamt werden. Bis ein dort entwickelter Anwendungsfall dann wirklich Einsatz in den Unternehmen findet, können Jahre vergehen. Daneben gibt es die Option, sich selbst an die Identifikation und Entwicklung von Anwendungsfällen zu machen. Hierbei kann man sehr schnelle Ergebnisse erzielen. Doch abgesehen vom Einsatz im eigenen Unternehmen findet eine Durchsetzung ausserhalb nur langsam oder gar nicht statt. Insbesondere bei der Bockchain kann das ganze Potenzial nur durch eine Beteiligung aller Anspruchsgruppen des Prozesses realisiert werden. Der Unternehmensberater M.L. fügt zum Vorgehen der Entwicklung von An-

wendungsfällen hinzu, dass zunächst geprüft werden soll, wie sehr die Prozesse des betrachteten Anwendungsfalls integriert sind. Dabei sollte auch erfasst werden, was die kritischen Messgrössen sind, die vom neuen Prozess zu erfüllen sind, damit der Anwendungsfall nicht schlechter mit Blockchain umgesetzt wird, als die heutige Umsetzung. Generell rät er deshalb, sich auf kleinere Anwendungsfelder zu fokussieren. Rao Jags fügt hinzu, dass insbesondere heute schon rein digitale Prozesse sich sehr gut für die Blockchain eignen und so ein schnelles Erfolgserlebnis gewährleisten, womit man dann weitere Anwendungsfälle treiben kann. Bei der Auswahl der Anwendungsfälle sollten heute entsprechend aktuelle Fälle herangezogen werden, um die Vorteile der Blockchain sichtbar zu machen.

Umgang traditioneller Unternehmen mit der Blockchain

Wie bereits mehrfach erwähnt, sehen traditionelle Unternehmen den Wert der Blockchain zurzeit als Prozessoptimierer. Die von Swiss Re und UBS entwickelten Machbarkeitsanalysen und Proof-of-Concept Projekte bestätigen dieses Bild.

Formen der Blockchain

Unterschieden werden von den Interviewpartnern die public und die permissioned Blockchain. Die Wahl einer dieser Formen ändert die Auswahl an Prinzipien, welche die Blockchain und der daraus entwickelte Anwendungsfall unterstützt. Es ist demnach sehr wichtig, sich ausgehend von den gebrauchten Prinzipien wie Dezentralisierung etc. auseinanderzusetzen, bevor die weitere Entwicklung eines Anwendungsfalls mit der Blockchain stattfindet. Laut dem Unternehmensberater M.L. bieten Permissioned Blockchains hierbei einen Investitionsschutz, da es sich durch eine oder mehrere Stellen kontrollieren lässt. Dies, räumt er ein, ist natürlich nicht im Sinne der ursprünglichen Blockchain. Lucas Silva stellt denn auch die Frage, ob für die Weiterentwicklung und den Einsatz der Blockchain all diese Prinzipien wirklich zu berücksichtigen sind.

Blockchain als Prozessoptimierer oder Solution

Die Unterscheidung zwischen Prozessoptimierer und Solution wurde schon zuvor aufgeführt. Im Kontext von Anwendungsfällen sollte man sich laut den Interviewpartnern jedoch auch damit auseinandersetzen, in welcher Form die Blockchain den Anwendungsfall bereichern kann. Innovativ wird es vor allem durch den Einsatz der Blockchain als Solution doch für traditionelle Unternehmen ist es auch sehr verlockend, diesen in einem evolutionären Schritt als Prozessoptimierer zu verwenden.

Weitere Punkte

Als wichtigste ergänzende Aussage meinen mehrere Interviewpartner, dass die konkrete Identifikation von Blockchain Anwendungsfällen zurzeit sehr schwierig ist. Gerade heute, wo fast alle zwei Tage ein

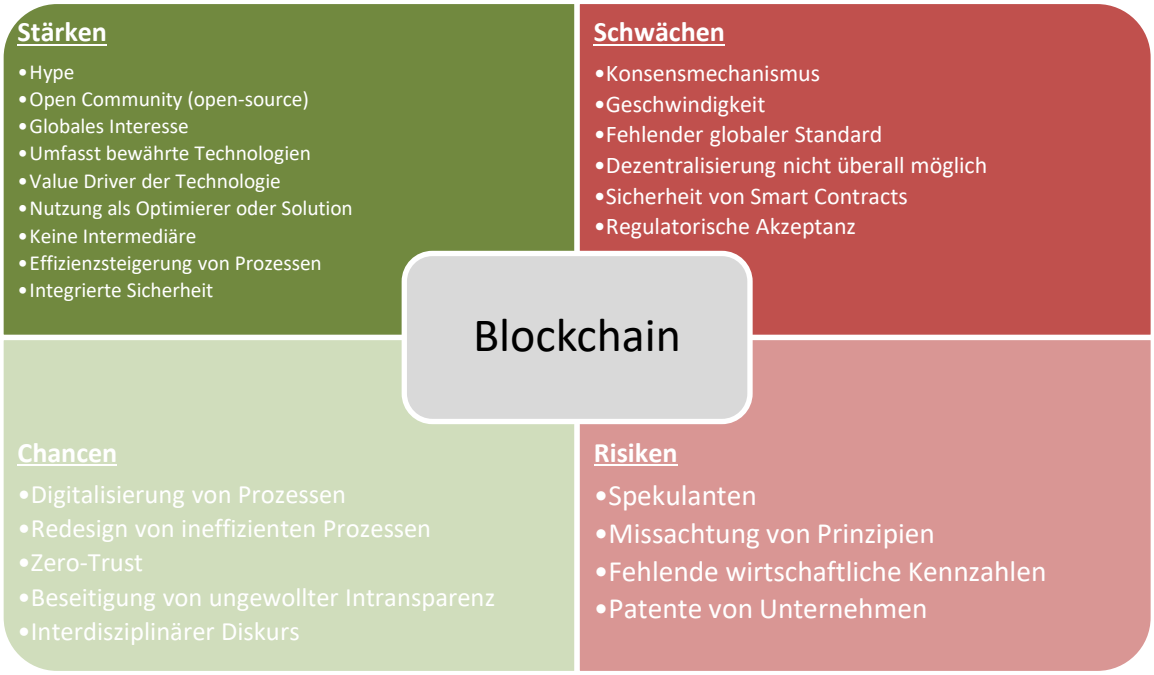
neuer Anwendungsfall mit Blockchain umgesetzt wird bzw. das Konzept dazu in einem Whitepaper gepackt wird, ist es schwierig, diese schnelle Entwicklung festzuhalten.

Eine Methode zur Identifikation von Anwendungsfällen für die Blockchain kann dabei helfen, dass bei weiteren Anspruchsgruppen das Interesse an der Technologie geweckt werden kann. Dies kann sich nur positiv auf deren Entwicklung auswirken.

Alle sind sich hierbei einig, dass die heutigen Anwendungsfälle der Blockchain wohl weit weg davon sind, was wir in den nächsten Tagen sehen werden. Die wirklich disruptiven und innovativen Anwendungsfälle sind noch nicht entdeckt worden und die Blockchain selbst bedarf noch einer weiteren Entwicklungszeit, bis sie solch einen innovativen und durchschlagenden Anwendungsfall unterstützen kann.

3.1.2 SWOT-Ergebnis aus den Interviews

Im Folgenden sind die Stärken und Stärken sowie die Chancen und Risiken aus den Experteninterviews zusammengefasst.



Nachfolgend werden diese Erkenntnisse mit den Grundlagen aus der qualitativen Literaturrecherche angereichert, um die Analyse zu vervollständigen.

3.2 Stärken und Chancen der Blockchain

Die Stärken der Blockchain aus Sicht der Literatur wiederspiegelt sich in den Prinzipien der Technologie:

- Ein verteiltes Netzwerk, welches eine direkte Interaktion der Teilnehmer ermöglicht und ein offenes System darstellt – *distributed power and resources - decentralisation, openness, transparency, integrity, scalability*
- Keine Drittpartei notwendig – *no trusted third party, zero-trust*
- Eine Transaktionskette, die nicht veränderbar ist – *immutability*
- Sicherheit durch Verwendung von kryptographischen Algorithmen – s*ecurity, anonymity*
- Automatisierung durch codierte Verträge – *automatization*
- Variable Anzahl an Verarbeitungsschritten einer Transaktion - *Interaction*

3.3 Schwächen und Risiken der Blockchain

Performance und Skalierbarkeit

Einer der Schwächen der Blockchain Technologie ist deren Performance insbesondere in Bezug auf die Geschwindigkeit.

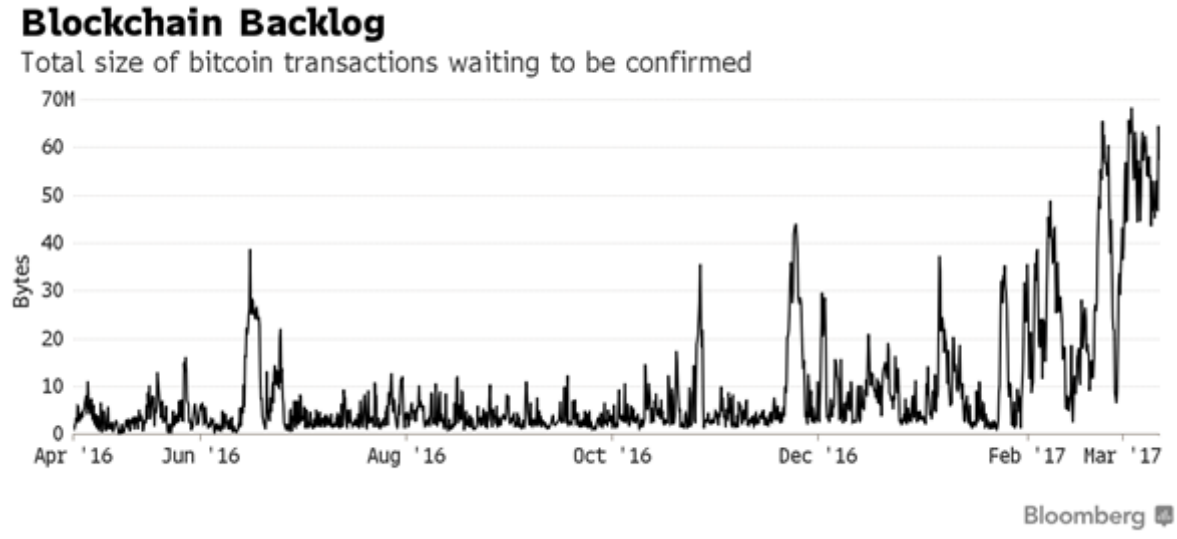


Abbildung 23: Entwicklung des Bitcoin Backlogs - Nicht verarbeitete Transaktionen (Nakamura & Chen, 2017)

Wenn hohe Transaktionsvolumen innerhalb von kürzester Zeit gehandhabt werden müssen, so raten auch Experten der Blockchain zu den traditionellen Systemen mit zentralisierter Datenbank. Blockchain Systeme sind langsam und es fallen bei jeder Transaktion Gebühren in Form der Entschädigung

der Miner an. Zentralisierte Datensysteme basierend auf einem Client-Server Modell sind schneller und dabei zurzeit noch günstiger.

Neben den Problemen der Geschwindigkeit ergibt sich ebenso ein bereits breit diskutiertes Thema der Skalierbarkeit. Konkret betrifft es hierbei die Grösse des Blocks, welches bei Bitcoin auf 1 MB limitiert ist (Bitcoin Wiki, 2016). Jeder Block, der grösser ist, gilt als invalid. Würde die Grösse des Blocks erhöht werden, so könnten mehr Transaktionen pro Sekunde verarbeitet werden und es würde die Erweiterung der Funktionalität begünstigt. Dies hätte einen positiven Effekt auf die zuvor angesprochene Geschwindigkeit der Blockchain (Croman et al., 2016). Doch ebenso führt eine Erhöhung der Blockgrösse zum Bedarf von mehr Rechenleistung und die Attraktivität von Bitcoin könnte darunter leiden. So gehen Kritiker auch davon aus, dass dadurch eine implizite Zentralisierung der Bitcoin stattfinden könnte, die nur die rechenstarken Miner inkludieren würde bzw. könnte (Bercovici, 2014). Die kontroverse Diskussion beschäftigt die Community bereits seit einigen Jahren und ein Konsens wurde hierbei noch nicht gefunden.

Sicherheit & Kontrolle

Nakamoto Satoshi schreibt selbst im Whitepaper zur Bitcoin (und Blockchain), dass ein gewisser Grad an Betrug akzeptiert werden muss, als das er unvermeidbar ist (Nakamoto, 2008). Taylor (2015) schätzt, dass die Thematik der Sicherheit und Kontrolle einer weiteren Entwicklung bedarf, bis sich durch die Blockchain Mainstream Applikationen erstellt werden können. Konkret kann gesagt werden, dass die derzeit verwendeten kryptographischen Verschlüsselungen sicher sind (Bonneau, et al., 2016).

Hard Forks

Die Hard Forks beschreiben eine erzwungene Abspaltung von der bestehenden Blockchain in eine parallele zweite Blockchain. Dies kann ausgelöst werden durch Änderungen der Blockchain Software. Dabei kann solch ein Prozess durchaus problematisch für die betroffene Blockchain sein. Bergmann (2015) unterscheidet zwischen folgenden Szenarien bei einem Hard Fork, welcher die Blocksize der Bitcoin erhöhen würde:

- Fehlende Miner-Unterstützung
  Zwar würden die Miner trotzdem weitere Blöcke erzeugen, diese eigenständig auf 1 MB beschränken. Die Miner entscheiden letztendlich, welche Transaktionen bestätigt werden und somit implizit, wie gross ein Block wird
- Fehlende Benutzer-Unterstützung
  Als theoretischer Ansatz kann aufgezählt werden, dass auch Benutzer wie Händler und Produzenten eine Hard Fork nicht unterstützen müssen. Somit werden die grösseren Blöcke einfach ignoriert, was dazu führt, dass keine Transaktion mehr akzeptiert wird

- Keine Mehrheit
  In diesem Szenario würden beide Forks weitergezogen, wobei jedoch mit der Zeit unterschiedliche Informationen in den beiden Ketten herrschen. So kann in einer Chain das Geld bereits beim Hersteller sein und bei der anderen noch gar nicht ausgegeben. Auch wenn dies eine schwierige Manipulation ist, so ist sie dennoch möglich

Die 51 Prozent Attacke

Die 51 Prozent Attacke betrifft den Konsensmechanismus der Blockchain. Auch wenn es bei der Anwendung des PoS-Ansatzes ziemlich kostenintensiv ist, so besteht dieses Risiko dennoch. Es handelt sich dabei um die Übernahme der absoluten Mehrheit (51%) im System durch eine Partei.

Regulatorisch Schwächen und Risiken

Nur durch den Fakt, dass Transaktionen in der Blockchain öffentlich sind und im Sinne der Technologie korrekt verifiziert wurden, heisst dies nicht, dass sie unter den heutigen gesetzlichen Auflagen legal sind. Die Firma Elliptic hat daraus ein neues Businessmodell entwickelt. Eine Software überprüft die Millionen von Transaktionen in der Bitcoin-Blockchain auf verdächtige Webseiten-Links. Die Identifikation illegaler Aktivitäten hilft Strafverfolgungsbehörden und Finanzinstituten (Gottlieb Duttweiler Institute, 2017).

Aufgrund der sich noch am Anfang ihrer Entwicklung befindliche Technologie sind viele Regulatoren noch in einer beobachtenden Stellung. Doch mehr und mehr Start-ups drängen auf den Markt mit ihren Anwendungsfällen und auch im Interview mit den Experten wurde klar, dass alle diese Anspruchsgruppen sehr verunsichert sind, solange die Regulatoren nicht mit klaren Auflagen kommen, welche nichtdiskriminierend sind, wie dies bei Bitcoin der Fall ist, welche als Kryptowährung pauschal unter das Geldwäscherei-Gesetz fällt (FINMA, 2015). Auch die Studie von Cofinpro mit dem Fokus auf Finanzakteure zeigt, dass die fehlende rechtliche Regelung eine Hürde für die Anwendung der Blockchain darstellt (Cofinpro AG, 2016). Dabei hält der NZZ Journalist Jan Flückiger (2017) treffend fest, dass die Politiker der digitalen Welt mit Gesetzen aus einer analogen Welt begegnen wollen. Nötig wäre aber vielmehr ein gesellschaftlicher Dialog über den Umgang mit Daten und neuen Technologien.

Moralische Bedenken

Stichworte wie der enormer Energieverbrauch des PoW, Korruption in China für billigen Strom, Waffenhandel, die illegale Plattform Silkroad sowie die Kombination der Bitcoin mit dem WannaCry Virus sind Themen, die zu dieser Kategorie gehören. So stellt sich die Frage, wie sich diese Problematiken weiterentwickeln und ob man einen solch dezentralen Ansatz wirklich fair und sauber umsetzen kann.

Alternativen

Was natürlich insbesondere bei der Überlegung von neuen Anwendungsfällen innerhalb der Blockchain wichtig ist, ist die Frage nach alternativen. So handelt es sich bei der Blockchain noch um eine in der Entwicklung befindlichen Technologie, welche einige Nachteile mit sich bringt und vielen Herausforderungen gegenüberstehen wird, welche noch zu lösen sind. Daneben gibt es aber schon heute sehr gut etablierte technische Alternativen, die meist für einen einfachen Anwendungsfall kostengünstiger wären und viele der oben genannten Probleme und Risiken nicht mitbringen würden. Die Frage ist ausserdem, ob es sich bei einer permissioned Blockchain nicht einfach um eine verteilte Datenbank handelt?

3.4 Implikationen

Die formale Implikation des Einsatzes der Blockchain Technologie bezogen auf die Anwendungsfelder kann ein weites Spektrum umfassen. Aufgrund der hypothetischen Prämisse, dass sich die Blockchain in den bisher genannten Anwendungsfeldern nachhaltig durchsetzen wird, handelt es sich bei den nachfolgenden Implikationen um hypothetische Urteile nach Menne (1957).

In der Analyse der Interviews konnten die folgenden Implikationen der Blockchain Technologie ermittelt werden:

Allgemeine Implikationen

- Die Blockchain führt zur Demokratisierung von allem
- Solch ein Paradigma Wechsel verläuft immer mit Turbulenzen
- Die Blockchain beschleunigt den Druck auf Unternehmen, kostengünstige Produkte durch effizientere Prozesse anzubieten und macht Geschäftsmodelle von gewissen Intermediären als langfristig obsolet
- Die Entlastung von administrativen Prozessen insbesondere im Back-Office
- Einen interdisziplinären Diskurs, welcher ausgelöst wird durch den Effekt der Blockchain auf mehreren Bereichen denn nur die technische oder wirtschaftliche Ebene (Stichwort illegale Aktivitäten und Transparenz)

Regulatorische Implikationen

- Regulatoren müssen die Konzepte von Blockchain überprüfen und Wege finden, die Aktivitäten daraus rechtlich abzusichern (Stichwort Kryptowährungen aber auch Smart Contracts)

Soziale Implikationen

- Die Gesellschaft muss sich an ein System ohne zentrale Autorität gewöhnen

- Menschen werden in neuen Berufen aktiv werden, um die Digitalisierung zu unterstützen und durch die offene Entwicklung der Blockchain kann jeder an dieser mitwirken

4 Methode zur Identifikation geeigneter Anwendungsfälle

Im folgenden Kapitel werden die aus der Analyse sowie dem Status Quo der Blockchain erhobenen Erkenntnisse in eine Methode zusammengeführt. Wie im Forschungsdesign beschrieben, soll basierend auf der Literatur sowie den Experteninterviews eine Methode gestaltet werden, welche Anwendungsfälle identifiziert, welche durch die Blockchain optimiert werden können. Hierbei unterscheidet der Autor zwischen den *Use case needs* und den *Blockchain offers*. Vereinfacht dargestellt sieht die Methode folgendermassen aus.

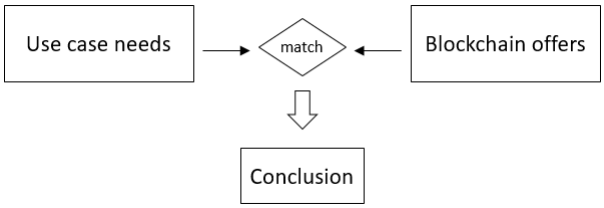


Abbildung 24: Modell zur Identifikation von Anwendungsfällen für die Blockchain (Eigene Darstellung)

Aufgrund der Verifikation der Methode mit u.a. Englisch sprechenden Experten wurde entschieden, die Bestandteile in Englisch zu erfassen. Dies soll auch einer zukünftigen Verwendung zuträglich sein.

Die nachfolgenden Kapitel gehen auf jedes Element der Methode ein und definieren deren Inhalt.

4.1 Blockchain offers

Um Anwendungsfälle zu bestimmen, muss zunächst die Blockchain in Parameter gefasst werden. Aus den betrachteten Anwendungsfällen konnte die Erkenntnis gemacht werden, dass diese insgesamt drei Formen der Blockchain nutzen:

- Public Blockchain *selten genutzt*
- Public Permissioned Blockchain *sehr häufig genutzt*
- Permissioned Blockchain *sehr häufig genutzt*
- Private Blockchain *nie genutzt*

Aufgrund dieser Erkenntnis beschränkt sich die Methode in dieser Arbeit auf zwei Formen: Die public Blockchain und die permissioned Blockchain. Des Weiteren konnte in der Analyse festgestellt werden,

dass die Prinzipien der Blockchain die Stärken der Technologie sehr gut zusammenfassen. Deshalb stellen die Prinzipien der Blockchain in Relation gebracht alle Parameter der Blockchain dar. Die nachfolgende Abbildung zeigt die Zusammenhänge der identifizierten Prinzipien der Blockchain in einer public Blockchain.

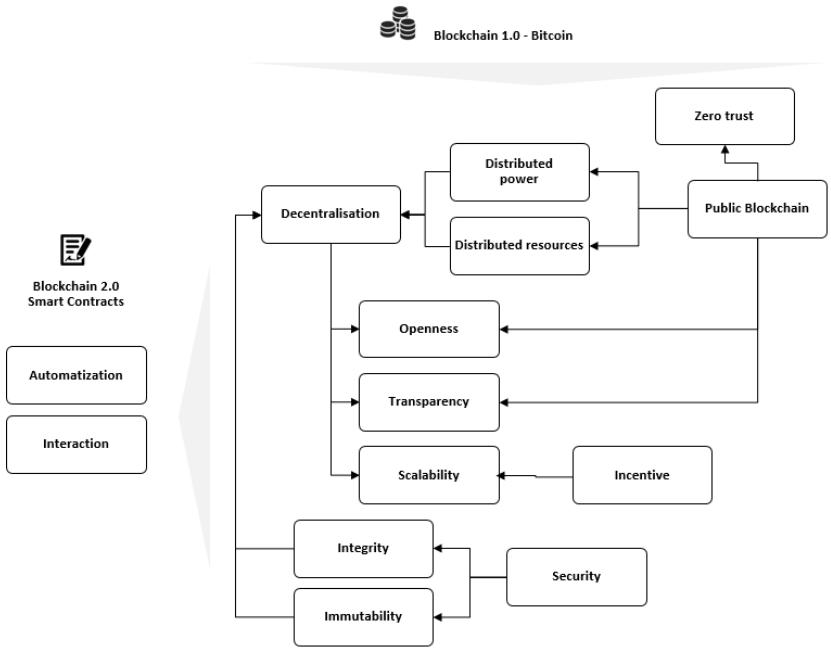


Abbildung 25: Relation der Prinzipien in einer public Blockchain (Eigene Darstellung)

Ausgehend hierbei ist die Wahl einer öffentlichen Blockchain, die dadurch das Prinzip des *Zero Trust* erforderlich macht. Denn die Teilnehmer des Netzwerks sind anonym und es existieren keine Prozesse, die eine Identifikation dieser Teilnehmer ermöglicht. Dies wiederum verleiht dem Netzwerk die Prinzipien *Openness* und *Transpanrency*. Denn jede Transaktion in diesem Netz wird bei jedem Teilnehmer abgelegt und die Daten sind in der Theorie lesbar – was nicht impliziert, dass sie für jeden verständlich sind. Durch die freie Teilnahme am Netzwerk kommt es zu einer *Decentralisation,* welche aus einer Verteilung von Ressourcen (Rechenleistung) und der dadurch verteilten Macht resultiert. Die *Decentralisation* wiederum trägt ebenfalls zur *Openness* und *Transparency* bei. In einem solch verteilten Netzwerk ist die Integrität der Daten – *Integrity* – essenziell. Korrupte Datensätze könnten das ganze System und die darauf basierenden Applikationen in Frage stellen. Die kryptographischen Algorithmen stellen diese sicher und machen das gesamte Netzwerk sicher – *Security.* Gleiches gilt für die *Immutability,* die zwingend erforderlich ist, da durch die Vielzahl an Teilnehmern ansonsten ein grosses Potenzial für Fälschungen vorhanden wäre. Zuletzt ist durch die *Decentralisation* die *Scalability* gegeben. Das Netzwerk ist durch neue Teilnehmer beliebig ausbaubar. Im Kontext einer public Blockchain ist jedoch wichtig, dass der Anreiz, *Incentive*, gegeben ist, um neue Teilnehmer zur Partizipation am Netzwerk zu motivieren.

Bei der Betrachtung von permissioned Blockchains unterscheidet sich das Bild wie folgt.

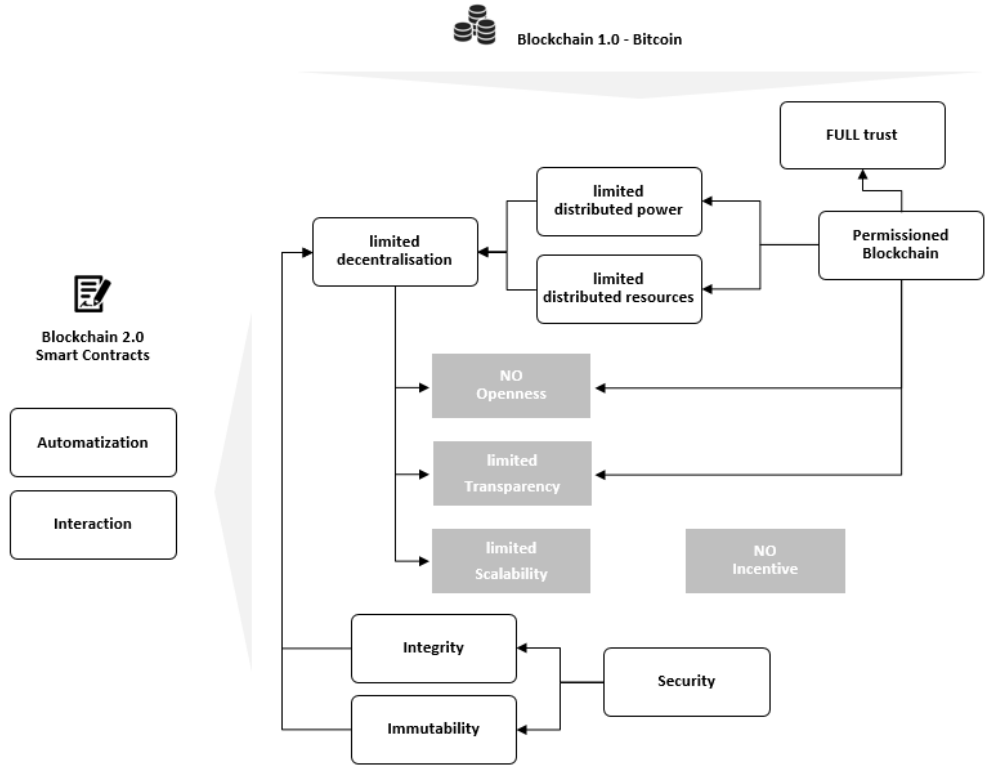


Abbildung 26: Relation der Prinzipien in einer privaten (permissioned) Blockchain (Eigene Darstellung)

Im Unterschied zu einer public Blockchain fallen die Prinzipien der *Openness* und des *Incentives* ganz weg. Daneben werden diverse andere Prinzipien limitiert durch Whitelists. Dadurch generiert sich jedoch auch ein neues Prinzip des *full trusts.* Jeder Teilnehmer kennt sich und verfügt so über ein explizites Vertrauen. Zentral für diese Form der Blockchain sind somit die verbleibenden Prinzipien *Integrity* und *Immutability*.

Auf Mischformen wird in dieser Methode, wie anfangs erwähnt, nicht eingegangen. Beide Formen der Blockchain bieten die Vorzüge der Blockchain 2.0, welche eine Erweiterung darstellt und die Eigenschaften der *Automatisation* und *Interaction* hinzufügt.

4.1.1 Schwächen und Risiken

Die Stärken der Blockchain sind in den zuvor aufgeführten Prinzipien der Blockchain implizit gefasst. Die Schwächen sind analog der vorhergehenden Analyse wie folgt:

Schwäche	*Public Blockchain*	*Permissioned Blockchain*
Konsensmechanismus	**x**	
Limitierte Skalierbarkeit	**(x)**	**x**
Mangelnde Interoperabilität der Systeme	**x**	**x**
Asynchrone Verschlüsselung	**x**	**x**
Irreversibilität von Transaktionen	**x**	**(x)**
Pseudoanonymität	**x**	
Mögliche Attacken	**x**	**(x)**

Tabelle 11: Schwächen der Blockchain mit Unterscheidung public / permissioned

Da die Schwächen unterschiedlich stark in den zwei betrachteten Formen auftreten – oder auch gar nicht, zeigt die Tabelle ebenfalls die Zuordnung der Schwächen zur jeweiligen Form. Nachfolgend werden jene Schwächen näher ausgeführt, welche nicht bei beiden gleich gewertet wurden.

Konsensmechanismus

Im Gegensatz zur public Blockchain exisitert in einer permissioned Blockchain das Vertrauen der einzelnen Teilnehmer bereits. Dadurch braucht es hier keine aufwändigen PoW oder ähnliche Ansätze zur Konsensfindung.

Limitierte Skalierbarkeit

Auch wenn die Skalierbarkeit bei beiden Formen eine Schwäche darstellt, so ist sie bei einer permissioned Blockchain durch die zentralisierte Whitelist schwieriger zu automatisieren. Nur zugelassene Teilnehmer dürfen sich dem Netzwerk anschliessen, was zu potenziell weniger Skalierbarkeit führt.

Irreversibilität von Transaktionen

Auch wenn es als grundsätzliche Stärke der Blockchain zählt (Immutability und Integrity) und auch in einer permissioned Blockchain bestand hat, so sieht der Autor bei einer permissioned Blockchain die Veränderung einer Transaktion durch die zentrale Autorität als möglich an, weshalb die Schwäche bei einer public Blockchain schwerer ins Gewicht fällt.

Pseudoanonymität

Durch den Fakt, dass die zentrale Autorität in permissioned Blockchains die Nutzer kennt, entfällt die Schwäche, wie auch die Stärke eines anonymen Netzes.

Mögliche Attacken

Durch die zentral gesteuerte Berechtigung kombiniert mit dem vorhandenen Vertrauen in die Teilnehmer ist die Wahrscheinlichkeit von möglichen Attacken innerhalb einer permissioned Blockchain tiefer, womit die Schwäche bzw. das Risiko bei einer public Blockchain höher gewertet wird.

4.1.2 Benchmarks

Bereits in der Analyse der Interview Experten wurde die Erkenntnis gemacht, dass es nur wenige bis keine Kennzahlen zur Blockchain gibt. Da sich die Entwicklung der Technologie erst am Anfang befindet, können keine Langzeitdaten erhoben werden. In der explorativen Literaturrecherche wurden trotz allem erste Benchmarks von verlässlichen Quellen gefunden, welche in die Methode mitberücksichtigt werden. Dabei handelt es sich teilweise um textuelle Aussagen ohne nummerischen Wert, welche dem Benutzer als Addendum in der Auswertung angezeigt werden.

- Anträge in komplexen Prozessen werden bis zu 4-mal schneller bearbeitet
- Kapitalbindung durch den Prozess wird um 40 Prozent reduziert
- Alle Stakeholder berichten von Effizienzsteigerungen
- Agiles, offenes und konsensorientiertes Management
- Dezentralisation der Organisation

(IBM Research, 2017), (Ethereum Homestead, 2016), (coindesk, 2017)

4.1.3 Parameter der Blockchain

Die in den vorhergehenden Teilen beschriebenen Elemente bilden die Parameter einer Blockchain, die in folgender Tabelle gemeinsam mit allfälligen Relationen und der Konnotation (Wertung) zusammengefasst sind.

ID	PARAMETER	RELATION	WERTUNG
1	Forms of Blockchain		+
1.1	Public Blockchain		+
1.2	Private / Permissioned Blockchain		+
2	Trust		+
2.1	Zero Trust	1.1	+
2.2	Full Trust	1.2	+
3	Decentralisation		+
3.1	Distributed Power		+
3.2	Distributed Resources		+
4	Integrity		+
5	Immutability		+

6	Openness	1.1;3	+
7	Transparency		+
8	Scalability		+
8.1	Incentive – BC with Mining	1.1	+
8.2	No incentive – BC without Mining	1.2	+
9	Automatization	BC 2.0	+
10	Interaction	BC 2.0	+
11	Near Real-time		+
12	Digitalization		+
12.1	Full digital		+
12.2	Digital tokenized Asset		+
13	(Pseudo)Anonymity	1.1	+
14	Consensus	1.1	-
15.1	Scalability – public	1.1	-
15.2	Scalability – permissioned	1.2	-
16.1	Interoperability – public	1.1	-
16.2	Interoperability – permissioned	1.2	-
17	Asynchronous cryptography		-
17	Immutability		-
18	Anonymity	1.1	-
19	Security		-

Tabelle 12: Parameter der Blockchain

4.2 Use Case needs

Der Prozess der Parametrisierung von Anwendungsfällen setzt eine initiale Klassifizierung des jeweiligen Anwendungsfalls voraus. Die Methode soll dem Anwender jeweils schnell Auskunft darüber geben, ob sich der gewählte Anwendungsfall für eine Umsetzung mit der Blockchain eignet. Deshalb werden Killerkriterien möglichst früh im Prozess ermittelt, sodass früh ungeeignete Anwendungsfälle aussortiert werden können. Aus den Experteninterviews und der Betrachtung von aktuellen Anwendungsfällen lässt sich hierbei der Digitalisierungsgrad als zentrales Kriterium identifizieren.

4.2.1 Digitalisierungsgrad

Der Digitalisierungsgrad eines Anwendungsfelds ist ein massgebender Faktor zur Bestimmung der Anwendungseignung der Blockchain Technologie. Es handelt sich hierbei nicht um ein Ausschlusskriterium – ganz im Gegenteil. Je analoger der derzeitige Anwendungsfall ausgeführt wird, desto grösser ist der potenzielle Mehrwert der Blockchain. Doch für eine Umsetzung ist ein solcher Anwendungsfall umso komplizierter, da viele Aspekte überarbeitet werden müssen. Bradley et al. (2015) haben in ihrer Untersuchung die Wirkung von disruptiven Technologien auf verschiedene Branchen untersucht und haben so eine Rangordnung zusammengestellt, die in folgender Abbildung visualisiert ist.

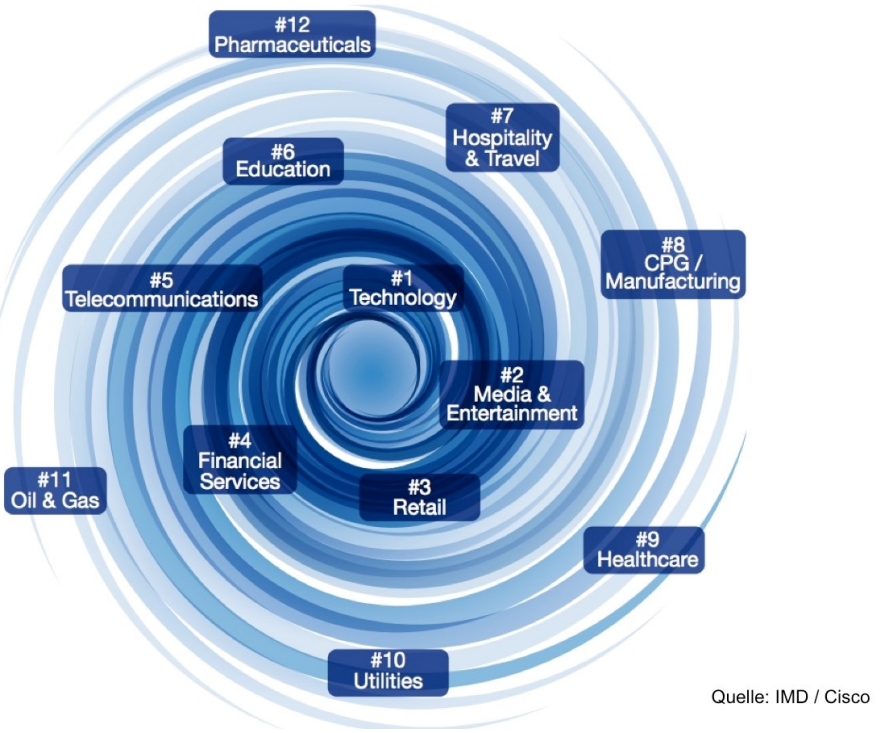


Abbildung 27: Wie disruptive Technologien die Branchen erfassen (Bradley, et al., 2015, p. 6)

Aufgrund dieser Grundlage wurden die Branchen als erster Use Case Parameter gesammelt. Hierbei wurden die Erkenntnisse aus der Studie von PwC (2016) zur Digitalisierung von Schweizer KMU sowie den Experteninterviews mitberücksichtigt, worauf die Reihenfolge der Branchen angepasst wurde und für die Methode wie folgt verwendet wird.

RANK	AREA	GEWICHTUNG
1	Technology	100
2	Banking	100
3	Insurance	100
4	Retail / Commerce	100
5	Healthcare	80
6	Utilities	80
7	Manufacturing	80
8	Education	75
9	Telecommunication	60
10	Hospitality & Travel	60
11	Oil & Gas	50
12	Pharmaceuticals	50
13	Others	50

Tabelle 13: Parameter des Use Cases

Die Gewichtung gibt an, wie sehr die entsprechende Branche eine positive Prämisse für den Einsatz der Blockchain Technologie bildet und wird so in der Auswertung der Methode verwendet. Bei der Bestimmung wurde geprüft, ob es schon aktuelle Anwendungsfälle in dieser Branche gibt. Zudem

wurde die Klassifizierung von Bradley et al. (2015) als weiterer ausschlaggebender Faktor mitberücksichtigt. Zuletzt haben auch die Experten ihre eigenen Vorstellungen miteingebracht, welche durch ihre Expertise zur Blockchain gestützt sind.

4.2.2 Weiterführende Fragen

Im Rahmen der ersten Iteration der Evaluation hat sich herausgestellt, dass noch weitere Fragen zu den Anwendungsfällen gestellt werden können, um eine akkuratere Erfassung der Use case needs zu erreichen:

- Finden Transaktionen statt, welche nicht digital erfasst werden können?
    - Was ist der maximale Digitalisierungsgrad des Anwendungsfalls?
- Wird ein Netzwerk genutzt?
- Müssen sich die Akteure des Anwendungsfalls kennen?
- Werden Intermediäre benötigt, um eine Transaktion zu validieren?
- Ist eine revisionssichere Speicherung der Transaktionsdaten notwendig?
- Gibt es ein Produkt im Anwendungsfall, welches fälschungssicher sowie nicht veränderbar sein muss?
- Ist eine Aktion final?
- Sind regulatorische Auflagen einzuhalten?

4.2.3 Gewichtung

In der Evaluation zeigte sich, dass die Anwendungsfälle primär durch die Parameter der Blockchain geprägt werden. Auch durch theoretische Tests kam der Autor zum Schluss, dass eine weitere Parametrisierung des Anwendungsfalls keine Änderung am Ergebnis gebracht hat. Es wurde deshalb entschieden, einen grossen Teil der Parameter der Anwendungsfälle zugunsten der Blockchain wegzulassen. Somit verbleibt für die Parametrisierung der Anwendungsfälle der Anwendungsbereich sowie die weiterführenden Fragen – welche jedoch ebenfalls eine Rückkopplung auf die Blockchain Parameter sind.

4.3 Match

Im Teil *Match* werden alle Parameter in Fragen umformuliert, welche der Nutzer jeweils binär beantworten kann und womit sich im Hintergrund ein Abgleich zwischen dem *Use Case needs* und den *Blockchain offers* ergibt. In den eckigen Klammern ist ein Wert enthalten, welcher die Gewichtung der Antwort ergibt. Bei Antworten ohne Wert ist die Wahl direkt aussagekräftig und führt zu einer Inklusion oder Exklusion eines Blockchain Parameters. Antworten mit einem Wert von 0 sind harte Ausschlusskriterien für die Blockchain Technologie. Bei der ersten Frage finden sich die Antwortmöglichkeiten wie auch die Gewichtung in Tabelle 13.

ID	*Question / Answer*	*Comment*
1	Is your use case related to one of these areas / fields? ☐ vgl. Tabelle 13	If the use case proposed is related to any of the top areas than it is highly probable that there is already a solution with blockchain in work or even existing.
	USE CASE DATA – "Is the data processed within the use case …"	
2.1	☐ confidential ☐ Internal ☐ public	If it is confidential / internal that excludes a public blockchain -> permissioned blockchain
2.2	☐ static [20] ☐ dynamic [100]	The advantages of blockchain are highest with dynamic data There are cheaper solutions to store static data
2.3	☐ physical [70] ☐ digital only [100] ☐ physical and digital [75]	Physical devices imply the use of tokenization
2.4	☐ Has to be deleted at a certain point [10] ☐ should be stored for the whole lifecycle [100]	Key benefit of blockchain is to store data (forever) No advantage in using a blockchain if data has to be deleted
2.5	☐ Modified just by yourself [0] ☐ modified by multiple users [100] ☐ modified by multiple users with interactions [100]	If there is only one party creating and editing data there is no point in using a blockchain -> cheaper alternatives Interactions call for Blockchain 2.0 (smart contracts)
2.6	☐ No data provenance required [50] ☐ Data provenance is important [100]	Securing data provenance is one of the key benefits of blockchain
2.7	☐ Controlled by a central authority [20]	Blockchain is not yet accepted with central authorities

	☐ Not centrally controlled [100]	It could yet be an option if exisiting systems provide little security
2.8	☐ Access-restricted ☐ Not access-restricted	Permissioned or public blockchain
2.9	☐ immutable (especially already stored data) [100] ☐ mutable [50]	Key principle of immutability
	USE CASE PROCESS: "Is an existing (or fictive – just imagine it) use case process…"	
3.1	☐ not digital [20] ☐ 50:50 [50] ☐ all-digital [100]	All-digital processes are easier to transform to a blockchain But if the current process is already lean there is no reason to change
3.2	☐ lean and affordable [30] ☐ ineffective and expensive [100]	Not digital and 50:50 requires tokenization
3.3	☐ fully integrated into a bigger environment [10] ☐ Partly integrated [40] ☐ Not integrated, full E2E [100]	If the process is fully integrated in the landscape it is hard to convert it to blockchain, the whole landscape therefore should be transferred which means also that the process should be challenged at first
3.4	☐ Matured and reliable [10] ☐ Less than 1yo [50] ☐ Not yet developped [100]	If the process is matured and well-established there is no direct need to change it. However, questions may be asked how blockchain could make it more efficient
3.5	☐ Single transaction based ☐ Multi staged transaction	The use of blockchain 1.0 (like cryptocurrencies) or blockchain 2.0 (like smart contracts)
3.6	☐ Fully automated [100] ☐ Interactions should be monitored and manually triggered [10] ☐ Does not matter [80]	Key principle of Blockchain 2.0
3.7	☐ Not audit-relevant [50] ☐ Audit relevant [100]	One of the key benefits of blockchain is data provenance
3.8	☐ Require a high performance (in milliseconds) [0] ☐ Accepts latency [100]	High performance is yet a goal to be achived by blockchain

		therefore traditional centralized systems are the better option for now
3.9	☐ Requiring inter-operability by using several interfaces [100] ☐ Stand Alone [80]	Blockchain enables several parties to operate on one network making processes more efficient
3.10	☐ Fullfilling regulatory obligations [5] ☐ Not regulated [100]	Blockchain is not yet accepted with central authorities It could yet be an option if exisiting systems provide little security
3.11	☐ Local [10] ☐ Based on a network [100]	Even though there are ways to handle off-chain transactions a fully offline process / use case is not suitable for the application of blockchain
3.12	☐ Used by a lot of ppl [100] ☐ Potentially used by a lot of ppl [100] ☐ Used by only a very limited amount of ppl [80]	Key principle of scalability and security
	Further Questions	
4.1	Should you or all be able to identify the participants in the use case? ☐ Yes ☐ No ☐ Does not matter	Value of trust / zero trust Permissioned or public Blockchain
4.2	Should the use case generate money by processing events? ☐ Yes [100] ☐ No [80]	Transaction fees ergo mining or not -> if no and a public BC is chosen than there might be an issue of finding ppl providing mining power

4.4 Conclusion

Die Auswertung der Ergebnisse des Fragebogens ergibt sich in durch die Zusammenrechnung der jeweiligen Gewichtung / Wertung der einzelnen Fragen. Bei einer vorhandenen Auswahl einer Antwort mit einer Wertung von 0 wird automatisch ein Hinweis eingeblendet, dass der Anwendungsfall möglicherweise kein Kandidat für die Blockchain ist. Diese spezifische Antwort wird in der Bewertung dann nicht weiter berücksichtigt. Dadurch soll es dem Benutzer ermöglicht werden, trotzdem eine Auswertung der restlichen Fragen zu erhalten.

Pro Antwort werden die folgenden Textblöcke angezeigt:

ID	*Text for Answers*
1	Is your use case related to one of these areas / fields?
	Score 100: The area your use case is related to is ideal for the application of Blockchain
	Score 80: The area your use case is related to is good for an application of Blockchain
	Score below 80: The area your use case is related to is probably good for an application of Blockchain (further details needed)
	USE CASE DATA – "Is the data processed within the use case …"
2.1	Confidential: you need a permissioned blockchain Internal: you need a permissioned blockchain Public: you can use a public blockchain
2.2	Static: a blockchain might not be much of an efficiency boost to your use case Dynamic: With dynamic data, you can use the advantage of blockchain
2.3	Physical: In order to use blockchain you need to digitalize your physical asset by tokenization digital only: As blockchain is all digital your use case is ideal for the use of blockchain physical and digital: In order to use blockchain you need to digitalize your physical asset by tokenization
2.4	Has to be deleted at a certain point: If you have to delete your already saved data, blockchain might not be for you should be stored for the whole lifecycle: Immutability of data is one of the key principles of blockchain
2.5	Modified just by yourself: If you are the only one using the data blockchain might be nothing for you modified by multiple users: blockchain offers you a system which can be used by multiple users modified by multiple users with interactions: blockchain can trigger events and keep track of status using smart contracts and therefore be ideal for your use case
2.6	No data provenance required: therefore, you will not use this key principle with the use of blockchain Data provenance is important: blockchain gives you data provenance as built-in function
2.7	Controlled by a central authority: Blockchain is not yet accepted with central authorities so this could be a showstopper Not centrally controlled: Since blockchain is not yet accepted with central authorities this is currently a good condition to implement the technology.
2.8	Access-restricted: you need to use a permissioned blockchain for your use case Not access-restricted: you can use a public blockchain for your use case
2.9	immutable (especially already stored data): you are using one of the key principles of blockchain
	mutable: data within a blockchain can be mutable by creating a new set of a record. If previous data has to be deleted permanently blockchain is not an option for you
	USE CASE PROCESS: "Is an existing (or fictive – just imagine it) use case process…"
3.1	not digital: you have to find ways to digitalize your process (e.g. by tokenization) in order to use blockchain

	50:50: you have to find ways to digitalize the whole process (e.g. by tokenization) in order to use blockchain to the fullest potential
	all-digital: perfect precondition to use blockchain
3.2	lean and affordable: congratulations! But blockchain can still give you a boost in efficiency. But therefore, further details are needed
	ineffective and expensive: not a bad thing to happen when there is blockchain you can use to improve your process
3.3	fully integrated into a bigger environment: the higher a process is integrated into a bigger environment the harder it is to just only convert this part into a blockchain. You need to check first whether there is an option to redesign all involved parts of the E2E process
	Partly integrated: it is difficult to say that blockchain would work for your use case. If the interfaces to other processes are flexible there is a chance to convert your process with blockchain
	Not integrated, full E2E: Perfect precondition. Be aware that by applying the blockchain technology to your process you might want to challenge the process itself to make it more efficient
3.4	Matured and reliable: you might want to challenge such a process and then check again whether blockchain is an option for you
	Less than 1yo: new processes always have a good chance to be even more efficient. Block-chain could be an option for you.
	Not yet developed: perfect precondition. Blockchain is a good option for you. Please revise the benefits of the application in order to design an efficient process from the beginning
3.5	Single transaction based: ideal for blockchain and easy to implement
	Multi staged transaction: ideal for blockchain. Please be sure that you know everything about correct events and activities before designing your blockchain application.
3.6	Fully automated: You are making use of a key principle of blockchain.
	Interactions should be monitored and manually triggered: there is little blockchain can do with manually triggered events. Please check whether such a manual process is really re-quired.
	Does not matter: Cool, it would be a key principle for blockchain though. Maybe you have tasks which would make the process more efficient once automated.
3.7	Not audit-relevant: A key benefit of blockchain is the ability to track mutations from the start. Not using it is not a showstopper
	Audit relevant: Great, the blockchain is ideal for your use case.
3.8	Require a high performance (in milliseconds): Sorry, but blockchain is not that fast at the time being. There are better and especially faster technical alternatives
	Accepts latency: When we are talking latency, we are talking about seconds. If you can live with that blockchain can add many other benefits to your use case
3.9	Requiring interoperability by using several interfaces: blockchain might not work with other solutions but vice versa. So, at the point implementing blockchain you might want to involve the other parties to join you in your efforts.

	Stand Alone: Blockchain might not offer you enough benefits in such a constellation where a switch to it would be beneficial enough for you.
3.10	Fullfilling regulatory obligations: Blockchain is not yet accepted with central authorities so this could be a showstopper
	Not regulated: Since blockchain is not yet accepted with central authorities this is currently a good condition to implement the technologie.
3.11	Local: blockchain works online. Even though there are ways to handle off-chain transactions with a blockchain, the current development still needs some time to come up with a viable solution for your use case.
	Based on a network: Blockchain is a great way to create an efficient use case.
3.12	Used by a lot of ppl: you are getting a secure and scalable option with blockchain by using the key principles of it.
	Potentially used by a lot of ppl: you are getting a secure and scalable option with blockchain by using the key principles of it.
	Used by only a very limited amount of ppl: with blockchain you can scale your network later if required but may want to go for a permissioned blockchain as less actors mean less security within a public blockchain.
	Further Questions
4.1	Should you or all be able to identify the participants in the use case?
	Yes: You can use a permissioned blockchain
	No: you can use a public blockchain
	Does not matter: you can use either a permissioned or a public blockchain
4.2	Should the use case generate money by processing events?
	In case of a public blockchain every transaction should be connected with a transaction fee for the one who administers the blockchain (Concept of Mining). Within a permissioned blockchain mining is not required and the people are motivated by other means to support your blockchain.

Neben dieser detaillierten Auswertung schlägt die Punktzahl auch eine Einsatzform der Blockchain vor.

Gesamtwertung: **unter 400**	Gesamtwertung: **400 - 1599**	Gesamtwertung: **1'600 - 2’000**
Blockchain as Optimizer but with further analysis	Blockchain as Optimizer	Blockchain as Solution

Zusätzlich werden statisch die Daten aus den Benchmarks als Motivation angezeigt.

4.5 Evaluation

Die erste Evaluation erfolgte mit dem Interviewpartner sowie Unternehmensberater von einer der Top 4 Beratungsunternehmen. Hierbei wurde die Methode inhaltlich untersucht und mit einem Prototyp von M.L. abgeglichen. Aus Vertraulichkeitsgründen dürfen hier keine Ausführungen hierzu gemacht werden. Jedoch wurde die Struktur der Fragen überarbeitet und die Bewertungen angepasst.

Aus Sicht von M.L. vermittelt die Methode eine gute initiale Standortbestimmung. Aufgrund von den meist allgemein gehaltenen Fragen kann der Anwendungsfall nicht sehr akkurat erfasst werden, weshalb er dem Autor geraten hat, den Fokus auf die Parameter der Blockchain zu legen.

In einer zweiten Iteration wurde die Methode mit aktuell auf Blockchain umgesetzten Anwendungsfällen geprüft, was erfolgreich abgeschlossen werden konnte.

Die dritte Iteration mit einem weiteren Gespräch, diesmal der Experte Jags Rao von der Swiss Re ist noch ausstehend und konnte aus Terminkonflikten bei Jags Rao (er ist Speaker an der Consensus 2017 in New York) nicht innerhalb der Abgabefrist dieser Arbeit durchgeführt werden. Dies wird jedoch trotzdem noch stattfinden, um neuen Input zu erhalten.

blockchain use.case navigator | prototyp

Während der Arbeit wurde ein technischer Prototyp der erarbeiteten Methode unter Nutzung von PHP und MySQL sowie passenderweise einer SHA256-bit Passwortverschlüsselung programmiert. Dieser ist verfügbar auf:

http://blockchain.saiten.click/
Login: ma99
Passwort: blockchain!

(Stand: 26. Mai 2017)

5 Diskussion und Ausblick

Das Schlusswort beschäftigt sich mit den während der Arbeit gewonnenen Erkenntnissen und formuliert ein Fazit basierend auf diesen Erkenntnissen. Der Ausblick soll aufzeigen, wie die Technologie und insbesondere die betroffenen Wirtschaftssektoren sich weiterentwickelt könnten und beleuchtet auch Möglichkeiten, wie die erarbeitete Methode zur Identifikation von Anwendungsfällen für die Blockchain Technologie weiterentwickelt werden kann, um die Anwendbarkeit weiter zu erhöhen.

5.1 Allgemeine Erkenntnisse

Die Verwendung der Blockchain Technologie beschränkt sich bei weitem nicht nur auf den bankfachlichen Bereich. So beschäftigt sich die aktuelle Literatur bereits vermehrt mit den potenziellen Anwendungsfällen der Blockchain. Dabei sind die Grenzen dieser disruptiven Technologie schier unendlich, solange man sich an die Value Driver, den mehrwertgenerierenden Attributen der Blockchain orientiert und entlangbewegt. Basierend auf der aktuellen Entwicklung konnten diese Attribute in der Methode zur Identifikation von Anwendungsfällen, welche sich für den Einsatz der Blockchain Technologie eignen, zusammengefasst werden. Es hat sich gezeigt, dass der aktuelle Fokus auf Kryptowährungen bei weitem nur einer von vielen möglichen Anwendungsfällen darstellt.

Neben dem Potenzial der Technologie wurden jedoch auch zentrale Problemfelder des derzeitigen Entwicklungsstands der Blockchain Technologie aufgedeckt. Darunter zählt das technisch funktionierenden aber ressourcen-raubenden Konzept der angewendeten Konsensmechanismen und deren noch nicht ausgereiften Alternativen wie auch die implizite Zentralisierung des eigentlich dezentralen Netzwerks. Auch die jüngsten Exploits von positiv wahrgenommenen Treibern der Technologie – zu nennen ist der Exploit von Ethereum und der daraus entstandene Hard Fork– haben bei Beobachtern wie auch Experten gewisse Zweifel an der Glaubwürdigkeit der Blockchain ausgelöst. Denn die Prinzipien die hinter der Blockchain stecken - Dezentralisierung, Transparenz, Offenheit, Sicherheit, und vor allem das Konzept des Zero-Trust Protokolls - wurden durch jüngste Entwicklungen stark gebrochen. Dies setzt sich fort in den Bestrebungen von privatwirtschaftlichen aber auch öffentlichen Institutionen, welche primär darum bedacht sind, ihre Stellung im Markt durch die Blockchain zu verstärken, wobei bewusst gewisse Prinzipien wie Transparenz und Offenheit ausgeschlossen werden. So setzten geschäftliche Anwendungen der Blockchain in jedem Fall auf geschlossene Systeme. Zudem sind öffentliche Institutionen bemüht, eine Überwachung von Blockchain-getriebenen Transaktionen zu ermöglichen. Dies eines von vielen Paradoxa, welches zeigt, dass die grundlegenden Prinzipien der Tech-

nologie untergraben werden. Auch wenn Experten von einer vollendeten Kombination der verschiedenen technologischen Komponenten in Form der Blockchain sprechen, so wurde festgestellt, dass die Standpunkte jeweils auch stark durch einen technischen und / oder ökonomischen Hintergrund geprägt sind. Während gewisse Probleme auf noch nicht ganz ausgereifte Konzepte der Blockchain zurückzuführen sind, eröffnet sich ein erweiterter interdisziplinärer Diskurs, welcher sich neben der technologischen und ökonomischen Disziplin nun auch um die sozialwissenschaftliche aber auch ökologische Stellung der Blockchain befassen muss.

Die Beispiele der Problemfelder lässt zudem die Frage zu, ob die Blockchain in ihrer Kombination von technologischen Bestandteilen wie auch all ihre Prinzipien für eine Monetarisierung im wirtschaftlichen Sinne als Ganzes übernommen werden muss oder kann. Auch wenn die grundlegenden Prinzipien für den einzelnen Kunden im Markt sehr viele Vorteile bietet, so ist ein Erhalt aller Prinzipien für ein profitorientiertes Unternehmen nur schwer umzusetzen. Kurzfristig vielversprechender ist die Betrachtung einzelner technologischer Konzepte / Komponenten der Blockchain, welche unter Nutzung bestehender Architekturen und Technologien bereits zu einer Optimierung von Prozessen in einem Unternehmen führen können. Dieser Ansatz wiederspiegelt auch der Konsens der Skeptiker.

Die Anwendung der Blockchain führt bei etablierten Unternehmen zwangsläufig zu einer Hinterfragung der gesamten Prozesslandschaft. Auch wenn dies isoliert betrachtet eine positiv zu wertende, implizite Eigenschaft der Technologie darstellt, so birgt dieser Umstand eine ebenso hohe Hemmschwelle für Unternehmen zur Anwendung der Technologie. Die Transformation eines einzelnen Geschäftsprozesses kann enorme Kosten verursachen und bestimmte Unternehmen könnten auch zur Erkenntnis gezwungen werden, dass ihr Geschäftsmodell durch den Einsatz von Blockchain keine Legitimation am Markt hat und somit von dieser Technologie substituiert wird.

Die aktuellen und potenziellen Anwendungsfelder der Blockchain konnten kompakt zusammengefasst werden. Es zeigt sich, dass die Blockchain alleine als Optimierer von bestehenden Anwendungsfällen genutzt werden kann, das wahre Potenzial jedoch erst in der Kombination mit weiteren technologischen Innovationen wie IoT oder künstlicher Intelligenz ausgeschöpft werden kann und innovative Anwendungsfälle erarbeitet werden können.

Die Implikationen der Blockchain haben ein weites Ausmass. Sofern die Technologie aktiv eingesetzt wird, ergeben sich neue Unternehmen, welche effizienter und somit kostengünstiger agieren können. Zudem trägt die Blockchain zu einer beschleunigten Globalisierung des Marktes bei. Stehen und fallen wird diese Entwicklung durch die Adaption der Regulatoren. Denn diese werden als grösster potenzieller Blocker einer Weiterentwicklung der Blockchain Technologie gesehen. Zwar ist die Problematik bei den meisten Regulatoren bereits adressiert, doch Reformen lassen zum heutigen Zeitpunkt noch

auf sich warten. Genauso verhaltet es sich mit globalen Standards, die eine globale Blockchain ermöglichen. Zurzeit entwickeln verschiedene Branchen eigene Produkte, womit das Potenzial der Blockchain limitiert wird.

Zuletzt wurde eine Methode erarbeitet, die Anwendungsfälle auf ihre Eignung für die Blockchain Technologie ermöglicht. Hierbei ist sie jedoch insofern limitiert, dass sie stark abhängig ist vom Input. Will heissen, die Innovationskraft liegt alleine in der Wahl des Anwendungsfalls. Zentral sind in diesem Modell die heutigen Grundprinzipien der Blockchain Technologie und die Gewichtung der einzelnen Eigenschaften. Die Methode bringt primär eine Effizienz- und Effektivitätssteigerung bei der Identifikation von Anwendungsfällen für die Blockchain, doch kann selbst keine innovativen Anwendungsfälle vorschlagen.

5.2 Fazit

Die Entwicklung der Blockchain setzt sich in rasantem Tempo fort. Fast jeden Tag werden neue Anwendungsfälle mit Einsatz der Blockchain Technologie publiziert. Dabei konnte bisher jedoch noch kein wirklich innovativer, disruptiver Anwendungsfall vorgestellt werden, welcher eine extreme Aufmerksamkeit ausserhalb der Reihen der Experten auslösen konnte. Es ist denn auch Bitcoin, die die globale Aufmerksamkeit auf sich zieht. Die negativen Schlagzeilen dazu vermehren sich täglich, insbesondere durch die Schadsoftware. Durch Spekulationen ist auch der Kurs der Kryptowährung explodiert und zieht weitere Aufmerksamkeit auf diesen einen Anwendungsfall der Blockchain Technologie.

Insgesamt lässt sich sagen, dass wir uns erst am Anfang der breit angelegten Entwicklung von Blockchain befinden. Glasesr und Bezzenberger (2016) bemerken, dass etablierte Institutionen auch in der Finanzbranche erst damit beginnen, das Potenzial der Blockchain für sich nutzbar zu machen. Noch sind die schlagkräftigen Innovationen (beispielsweise die Verdrängung von Intermediären) nicht umgesetzt und Fachexperten wie auch die Literatur sind sich nicht einig, ob dies in absehbarer Zeit passieren wird. Sicher ist jedoch, dass Gartner (2016) mit der Einordnung der Technologie im HypeCycle richtig liegt. Denn die Fachexperten gehen davon aus, dass sich die Technologie erst in den nächsten fünf bis zehn Jahren durchsetzen wird. Die in der Arbeit gefassten Herausforderungen sind heute entsprechend noch gross und müssen zunächst noch gelöst werden, bevor es zu einer massenhaften Anwendung kommt. Positiv zu erachten ist das grosse Interesse, welches die Blockchain geniesst. Dieser Umstand wird dazu führen, dass die Herausforderungen und heutigen Probleme der Blockchain schneller gelöst werden.

Wie im vorhergehenden Kapitel erwähnt, konnte eine Methode erarbeitet werden, welche den Prozess der Identifikation von Anwendungsfällen für die Blockchain Technologie vereinfacht, indem die

heutigen Eigenschaften der Blockchain kompakt zusammengefasst wurden und in Form eines gewichteten Fragekatalogs umgesetzt wurden. Hierbei handelt es sich um ein unterstützendes Instrument beim Prozess der Entwicklung von Anwendungsfällen mit Blockchain. Der innovative Aspekt dieses Prozesses verbleibt beim Benutzer, der durch die Auswahl des Anwendungsfalls demnach ein gewisses Mass an Kreativität bedarf. Mit der Weiterentwicklung der Blockchain Technologie wird es jedoch immer mehr Anwendungsszenarien geben, welche durch die Blockchain Technologie umgesetzt werden können.

5.3 Ausblick

Der Ausblick bezieht sich auf zwei Themen. Zum einen wird eine weitere Entwicklung der Blockchain Technologie an sich skizziert. Daneben soll jedoch auch die Weiterentwicklung der in dieser Arbeit entwickelten Methode zur Identifikation von Anwendungsfällen für die Blockchain Technologie definiert werden.

5.3.1 Die Entwicklung der Blockchain Technologie

Mit dem Technology Adoption Life Cycle hat Moore (2014) erkannt, dass innovative und disruptive Technologien in ihrer Entwicklung jeweils zu einem Punkt kommen, von welchem sie den Sprung von den Visionären, «Early Adopters», zu den Pragmatikern, «Early Majority», schaffen müssen. Dieser Sprung wird von Moore als «The Chasm» bezeichnet (Moore, 2014) wie aus nachfolgender Abbildung ersichtlich wird.

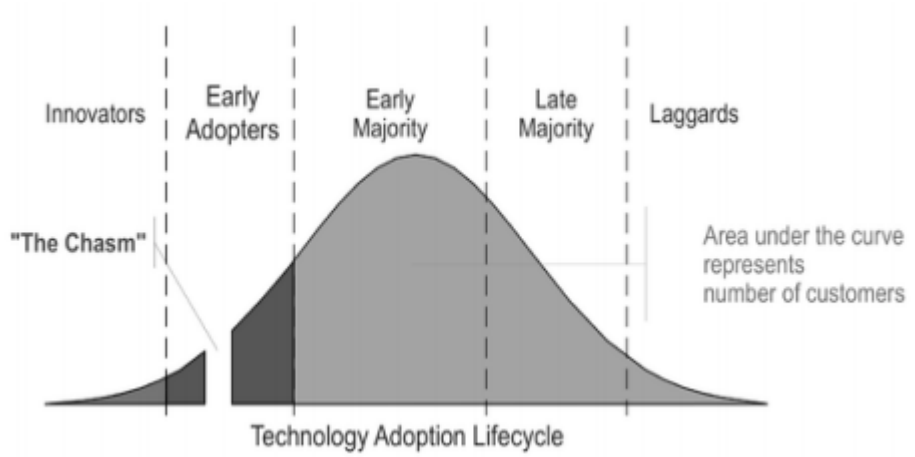


Abbildung 28: Moore's Technology Adoption Life Cycle (Moore, 2014)

Die Blockchain Technologie nähert sich nach Ansicht des Autors dieser Schlucht. Es gibt zwar zahlreiche Unternehmen, welche sich mit der Weiterentwicklung der Technologie beschäftigen, doch aufgrund

des Ausbleibens von massentauglichen Anwendungsfällen lassen sich weitere Forschungsressourcen nicht sehr viel länger legitimieren. Ausschlaggebend ist entsprechend ein sich durchsetzender Anwendungsfall, welcher es ermöglicht, diesen «Chasm» zu überwinden. Dies bedingt, dass die in dieser Arbeit erwähnten Problemstellungen sowie Herausforderungen an die Blockchain demnächst gelöst werden. Der Autor sieht es aber im Hinblick auf die derzeitige Entwicklung als sehr wahrscheinlich an, dass der durchschlagende Anwendungsfall in naher Zukunft veröffentlicht wird und somit weitere Massen an Anspruchsgruppen anziehen kann.

Die zukünftige Entwicklung der Blockchain wird sich nach Meinung des Autors neben den heutigen Problemen und Herausforderungen mit der Kombination weiterer Technologien beschäftigen. Hierzu sind die vielversprechendsten Kandidaten IoT und die maschinenbasierte künstliche Intelligenz.

5.3.2 Methode zur Identifikation von Anwendungsfällen für die Blockchain Technologie

Die in dieser Arbeit entwickelte Methode zur Identifikation von Anwendungsfällen für die Blockchain Technologie ermöglicht dem Anwender die Einordung des als Input betrachteten Anwendungsfalles – genauer, Prozesses - im Rahmen der ermittelten Kriterien von Blockchain. Nachdem das Inputobjekt (ein Anwendungsfall) parametrisiert wurde, findet ein Mapping dieser Parameter mit den Attributen der Blockchain Technologie statt. Der Prozess der Parametrisierung des Inputobjekts sowie die Attribute der Blockchain sind gebunden an eine strukturierte, jedoch statische Datenquelle.

Folgend werden zwei aus Sicht des Autors zukünftig wichtige Entwicklungsschritte in Bezug auf die erarbeitete Methode erläutert.

In einer Weiterentwicklung müssen, insbesondere angesichts der stetig voranschreitenden Entwicklung der Blockchain Technologie, die Attribute laufend um diese Entwicklungsstadien ergänzt werden. Der Autor schlägt dabei vor, dass in einem weiteren Schritt der zunächst manuelle Prozess der Ermittlung von Blockchain-spezifischen Attribute durch einen technischen Algorithmus ersetzt wird, welcher aus der Disziplin der maschinenbasierten Informationsgewinnung entstammt. Mit Instrumenten und Tools wie IBM Watson lassen sich die dynamischen Entwicklungsstadien der Blockchain Technologie zu jeder Zeit fassen und ermöglichen ein akkurateres und allzeit korrektes Resultat der Methode. Im Rahmen der Bearbeitung dieser Masterarbeit wurde bereits ein Versuch mit den semantischen Tools von IBM gestartet, konnte jedoch aus zeitlichen Gründen nicht vollendet werden. Das Potenzial einer solchen Weiterentwicklung ist jedoch erwiesen.

Die Methode konnte in mehreren Versuchen einen validen Output liefern. Die zukünftige Weiterentwicklung betrifft jedoch die Detailtiefe der gesamten Methode. Die Empfehlungen sind in der jetzigen Ausarbeitung noch sehr generisch und zielen primär darauf ab, einen möglichst grossen Anwenderkreis auf Kosten von konkreteren Aussagen zu bedienen. Die einzelnen Fragen im Identifikationsprozess sind ebenso weit gefasst und müssen in einem nächsten Schritt an Detailtiefe gewinnen. Dies kann erreicht werden durch den Einbezug von weiteren Anwendungsfällen, welche eine gänzlich andere Charakteristik aufweisen, als dies in der vorliegenden Arbeit betrachtet wurde. Interessant ist aus der Sicht des Autors eine Verifikation der erarbeiteten Methode mittels einer quantitativen Forschungsmethode. Unter Berücksichtigung einer repräsentativen Stichprobe können so weitere Erkenntnisse zur Verbesserung der Methode gewonnen werden. Durch eine quantitative Analyse von bestehenden und sich in Zukunft etablierten Anwendungsfällen lassen sich ebenfalls weitere Kriterien und Attribute zur Verbesserung der Methode ableiten.

Abschliessend kann aus einer Aggregation der Daten, die unter Nutzung der Methode generiert wurden, eine weitere übergeordnete Analyse durchgeführt werden. Diese kann beispielsweise durch statistische Analyseverfahren wie einer Regressionsanalyse aufzeigen, welche Anwendungsfälle unter sich eine Korrelation aufweisen und gegebenenfalls komplementär oder aber äquivalent zueinander verhalten. Der Autor sieht es dabei als möglich an, dass sich daraus neue oder optimierte Geschäftsmodelle ableiten lassen, sollte die Methode mittels der zuvor genannten zwei wichtigen Schritte weiterentwickelt werden.

6 Kritische Würdigung der Arbeit

Aufgrund der schnelllebigen Entwicklung der Blockchain und des Technologiesektors im Ganzen möchte der Autor selbst eine kritische Würdigung der Arbeit anfügen und geht dabei auf drei essentielle Elemente ein, die der Arbeit zugrunde liegen oder deren Inhalt betreffen.

Die in dieser Masterarbeit erarbeitete Methode zur Identifikation von Anwendungsfällen für die Blockchain basiert auf den derzeitig verfügbaren Informationen aus Literatur und Experteninterviews und soll somit als Momentaufnahme der aktuellen Entwicklung der Blockchain Technologie gesehen werden. Viele Attribute der Methode sind hergeleitet aus dem zu diesem Zeitpunkt vorhersehbaren Potenzial sowie den bestehenden Limitationen der Blockchain und schliessen zukünftige, technische Entwicklungen nicht komplett ein. Wie bereits im Ausblick erwähnt, entwickelt sich die Technologie immer weiter und durch interdisziplinären Entwicklungen lässt sich auch die Blockchain in ihrer Möglichkeit auf weitaus mehr Attribute zusammenfassen, als jene, welche in der erarbeiteten Methode berücksichtigt wurden. Entsprechend muss sich auch die Methode weiterentwickeln, um weiterhin das volle Spektrum der Blockchain Technologie erfassen zu können.

Bei der Auswahl der Literatur wurde darauf geachtet, dass es sich um sehr aktuelle Quellen handelt, welche einen guten Überblick der aktuellen Entwicklung vermitteln, dabei aber trotzdem einen empirischen Hintergrund aufweisen. Da sich der Hype um die Blockchain noch immer auf der Höhe der überzogenen Erwartungen befindet (Gartner Research, 2016), gibt es vor allem bei Online-Quellen einen grossen Spielraum für Falschinformationen oder nicht ganzheitlich belegbare Aussagen. Diese Quellen wurden zur Erreichung einer höheren Aussagekraft sowie einer gesteigerten empirischen Abstützung nur in Ausnahmen für explorative Ausführungen miteinbezogen und entsprechend gekennzeichnet. Der Autor selbst sah sich zum Zeitpunkt der Auswahl nicht immer als Fachexperte zur Thematik, weshalb die Auswahl nicht immer eine vollkommene Plausibilität aufweist und somit auch Fehleinschätzungen nicht gänzlich ausgeschlossen werden können.

Die Selektion der Interviewpartner wird vom Autor daneben als grundlegend für die Verifikation der Methode gewertet. Die einzelnen Experten sind dabei durch ihre eigenen Tätigkeiten in ihrer Wahrnehmung beeinflusst. Die Erfassung des Wissensprofils soll dazu beitragen, dass eine klare Einordnung ihrer Aussagen sowie deren Vergleich ermöglicht wird. Trotz allem ist es nicht ganz auszuschliessen, dass einzelne, wiederspiegelte Meinungen die Resultate der Arbeit übermässig stark beeinflusst haben. Zusätzlich ist der Fokus der Experten bis auf wenige Ausnahmen auf den Schweizer Markt ausgerichtet und kann entsprechend zu einer einseitigen Betrachtung der Thematik führen.

Neben diesem Aspekt möchte der Autor erneut darauf hinweisen, dass die Entwicklung der Blockchain vergleichbar mit allen IT-Technologien stetig weitergetrieben wird und bestimmte Aussagen nur eine kurze Validität haben. Dieser Umstand führt zur abschliessenden Aussage, dass sich neben der Standortbestimmung im ersten Teil der Arbeit verbunden mit den daraus abgeleiteten Problemen und hypothetischen Implikationen auch die Erkenntnisse und Aussagen aus dieser Masterarbeit einer dynamischen Entwicklung unterwerfen wird und nur durch eine Anpassung an die sich ändernden Prämissen ihre Gültigkeit erhalten kann.

7 Literaturverzeichnis

Alexander, R., 2014. *The first Blockchain wedding.* [Online]
Available at: https://bitcoinmagazine.com/articles/first-blockchain-wedding-2-1412544247/
[Zugriff am 10 03 2017].

Allison, I., 2015. *Deloitte is delving into Ethereum, Eris and Ripple.* [Online]
Available at: http://www.ibtimes.co.uk/deloitte-delving-into-ethereum-eris-ripple-1515494
[Zugriff am 09 03 2017].

Alpar, P. et al., 2014. *Anwendungsorientierte Wirtschaftsinformatik.* Wiesbaden: Springer Fachmedien.

Anon., 2017. *Konto.* [Online]
Available at: https://retail.bitcoinsuisse.ch/de/account
[Zugriff am 01 05 2017].

Anon., . *Introducing R3 Corda: A Distributed Ledger Designed for Financial Services.* [Online]
Available at: https://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services
[Zugriff am 30 4 2017].

Antonopoulos, A., 2014. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* Sebastopol: O'Reilly Media.

Bercovici, J., 2014. *Amazon Vs. Book Publishers, By The Numbers.* [Online]
Available at: http://www.forbes.com/sites/jeffbercovici/2014/02/10/amazon-vs-book-publishers-by-the-numbers/
[Zugriff am 20 Oktober 2015].

Bergmann, C., 2015. *Was passiert bei einem Hard Fork?.* [Online]
Available at: https://bitcoinblog.de/2015/06/15/was-passiert-bei-einem-hard-fork/
[Zugriff am 12 03 2017].

Bitcoin Mining, 2015. *How does Mining work?.* [Online]
Available at: https://www.bitcoinmining.com/
[Zugriff am 15 02 2017].

Bitcoin Wiki, 2016. *Block size limit controversy.* [Online]
Available at: https://en.bitcoin.it/wiki/Block_size_limit_controversy
[Zugriff am 11 03 2017].

Bitcoinblockhalf, 2017. *Bitcoin Block Reward Halving Countdown.* [Online]
Available at: http://www.bitcoinblockhalf.com/
[Zugriff am 10 05 2017].

Boneh, D., 2011. Digital Signature Standard. *Encyclopedia of Cryptography and Security,* pp. 347-347.

Bonneau, J. et al., 2016. *Bitcoin and cryptocurrency technologies.* Princeton: Princeton University Press.

Bradley, J. et al., 2015. *How Digital Disruptioin Is Redefining Industries,* New York: Digital Vortex.

Branigin, W., 1998. Delay Caused by Y2K Bug Will Cost Most Medicare Recipients. *The Tech,* 31 08, 118(36), pp. 61-67.

Brooks, R., 2000. AI : the tumultuous history of the search for artificial intelligence. *Trends in Cognitive Sciences,* 4(7), p. 291.

Brown, R. G., 2015. *A simple model for Smart Contracts.* [Online]
Available at: https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/
[Zugriff am 15 04 2017].

Buchmann, J. et al., 2007. Merkle Signatures with Virtually Unlimited Signature Capacity. *Applied Cryptography and Network Security,* pp. 31-45.

Bühler, K. et al., 2015. *Beyond the Hype: Blockchains in Capital Markets,* New York: McKinsey&Company.

Burgwinkel, D., 2016. *Blockchain Technology: Einführung für Business- und IT-Manager.* 1st Hrsg. Berlin: De Gruyter Oldenbourg.

Christidis, K. & Devetsikiotis, M., 2016. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access,* 4(1), pp. 2292-2303.

Ciaian, P., Rajcaniova, M. & Kancs, d., 2016. The economics of BitCoin price formation. *Applied Economics,* 48(19), pp. 1799-1815.

Cofinpro AG, 2016. *Blockchain. Zukunft oder Ende des Bankings?,* Frankfurt am Main: Cofinpro.

Coindesk, 2014. *How Bitcoin Mining Works.* [Online]
Available at: http://www.coindesk.com/information/how-bitcoin-mining-works/
[Zugriff am 12 03 2017].

coindesk, 2017. *A (Short) Guide to Blockchain Consensus Protocols.* [Online]
Available at: http://www.coindesk.com/short-guide-blockchain-consensus-protocols/
[Zugriff am 20 03 2017].

Coindesk, 2017. *Bitcoin Price.* [Online]
Available at: http://www.coindesk.com/price/

Coindesk, 2017. *Isle of Man.* [Online]
Available at: http://www.coindesk.com/?s=isle+of+man
[Zugriff am 11 03 2017].

Condos, J., Sorrel, W. & Donegan, S., 2016. *Blockchain Technology: Opportunities and Risks,* Vermont: Vermont.

consensys, 2015. *About.* [Online]
Available at: https://consensys.net/about/
[Zugriff am 01 05 2017].

Courtneidge, R. & Buelli, F., 2015. *Blockchain and Financial Services - Industry snapshot and possible future developments,* New York: LLP.

Croman, K., Decker, C., Eyal, I. & Gencer, A., 2016. *On Scaling Decentralized Blockchains.* Berlin, Springer, pp. 106-125.

Daian, P., 2016. *Analysis of the DAO exploit.* [Online]
Available at: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/
[Zugriff am 02 05 2017].

datatrans, 2017. *Übersicht.* [Online]
Available at: https://www.datatrans.ch/de/unternehmen/uebersicht
[Zugriff am 02 04 2017].

DeMartino, I., 2016. *The Bitcoin Guidebook.* 1st Hrsg. New York: Skyhorse.

DNA.Bits, 2015. *About DNA.Bits.* [Online]
Available at: http://socialm1.wixsite.com/dnabits/about
[Zugriff am 20 03 2017].

Douceur, J. R., 2002. *The Sybil Attack,* Redmond: Microsoft Research.

Ethereum Homestead, 2016. *Developer Tools.* [Online]
Available at: http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html?highlight=language
[Zugriff am 10 05 2017].

Ethereum Homestead, 2017. *Glossary.* [Online]
Available at: http://ethdocs.org/en/latest/glossary.html
[Zugriff am 08 03 2017].

Euro Banking Association, 2015. *Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios An exploration for transaction banking and payments professionals,* Brüssel: EBA Working Group.

FINMA, 2015. *FINMA veröffentlicht totalrevidierte Geldwäschereiverordnung-FINMA.* [Online]
Available at: https://www.finma.ch/de/news/2015/06/mm-gwv-finma-20150623/
[Zugriff am 29 12 2016].

Flückiger, J., 2017. *Den Wandel nicht verschlafen.* [Online]
Available at: https://www.nzz.ch/meinung/digitalisierung-den-wandel-nicht-verschlafen-ld.1292328
[Zugriff am 15 05 2017].

followmyvote, 2016. *Online Voting Platform FAQ's.* [Online]
Available at: https://followmyvote.com/online-voting-platform-faqs/
[Zugriff am 20 05 2017].

Förster, M., 2017. *Hyperledger Fabric: IBM startet seine Blockchain as a Service.* [Online]
Available at: https://www.heise.de/newsticker/meldung/Hyperledger-Fabric-IBM-startet-seine-Blockchain-as-a-Service-3660165.html
[Zugriff am 29 03 2017].

Forte, P., Romano, D. & Schmid, G., 2015. *Beyond Bitcoin - Part 1: A critical look at blockchain-based systems,* New York: International Association for Cryptologic Research .

Froschauer, U. & Lueger, M., 2003. *Das qualitative Interview - Zur Praxis interpretativer Analyse sozialer Systeme.* 1st Hrsg. Wien: facultas.

Gartner Research, 2016. *Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage.* [Online]
Available at: http://www.gartner.com/newsroom/id/3412017
[Zugriff am 12 02 2017].

github, 2016. *yep/eth-tweet.* [Online]
Available at: https://github.com/yep/eth-tweet
[Zugriff am 21 05 2017].

Goldin, M., 2017. *Ethereum: Bitcoin Plus Everything.* [Online]
Available at: https://medium.com/@ConsenSys/ethereum-bitcoin-plus-everything-a506dc780106
[Zugriff am 02 05 2017].

Google Trends, 2017. *Suchbegriffe: Blockchain, Bitcoin, Kryptowährung.* [Online]
Available at: https://trends.google.com/trends/explore?q=blockchain,bitcoin,%2Fm%2F0vpj4_b
[Zugriff am 17 05 2017].

Gottlieb Duttweiler Institute, 2017. *Mehr als Bitcoin: Warum Blockchain alle betrifft.* [Online]
Available at: http://www.gdi.ch/de/Think-Tank/Trend-News/Mehr-als-Bitcoin-Warum-Blockchain-alle-betrifft
[Zugriff am 01 03 2017].

Gottlieb Duttweiler Institute, 2017. *Think Tank Studien: Karin Frick.* [Online]
Available at: https://www.gdi.ch/de/Think-Tank/Studien/Karin-Frick
[Zugriff am 01 05 2017].

Hevner, A. & Chatterjee, S., 2010. *Design Research in Information Systems.* 22 Hrsg. New York: Springer Science+Business Media.

Hevner, A. R., March, S. T., Park, J. & Ram, S., 2004. Design science in information system research. *MIS Quarterly*, pp. 75-105.

Hilbert, M. & López, P., 2011. The World's Technological Capacity to Store, Communicate, and Compute Information. *Science Magazine*, 1 April, 332(6025), pp. 60-65.

Hüfner, D., 2016. *Arcade City: Dieses wagemutige Startup liefert die Blockchain-basierte Antwort auf Uber.* [Online]
Available at: http://t3n.de/news/arcade-city-uber-673466/
[Zugriff am 23 02 2017].

IBM Institute for Business Value, 2017. *Trust me: Digital identity,* New York: IBM Institute for Business Value.

IBM Research, 2017. *IBM Blockchain.* [Online]
Available at: https://www.ibm.com/blockchain/infographic/finance.html
[Zugriff am 10 02 2017].

IBM, 2015. *IBM Adept.* [Online]
Available at: https://de.slideshare.net/_hd/ibm-adept
[Zugriff am 25 03 2017].

Juels, A., Kosba, A. & Shi, E., 2015. *The Ring of Gyges: Using Smart Contracts for Crime,* New York: Cornell University.

Kaltofen, T., 2016. *Blockchain im Einsatz.* [Online]
Available at: https://www.computerwoche.de/a/blockchain-im-einsatz,3316539
[Zugriff am 13 02 2017].

Kannenberg, A., 2014. *Bitcoins für die Massen: Zahlungsdienst Circle öffnet seine Pforten.* [Online]
Available at: https://www.heise.de/newsticker/meldung/Bitcoins-fuer-die-Massen-Zahlungsdienst-Circle-oeffnet-seine-Pforten-2408539.html
[Zugriff am 21 03 2017].

Keller Informatik AG, 2016. *Entwicklung von Lösungskonzepten.* [Online]
Available at: http://www.kellerinfo.ch/site/dienstleistung/konzept/?oid=1877&lang=de
[Zugriff am 16 November 2016].

Kohlmann, F., 2015. *Digitalisierung im Banking – Trends & Innovationen.* [Online]
Available at: http://www.saleslex.ch/public/portfolio/Digitalisierung%20im%20Banking.pdf
[Zugriff am 29 Oktober 2015].

Kôlvart, M., Poola, M. & Rull, A., 2016. Smart Contracts. In: T. Kerikmäe & A. Rull, Hrsg. *The Future of Law and eTechnologies.* Basel: Springer International Publishing, pp. 133-147.

KYC-Chain, 2017. *The KYC-Chain.* [Online]
Available at: https://kyc-chain.com/
[Zugriff am 01 05 2017].

Manyika, J. et al., 2015. *The Internet of Things: Mapping the value beyond the hype,* Atlanta: McKinsey.

Matusiewicz, K. et al., 2016. *Analysis of simplified variants of SHA-256,* Graz: Graz University of Technology.

McConaghy, T., 2017. *Blockchains for Artificial Intelligence.* [Online]
Available at: https://bravenewcoin.com/news/blockchains-for-artificial-intelligence/
[Zugriff am 20 04 2017].

McLean, J., 2016. *Banking on Blockchain: Charting the Progress of Distributed Ledger Technology in Financial Services,* New York: IBM.

Meier, M., 2017. *Kryptowährungen zur Lösung des Geldproblems.* [Online]
Available at: http://blog.tagesanzeiger.ch/nevermindthemarkets/index.php/41842/loesen-kryptowaehrungen-das-geldproblem/
[Zugriff am 12 05 2017].

Menne, A., 1957. Implikation und Syllogistik. *Zeitschrift für philosophische Forschung,* 11(1), pp. 375-386.

Monetas, 2016. *About.* [Online]
Available at: https://monetas.net/about/
[Zugriff am 03 05 2017].

Moore, G. A., 2014. *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers.* 3rd Hrsg. New York: Harper Collins.

Morabito, V., 2017. *Business Innovation Through Blockchain.* Milan: Springer.

Mougayar, W., 2016. *The Business Blockchain: promise, practice and application of the next Internet technology.* 1st Hrsg. Hoboken: Wiley.

Müller, C. & Hasic, D., 2016. *Blockchain: Technology and Applications,* Salzburg: University of Salzburg.

Myers, K., 2015. *W3C Starts Web Payments Standards Work to Streamline the Online "Check-out" Process.* [Online]
Available at: https://www.w3.org/2015/09/webpaymentswg.html.en
[Zugriff am 16 03 2017].

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System,* s.l.: bitcoin.org.

Nakamura, Y. & Chen, L. Y., 2017. *Bitcoin Miners Signal Revolt Amid Sluggish Blockchain.* [Online]
Available at: https://www.bloomberg.com/news/articles/2017-03-13/bitcoin-miners-signal-revolt-in-push-to-fix-sluggish-blockchain
[Zugriff am 20 03 2017].

Napkin Finance, 2016. *Blockchain - Break the Bank.* [Online]
Available at: https://napkinfinance.com/napkin/bitcoin-blockchain/
[Zugriff am 12 03 2017].

National Institute of Standards and Technology, 2001. Announcing the Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication,* 26 11.pp. 13-20.

Needham, R. & Schroeder, M., 1978. Using encryption for authentication in large networks of computers. *Communications of the ACM,* 12, 21(12), pp. 993-999.

Nestler, F., 2017. *Bitcoin erstmals teurer als Gold.* [Online]
Available at: http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-bitcoin-ist-wertvoller-als-gold-14907983.html
[Zugriff am 15 04 2017].

NZZ, 2014. *Zürcher Bitcoin-Automat wieder in Betrieb.* [Online]
Available at: https://www.nzz.ch/digital/bitcoin-suisse-ag-darf-wieder-zuercher-bitcoin-automaten-betreiben-1.18353938
[Zugriff am 01 05 2017].

Oram, A., 2011. *Harnessing the power of disuptive technologies.* 2nd Hrsg. Sebastopol: O'Reilly.

Paar, C. & Pelzl, J., 2009. *Understanding Cryptography - A Textbook for Students and Practitioners.* Heidelberg: Springer.

Palmer, D., 2016. *7 Cool Decentralized Apps Being Built on Ethereum.* [Online]
Available at: http://www.coindesk.com/7-cool-decentralized-apps-built-ethereum/
[Zugriff am 21 05 2017].

Petersen, M., 2015. *Xapo-Debit-Card: Mit Bitcoin in fast jedem Laden zahlen – diese Karte macht es möglich.* [Online]
Available at: http://t3n.de/news/xapo-debit-card-bitcoin-fast-636081/
[Zugriff am 02 05 2017].

Peters, G. W. & Panayi, E., 2015. *Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money,* London: SSRN.

Pfeffers, K., Tuunanen, T., Rothenberger, M. & Chatterjee, S., 2008. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems,* 24(3), pp. 45-78.

Porter, M. E. & Heppelmann, J., 205. *Device democracy - Saving the future of the Internet of Things,* New York: IBM.

Prisco, G., 2015. *Enigma, MIT Media Lab's Blockchain-based Encrypted Data Marketplace, to Launch Beta.* [Online]
Available at: https://bitcoinmagazine.com/articles/enigma-mit-media-lab-s-blockchain-based-encrypted-data-marketplace-to-launch-beta-1450810499/
[Zugriff am 23 03 2017].

PwC, 2016. *Blurred lines: How FinTech is shaping Financial Services,* New York: PwC Research.

PwC, 2016. *Demografie und Digitalisierung - von Menschen und Branchen.* [Online]
Available at: https://www.pwc.ch/de/publikationen/online-studien/digitalisierung-wo-stehen-schweizer-kmu/demografie.html
[Zugriff am 20 04 2017].

Roy, J., 2013. *Everything You Need to Know About Silk Road, the Online Black Market Raided by the FBI.* [Online]
Available at: http://nation.time.com/2013/10/04/a-simple-guide-to-silk-road-the-online-black-market-raided-by-the-fbi/
[Zugriff am 12 03 2017].

Safi, M., 2016. *Australian Craig Wright claims he is bitcoin founder Satoshi Nakamoto.* [Online]
Available at: https://www.theguardian.com/technology/2016/may/02/craig-wright-bitcoin-founder-satoshi-nakamoto-claim
[Zugriff am 03 03 2017].

Santander InnoVentures, 2015. *The Fintech 2.0 Paper: rebooting financial services,* Jersey: Santander InnoVentures.

Saunders, M., Lewis, P. & Thornhill, A., 2012. *Research Methods for Business Students.* Essex: Pearson.

Setl, 2017. *Real-time Blockchain Settlement.* [Online]
Available at: https://www.setl.io/opencsd/
[Zugriff am 01 05 2017].

Spagnuolo, M., Maggi, F. & Zanero, S., 2014. BitIodine: Extracting Intelligence from the Bitcoin Network. *International Conference on Financial Cryptography and Data Security,* 8437(12), pp. 457-468.

Specht, G., Beckmann, C. & Amelingmeyer, J., 2002. *F&E-Management – Kompetenz im Innovationsmanagement.* 4. Auflage Hrsg. Stuttgart: Schäffer-Poeschel Verlag.

Stanford University, 2015. *About Folding@Home.* [Online]
Available at: http://folding.stanford.edu/about/
[Zugriff am 02 05 2017].

Steinmetz, R. & Wehrle, K., 2005. What Is This “Peer-to-Peer” About?. In: *Peer-to-Peer Systems and Applications.* Berlin: Springer Berlin Heidelberg, pp. 9-16.

Swan, M., 2015. *Blockchain: Blueprint for a New Economy.* 1st Hrsg. Sebastopol: O'Reilly.

Swanson, T., 2015. *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems,* Sidney: R3cev.

Swanson, T., 2015. *Watermarked tokens and pseudonymity on public blockchains,* Sidney: R3cev.

Szabo, N., 1997. Formalizing and Securing Relationships on Public Networks. *Internet economics and Security,* 2(9), pp. 5-22.

Tanenbaum, A. S. & Van Steen, M., 2007. *Distributed Systems: Principles and Paradigms.* 2nd Hrsg. New Jersey: Pearson.

Tapscott, D. & Tapscott, A., 2016. *Blockchain Revolution.* New York: Penguin Random House LLC.

Taylor, S., 2015. *Blockchain: understanding the potential,* London: Barclays.

The Hindu, 2016. *Microsoft unveils Azure Blockchain as Service.* [Online]
Available at: http://www.thehindu.com/sci-tech/technology/Microsoft-unveils-Azure-Blockchain-as-Service/article16785197.ece#
[Zugriff am 29 04 2017].

Theis, D., 2015. *Rolle von Bitcoin gegenüber etablierten Währungen und Online Bezahlsystemen,* Köln: TH Köln.

Theymos, 2015. *Block Chain.* [Online]
Available at: https://en.bitcoin.it/wiki/Block_chain

Tuesta, D. et al., 2015. *Smart contracts: the ultimate automation of trust?,* Bilbao: BBVA.

UK Government Office for Science, 2016. *Distributed ledger technology: beyond block chain.* [Online]
Available at: https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain
[Zugriff am 11 03 2017].

University of Nicosia, 2015. *Academic Certificates on the Blockchain.* [Online]
Available at: http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/
[Zugriff am 10 03 2017].

Venture Scanner, 2017. *Bitcoin/Blockchain Startup Landscape Trends and Insights - Q1 2017.* [Online]
Available at: https://www.venturescanner.com/blog/2017/bitcoin-blockchain-startup-landscape-trends-and-insights-q1-2017
[Zugriff am 15 03 2017].

Vermesan, O. et al., 2013. Internet of Things Strategic Research and Innovation Agenda. In: O. Vermesan & P. Friess, Hrsg. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems.* Aalborg: River Publishers, pp. 7-152.

Vigna, P. & Casey, M., 2016. *The Age of Crypto Currency,* New York: The Investors Podcast.

von Freytag-Löringhoff, B. B., 1955. Über das hypothetische Urteil und den Rückschluß auf seine Prämissen. *Zeitschrift für philosophische Forschung,* 9(1), pp. 56-76.

Walport, M., 2015. *Distributed Ledger Technology: beyond block chain.* [Online]
Available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
[Zugriff am 03 12 2016].

Wilkinson, S. et al., 2016. *Storj: A Peer-to-Peer Cloud Storage Network,* Atlanta: Storj.

World Economic Forum, 2015. *Deep Shift - Technology Tipping Points and Societal Impact.* [Online]
Available at:
http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf
[Zugriff am 09 12 2016].

xapo, 2016. *Debitcard.* [Online]
Available at: https://xapo.com/card/
[Zugriff am 01 05 2017].

Yelowitz, A. & Wilson, M., 2015. Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters,* 07 01, 22(13), pp. 1030-1036.

Zarkadakis, G., 2017. *How AI and blockchain will change business organization.* [Online]
Available at: http://www.huffingtonpost.com/entry/how-ai-and-blockchain-will-change-business-organization_us_58cc33f5e4b07112b6472d4a
[Zugriff am 20 03 2017].

Zepf, T., 2016. *Blockchain. Technologien, Innovationen und Anwendungen.* 1st Hrsg. Frankfurt: Grin.

Anhang

A Elektronische Abgabe

Zusammen mit der physischen Version wurde ein elektronischer Datenträger mit zusätzlichen Daten eingereicht. Folgend ist die Ordnerstruktur aufgeführt.

Ordner	**Beschreibung**
CD/root	…
__/01_Quellen	Elektronisch verfügbare Literatur
__/02_Interviews	Metainformationen und Profil Interviewpartner
__/02_Interviews/01_Audio_Rohdaten	Aufnahmen der Interviews (m4a, mp3)
__/02_Interviews/02_Transkripte	Einzelne Transkripte der Interviews
__/03_Analyse_Rohdaten	Rohdaten der Analysen
__Mooken_Anand_Masterthesis_FS2017.pdf	Masterthesis als PDF/a
__Mooken_Anand_Masterthesis_FS2017.docx	Masterthesis als Word (.docx)

B Interviews

Master Thesis | **Die Blockchain Technologie und ihre Anwendungsfelder**

Autor: **Anand Paul Mooken**

Interviewleitfaden

Experteninterview mit Herrn Dr. Andreas Hirstein

Zürich, den 28.04.2017

Vorname, Name	*Dr. Andreas Hirstein*
Position	Ressortleiter Wissen – NZZ am Sonntag
Unternehmen	Neue Zürcher Zeitung, NZZ
	Falkenstrasse 11
	8021 Zürich
Kontakt	Telefon: +41 (0)44 258 14 15
	Mail: andreas.hirstein@nzz.ch
Selektionskriterien	Verfasser des Artikels «Blockchains sind so bedeutend wie das Internet»

Forschungsfragen:

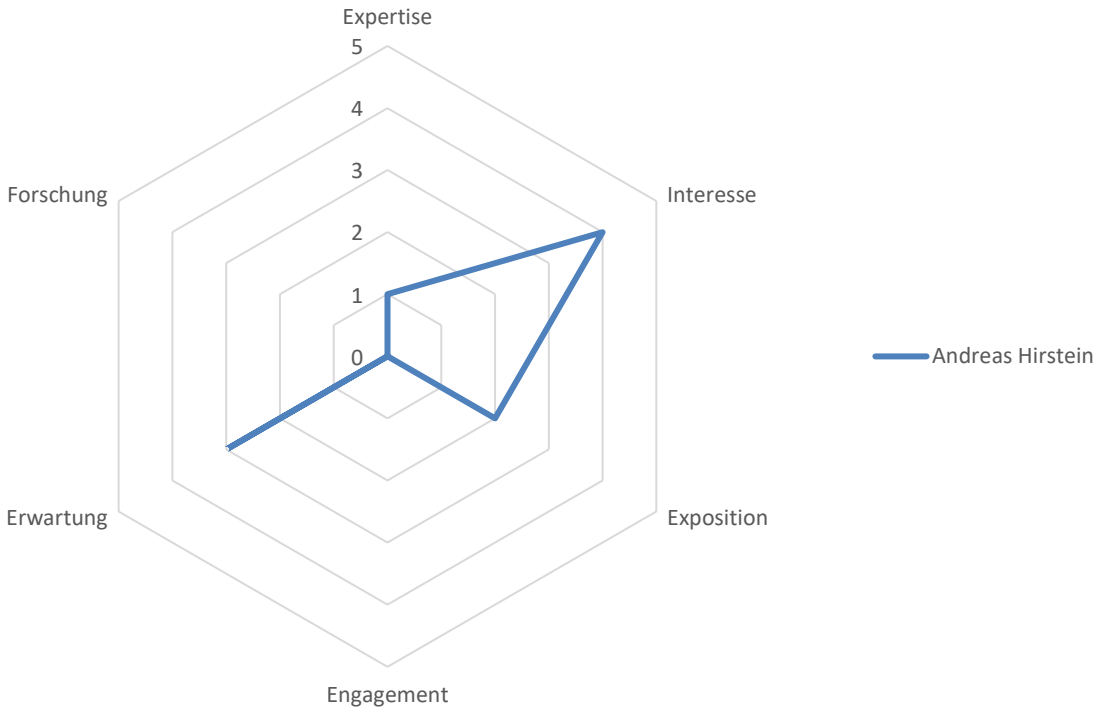
Was ist der Status Quo von Blockchain Technologie?

Wo liegen aktuell die Anwendungsfelder der Technologie?

Was sind mögliche Implikationen der Anwendung der Blockchain Technologie?

Wie können potenzielle Anwendungsfelder für die Blockchain Technologie systematisch identifiziert

Profil des Interviewpartners im Kontext Blockchain:



Legende: Expertise = Wissen über Blockchain; Interesse = .. zum Thema Blockchain; Exposition = Aktivitäten zum Thema Blockchain; Engagement = Geschäftliche Interaktion mit Blockchain; Erwartungen = .. an Blockchain; Forschung = .. zum Thema Blockchain

Andreas Hirstein studierte Physik an der Universität Bonn und der ETH Lausanne, wo er mit einer Dissertation auf dem Gebiet der Festkörperphysik abschloss. Das Interviewprofil von Andreas Hirstein wiederspiegelt seine Person als Journalist und somit seines Beobachterstatus. Seine Expertise basiert auf seinen Recherchen sowie seinen eigenen Interviews mit Experten der Thematik Blockchain. Sein Interesse zum Thema ist sehr gross und durch seine journalistischen Aktivitäten ist er der Thematik zu einem gewissen Grad exponiert. Dagegen ist er selbst, wie es sich als Beobachter verhält, nicht direkt an einer geschäftlichen Verwertung mit Blockchain beteiligt. Dies führt zu einem nicht vorhandenen Engagement zur bzw. mit Blockchain. Entsprechend forscht er selbst neben den Recherchen nicht aktiv zum Thema. Seine Erwartungen sind jedoch verhalten hoch, da er durch eben diese Recherchen der Technologie einige positive Aspekte abgewinnen konnte.

Transkript:

Anand Mooken: Guten Tag Herr Hirstein, vielen Dank, dass Sie sich die Zeit nehmen, mit mir über die Blockchain Technologie zu sprechen. Können Sie mir etwas zu Ihrer Person und der Tätigkeit bei der NZZ sagen?
Andreas Hirstein: Ich habe in Bonn und Lausanne Physik studiert und anschliessend für eine Fachzeitschrift gearbeitet. Seit 2002 bin ich bei der NZZ am Sonntag, seit 2008 Ressortleiter im «Wissen»

AM: Was sind Ihre Hauptthemen, welche Sie bei der NZZ bearbeiten?
AH: Ich schreibe über viele Technikthemen, aber auch über Umwelt- und Klimathemen. Grundsätzlich suchen wir Themen, die gesellschaftlich und wirtschaftlich relevant sind und zu denen die Wissenschaft etwas zu sagen hat.

AM: In Ihrem Artikel «Blockchains sind so bedeutend wie das Internet» haben Sie aufgezeigt, dass die Blockchain ein hohes Potenzial mit disruptivem Charakter besitzt. Wie sind Sie auf die Idee für diesen Artikel gekommen?
AH: Ich lese Fachzeitschriften und Zeitungen und besuche manchmal auch Tagungen. Dort taucht das Thema derzeit häufig auf. Ich fand aber, dass die Technik in den Publikumsmedien noch nicht gut erklärt wurde. Jedenfalls hatte ich selbst nicht verstanden, um was es wirklich geht. Das war eine Motivation für mich.

AM: Blockchain als Begriff ist derzeit in aller Munde. Sehen Sie diesen Hype als berechtigt an?
AH: Schwer zu sagen. Ich bin immer skeptisch, wenn von disruptiven Techniken gesprochen wird. In diesem Fall finde ich die Technik aber faszinierend. Die Vorstellung, legale Konstrukte wie Verträge, Zentralbanken und Behörden, durch Algorithmen zu ersetzen, hat ja auch eine anarchische Seite.

AM: Was ist für Sie die Blockchain und wo sehen sie diese heute?
AH: Das haben Sie ja schon selbst gesagt: eine verteilte Datenbank, die auf kryptografischen Methoden beruht. Noch zumeist im Forschungsstadium. Was daraus werden könnte, vermag ich nicht abzuschätzen. Ganz grundsätzlich finde ich jedoch bei einer neuen Technologie, dass man ihren Versprechen misstrauen sollte. Die Welt, so wie sie heute ist, ist nicht unbedingt so ineffizient, wie die Verfechter neuer Ideen jeweils behaupten. Hinter der bestehenden Technik stecken ja Jahrzehntelange Entwicklungen. Eine neue Technik muss schon deutlich besser sein, um sich durchzusetzen. Nur weil etwas auf dem Papier sehr viel besser aussieht, heisst das nicht zwingend, dass es in der Praxis eine Chance hat. Als gutes Beispiel möchte ich die Lithium-Ionen-Batterien erwähnen.

Da gibt es zwischenzeitlich auf Papier neue Ansätze, die theoretisch viel höhere Energiemengen speichern können. Aber die haben in der Praxis keine Chance, da man beispielsweise die ganze Produktion umstellen müsste. Das wird immer unterschätzt. Da wird auch in den Medien viel geschrieben, aber keiner fragt sich dann, ob dies bezahlbar herstellen lässt.

AM: Bitcoin geniesst einen verhaltenen Ruf und ist zuletzt mit negativen Schlagzeilen aufgefallen. Sehen Sie dies als negatives Vorzeichen für die Blockchain Technologie?
AH: Nein. Ich denke, dass die Probleme in kommerziellen Anwendungen nicht auftreten werden, weil vermutlich die Anonymität innerhalb des Blockchain-Netzes nicht mehr erwünscht sein wird. Vielleicht wird es andere Probleme und Gefahren geben: Angriffe von Hackern, Geheimdiensten und anderes.

AM: Wie schätzen Sie den Einfluss der Blockchain in unserem Leben heute ein (1-5, wobei 5 stark ist)? **AH:** Eine klare 1.

AM: Wie schätzen Sie den Einfluss der Blockchain in unserem Leben in 5 und 10 Jahren ein (1-5, wobei 5 stark ist)?
AH: Ich könnte mir vorstellen, dass es bis dahin konkrete Anwendungen in einigen Wirtschaftssektoren geben wird. Glaube aber, dass das für den Bürger und Konsumenten eher nicht sichtbar sein wird.

AM: Viele Drittinstanzen wie Banken aber auch gewisse Behörden und gar Anwälte könnten durch Blockchain obsolet werden, stimmen Sie dieser Aussage zu? Und wo sehen Sie potenzielle, neuaufkommende Implikationen?
AH: Nein. Ich glaube, dass die Banken nicht obsolet werden, sondern allenfalls die neue Technik in ihre Prozesse integrieren werden. Für die Kreditvergabe wird es sie weiter brauchen, vermute ich. Dass Anwälte und Notare überflüssig werden, glaube ich nicht. Vielleicht wird sich ihre Arbeit in einigen Bereichen verändert. Aber zu mehr reicht meine Vorstellungskraft nicht aus. Mit einem ganz radikalen Ansatz kann ich dieses Szenario natürlich nicht ganz ausschliessen. Aber wer würde dann am Beispiel einer Bank das Geld für einen Kredit aufbringen? Das Vertrauen ist in solche Institute nach wie vor hoch. Ich denke, dass es sich hierbei um eine weitgefasste Zukunftsvorstellung handelt.

AM: Wie kann man denn das Vertrauen der Endkunden in Blockchain steigern, um eben diese Technologie besser zu etablieren?
AH: Ich denke, dass der Endkunde im Endeffekt gar nicht zu wissen braucht, dass hinter einer Dienstleistung eine spezifische Technologie wie beispielsweise Blockchain steckt. Ich denke, das

Vertrauen darin wird nur mit der langsamen Umsetzung wachsen. Der derzeitig theoretische Ansatz hilft nicht. Bei Paypal waren die Leute lange sehr skeptisch. Ebenso beim Einsatz von Kreditkarten. Diese Technologien haben sich ebenfalls nur langsam etabliert. Ich denke, dass Anwendungsfälle im Geschäftsbereich [Business-to-Business] sich schnell durchsetzen werden, doch für den Privatkunden braucht es mehr Zeit, auch für das Vertrauen.

AM: Blockchain wurde mit Open-Source Gedanke eingeführt. Nun versuchen insbesondere Banken, sich des Systems zu ermächtigen, in dem proprietäre Lösungen entwickelt werden. Wie stehen Sie dieser Entwicklung gegenüber?
AH: Das überrascht mich nicht. Ich finde es auch nicht verwerflich. IBM hat sich ja einer Open-Source-Stiftung im Bereich Blockchain angeschlossen. Das heisst aber natürlich nicht, dass die Firma kein Geld verdienen will. Im Gegenteil, die tun das, weil sie denken, dass es sich auszahlt. Die Unternehmen, die sowas einsetzen, wollen natürlich Gewinne machen. Dies ist auch ihr Zweck. Es sind keine karitativen Vereine und somit ist es ihre Pflicht. Ich finde, man sollte mit der Idealisierung der Open-Source-Bewegung aufhören.

AM: Basierend auf Ethereum – einem Schweizer Kryptowährung-Start-up – haben die Sponsoren des EtherIndex Ether Trust einen Antrag auf Genehmigung eines ETF an der NYSE Arca Börse eingereicht. Der Antrag wird derzeit von der Aufsichtsbehörde SEC geprüft. Ähnliche Bestreben mit Bitcoin wurden bisher stets mit der Begründung der unzureichenden Marktüberwachung und mangelnder Regulierbarkeit abgelehnt. Wie sehen Sie die Thematik der Regulierung bei einer Kryptowährung bzw. einem anderen Use Case (Gefälschte Medikamente, Lebensmittel etc.)?
AH: Zum erwähnten Beispiel kann ich nichts sagen. Ich denke aber bei Marktüberwachung sowohl bei Lebensmitteln als auch den Medikamenten, dass sich die Blockchain Technologie sehr gut integrieren könnte. Es ist ja in erster Linie dem Hersteller überlassen, wie er dafür garantiert, dass die Produkte, die er über sein Netz vertreibt, wirklich original sind und keine Fälschungen. Wenn der Medikamentenverkäufer das Gefühl hat, dass dies durch die Blockchain gewährleistet sein kann, dass er vor Fälschungen geschützt ist, dann kann er das ja machen – solange er damit die gesetzlichen Vorgaben erfüllt. Ich bin aber ein Laie, das müsste man die Regulatoren fragen, welche Ansprüche und Bedingungen die Pharmafirmen zu erfüllen haben.

AM: Das Mining bezeichnet vereinfacht die Erzeugung eines weiteren Blocks in der Blockchain. Dies wiederum ergibt dem Erzeuger einen Verdienst – im Falle von Bitcoin sind es 12,5 Bitcoins pro Block. IBM entwickelte ein Verfahren ohne dieses bezahlte Mining. Welches Modell erachten Sie in welchem Anwendungsfall als sinnvoll?

AH: Das hängt offenbar von der Anzahl der Teilnehmer ab und ob sie sich gegenseitig vertrauen, ob sie anonym bleiben und anderes. Ich war ja auch bei IBM für diesen Artikel und habe mit dort mit dem Wissenschafter Andreas Kind gesprochen und er sagte mir, dass in den kommerziellen Anwendungen, wo sich die Nutzer schon kennen können oder wissen, wer mein Geschäftspartner ist – da muss es nicht so anonym sein – da braucht man das Mining nicht zu nutzen. So wie ich das verstanden habe, benötigt man das Mining in den vollkommen anonymen Blockchain. Wenn das in einer kommerziellen Umgebung zwischen Geschäftspartnern stattfindet, dann scheint mir das IBM-Verfahren mit den fehlertoleranten Algorithmen auszureichen.

AM: Blockchain bedeutet eine weitere Digitalisierung von Anwendungsfeldern. Werden wir demnächst keine Interaktionen mehr mit Menschen benötigen? Was sind Ihre Gedanken hierzu?
AH: Ich denke, dass sieht man bereits ohne Blockchain, dass die Digitalisierung dazu führt, dass die Interaktion mit Menschen abnimmt. Vermutlich wird dieser Prozess mit der Blockchain beschleunigt, wenn man sich zum Beispiel den Immobilienmarkt anschaut, ein Hauskauf zum Beispiel, wieviel Leute hier mitreden – die Gemeinden mit den Grundbuchämtern, die Notare, Verkäufer, Makler, und natürlich die Bank… Wenn alle die Blockchain nutzen, dann gibt es weniger Bedarf und weniger Kommunikation. Aber andererseits finde ich, dass uns durch die Digitalisierung nicht die Arbeit ausgehen wird. Darüber wird ja bereits geredet, seit es eine Industrialisierung gibt und bis jetzt ist die Arbeit nie ausgegangen – sie hat sich einfach verändert. Ich wüsste nicht, warum uns die Arbeit ausgehen sollte. Eine Wirtschaft, die autonom nur mit Maschinen und Robotern funktioniert, die braucht es ja gar nicht, weil ein Roboter ja nicht überleben muss. Es gibt kein Interesse, dass es zu einer Wertschöpfung kommt.

Wenn kein Mensch mehr eine Arbeit hat, dann gibt es auch keinen, der für eine Dienstleistung zahlen kann. Es kann nur immer soweit automatisiert werden, wie es Kapital gibt, diese Entwicklung zu finanzieren.

AM: Damit sind wir am Ende der Zeit und des Interviews. Vielen Dank nochmals für Ihre Zeit und die spanenden Ansichten.

Master Thesis | **Die Blockchain Technologie und ihre Anwendungsfelder**

Autor: **Anand Paul Mooken**

Interviewleitfaden

Experteninterview mit Simon Schweri und Oliver Heister

Zürich, den 03.05.2017

Vorname, Name	*Simon Schweri*
Position	Product Manager
Unternehmen	Datatrans AG Kreuzbühlstrasse 26 8008 Zürich
Kontakt	Mail: simon.schweri@datatrans.ch
Selektionskriterien	Aktiver Beobachter der Technologie zur möglichen Adaption für das eigene Produktportfolio

Vorname, Name	*Oliver Heister*
Position	Chief Technology Officer (CTO)
Unternehmen	Datatrans AG Kreuzbühlstrasse 26 8008 Zürich
Kontakt	Mail: oliver.heister@datatrans.ch
Selektionskriterien	Aktiver Beobachter der Technologie mit einem zusätzlich technischen Aspekt

Forschungsfragen:

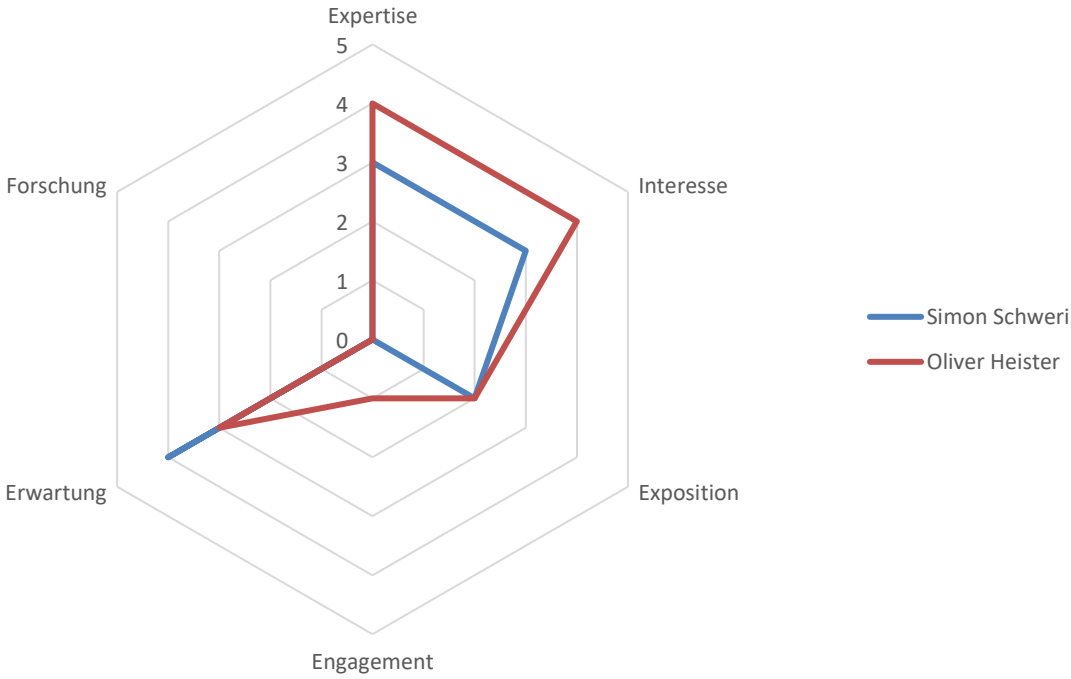
Was ist der Status Quo von Blockchain Technologie?

Wo liegen aktuell die Anwendungsfelder der Technologie?

Was sind mögliche Implikationen der Anwendung der Blockchain Technologie?

Wie können potenzielle Anwendungsfelder für die Blockchain Technologie systematisch identifiziert werden?

Profil der Interviewpartner im Kontext Blockchain:



Legende: Expertise = Wissen über Blockchain; Interesse = .. zum Thema Blockchain; Exposition = Aktivitäten zum Thema Blockchain; Engagement = Geschäftliche Interaktion mit Blockchain; Erwartungen = .. an Blockchain; Forschung = .. zum Thema

Simon Schweri und Oliver Heister arbeiten für Datatrans, welches der führende Schweizer Payment Service Provider ist. Datatrans konzentriert sich auf die technische Zahlungsverarbeitung im Online-Handel– als technischer Dienstleister ist Datatrans nicht involviert in den Geldfluss. Das eigentümergeführte Unternehmen ist unabhängig und kooperiert mit einer Vielzahl von Finanzdienstleistern. Datatrans ist international ausgerichtet und agiert ausschliesslich im Interesse der Online-Händler (datatrans, 2017).

Als Produktmanager ist Simon Schweri interessiert an technologischen Entwicklungen zur Optimierung seiner Produkte. Dem gegenüber ist Oliver Heister als Leiter der Informatik noch ein wenig skeptischer gegenüber der Blockchain.

Das Interview fokussiert auf die Prinzipien der Blockchain, wobei Intermediäre in der Theorie wegfallen sollten.

Transkript:

Anand Mooken: Guten Tag, geschätzte Herren Schweri und Heister. Vielen Dank, dass sie sich die Zeit nehmen, mit mir über die Blockchain Technologie zu sprechen. Können sie mir etwas zu Ihrer Person und der Funktion bei datatrans sagen?
Simon Schweri: Mein Name ist Simon Schweri, Product Manager bei Datatrans. Ich bin die Schnittstelle zwischen Sales und Technik auf einer Seite und auf der anderen Seite laufen all die Themen bezüglich Weiterentwicklungen, Seitens Technik und Business, bei mir zusammen. Es geht um die ständige Hinterfragung unserer Services. Sind sie gut genung? Gibt es Potenzial für Weiterentwicklungen, klassischerweise haben wir neue Zahlungsmittel. Wo ist der Bedarf seitens Kunden und auch unsererseits. Unsere Kunden sind die Händler, also e-Commerce Plattformen. Was erwarten diese von einem Payment Service Provider wie wir einer sind.
Oliver Heister: Oliver Heister ist mein Name, ich bin Leiter der Informatik. Was bei mir vor allem anliegt, sind Software Entwicklung und System Engineering im Betrieb. Ansonsten habe ich persönlich viel zu tun mit Security, Compliance, Verfügbarkeit und letztendlich auch technisch gesehen die Beurteilung von neuen Entwicklungen und Zahlungsarten.

AM: Es gibt verschiedene Entwicklungen im Bereich der elektronischen Zahlungsmöglichkeiten. Es ist bereits klar, dass ihr die Entwicklungen aktiv mitverfolgt. Wie haltet ihr euch auf dem neusten Stand und informiert euch über aktuelle Entwicklungen?
SS: Es sind die zwei Kanäle [Internet / Austausch]. Intern natürlich tauschen wir uns sehr stark aus, was wir sehen, lesen und wie wir das einschätzen. Also sprich Internet und dann der Austausch innerhalb der Firma. Daneben haben wir einen ziemlich nahen Kontakt zu den Playern des e-Commerce Business. Dort findet ein Austausch statt und wir gehen regelmässig auch an Konferenzen häufig in Bezug auf e-Commerce, an denen wir die Themen und deren Impact besprechen. Das sind unsere Informationsquellen.
OH: Dies deckt sich mit meinen Quellen.

AM: Was ist für Sie die Blockchain und wo sehen sie diese heute?
SS: Blockchain ist einer dieser IT Hype Themen, also Schlagwort, worauf sich die ganze IT Szene zurzeit fokussiert und sehr viele Menschen sich damit befassen. Dabei gibt es viele weitere Schlagwörter, welche um diese Blockchain kursieren, wie disruptiv oder erneut wieder mal Digitalisierung. Blockchain ist jedoch für mich nur eines von vielen Themen wie zum Beispiel Big Data auch, um mal ein wenig despektierlich zu werden. Auf der anderen Seite ist die Blockchain jedoch innovativ, man beginnt dadurch wieder, bestehende Business Prozesse zu hinterfragen. Man hat die

Technik, welche ein grosses Potenzial hat und somit die Grundlage, Bestehendes effizienter zu gestalten. Dieser Fakt finde ich neben der Technik etwas sehr spannendes an Blockchain. Was nach dem ganzen Hype und Gerede übrigbleibt, das ist offen. Und auch die Frage, ob dies dann auch wirklich kommen wird.

OH: Ich sehe die Thematik sehr ähnlich. Ich könnte sogar noch mit vielen weiteren sogenannten Schlagwörtern kommen wie Machine Learning, selbstfahrende Autos etc. Es gibt diverse Hype Themen, die durch entsprechende Firmen mit Ressourcen mit ihren Pilotprojekten Medienberichte generieren. Im Bereich Blockchain ist das ebenso. Ich glaube nicht, dass die Firmen in diesem Bereich bereits Geld verdienen oder aber sie verkaufen Technologien an andere Firmen, die darauf beruhen, aber die fahren selbst keine grossen Gewinne damit. Bitcoin zum Beispiel ist auch keine neue Technologie. Gibt es ja schon bereits seit ca. 8 Jahren. Bei unseren Händlern im Schweizer e-Commerce Bereich hat sich diese Zahlungsart jedoch nicht durchgesetzt. Es gibt ein Paar, welche es einsetzten, um als innovativ aufzutreten, doch verdienen beziehungsweise sparen sie dabei nicht wirklich was. Und dann hat es sich natürlich im Graubereich durchgesetzt. Erpressung oder Darknet mit Drogenhandel, VPN Dienstleistungen, wo unerlaubt Beschränkungen umgangen werden. Produkte, bei denen die Leute nicht identifiziert werden wollen mit ihren Kreditkarten und so weiter da diese Produkte am Rande der Legalität sind. Und natürlich gibt es auch Enthusiasten, in Berlin zum Beispiel, in Computer Clubs, welche Spass an der Technik haben und diese deshalb benutzen. Aber insgesamt glaube ich, dass das Thema extrem gehyped ist, Bitcoin wie auch Blockchain. Für mich ist die Blockchain an sich auch kein technologisches Wunder. Es werden Hashes berechnet die wieder in den nächsten Block miteingehen. Für viele Prozesse, die für uns relevant sind, würde es auch ausreichen, wenn wir irgendwelchen Parteien direkt vertrauen und irgendwas direkt signieren. Das müssen nicht zwangsläufig Blöcke sein. In diesem Sinne sehe ich für die nächsten paar Jahre keinen grossen Nutzen, ganz im Gegenteil. Vielfach ist es so mit Firmen, mit welchen wir zusammenarbeiten, dass zum Beispiel die IT Systeme der Banken, welche Kreditkartentransaktionen für die Händler abrechnen, Protokolle nutzen, die 20 bis 30 Jahre alt sind. Da wäre ich schon froh, wenn sie auf dem Stand der Technik von vor fünf Jahren wären und mal Webservices, XML oder JSON nutzen würden. Da muss es nicht direkt der Superhype sein. Standardisierung ist in unserer Branche natürlich ein Thema. Letztendlich hat jedes Zahlungsmittel, jede Bank noch ihre eigene Spezifikation. Also es gibt andere Sachen, die aus meiner Sicht noch vorher machen könnte.

AM: Blockchain als Begriff ist derzeit in aller Munde. Sehen Sie diesen Hype als berechtigt an?
SS: Es ist ein Einmaleins in diesen Themen. Es ist ein klassisches Modell [Gartner HypeCycle]. Wir befinden uns mit Blockchain zurzeit auf dem Höchststand als Hype und was danach kommt, ist bei

jeder dieser Hype Themen wieder anders. Dabei kann es auch dazu kommen, dass das Thema letztendlich wieder ganz verschwindet. Ich glaube, die Blockchain hat wirklich Potenzial, aber was dann letztendlich davon realisiert wird, ist noch ganz offen. Mir sind keine wirklich guten Business Cases oder Geschäftsmodelle bekannt, in der die Blockchain so richtig gut funktioniert und wo jetzt 'voll abgeht'. Man sucht zurzeit eher nach Anwendungsfällen. Auch wenn das jetzt kritisch klingt, so möchte ich nicht allzu kritisch werden. Es ist nun mal ein Hype Thema und so sollte man es auch sehen. Persönlich hoffe ich natürlich, dass daraus auch was wird.

AM: Wie schätzen Sie den Einfluss der Blockchain in unserem Leben heute ein (1-5, wobei 5 stark ist)?
SS: Also jetzt ist es natürlich keiner also eine 1. Noch sehe ich nicht, wie die Blockchain unser Geschäftsmodell zum positiven oder negativen beeinflussen wird, das müsste man noch antizipieren. Da wird zwar ziemlich sicher was kommen, aber den zeitlichen Rahmen dazu festzulegen ist heute noch recht schwierig.
OH: In diesem Bereich haben wir ja auch noch keine Händler und somit hat es einen ziemlich kleinen Einfluss.

AM: Wie schätzen Sie den Einfluss der Blockchain in unserem Leben in 5 und 10 Jahren ein (1-5, wobei 5 stark ist)?
SS: Hier würde ich bei der Skala eine 4 wählen. Ich denke, dass die Blockchain zukünftig definitiv einen Einfluss haben wird. Nicht nur generell, sondern auch für uns als Firma. Es gibt einem Kunden mehr Möglichkeiten, an einem Ort Handel zu treiben, die heute ziemlich schwierig sind. Beispiel Diamanten oder aber Rohstoffe im Generellen. Es ist heutzutage ziemlich schwierig, die Kontrolle über die gesamte Wertschöpfungskette zu haben. Wenn man in solchen Bereichen mit Themen wie Missbrauch und Betrug aufräumen kann, dann eröffnet sich dieser Bereich auch für seriöse Marktteilnehmer. Und dies könnte die Blockchain Technologie ermöglichen. Sobald ein so starker Mehrwert auch in anderen Branchen erzielbar ist, wird die Technologie abheben und auch wir werden definitiv dabei sein.
OH: Dies wollte ich auch so sagen. Wir sind eine kleine Firma und haben nicht grosse Forschungsbudgets. Ich gehe nicht davon aus, dass wir irgendein Blockchain Produkt selber entwickeln und am Markt durchsetzen können. Aber sobald sich irgendein Produkt durchsetzt und unseren Händlern einen Mehrwert bietet, werden wir uns nicht sträuben, sondern dies einbauen und nutzen.
SS: Ein grosser Vorteil unserer Firma ist: Wir sind Early Adopters. Wir sind sicher nicht an der vor-

dersten Front. Wir müssen immer einen Nutzen haben, können nicht aus Spass einfach was ausprobieren, dazu sind wir zu klein. Aber dafür sind wir relativ schnell und ziemlich weit vorne dabei, wenn wir Händler haben, denen das Produkt etwas bringt.

AM: Viele Drittinstanzen wie Banken aber auch gewisse Behörden und gar Anwälte könnten durch Blockchain obsolet werden, stimmen Sie dieser Aussage zu? Und wo sehen Sie potenzielle, neuaufkommende Implikationen?
SS: Datatrans ist ja ein Intermediär, wir sind zwischen Webshop und Zahlungsmittel. Die derzeitige Diskussion fokussiert ja darauf, mit der Blockchain Intermediäre auszuschalten um folglich eine Effizienzsteigerung zu erzielen. Dies kann ich so noch nicht abschätzen. Wir sind ja nicht nur ein Durchlauferhitzer, wir generieren ebenfalls eine Wertschöpfung. […] Ich finde es aber eine spannende Diskussion. Blockchain ist ja eigentlich wie eine Revolution von unten. Der ganze Overhead sollte ausgeschaltet werden. Auf der anderen Seite sind treibenden Kräfte je länger desto weniger die kleinen Start-ups, sondern grosse Firmen wie IBM, UBS oder Swisscom. Mit ihren Investments sichern sie ab, dass sich die Entwicklung in den von ihnen gewünschten Gefilde verläuft. Für mich ein spannender Widerspruch. Für uns ist ausschlaggebend, dass wir für unsere Kunden [Händler] effizient sind. Ein Webshop kommt zu uns, weil wir für ihn effizienter sind. Wenn wir es nicht sind, so sucht er sich einen anderen Weg. Und Blockchain muss eine Effizienzsteigerung bringen. […] Blockchain wird aber ganz sicher einen Einfluss haben, doch wie disruptiv es sein wird und wie stark sich bestehende Geschäftsmodelle ändern, ist für mich schwer zu sagen. Bezogen auf datatrans bin ich sehr positiv.

AM: Interessant ist ja aber auch die derzeitige Entwicklung, wenn wir mal Blockchain ausser Acht lassen. Grosse Firmen wie Apple, Google oder gar Samsung versuchen teileweise sehr erfolgreich, im Zahlungsverkehr mitzumischen. Wie seht ihr diese Entwicklung?
OH: Also erstens arbeiten wir mit den erwähnten Händlern ebenfalls zusammen. So bieten wir unseren Händlern auch die Zahlungsart Apple Pay an. Potenziell ist natürlich jede neue Art zu Zahlen mit einem hohen Marktanteil fähig, ihre eigenen Regeln zu machen und versucht, Mittelsmänner zu umgehen und somit auszuschalten. Die letzten Jahre haben wir aber gesehen, dass es viele Entwicklungen gegeben hat, viele neue Zahlungsarten, aber in Summe hat sich in der Schweiz nicht so viel geändert. Wir verfolgen das Ganze und schauen, dass wir bei sinnvollen Entwicklungen auch mitmachen. Aber solange eine einzelne Zahlungsart noch keine marktbeherrschende Stellung eingenommen hat und somit Alternativen verdrängt, solange macht das Geschäftsmodell von datatrans Sinn. E-Commerce Händler haben aber gar kein Interesse daran, dass sich nur eine einzige

Zahlungsart durchsetzt, da somit eine grosse Abhängigkeit entstehen kann, welche durch den Anbieter natürlich ausgenutzt werden kann, wie Preiserhöhungen und so weiter. Es gibt viele Player im Markt, die ein Interesse haben an einer gewissen Diversität.

SS: Ich finde es eine sehr interessante Frage, sollte die Frage direkt das Geschäftsmodell von datatrans kritisieren?

AM: Die Frage ist als solche für alle Interviewpartner gedacht, welche in die Definition von Blockchain als Intermediär agieren. Sei dies ein Payment Service Provider wie Datatrans aber auch Institutionen wie Banken, Börsen oder Ähnliches. Man kann diese Frage aber auch erweitern und nicht nur sehr gut etablierte Institutionen, sondern auch ziemlich junge Firmen wie Airbnb oder Uber einbeziehen und deren Geschäftsmodell mit dem Potenzial der Blockchain herausfordern.
SS: Die Frage ist sehr gut. Der Effekt ist aber andersrum. Der Fakt, dass sich mittlerweile sehr viele neue Player auf dem Markt der Zahlungsmittel tummeln – da das Thema sehr gehyped wird – da ist der Druck für einen Webshop, dass man einen sehr guten Partner hat – da zählen Fragen wie Sicherheit, regulatorische Fragen oder Haftung dazu – sehr gross. Da hat ein einzelner Shop keine Chancen mehr. Datatrans als Beispiel ist eigenfinanziert und wächst auch sehr Schweizerisch und nachhaltig. Es gibt aber auch sehr viele Intermediäre, die die gleichen oder sehr ähnlichen Geschäftsmodelle verfolgen wie datatrans und sehr gepushed werden. […] Man muss als Drittanbieter sehr flexibel sein und sich den aktuellen Gegebenheiten anpassen können.

AM: Somit kann man sagen, dass in eurer Branche der Händler trotz allem ein reges Interesse daran hat, einen kompetenten Partner zu haben und die Sorgen darum somit auch an diesen Partner abzugeben. Doch wie sieht es mit Banken oder Börsen auf? Hier gibt es viele Angriffsflächen mit der Blockchain Technologie. Siehst du es als mögliches Szenario, dass es dadurch in den nächsten Jahren eine andere Definition einer Bank geben wird, als wir diese heute kennen?
SS: Man kann bereits heute sehen, dass die Banken, wie sie heute agieren, Schwierigkeiten haben. Durch die Trägheit wie auch ein Wirtschaftssystem, welches auf Regulatoren besteht, wird es zu einer Veränderung kommen. Blockchain ist dabei einfach ein System mehr, was in diese Umwelt kommt und einen Einfluss auf eine Veränderung hat. Dabei glaube ich nicht, dass es zu einer radikalen Veränderung zu heute kommt. Die Blockchain Technologie wurde auch nur von Menschen entwickelt und auch wenn es schön ist, den Experten zuzuhören, so glaube ich nicht, dass es eine solch extreme Veränderung auslösen kann. […] Am Beispiel der Swisscom sieht man, sie machen ihren grössten Umsatz auch nicht mehr mit den traditionellen Festnetzanschlüssen. So muss sich auch das Geschäftsmodell von anderen Marktteilnehmern anderer Branchen anpassen.

AM: Was wären denn die Implikationen, die sich bei so einem Szenario ergeben würden?
SS: Die Implikationen sind, dass es natürlich neue, effizientere Services und Produkte geben wird. Das wird in der Finanzbranche sein aber auch andere Branchen. Wenn man bedenkt, auf welchen Kanälen wir heute schon Informationen beziehen, ist dies sehr wahrscheinlich. Man muss jedoch lernen, wie man damit umzugehen hat, dies trifft auch auf Blockchain zu. Es wird zu einer weiteren neuen Möglichkeit werden. Vielleicht redet man in einigen Jahren nicht mehr über Digitalisierung und Automatisierung, sondern über Prozessoptimierungen mittels Blockchain.

AM: Stichwort Regulatorien. Heutzutage wird vermehrt über das Element von Smart Contracts geredet. Dabei handelt es sich um ausführbaren Code der nach dem Schema «If this than that» funktioniert. Sind regulatorische Auflagen so statisch genug, um dies in die Blockchain einzubinden?
SS: Dies kann ich so nicht beantworten. Generell kann man aber sagen, dass bei Blockchain wie bei jeder anderen neuen Technologie zunächst erste Piloten auf den Markt kommen, gefolgt von ersten Missbrauchsfällen und daraus resultierenden Schäden. Dann beginnen sich Gesetztes- und Justizmühlen zu drehen – sehr langsam. Du hast ein System und eine Gesetzgebung, die immer hinterherhängen werden und dann eine Technologie und auch Kultur, die in irgendeiner Art einen Wandel haben muss, um mit der Technologie umgehen zu können.

AM: Bitcoin geniesst einen verhaltenen Ruf und ist zuletzt mit negativen Schlagzeilen aufgefallen. Sehen Sie dies als negatives Vorzeichen für die Blockchain Technologie?
SS: Für mich persönlich jetzt nicht. Aber als Händler bist du auf das Vertrauen der Kunden angewiesen. Ich gehe auch nicht zu einem Händler einkaufen, der kein sauberes Geschäftsverhalten aufweist. Als Händler, welcher Bitcoin einsetzen möchte, und die Währung ist negativ in der Presse, so wird dies effektiv ein Problem für Bitcoin sein. Das ist auch ein bestehendes Problem für Bargeld, denn man möchte wissen, woher das Geld kommt und ob dies einen legalen Hintergrund hat. Systembedingt steht die Nachvollziehbarkeit im Mittelpunkt der Diskussionen. Denn man möchte hier nicht illegale Aktivitäten fördern. Insbesondere in der Schweiz ist dies kulturbedingt. Bitcoin haftet ebenfalls diese negative Perzeption. […] Ein Endkunde muss sich nicht mit diesen Problemen auseinandersetzen – es sei denn, man wird erpresst. Somit hat es für den Enduser keinen Einfluss, es zählt eher der Komfort, den eine neue Technologie mitbringen kann.

AM: Kritiker von Kryptowährungen wie Bitcoin sehen eine unzureichende Marktüberwachung und mangelnde Regulierbarkeit seitens der gesetzgebenden und überwachenden staatlichen Organe. Befürworter hingegen loben die Entbündelung von Finanzwirtschaft und Politik. Wie seht ihr diese Thematik?

SS: Das ist jetzt eine sehr persönliche Meinung. Auf der einen Seite bin ich kein Freund von technokratischen Regierungen und Systemen. Ich bin eher auf der menschlichen Seite. Ein rein technisches System ist zwar sehr schön in sich stimmig aber es fehlt halt der menschliche Aspekt. Aber ich bin auch kein Fan von der derzeit gelebten Politik. Es sind sehr viele Emotionen und Stichworte wie Fake News sollten meinen Standpunkt klarmachen. Aber Blockchain kann keine Lösung sein für diese Probleme. Es ist ein sehr kontroverses Thema. Ob die Nationalbank mit ihrer Fiskalpolitik nun korrekt handelt oder eben nicht, da findest du immer Personen, die dafür sind oder dagegen. Letztendlich sollten es aber Menschen entscheiden, die in dieser Welt leben. Dafür braucht es auch Instanzen, die sich um diese Probleme kümmern. Dies ist auch das Schöne an der Schweiz, dass es diese Instanzen gibt und der Diskurs gefördert wird. Eine Entkopplung durch Technologie ist für mich entsprechend nicht wünschenswert.

AM: Diese Frage war jetzt sehr spezifisch auf Bitcoin als Kryptowährung ausgerichtet. Wenn man den Fokus wieder auf die Blockchain als Technologie legt, wurde bereits der Diamantenhandel als sinnvolles Anwendungsgebiet dafür erwähnt. Gibt es weitere Anwendungsfelder, in welchen ihr einen Einsatz der Technologie sehen würdet?
SS: Es gibt viele potenzielle Anwendungsfelder. Ich persönlich sehe vor allem diese Anwendungsfelder im Fokus, wo derzeit sehr viel verschleiert und mit unfairen Mitteln gehandelt wird. Dort, wo es eine Nachvollziehbarkeit braucht, Ausweise, Steuern und so ähnlich. Mein Wunsch wäre, dass man, wie beim Diamantenhandel, bestehende Unstimmigkeiten lösen könnte. Doch da kann die Blockchain alleine nicht viel ausrichten, denn es gibt entsprechen viele Anspruchsgruppen, die nicht wollen, dass diese Unstimmigkeiten gelöst werden. Solange kein Interesse für eine Nachvollziehbarkeit bestehet, kann sich auch eine Blockchain nicht durchsetzen. Fundamentalisten der Blockchain sind hier sehr idealistisch. Trotz allem führt dies nicht dazu, dass es effektiv zu einer Verbesserung führt. Denn die heutigen Probleme könnte auch schon mit der heutigen Technologie gelöst werden. Es ist wohl eher ein kulturelles denn ein technologisches Problem.

AM: Blockchain in der Privatwirtschaft. Wie würden Sie ein mögliches Szenario für Blockchain in der Privatwirtschaft beschreiben?
SS: Es wird dazu führen, dass sich im privatwirtschaftlichen Bereich zu Zusammenschlüssen kommen wird und diese ihre Dienstleistungen auch anderen Marktteilnehmern anbieten werden.

AM: Abschliessend: Gibt es Punkte, welche ihr noch gerne zur Thematik Blockchain und Anwendungsfelder erwähnen möchten? Persönliche Sichtweisen, Favorisierte Anwendungsfelder etc.
SS: Wir haben sehr viele Themen angesprochen und es gibt viele Themen, die noch offen sind. Wenn man die Entwicklung der Blockchain betrachtet, so kommt diese aus dem Technikbereich.

Ein Blockchain Fundamentalist wird sich mehrheitlich für die technisch messbaren Vorteile der Technologie interessieren und sich nicht mit den weiteren Implikationen auseinandersetzen, wie es beispielsweise die sozialen aber auch moralischen Aspekte betreffen. Dies ist nicht, weil die Person böse ist, es ist schlicht und einfach nicht sein Job.

Master Thesis | **Die Blockchain Technologie und ihre Anwendungsfelder**

Autor: **Anand Paul Mooken**

Interviewleitfaden

Experteninterview mit Jags Rao

Zürich, den 03.05.2017

Vorname, Name	*Jags Rao*
Position	Blockchain Workstream Lead - Reinsurance Technology Strategic Initiatives
Unternehmen	Swiss Re Soodring 6, 7 and 33 8134 Adliswil Switzerland
Kontakt	Mail: jags_rao@swissre.com
Selektionskriterien	Leiter des Blockchain Workstreams der Swiss Re mit aktiven Teilnahmen als Referat an wichtigen Blockchain Konferenzen weltweit

Forschungsfragen:

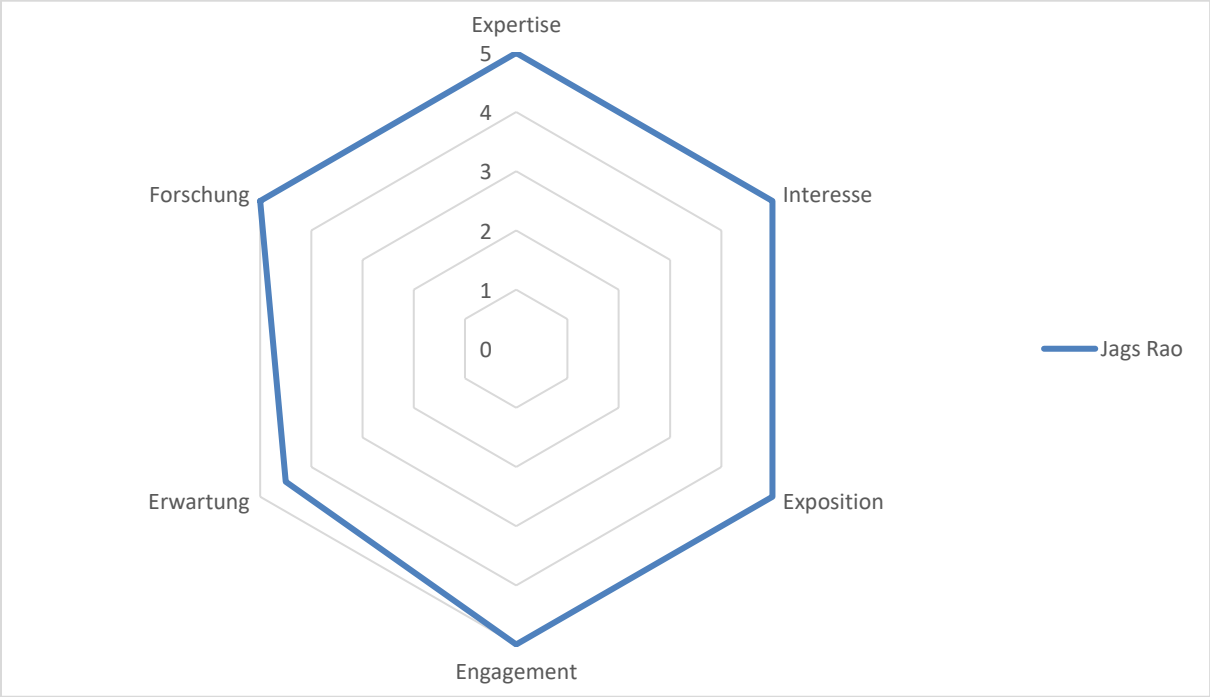
Was ist der Status Quo von Blockchain Technologie?

Wo liegen aktuell die Anwendungsfelder der Technologie?

Was sind mögliche Implikationen der Anwendung der Blockchain Technologie?

Wie können potenzielle Anwendungsfelder für die Blockchain Technologie systematisch identifiziert werden?

Profil des Interviewpartners im Kontext Blockchain:



Legende: Expertise = Wissen über Blockchain; Interesse = .. zum Thema Blockchain; Exposition = Aktivitäten zum Thema Blockchain; Engagement = Geschäftliche Interaktion mit Blockchain; Erwartungen = .. an Blockchain; Forschung = .. zum Thema Blockchain

Jags Rao arbeitet seit mehr als zwei Jahren bei der Swiss Re als Leiter des Blockchain Workstreams. Durch sein grosses Engagement im Blockchain Inkubator der Swiss Re und den zahlreichen Konferenzen, in denen er nicht nur Teilnehmer, sondern auch Referent ist, hat er eine grosse Exposition zu neuen Technologien. Die Swiss Re beschäftigt sich zurzeit stark mit der Blockchain und hat schon einige White Papers gemeinsam mit Kunden in der Strategie-Initative B3i - Blockchain Insurance Industry Initiative - verfasst. Auch erste Projekte wurden basierend auf Hyperledger und Ethereum umgesetzt und laufen als Proof-of-Concept in den Labs des Unternehmens.

Aufgrund der Vertraulichkeit wurde das Interview nicht aufgezeichnet und das Transkript gekürzt, wo dies auf Wunsch des Interviewpartners notwendig war.

Das Interview wurde auf English geführt und auf Deutsch transkribiert.

Transkript:

Anand Mooken: Hallo Rico, vielen Dank, dass du dir die Zeit nimmst, mit mir über die Blockchain Technologie zu sprechen. Kannst du mir etwas zu deiner Person und der Tätigkeit bei der Swiss Re sagen?

Jags Rao: Vor mehr als zehn Jahren habe ich meine Ausbildung in der Swiss Re begonnen. Dies war damals in der Informatik. Über die Zeit bin ich rumgekommen und habe das Rückversicherungsgeschäft kennengelernt.

AM: Blockchain als Begriff ist derzeit in aller Munde. Sehen Sie diesen Hype als berechtigt an?

JR: Ganz klar nein! Persönlich hatte ich zunächst gewisse Vorbehalte gegenüber dem Begriff Blockchain. Wenn man es aus einer technischen Sicht betrachtet, handelt es sich ja mehr um eine Kombination von bereits bestehenden Technologien. Nachdem ich aber in meiner Aktivität mehr von der Technologie und den Anwendungsfällen sehen konnte, habe ich meine Meinung grundlegend geändert. […] Klar handelt es sich auch um einen Hype. Ich finde diesen Fakt jedoch vorteilhaft für die Blockchain, da es so mehr und mehr Anhänger bekommt. Ein wichtiges Argument für die Durchsetzung von solch einer Technologie. […] Wir haben hierbei gute Erfahrungen gemacht mit all jenen Projekten, die wir zurzeit im Pilot haben. Soweit alles stabil, aber das ist ja auch kein Ernstfall-Szenario. Wir wagen uns langsam ran.

AM: Was ist für Sie die Blockchain und wo sehen sie diese heute?

JR: Eine Kombination aus sehr gut etablierten Technologien. Was interessanter ist, ist die Umsetzung von Anwendungsfällen mit diesem Konstrukt. Früher musste man sich dazu jeweils aus verschiedenen Elementen sozusagen einen Baukasten zusammenbasteln. Mit Blockchain hat man alles aus einer Box. Und am Beispiel der Smart Contracts sieht man auch sehr gut, wie sich die Blockchain weiterentwickelt und somit immer mehr Möglichkeiten zulässt. Und auch wir sind hierbei nicht nur passive Beobachter, sondern können mit unserem Engagement über die Initiative B3i [Blockchain Insurance Industry Initative] unsere eigenen Anwendungsfälle konstruieren. […] Dabei sehe ich sehr gute Gründe, wieso die Technologie ein 'Game-Changer' ist. Zunächst mal ist die Blockchain einfach nur einfach! Es erinnert mich dabei stark an Lego Blöcke, wir bauen etwas Block für Block und jeder Block ist alleine nichts aussagend aber im Gesamten ist der einzelne Block ein wichtiger Teil vom Ganzen und damit lassen sich grossartige Sachen bauen. Es ist denn auch die Sicht des Ganzen, welches uns zugegebenermassen in der Versicherungsbranche fehlt. Wir verarbeiten zwar tonnenweise Daten über viele verschiedene Plattformen, doch konzentrieren uns nur auf spezifische Segmente oder Märkte. Wir müssen uns weg von dieser limitierten Sichtweise zu

einer gesamthaften Lösung bewegen, ganz ähnlich, wie es Swift [Society for Worldwide Interbank Financial Telecommunication] in der Bankenbranche vollbracht hat. […] Dann gibt es natürlich auch das Prinzip der Immutability. Dies ist für uns eine grosse Herausforderung, wir müssen alles beim ersten Mal richtig hinbekommen [referenziert auf Smart Contract]. In grossen Versicherungsverträgen deklarieren die Parteien die Entwicklung ihres Portfolios selbst; will heissen, sie gegen Auskunft über den Geschäftsverlauf, Verluste, Reserven und so weiter. Da können dann auch mal Fehler passieren und man muss viel Arbeit reinstecken, damit man solch ein Reporting sauber hinbekommt. Arbeit, die eigentlich keinen Mehrwert bringt. Darum finde ich die Idee, alles beim ersten Mal richtig hinzukriegen, sehr verlockend. Eine verteilte Plattform, welche Fakten so ablegt, dass Änderungen jederzeit nachvollziehbar, revisionssicher und vor allem [nachträglich] nicht mehr veränderbar sind , ist für uns [Versicherungsbranche] neu und machtvoll und kann unsere Geschäftsprozesse essentiell verbessern. […] Ich könnte hier sehr viele weitere Vorteile der Blockchain für uns aber auch für viele andere Branchen aufzählen, die ich so schon heute sehe, dass würde dann aber den zeitlichen Rahmen sprengen. [Die Diskussion wurde bei der Besprechung der Methode vertieft und ist als Input miteingeflossen]

AM: Bitcoin geniesst einen verhaltenen Ruf und ist zuletzt mit negativen Schlagzeilen aufgefallen. Sehen Sie dies als negatives Vorzeichen für die Blockchain Technologie?

JR: Es ist nicht wegzuweisen, dass Bitcoin eine negative Assoziation durch die negativen Anwendungsfälle erhalten hat. Aber wir fokussieren uns ja auf die Blockchain Technologie. Hier ist es sehr wichtig, so zu differenzieren. Ich glaube, dass der Endkunde diesen Hintergrund heute noch gar nicht kennt. Und die Unternehmen sehen die Vorteile der Technologie überwiegend positiv und können entsprechend differenzieren. Disruptoren sind dabei ja nicht wirklich etwas, was wir ablehnen. Sie können ganz neue Produkte hervorbringen. Beispielsweise gibt es heute schon digitale Vergleichsportale für Versicherungsprodukte, welche als neuer Vertriebskanal genutzt werden. […]

AM: Wie schätzen Sie den Einfluss der Blockchain in unserem Leben heute ein (1-5, wobei 5 stark ist)?
JR: Kommt ganz darauf an, welchen Kontext du einschliesst. Bei mir persönlich hat die Blockchain kaum einen Einfluss. Ich habe zwar Bitcoins… Darum subjektiv wohl zwischen 1 und 2, bei Anbetracht der Kursentwicklung von Bitcoin definitv eine 2. Unternehmen fahren ja schon gewisse Piloten, deshalb hier ganz sicher eine 2.

AM: Wie schätzen Sie den Einfluss der Blockchain in unserem Leben in 5 und 10 Jahren ein (1-5, wobei 5 stark ist)?

JR: Wieder die Unterscheidung zwischen Privatperson und Unternehmen, kurz gesagt 3 und 5.

AM: Viele Drittinstanzen wie Banken aber auch Versicherungen könnten durch Blockchain obsolet werden, stimmen Sie dieser Aussage zu? Und wo sehen Sie potenzielle, neuaufkommende Implikationen?

JR: Bei Banken sehe ich hier ein mögliches Szenario einer Verdrängung. Doch hier rede ich von einem Zeitraum von über 20 Jahren. Denn das Vertrauen zu diesen Instituten wurde ja auch über die Jahre hinweg aufgebaut. So schnell kann man die Gesellschaft nicht von neuen Modellen überzeugen. Es geht ja meist auch um viel Geld und da möchte ich entgegen aller Logik nicht einem reinen System vertrauen […] Es ist wohl auch ein wenig die Gewohnheit und die soziale Interaktion, welche zumindest heute noch ein Element der Bank ausmacht. […] Versicherungen und auch wir als Rückversicherer wird es aber immer geben. Wir gehören ja auch nicht zu der definierten Gruppe von Intermediären, welche durch die Blockchain ausgeschaltet werden kann, da wir eine Dienstleistung anbieten. In unserer Branche werden eher Broker oder Makler betroffen sein. Sie sind die typischen Zwischenhändler in der Versicherungsbranche. Aber wir reden ja auch nicht über reine Durchlauferhitzer. Makler bzw. Broker spielen eine wesentliche Rolle bei der Risikoeinschätzung und generieren dadurch einen wertvollen Mehrwert für die Versicherungsunternehmen. Ich sehe hier eher eine Beschleunigung der Administration, also der Automatisierung von Prozessen, welche primär im Hintergrund laufen.

AM: Wie kann man denn das Vertrauen der Endkunden in Blockchain steigern, um eben diese Technologie besser zu etablieren?

JR: Ich glaube, in der Phase in der wir zurzeit sind, ist das Vertrauen der Endkunden gar nicht so wichtig. Es geht darum, dass wir Unternehmen uns zunächst an die Möglichkeiten der Blockchain heranwagen und mittels guten Anwendungsfällen beweisen. Da sind wir natürlich stolz, ein Teil der Bewegung zu sein.

AM: Blockchain wurde mit Open-Source Gedanke eingeführt. Nun versuchen insbesondere Banken, sich des Systems zu ermächtigen, in dem proprietäre Lösungen entwickelt werden. Wie stehen Sie dieser Entwicklung gegenüber?

JR: Naja, es kommt drauf an wie man es sieht. Open Source ist ja Ansichtssage. Ich glaube, dass das R3 Konsortium, welches einer der grössten Blockchain Initiativen in der Bankenwelt ist, drauf und dran ist, ihre Blockchain zu öffnen, also open-source zu machen. Aber sie wird woll eine permissioned Blockchain bleiben, denn wie bei unserem Geschäft müssen auch die Banken ihre Kunden kennen. Ganz alleine schon bezüglich der regulatorischen Auflagen.

AM: Basierend auf Ethereum – einem Schweizer Kryptowährung-Start-up – haben die Sponsoren des EtherIndex Ether Trust einen Antrag auf Genehmigung eines ETF an der NYSE Arca Börse eingereicht. Der Antrag wird derzeit von der Aufsichtsbehörde SEC geprüft. Ähnliche Bestreben mit Bitcoin wurden bisher stets mit der Begründung der unzureichenden Marktüberwachung und mangelnder Regulierbarkeit abgelehnt. Wie sehen Sie die Thematik der Regulierung bei einer Kryptowährung bzw. einem anderen Use Case (Gefälschte Medikamente, Lebensmittel etc.)?

JR: Generell sehe ich hier zwei entgegenlaufende Prämissen. So wird zum einen in einer offenen Blockchain, wie es Bitcoin nutzt, keine Regulation geduldet. Zum anderen möchte man sich mit so einer Technologie in einen Markt bringen, in welchen klaren Auflagen existieren. Dies macht doch keinen Sinn?! […] Aber wir haben aus unserer Initiative raus ebenfalls schon Gespräche mit den hiesigen Regulatoren gehabt. Daraus hat sich ergeben, dass sie die Blockchain mehrheitlich positiv sehen. […] Am Beispiel der Kryptowährung kann man den Zahlungsverkehr als eigenes Geschäft betrachten. Die Banken sind hierbei an weniger Kapitalvorschriften gebunden, als wenn du hier Kraut und Rüben vermischt [Hypotheken, Anlagegeschäft etc.]. Das würde die Arbeit der Regulatoren natürlich implizit vereinfachen, da man sich voll auf die riskanten Geschäfte fokussieren kann - natürlich auch vorteilhaft für Banken, aber meiner Meinung nach nicht so extrem wie für die Regulatoren. Zusätzlich sehen sie, wie wir und weitere Experten, die Blockchain als Single source of truth. Das ist natürlich ein entscheidender Vorteil für alle Parteien - die ein sauberes Geschäft machen wollen. […] Dann werden aber insbesondere von den Regulatoren auch Nachteile gesehen. Denn die Privatsphäre, die Sicherheit aber auch eine mögliche Kartellbildung sind im Interesse bzw. eben nicht im Interesse des Regulators. Nur haben wir auch gemerkt, dass Regulatoren sehr reaktiv agieren. Dies zeigt sich bereits bei Kryptowährungen. Die Schweiz ist hierbei noch relativ liberal im Vergleich zum benachbarten Ausland. Aber auch hier müssen noch einige Anpassungen erfolgen, bis wir aus Sicht der Regulatoren innovative Produkte auf den Markt bringen können. […] Es handelt sich nicht nur um unser Empfinden. Am erst kürzlich von uns organisierten Blockchain Event für Versicherer haben sich auch andere Partner und Besucher so oder ähnlich zur Problematik mit den Regulatoren geäussert. Da muss man aber auch das Verständnis dafür haben. Mir ist es ja auch lieber, wenn unsere Regierung mit Bedacht agiert und dabei die richtigen Entscheidungen trifft, als dass wir einen kurzlebigen Schnellschuss erleben. Dazu wäre die Blockchain viel zu schade. Und der Regulator beschäftigt sich ja auch mit der Thematik.

AM: Das Mining bezeichnet vereinfacht die Erzeugung eines weiteren Blocks in der Blockchain. Dies wiederum ergibt dem Erzeuger einen Verdienst – im Falle von Bitcoin sind es 12,5 Bitcoins pro Block. IBM entwickelte ein Verfahren ohne dieses bezahlte Mining. Welches Modell erachten Sie in welchem Anwendungsfall als sinnvoll?

JR: Ohne hier auf Details einzugehen, würde ich persönlich meinen, dass sich das Mining für öffentliche Blockchains eignet oder wohl fast schon ein Zwang ist. Denn es bildet die Motivation für die Full Nodes, ihre Rechenkapazität dem Zweck zu opfern. Ich nehme das als Endbenutzer als Transaktionskosten wahr. Bei kommerziellen Systemen sehe ich den Zweck einer solchen Incentivierung nicht. Denn die Mehrheit der kommerziellen Systeme bedingen, dass man sich wie bereits erwähnt untereinander kennt und vertraut - zumindest hypothetisch. Das schliesst eine public Blockchain aus und man entwickelt - wie du wahrscheinlich auch gesehen hast - auf permissioned Blockchains. Wer da teilnimmt, sollte auch davon profitieren. Es handelt sich hierbei um den Austausch von Rechenkapazität gegen Dienstleistung. Insbesondere im B2B Markt reicht dieser Anreiz aus, würde ich meinen.

AM: Damit sind wir am Ende der Zeit und des Interviews. Vielen Dank nochmals für Ihre Zeit und die spanenden Ansichten.

Kommentar: Interview wurde stark gekürzt wiedergeben. Der Autor konnte im Anschluss noch spezifische Anwendungsfälle besprechen und konnte dadurch weitere Erkenntnisse erfassen.

Master Thesis | **Die Blockchain Technologie und ihre Anwendungsfelder**

Autor: **Anand Paul Mooken**

Interviewleitfaden

Experteninterview mit Peter Ivankay

Zürich, den 03.05.2017

Vorname, Name	*Peter Ivankay*
Position	Projektleiter UBS WM Innovation Lab
Unternehmen	UBS AG WM Innovation Lab Max-Högger-Strasse 80 / 82 8048 Zürich
Kontakt	Mail: peter.ivankay@ubs.com
Selektionskriterien	Teil des Wealth Management Innovation Labs mit starkem Fokus auf die Blockchain inklusive Verfasser von wissenschaftlichen Arbeiten zur Blockchain

Forschungsfragen:

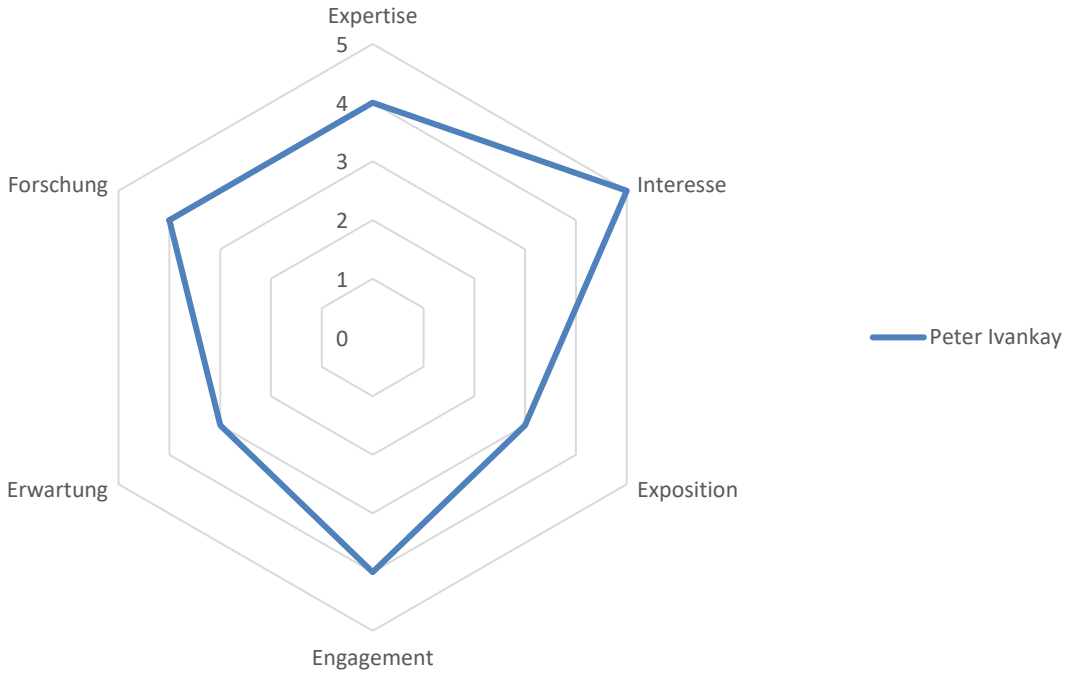
Was ist der Status Quo von Blockchain Technologie?

Wo liegen aktuell die Anwendungsfelder der Technologie?

Was sind mögliche Implikationen der Anwendung der Blockchain Technologie?

Wie können potenzielle Anwendungsfelder für die Blockchain Technologie systematisch identifiziert werden?

Profil der Interviewpartner im Kontext Blockchain:



Legende: Expertise = Wissen über Blockchain; Interesse = .. zum Thema Blockchain; Exposition = Aktivitäten zum Thema Blockchain; Engagement = Geschäftliche Interaktion mit Blockchain; Erwartungen = .. an Blockchain; Forschung = .. zum Thema

Peter Ivankay verfügt über einen Master of Arts HSG in Banking and Finance und ist Projektleiter im UBS Wealth Management Innovation Lab, welches sich mit neuen Technologien beschäftigt. Er hat bereits an einigen Projekten der Abteilung gearbeitet, welche mittels Ethereum umgesetzt wurden und kennt entsprechend die Vor- und Nachteile der Technologie. Neben dieser praxisorientierten Expertise hat er seine Masterarbeit über die Blockchain verfasst und verfügt entsprechend über ein grosses theoretisches Wissen.

Das Interview fokussiert auf die Aktivitäten des WM Innovation Labs der UBS sowie die Bewertung, wie Anwendungsfälle für Blockchain in diesem Kontext identifiziert werden. Und zuletzt auch die Sicht auf Konkurrenten, insbesondere den Start-up-Unternehmen.

Transkript:

Anand Mooken: Hallo Peter. Vielen Dank, dass du dir die Zeit nimmst, mit mir über die Blockchain Technologie zu sprechen. Kannst du mir etwas über deine Person und Funktion beim UBS WM Innovation Lab sagen?
Peter Ivankay: Also mein Interesse an Blockchain kam eher aus der Forschung noch im Master an der HSG, wo ich mich umgeschaut habe. Technologie war das Thema. Mit meinem betreuenden Dozenten zur Masterarbeit habe ich die Blockchain angeschaut. Dann bin ich aber auch hierher [UBS] gekommen und habe begonnen, zu arbeiten – wobei Blockchain als Thematik ein wenig in den Hintergrund gerückt ist. Doch kurz darauf habe ich dann innerhalb von Projekten mit der Blockchain begonnen, zu arbeiten. Ich habe verschiedene Projekte zu Blockchain geleitet bzw. dabei mitgearbeitet. Ich mache sehr viel Education für Leute zum Thema Blockchain innerhalb der Bank. Leute, die eine kleine bis mittelmässige technologische Expertise haben. Ich zeige ihnen auf, was man mit der Blockchain alles machen kann, zum Beispiel im Bereich der Kundenberatung und gehe auch auf Punkte ein, die sie gerne besprechen wollen.

AM: Was sind Ihre Hauptaufgaben, welche Sie bei UBS bearbeiten?
PI: 20% meiner Kapazität investiere ich in Projekte zu Blockchain. Ich habe aber auch zu anderen Themen beigetragen innerhalb der Bank wie beispielsweise Business Analyse und so ähnlich. Der Hauptforschungsteil der UBS findet in London statt [UBS Innovation Lab namens Level39].

AM: Dann möchte ich doch gleich übergehen zum Thema und zu Beginn mit einer ganz offenen Frage starten: Was ist für Sie die Blockchain und wo sehen sie diese heute?
PI: Naja, Blockchain ist für mich zuallererst ein Hype. Es ist ein Verkaufsinstrument mit welchem man verschiedene Lösungen verkaufen kann innerhalb der Bank, bei verschiedenen Projekten, extern wie auch intern. Das ist das Eine. Auf der anderen Seite steckt da wirklich, meiner Meinung nach, viel dahinter. Für mich ist die Blockchain nicht nur eine verteilte Datenbank, so wie man es verstehen könnte. Sondern für mich ist es wirklich dieses Ökosystem an Apps die man ohne eine zentrale Autoritätsfigur machen kann. Das ist meiner Meinung nach Blockchain. Vielleicht noch ein dritter Punkt: Was aus einem Corporate Standpunkt aus die Blockchain ist, ist für mich Effizienzsteigerung, also ein System, mit welchem ich mich viel besser mit anderen Leuten abstimmen kann.

AM: Entsprechend auch deiner Auffassung gibt es einen grossen Hype um Blockchain. Siehst du diesen als gerechtfertigt?
PI: Ich denke, hinter dem Hype, so wie er jetzt ist, ist es ein bisschen viel. Besonders die ganzen extremen Blockchain-Evangelisten, welche eine absolut verteilte Welt mit keiner zentralen Third-

Party mit Zero Trust sehen – daran glaub ich nicht, meiner Meinung nach sehe ich nicht, dass dies unbedingt nötig wäre wie beispielsweise bei Finanzinstituten. Es ist nicht immer ineffizient, wenn man eine zentrale Node hat. Wenn man irgendwas hat, wohin man sich wenden kann. Und ich glaube, Leute haben schon Vertrauen in verschiedene Institute. Und es ist auch etwas was ich sehe. Sie brauchen so etwas von der Tradition her. Ich glaube, kurzfristig ist es kaum etwas, wobei ich Grosses erwarte. Dann, später, hat es wirklich etwas an sich mit dem Hype. Wenn wir es wirklich schaffen, so ein System zu entwickeln und wirklich viele Sachen, besonders in den Banken-Ökosystemen […] wenn man es schafft, wie es Vault OS [ein Betriebssystem aber auch Konzept, das Banking der Zukunft in der Cloud bereitzustellen] versucht, es hinzukriegen, sehr viele von diesen Blockchains zusammenzuführen in verschiedenen Funktionalitäten, dann kann es sehr stark werden. Aber bis jetzt sehe ich das Problem nicht in der Technologie selbst, ob diese jetzt gut ist oder nicht. Ich sehe diese eher bei der Adaption.

AM: Es steht und fällt also abhängig dazu, wie Unternehmen die Blockchain in ihrer Umgebung adaptieren. Aber doch noch zurück zu einem Stichwort, welches du selbst genannt hast. Keine Third-Parties mehr. Viele Drittinstanzen wie Banken aber auch gewisse Behörden und gar Anwälte könnten durch Blockchain obsolet werden, stimmen Sie dieser Aussage zu? Und wo sehen Sie potenzielle, neuaufkommende Implikationen?
PI: Langfristig, absolut! Ich muss dazu sagen, dass unsere Bank soweit schon so aufgestellt ist, dass man viele Prozesse dann gegebenenfalls ersetzen kann. ABER, und genau das mein ich ein bisschen mit der Sache; Blockchain ist sehr disruptiv, sehr viele Sachen, meiner Meinung nach – wie ich es bei den Lösungen soweit gesehen habe – haben einen ganz spezifischen Teil von dieser Value Chain nicht angegriffen aber ersetzt, aber es sind sehr viele andere Services und Funktionen, die eine Bank in dieser ganzen Wertschöpfungskette abdeckt, die mit der Blockchain nicht abgedeckt werden können. Ganz einfache Beispiele mal: Regulatorik. Das kann natürlich sein, dass es dann wirklich mal über Blockchain gemacht wird, aber es gibt noch so viele kleine anderen Sachen diesbezüglich, die man beachten muss, die mit den jetzigen Technologien noch sehr schwer sind, abzudecken. Dementsprechend würde ich sagen: Ja, es ist sehr disruptiv in unserem Sinne, aber bestimmt nicht kurzfristig. Und später auch – wenn es die Bank schafft – führt es zurück zum globalen Punkt: Wie kann sich ein Unternehmen den neuen Bedingungen anpassen. Ich kann dir noch ein Beispiel nennen: Im Wealth Management, welche international gesehen die Haupttätigkeit der UBS ist, wobei die Beratung einer der wichtigsten Services ist, die wir anbieten. Und der Teil wird von der Blockchain nie ersetzt werden, weil du Expertise anbietest. Es hilft sogar, wenn du dich wirklich nicht mit Themen auseinandersetzen musst wie beispielsweise, dass die IT-Systeme lang-

sam sind oder das irgendwelche Aktion nicht übertragen worden sind in dein Depot oder es irgendwelche Probleme gibt mit Zahlungen, sondern du wirklich sagen kannst: Hier, ich biete dir finanzielle Expertise an, ich berate dich auf diese verschiedenen Produkte. Alles andere ist super schnell im Hintergrund. Dadurch hast du eine fast noch stärkere Value Proposition als andere Anbieter. Du kannst den Fokus [als Unternehmen] auf wirklich wichtige Sachen legen. Du brauchst keine Bank mit 60'000 Angestellten, wovon vielleicht 50'000 im Back-Office irgendwelche Prozesse anpassen. Es werden weniger werden, evtl. einfach andere Prozesse. Du kannst dich auf Sachen konzentrieren, die wirklich Wert generieren.

AM: Du siehst also eher eine Veränderung, als ein radikaler Wechsel. Kannst du noch genauer erläutern, wie sich die Banken in dieser Hinsicht ändern werden oder müssen?
PI: Die Banken sehen das Ganze bereits kommen und bereiten sich schon vor. Es ist nicht unbedingt die technische Vorbereitung oder eine Weisung vom Top-Management, dass man eine ganz neue Strategie fahren soll. Aber wir merken mehr und mehr, dass es da [mit dieser Entwicklung] verschiedene Sachen geben kann. Jetzt werden meiner Meinung nach bestehende Blockchain Technologien von Banken genommen, und sie versuchen diese an den jetzigen Produkten und Services anzupassen. Klar, dass kannst du am einfachsten machen und da kannst du am einfachsten sehen, wo entlang der Wertschöpfungskette du etwas Ersetzten könntest, Zahlungsprozesse, Investitionsprozesse etc. Auf der anderen Seite, wenn man von einer ganzheitlichen Blockchain Perspektive kommt, sind viele der betrachteten Prozesse meiner Meinung nach gar nicht nötig. Das ist ein ganz anderer Ansatz und ich glaube, den Ansatz fahren Banken noch nicht.

AM: Das bringt mich auf den holistischen Ansatz von Blockchain, welcher seinen Ursprung in der offenen Community hat. Blockchain wurde mit Open-Source Gedanke eingeführt. Nun versuchen insbesondere Banken, sich des Systems zu ermächtigen, in dem proprietäre Lösungen entwickelt werden – im Rahmen des R3 Konsortiums. Die Banken wie die UBS versuchen hierbei, in einer Gatekeeper Rolle die Blockchain zu kontrollieren. Wie stehst du dieser Entwicklung gegenüber?
UPDATE: Wurde nun open-source gemacht
PI: Der Code des R3 Konsortiums ist sicher open-source. Aber es handelt sich ja dabei immer noch um eine private Blockchain. Die UBS als Gatekeeper? Nicht unbedingt, weil ein Gatekeeper zu sein bei einer Technologie, die schon stark darauf aufgelegt ist, offen zu sein, ist sehr schwer. Und das ist eine Strategie, die du wahrscheinlich langfristig nicht fahren kannst. Andererseits denke ich, dass auf der Blockchain eher verschiedene Services angeboten werden. Du brauchst die Gatekeeper um KYC [das Konzept Know your Client], AML [Anti-Money-Laundry] und Ähnliches hinzukrie-

gen. Das ist regulatorisch so gemacht. Natürlich gibt es meiner Meinung nach Prozesse, wo so etwas nicht notwendig ist. Beispielsweise Zahlungen, besonders in kleinerem Bereich. Doch im Wealth Management beispielsweise gibt es immer wieder grössere Zahlungen, die auch einen terroristischen Hintergrund haben könnten. Da muss man aufpassen, solche Zahlungen dann freizugeben. Aber andererseits werden solche Zahlungen ja eh schon über Bitcoin gemacht. Aber im Allgemeinen wird es solche Sachen [Anwendungsfälle] sicher geben, in dem man es open-source [als öffentliche Blockchain] machen kann. Die anderen Fälle brauchst du zunächst mal das Vertrauen. Bondfinanzierung ist ja ein gutes Thema. Es gibt viele Bonds, die auf Basis von Ethereum nachgemacht sind. Da ist es sehr wichtig, dass die Due Dilligence einmal gemacht wurde. Da ist es sehr wichtig, dass die anderen Wertschöpfungsprozesse, bevor der Bond ausgegeben wird, einmal gemacht wurden. Und da brauchst du immer noch einen Gatekeeper.

AM: Du würdest also sagen, dass die Blockchain doch noch gewisse Limitationen aufweist, bei welchen man einen Drittanbieter benötigt?
PI: Absolut. Ich glaube, dass Blockchain eine super Datenbank ist. […] Viele Prozesse lassen sich nicht einfach ohne weiteres mittels einer Blockchain mit heutigem Technologiestand umsetzen bzw. ersetzen. Dazu ist die Umwelt zum einen noch zu dynamisch und zum anderen sind die Auflagen sehr komplex und schwierig in eine Blockchain, beispielsweise mittels eines Smart Contracts, zu kapseln.

AM: Stichwort Ethereum. Dieses Start-up versucht ja explizit solche komplexeren Anwendungsfälle umzusetzen. Ist dies nicht ein möglicher Lösungsansatz zu den von dir erwähnten Limitationen der Blockchain?
PI: Ethereum ist top! […] Sehr viele Projekte werden bei uns auf Ethereum gemacht und sehr viele Projekte kannst du eigentlich nur auf Ethereum machen, nicht nur, aber Ethereum ist etwas, wo du bereits eine gewisse Liquidität drin hast und beispielsweise Smart Contracts auch wirklich so ausgeführt werden wie sie es müssen. Trotz allem muss man sagen, dass man sich hierbei noch immer in der Entwicklung befindet und es noch einige Herausforderungen gibt, bevor man sich an solch komplexe Anwendungsfälle herantrauen kann. […] Wir haben aber neben all den Good News auch die Bad News mitbekommen. Also wenn du dann mal so ein Down hast und einen Hard Fork machen musst, ist das natürlich nicht das Beste. Ich bin hier leider der Meinung, dass es der falsche Weg war aus Sicht des globalen Ökosystems. Denn wenn du sagst, Code is King, und was somit im Smart Contract steht [kodiert ist] wird auch so ausgeführt und jemand dies ausnutzen kann [und einen Exploit wie geschehen] stattfindet; dann ist das eben so. Hier müsste man konsistent bleiben

und es voll durchziehen. Natürlich ist es zu diesem Zeitpunkt nicht so schlimm gewesen für Ethereum, aber in Zukunft könnte das schwerwiegende Konsequenzen haben. Hätte Ethereum von dieser Hard Fork abgesehen, wäre es eventuell zwar untergegangen, aber nachfolgende Projekte hätten aus diesen Fehlern lernen können und vor allem gesehen, dass es [das System, Blockchain] konsequent durchgesetzt wird. […] Aber sicher, es [Ethereum] hat grosses Potenzial und man darf gespannt sein, was hier noch alles kommt.

AM: Wenn wir gleich bei Ethereum bleiben. Basierend auf Ethereum – einem Schweizer Blockchain-Startup – haben die Sponsoren des EtherIndex Ether Trust einen Antrag auf Genehmigung eines ETF an der NYSE Arca Börse eingereicht. Der Antrag wird derzeit von der Aufsichtsbehörde SEC geprüft. Ähnliche Bestreben mit Bitcoin wurden bisher stets mit der Begründung der unzureichenden Marktüberwachung und mangelnder Regulierbarkeit abgelehnt. Wie siehst du diese Bestrebungen?

PI: Ich muss hierzu sagen, dass ich da relativ auf ihrer Seite [Aufsichtsbehörde SEC] bin aus zwei Gründen. Der eine ist, wenn man sagt, man will ein offenes System, man will Bitcoin, man will keine Überwachung, dann soll man nicht versuchen, Produkte anzubieten, die aber überwacht werden müssen. […] Man kann ja einen ETF mit Bitcoin oder Ethereum machen, aber das muss dann auch nicht an der Börse sein. Da gehen die zwei Sachen irgendwie ein wenig gegeneinander aufgrund der Grundvorstellung. Die andere Sache, dass sowas abgelehnt wird, ist, dass die Regulatoren gegebenenfalls nicht so offen sind, um so etwas zuzulassen. Hier bin ich nicht zu hundert Prozent einverstanden. Hier könnte man schauen, dass man auch etwas Anderes [an der Börse] anbieten kann. Denn ich glaube, dass Bitcoins nicht wirklich riskanter sind als andere Assets.

AM: Ethereum ist ein gutes Stichwort. Eines der vielen Blockchain Softwares, welche auf Blockchain aufsetzen oder die Philosophie dahinter nutzen, um eine Dienstleistung anzubieten. Wie arbeitet ihr im Blockchain Lab?

PI: Wir haben sehr viele Projekte auf Ethereum gemacht. Es gibt auch andere Alternativen aber Ethereum ist eine Initiative, welche schon sehr viel Liquidität aufweist. Und die Smart Contracts sind auch solche, die ausgeführt werden müssen. Die App Coins kannst du nicht von irgendeiner Quelle nehmen, dies muss schon klar geregelt sein. Und doch haben wir natürlich die guten und die schlechten Nachrichten zu Ethereum mitbekommen. Also wenn mal so ein Down (Exploit) wirklich stattfindet und ein Hard Fork gemacht wird, ist dies nicht das Beste. Ich bin der Meinung, dass es generell der falsche Weg war. Für Ethereum und dessen Weiterbestand war es unumgänglich doch das Vertrauen in das Projekt wurde extrem geschwächt. Wenn du sagst, Code is King, was im Smart Contract steht, hat globale Gültigkeit, dann soll dies auch so sein. Wenn dann jemand eine Schwachstelle findet und diese gezielt ausnutzt, dann soll dies auch so passieren. Man muss konsequent bleiben, auch wenn das für Ethereum der Untergang bedeutet hätte. Doch es wäre für

Blockchain ein positives Zeichen gewesen. Nachfolgende Projekte würden die Fehler kennen und ein besseres Produkt auf den Markt bringen. Man muss hinzufügen, dass dieser Vorfall nur sehr wenigen Personen bekannt war. Nur aktive Beobachter und Experten haben wohl davon mitbekommen.

AM: Welche Enabler würdest du identifizieren, welche den Einsatz von Blockchain begünstigen würden?

PI: Bestehende Prozesse zu verbessern, ist ein gutes Setting, um die Blockchain neben anderen Technologien einzusetzen. Man muss dabei bedenken, dass Blockchain nur einer von vielen Technologien ist, welche die derzeitigen Ineffizienzen von Prozessen verbessern kann. Es ist wichtig zu wissen, dass Blockchain nicht all deine Probleme im Leben lösen kann. Die Vorteile können sehr stark in einem Corporate Environment liegen, man kann sehr gut damit wie erwähnt Prozesse verbessern. Aber zwei Welten, von geschlossen zu offen, miteinander zu verbinden, ist sehr schwer und eventuell gar nicht wünschenswert. […] *Die Value Driver von Blockchain sind nach meiner Meinung: Intransparenz*: Ziemlich klar liegt der Vorteil bei der Transparenz, welche die Technologie mit sich bringt. *Automatisierung*: Dieser Vorteil wirkt besonders stark, da viele Prozesse derzeit noch nicht wirklich automatisiert sind. Mit den darauf aufbauenden Smart Contracts kann man auch komplexere Abläufe gut in eine Blockchain integrieren. *Sicherheit*: Ein Aspekt, den auch andere Technologien aufweisen. Doch die Blockchain hat dies sehr tief in den Ablauf integriert und integriert diese Sicherheitsaspekte sehr gut in die gesamte Technologie im Vergleich zu beispielsweise einem Backend System, auf dem du dann noch einen Security-Layer draufbaust. *Immutability*: Die Unveränderbarkeit von all den Transaktionen, welche in der Blockchain abgelegt sind, ist glaube ich auch sehr wichtig. In Bezug auf Banken kann man sagen, dass sie natürlich generell kein Interesse daran haben, dass die Transaktionen überhaupt geändert werden. Aber die Transparenz in diesen Transaktionsketten ist ein grosser Mehrwert und dass man schnell zugreifen kann auf die gesamte Kette mittels den angewendeten *Merkle-Trees*. Dies führt natürlich wieder zu einer Steigerung der Prozesseffizienz.

AM: Der Hype ist auch ein wenig dadurch gegeben, da viele Prozesse noch gar nicht automatisiert sind, würdest du dem auch zustimmen?

PI: Ich würde sagen, das ist der wichtigste Grund für den derzeitigen Hype um die Blockchain. Die Blockchain ermöglicht es das erste Mal, alles digital zu machen. Wirklich digital und nicht irgendwas offline digital nachzubilden und so einen unschönen Kompromiss einzugehen. Die Assets sind digitale Assets. Es ist eine End-to-end Digitalisierung des Prozesses. Und das ist das erste Mal, dass eine Techologie in der Kombination mit den Value Drivern diese Möglichkeit erlaubt. […] Ich sage immer, dass die Blockchain eine geniale Idee ist. Es nutzt existierende Elemente und kombiniert

sie zu einem genialen Ganzen das in sich perfekt ist. Das originale White Paper ist so simpel, es ist so schön.

AM: Wenn wir nun mal zu einem bereits von dir genannten Stichwort wechseln: Regulatorien und die dazugehörige Standardisierung. Es gibt immer mehr Technologien und Anwendungen, die verschiedene Derivate der Blockchain nutzen. Wie siehst du den Aspekt der Standardisierung in diesem Kontext?

PI: Es gibt sehr viele Ansätze, welche auch von Banken genutzt werden. Banken nutzen dabei zwei Schienen. Standardisierung ist sehr wichtig. Eine gute Standardisierung wirst du jedoch nicht hinkriegen. Viele Netzwerke sind demnach auch relativ «unstandardisiert». Vielleicht ist Blockchain ein Auslöser dieser grossen Standardisierung, vielleicht auch nicht. Man hat zwei Ansätze zur Entwicklung der Use Cases: Einerseits geht man in Konsortien, R3 als Beispiel aber auch andere versuchen gemeinsam mit anderen Partnern Lösungen zu diesem Problem zu entwickeln. Der grosse Nachteil davon: Es geht langsam, weil du Standardisierung erschaffen musst. Eine andere Lösung ist; du versuchst etwas selbst zu entwickeln, intern. Du schaust dir einen Prozess an, den du intern verbessern kannst und dir den Mehrwert gibt, um es auf Blockchain entwickeln zu können. Danach versuchst du, weitere Player von dieser Entwicklung zu überzeugen und ins Boot zu holen. Der Nachteil davon ist, dass die Blockchain Technologie nicht wirklich dafür ausgelegt ist, dass du alleine deine eigene Blockchain entwickelst. Zwischen den beiden Ansätzen gibt es Trade-offs und du musst schauen, was der Beste ist. […] JP Morgan ist jetzt auch weg aus dem R3 Konsortium und arbeitet an ihrer eigenen Lösung. Wir haben auch die Erfahrung mit dem R3 Konsortium gemacht. Du hast unglaublich viele Experten dort und einen grossen Meinungsaustausch. Aber die Projekte dann durchzusetzen, ist sehr schwer. Da muss ich sagen, bei der ganzen Blockchain Thematik wird es (die Ideen und Konzepte aus dem R3 Konsortium) sehr schwer, diese auf die einzelne Bank anwenden zu können. Denn hier geht es nicht mehr um die einzelnen technischen Aspekte, sondern eine Vielzahl an anderen Aspekten, die man erfüllen muss, um die Blockchain Technologie anzuwenden. […] Zum einen stellt sich die Frage, ob der Prozess, welchen man mit der Blockchain Technologie anpassen möchte, bereits digital ist. Wie sehr ist dieser eine Prozess dann auch integriert in die Prozesslandschaft des Geschäftsbereichs und danach kommen natürlich all die regulatorischen Aspekte, die zu berücksichtigen sind. Diese Linse muss man auch haben. […] Dann Volumen etc. (also technische Aspekte) die man auch mit der Blockchain Lösung erreichen muss. Es ist eine sehr flexible Technologie aber es bleibt immer noch ein Aspekt, der zu berücksichtigen sind. Speed wird mit Lightning sehr gut erfüllt. Die technischen Aspekte sind meist nie ein wirkliches Problem. Der echte Teil, welcher die Stopper für die Blockchain bringen, ist der Business Teil. Die Investitionen, welche notwendig sind, um die Einführung zu ermöglichen, den finanziellen Mehrwert, den die Technologie mitbringen muss, um als Business Case strategisch für das Unternehmen bestehen

zu können. Und dies nicht mal unbedingt aus Kotengründen. Kostenkalkulationen sind meiner Meinung nach ohnehin nicht oft da. Es gibt die verschiedenen Analysen von McKinsey und so, wie 80 Millionen oder Trillionen können mit der Technologie eingespart werden, ja… super. Bei sehr, sehr vielen Projekten, an denen wir gearbeitet haben, gibt es keine eindeutige Kostenkalkulation, die man auch so gebrauchen könnte. Es ist schwer, dies einzuschätzen. Das ist noch ein grosses Problem. Und es ist hoch komplex. Bei einer Zahlung ist es noch relativ einfach, die Kostenkalkulation zu machen. Da kennst die Kosten der Transaktion und kannst sie demnach ziemlich einfach aufrechnen. Bei komplexeren Prozessen hast du diese Basis meist nicht bzw. fehlen gute Zahlen, da du im Falle von Banken die Zahlen nicht aufgrund von Prozessen berechnen, sondern vom Input, den die Bank normalerweise dafür erarbeitet. Dementsprechend ist dieser Teil sehr wichtig, wie kannst du es verkaufen, was sind die politischen und institutionellen Treiber dahinter. Und diese Komponenten sind wichtig über die Etablierung der Blockchain. Meine Erfahrung zeigt auch selbst, dass es meist nicht an den technologischen Aspekten lag, sondern immer an den anderen Komponenten, die eine Einführung der Blockchain Lösung erschwerten oder gar verunmöglichten.
Ein weiterer Aspekt: Wie integriert ist ein Prozess, dies gehört für mich auch zum Business Teil und löst auch meist politische Diskussionen aus.

AM: Wie würdest du für eine Analyse der möglichen Prozesse zur Umsetzung in Blockchain dann vorgehen?

PI: Ich würde mit ganz kleinen Use Cases starten. Das sind dann die Proof-of-Concepts für die einzelnen Unternehmen. Dabei handelt es sich um MVPs (Minimal viable Product). In einem zweiten Schritt kann man dann auch das grössere System an sich mit Blockchain optimieren. Von Grund auf das Grosse zu ersetzen, das geht nicht.

AM: Daneben gibt es natürlich dich anderen Players, wie es derzeit die Startups sind. Neu auf dem Markt haben sie keine Legacy, welche sie in die neuen Prozesse integrieren oder ersetzen müssen. Wie kann sich ein etabliertes Institut gegen solche Konkurrenten behaupten?

PI: Ich glaube sehr stark, dass Banken sich sehr schwer tun, die Technologie zu nutzen und sich anzupassen. Da hast du genau diese kleinen Unternehmen, die jedoch grosse Probleme damit haben, das Vertrauen der Leute zu gewinnen. Was witzig ist, da Blockchain kein Vertrauen braucht. Du merkst trotzdem, dass Menschen nicht ganz so ticken. Die erste Frage bei Bitcoin zum Beispiel ist: Wer reguliert Bitcoin. Niemand. Und dann habe ich von vielen Leuten gehört, dass es somit nichts für sie ist. Die Thematik, warum es schwer ist, Blockchain in der Bankenwelt einzusetzen, ist ja nicht deswegen so, weil wir schlecht sind im technologischen Bereichen. Klar, es gibt auch politische Einflüsse. Aber das ganze System ist mittlerweile so komplex geworden. Das alles nachzubilden, ist sehr schwer für kleine Unternehmen. Und wenn mans nachbilden will, kommt man in die gleichen Probleme rein, wie es heute schon die Banken haben. Das man Regulatorien beachten

muss, dass man so und solche Prozesse zusätzlich machen muss. Deshalb findet man derzeit Startups nur in den Bereichen, wo sich solche Probleme nur begrenzt abzeichnen. Zahlungsverkehr ist ein Beispiel, aber auch selbst da ist es relativ schwer. Aber ich hoffe, dass es Startups geben wird, welche sich durchsetzen werden. Jetzt sehe ich es noch nicht, da das Vertrauen in die Technologie noch nicht gegeben ist. Der Markt ist noch nicht soweit und sie haben demnach auch noch keine Kunden für ihr Geschäftsmodell. In fünf bis zehn Jahren könnte es aber so weit sein.

AM: Wie schätzt du den Einfluss der Blockchain in unserem Leben heute und in fünf Jahren ein?

PI: Der Einfluss selbst ist heute noch ziemlich begrenzt. Aber genau heute hat man den Hype, man muss ihn nutzen, um die Etablierung von Blockchain für die Zukunft zu sichern. Bitcoin war ein super Produkt – es war ein Proof-of-concept. Diesen Drive muss man jetzt nutzen, so dass es sich auch langfristig durchsetzen wird und die Leute nicht das Interesse daran verlieren.

AM: Abschliessend: Gibt es Punkte, welche Sie noch gerne zur Thematik Blockchain und Anwendungsfelder erwähnen möchten? Persönliche Sichtweisen, Favorisierte Anwendungsfelder etc.

PI: Ich glaube, alle Use Cases die man sich jetzt anschaut, sind nicht die Use Cases, die später sehr disruptiv sein werden. Ich habe viel interessante Anwendungsfälle gesehen, ausserhalb des Bankenbereichs. Es ist bei sehr vielen Technologien so. Was du am Anfang denkst, wozu es gut ist, ist meist nicht das, wozu es dann wirklich super gut ist. Es gibt noch nicht die Killer-App für Blockchain. Ich glaube, der interessanteste Teil wird wo anders liegen.

Master Thesis | **Die Blockchain Technologie und ihre Anwendungsfelder**

Autor: **Anand Paul Mooken**

Interviewleitfaden

Experteninterview mit Lucas Silva

Zürich, den 03.05.2017

Vorname, Name	*Lucas Silva*
Position	Software Engineer
Unternehmen	Ergon Informatik AG Merkurstrasse 43 8032 Zürich
Kontakt	Mail: lucas.silva@ergon.ch
Selektionskriterien	Aktiver Beobachter der Blockchain Technologie mit Beteiligung am github Repository der Community

Forschungsfragen:

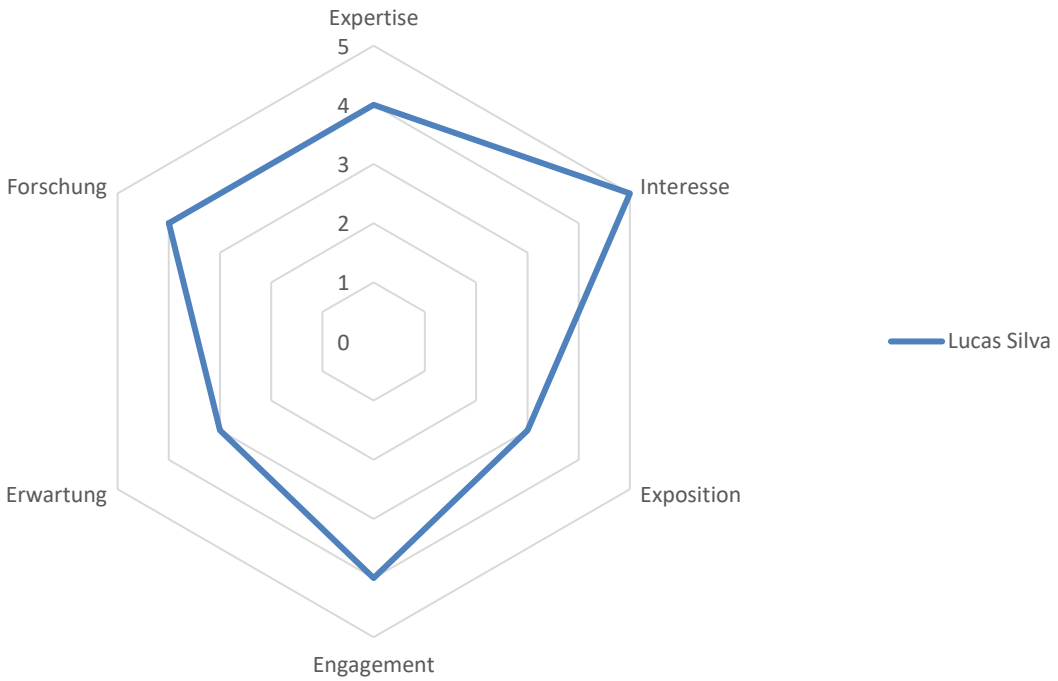
Was ist der Status Quo von Blockchain Technologie?

Wo liegen aktuell die Anwendungsfelder der Technologie?

Was sind mögliche Implikationen der Anwendung der Blockchain Technologie?

Wie können potenzielle Anwendungsfelder für die Blockchain Technologie systematisch identifiziert werden?

Profil der Interviewpartner im Kontext Blockchain:



Legende: Expertise = Wissen über Blockchain; Interesse = .. zum Thema Blockchain; Exposition = Aktivitäten zum Thema Blockchain; Engagement = Geschäftliche Interaktion mit Blockchain; Erwartungen = .. an Blockchain; Forschung = .. zum Thema

Lucas Silva hat einen Master of Science ETH in Computer Science und arbeitet als Senior Software Engineer seit 2011 für das Unternehmen ergon Informatik. Als Software Engineers hat er sich insbesondere mit der technischen Thematik der Blockchain befasst und kennt deren Vor- und Nachteile. In seinen Arbeiten hat er bereits einige Selbstversuche mit der Technologie gemacht und hat eine eher skeptische Sichtweise. Seine Recherchen haben sich insbesondere auf die Bitcoin fokussiert. Die Erkenntnisse lassen sich jedoch oft auf die Blockchain zurückschliessen.

Das Interview fokussiert auf technische Aspekte der Blockchain und geht insbesondere auf die Limitationen der Technologie ein.

Transkript:

Anand Mooken: Hallo Lucas. Vielen Dank, dass du dir die Zeit nimmst, mit mir über die Blockchain Technologie zu sprechen. Kannst du mir etwas zu deiner Person und der Funktion bei ergon Informatik sagen?

Lucas Silva: Ich selbst bin Software Engineer und meine Tätigkeiten liegen hierbei in der Weiterentwicklung unseres Software Portfolios aber auch in der Erforschung von neu aufkommenden Technologien, wie es die Blockchain ist. […] Wir arbeiten derzeit in einem Lab daran, zu evaluieren, ob sich der Einsatz einer Blockchain lohnen würde oder nicht. Es gibt schon etliche Startups, welche sich mit der Blockchain beschäftigen.

AM: Offene Frage: Was ist die Blockchain für dich:

LS: Es ist schwierig. Es gibt die public Blockchain sowie die private Blockchain. In meiner Sicht ist es eine Technologie, die einen Standard für Transkationen definieren möchte. In einer öffentlichen Blockchain hat man sehr viel mehr Features, die man verwenden kann im Vergleich zu einer geschlossenen Blockchain, die zum Beispiel eine Bank verwendet. Es ist ein Standard, mit welcher man Transaktionen in der Finanzbranche kontrollieren kann.

AM: Stichwort Standard: Wie siehst du es mit der Standardisierung?

LS: Standards sind immer positiv. Es macht die Entwicklung einfacher sowie die Kommunikation. Aber am Beispiel des Internet Explorers sieht man sehr gut, dass solche Standards nicht immer befolgt werden. Im Finance ist es gar schwieriger, solche Standards zu definieren und durchzusetzen. Ich glaube, dass die Incentives in diesem Bereich nicht so gross sind, um solche Standards zu definieren.

AM: Blockchain wurde mit Open-Source Gedanke eingeführt. Nun versuchen insbesondere Banken, sich des Systems zu ermächtigen, in dem proprietäre Lösungen entwickelt werden. UPDATE: Wurde nun open-source gemacht. Wie stehen Sie dieser Entwicklung als Zahlungsanbieter gegenüber?

LS: In meiner Recherche habe ich festgestellt, dass die Bank of America beispielsweise bereits 20 Patente zur Blockchain angemeldet hat. In einer private Blockchain ist ein Standard noch schwieriger zu definieren.

Die ganze Blockchain ist offen und Community-getrieben. Die Banken haben versucht, das Konzept als geschlossene Technologie voranzutreiben. Es wiederspricht der Philosophie von Blockchain. Und trotzdem funktioniert dieser Ansatz für Banken natürlich nicht. Denn es ist in ihrem Interesse, dass es zentralisiert und geschlossen angewendet wird. Es gibt eine grosse Challenge hier. Wenn die Blockchain nicht open-source ist und auch nicht P2P, dann stellt sich die Frage ob die Vorteile

der Blockchain noch bestehen werden, insbesondere im Vergleich zu anderen Technologien. Es würde nicht so gut skalieren, wie es heute eine Datenbank schon tut.

AM: Wo siehst du denn die Probleme, die sich ergeben würden, wenn eine Bank entgegen der Abschottung in eine geschlossene Blockchain denn doch für eine public Blockchain entscheidet?

LS: Das ist eine interessante Frage. Man müsste sich zunächst diversen Herausforderungen stellen. Ethereum zum Beispiel speichert Smart Contracts. Es ist jedoch nicht dynamisch. Ich glaube, dass es unmöglich sein wird, einen solch statischen Contract nur einmal ganz zu Beginn zu definieren. Und hier kommt der Ethereum Hack ins Spiel. Denn hier wurde ein statischer Contract mit einem Exploit gehackt. Doch der Grundsatz der Blockchain im Kontext der Immutability besagt, dass auch in diesem Fall der Contract mit all seinen Schwächen ausgeführt wird, und nicht wie passiert, ein Hard Fork gemacht wird und somit die Gültigkeit des Smart Contracts untergraben wird. Es gibt Ansätze, wie man diese Problematik lösen könnte. Zum einen soll die genutzte Sprache in den Smart Contracts, bei Ethereum ist es Solidity, mehr formalisiert, so dass man beweisen kann, dass der Contract richtig geschrieben wird und trotzdem im Falle von Schwachstellen reagieren kann. Trotzdem ist und bleibt es sehr schwierig, einen Vertrag einmal und von Anfang an korrekt aufzusetzen.

AM: Hätte man dort also keinen Hard Fork machen sollen, sondern die Konsequenzen tragen müssen?

LS: Ich bin kein echter Fan der Immutability. Aber das ist die Philosophie von Blockchain. Ich bin demgegenüber skeptisch. Bei einem einfachen Contract wird das wohl noch funktionieren, aber wenn wir Hunderte von Banken und Leuten haben, die einen eigenen Smart Contract programmieren müssen, dann wird es sicher zu weiteren solchen Schwachstellen kommen. Hier gibt es aber bereits Alternativen. Es gibt Smart Contracts, welche die Möglichkeit anbieten, die einzelnen Klauseln mittels Update zu verändern. Hier gibt es Möglichkeiten, die Smart Contracts zu referenzieren, und so notwendige Mutationen vorzunehmen. Aber das sind alles Workarounds und man sollte diese nicht wirklich einsetzen. Denn man sollte Immutability unterstützen oder eben nicht.

AM: Wo siehst du dann weitere Herausforderungen, welche noch zu lösen sind?

LS: Bei der public Blockchain gibt es […] Herausforderungen. Zum einen der ganze Konsensautomatismus. Bei Proof-of-Work liegen mehr als 60 Prozent der Full Nodes in China. Nicht nur wegen den günstigen Strompreisen, sondern auch wegen den Anforderungen an der CPU. Als Alternative gibt es dann noch den Proof-of-Stake, aber auch Proof-of-Space, statt Arbeit muss man nur beweisen, dass man z.B. 2 GB Speicherkapazität hat. Dann ganz neu ist das Konzept der Proof-of-time, die aus der Forschung kommt. Hier gibt es einen Satelliten auf dem Mond mit einer entsprechenden Encryption und man muss beweisen, dass man den Roundtrip über das All gemacht hat. Es ist insofern effizienter als die anderen Konzepte, da man keine Ressourcen wie Strom verschwenden

muss. Zum Beispiel nutzt Bitcoin mit Proof-of-Work mehr Strom als Irland. Ohne das man den Grossteil des Verbrauchs in Produktivität umsetzten würde. Es geht hier nur um den Beweis, dass man den Block erstellen darf. Wasted energy! Eine weitere Herausforderung sind die Smart Contracts an sich und insbesondere die Sprache, mit denen sie kodiert werden. Die Ansätze mit Javascript oder Solidity [Smart Contract Coding Sprache von Ethereum] sind noch nicht schnell genug. Ich habe in Studien zudem gelesen, dass mehr als 40 Prozent der Smart Contracts verwundbar sind und durch Exploits gehackt werden können. […] Auf Ethereum wollte ich in einen Proof-of-Concept machen. Doch ich konnte den Client nicht in unserem Browser nutzen. Wir mussten einen Browser von Ethereum nutzen. Sie bauen alle ein eigenes Framework und das macht es schwieriger. Dies ist aber ein Ehtereum spezifisches Problem. Eine weitere Herausforderung ist die Skalierbarkeit. Es skaliert noch nicht so gut wie es bereits etablierte Technologien können. So habe ich den Vergleich der derzeit führenden Blockchain Anwendungen mit dem Visa Network gemacht. Und man sieht, dass das verarbeitete Transaktionsvolumen der Blockchain Anwendungen stark unterhalb dessen liegt, was mit dem Visa Network möglich ist. Juno war noch einer der besten Blockchain basierten Anwendungen. Trotz allem ist es noch lange nicht auf dem Niveau, wo Visa mit ihrem Visa Network liegt. Dort können mehr als 100 000 Transaktionen pro Sekunde verarbeitet werden. Eine weitere Herausforderung: Die Zentralisierung des dezentralen Netzes. Verschiedene Regionen der Welt weisen eine bessere Performance auf als andere. So gibt es eine implizierte Zentralisierung des eigentlich dezentralen Bitcoin Ökosystems. Die Anzahl stalled Blocks [erzeugte, aber nicht genutzten Blöcke] die sich dadurch ergeben, sind in einer Statistik zusammengefasst. So gibt es eine grosse Anzahl von verschwendeten Ressourcen.

AM: Ich gehe nochmals zurück zu einem der ersten Herausforderungen, die du zuvor genannt hast. Nämlich der verschwendeten Energie durch den Proof-of-Work Ansatzes. IBM arbeitet mit ihrem Produkt – Hyperledger – an einem Ansatz des Konsenses, welcher keine Incentives mehr anbietet, weshalb auch der Proof-of-Work Ansatz durch den Proof-of-Stake geändert wird. Ist dies nicht schon eine Lösung zu der genannten Herausforderung?

LS: Hyperledger hat den Fokus auf das Business. Hier hat das Modell der Incentivierung von der Blockgenerierung keinen grossen Stellenwert wie es das bei Bitcoin hat. Man muss also immer wieder die Trennung zwischen der private und der public Blockchain machen. Bei einer privaten und somit geschlossene Blockchain fallen viele Faktoren wie die Incentivierung zur Transkationsverarbeitung weg. Das Business selbst hat bereits einen grossen Anreiz durch die Anwendung der Blockchain als Prozessoptimierung. Und es eröffnen sich auch viele alternative Möglichkeiten anstelle der Incentivierung, wenn man von der Nutzung der Blockchain als Kryptowährung absieht. In diese Richtung gibt es viele Ansätze, an denen derzeit geforscht wird. […] Intel hat aber ebenfalls

eine Lösung des Problems. Es wird beispielsweise bei der XBOX von Microsoft verwendet und findet Anwendung im SecureBoot. Es handelt sich dabei auch um den Ansatz des Proof-of-Time kombiniert mit weiteren Elementen. […] Aber letztendlich konnte dieser Prozess doch noch geknackt werden, als ein Hacker mittels den Supercomputern des MIT die notwendige Rechenleistung zu eigen machte.

AM: Für ein Unternehmen wird man wohl eher die private Blockchain nutzen. Was wären denn die Anwendungsfälle für eine public Blockchain?

LS: Dort hat man noch einige Herausforderungen. Immer, wenn man heute eine Transkation vollzieht, benötigt man einen Mittelmann. Hier hat man den Vorteil, dass man mit der Blockchain P2P Transaktionen ganz ohne Mittelmann durchführen kann. Und es gibt Kosten sowie Zeitgewinne. Die Bitcoin Macher propagieren, dass man ohne grossen Aufwand Geld länderübergreifend und kosteneffizient übertragen kann. Doch in der Praxis reagieren nun auch die einzelnen Länder auf diese Entwicklung und setzen Auflagen durch, die diese Transaktionen limitieren. Am Ende ist es dann doch nicht so eine freie Währung. Und sobald es dann wirklich um Themen wie Geldwäscherei oder Steuerhinterziehung geht, dann wird es noch kritischer. Und ein weiteres Problem der Kryptowährung ist die Volatilität. Wie man dieses Problem lösen kann, ganz ohne Zentralbank, ergibt sich mir nicht. […] Die Blockchain kann aber gut eingesetzt werden in Bereichen, in denen das P2P Konzept umgesetzt werden kann. […] Die Blockchain kann jedoch auch noch für einen anderen Use Case genutzt werden, dem des Content Payments. Nehmen wir zum Beispiel ein Youtube Video. Beim Anschauen des Videos wird dir ein gewisser Betrag von deiner Bitcoin Wallet abgezogen.

AM: Die Probleme referenzieren stark auf die Verwendung der Blockchain für eine Kryptowährung als einer der Use Cases. Doch wie kann eine Blockchain für vollkommen andere Anwendungsfälle eingesetzt werden? Nehmen wir als Beispiel das Wählen.

LS: Ich komme ja aus Brasilien, wo man seit kurzem auch ein eVoting System nutzt. Ich habe mich dabei immer gefragt, weshalb dies nicht auch schon in anderen Ländern eingesetzt wird. Das Problem ist, dass die Menschen super skeptisch gegenüber elektronischen Wahlsystemen sind. Sie denken, dass man hier noch einfacher Manipulationen vornehmen kann. Die Frage hier ist, wie man die Leute überzeugen kann, das Blockchain wirklich sicher sind. Für eine Wahl eines Präsidenten werden die Leute wohl noch zu skeptisch sein, um die Technologie als solches zu akzeptieren. Da braucht es noch einiges an Überzeugungsarbeit. […] Wenn man aber andere Use Case in Betracht zieht, fällt mir der Einsatz von elektronischen Zahlungssystemen in Afrika auf. Die Leute leben sehr verteilt und haben nicht überall die Möglichkeit, ein Konto zu eröffnen oder Geld abzuheben. Hier arbeiten Unternehmen bereits daran, die Blockchain als Lösung zu implementieren. Hier überzeugt die Blockchain durch ihre Accessability [niemand wird ausgeschlossen, jeder kann teilnehmen]. […]

Aber auch die Eigenschaft der Transparenz ist sehr interessant. Denn in Amerika gibt es einen Anwendungsfall, bei dem die Parteispenden veröffentlicht werden. Dies zeigt einmal mehr auf, dass die Technologie dort eine grosse Wirkung zeigt, wo zuvor bereits ein hohes Misstrauen herrschte und Blockchain somit einen grossen Mehrwert bietet.

AM: Siehst du Gründe oder direkte Probleme, die den Einsatz der Blockchain jedoch verhindern könnten?

LS: Privacy. Momentan ist die Blockchain aus technischer Sicht nicht wirklich anonym. Neben den bereits erwähnten Herausforderungen wie eine bessere Lösung zum Proof-of-Work Ansatz ist es auch die Volatilität. Die Idee von Blockchain ist, dass sie offen und transparent ist. Aber für viele Use Cases brauchen wir die Privacy. Das geht leider nicht. Es ist das Gleiche wie bei Skalierbarkeit und Dezentralisierung. Beides kann man nicht auf einmal haben. Da gab es 2015 einen grossen Streit über die Blocksize. Die einen wollten eine grössere Blocksize und die anderen wollten dadurch nicht die Dezentralisierung riskieren. Dies führte zu einem Hard Fork. […] Da sieht man, dass es nicht immer leicht ist, eine Lösung zu finden. Zurzeit ist das ganze ja auch noch open-source und von der Community getrieben. Wenn wir diese Philosophie zugunsten gewissen Anforderungen von Anwendungsfällen verwerfen… Finden sich dann noch Leute in der Community, die diesen Ansatz unterstützen würden?

AM: Viele Drittanbieter wie Banken wie auch Bösen könnten durch Blockchain obsolet werden. Siehst du dies als mögliches Szenario an?

LS: Dies ist sehr gut möglich, ich glaube an ein solches Szenario. […] Jede grosse Transaktion birgt ein Risiko. Wenn man es in einem Smart Contract verpackt, liegt das Risiko voll darin. Aber ich glaube auch, dass man für gewisse Dinge trotz allem eine Drittpartei brauchen. Wenn man mal ein heutiges Beispiel nimmt. […] Man möchte eine Hypothek abschliessen. Ich bin ein Software Entwickler und verstehe nicht wirklich viel davon. Man beauftragt deshalb eine Drittpartei um das Knowhow hinzuzuholen. Man versteht den Inhalt des Vertrags nicht und dies kompensiert man, indem man eben diese Drittpartei involviert. Für komplexere Geschäfte wird es demnach auch bei Drittparteien bleiben.

AM: Würdest du der Hypothese zustimmen, dass man somit auch mit den weniger komplexen Prozessen beginnen wird, auf Blockchain umzustellen?

LS: Genau! Dies ist der einfachste Weg, die Blockchain ohne grosse Risiken anzuwenden. Mit fortschreitender Entwicklung können dann nach und nach auch komplexere Use Cases umgesetzt werden. […] Ich habe in verschiedenen Arikeln gelesen, dass revolutionäre Technologien auch jeweils sehr lange brauchen, bis sie effektiv eine disruptive Wirkung im Markt erzielen. Hier reden gewisse von sieben oder mehr Jahren. Danach wird es [die Entwicklung, die Umsetzung] jedoch sehr schnell

explodieren […] Zurzeit gibt es viele Working Forces und Experten, die sich mit der Blockchain befassen, doch man braucht zunächst einen wirklich guten Use Case, der dann auch sauber funktioniert, damit man weitere Unternehmen zum Einsatz der Technologie motivieren kann. Dies sehe ich heute noch nicht als gegeben. Die meisten Use Cases, die ich zurzeit beobachte, sind vor allem in der Privatwirtschaft und wiedersprechen sich zum Teil sehr stark mit der Philosophie der eigentlichen Blockchain. Wir haben noch keine Working Force, die sich mit einem guten Use Case beschäftigt. Somit fehlt ein Leader.

AM: Abschliessend: Gibt es Punkte, welche du noch gerne zur Thematik Blockchain und Anwendungsfelder erwähnen möchtest? Persönliche Sichtweisen, Favorisierte Anwendungsfelder etc.

LS: Es gibt sehr grosse Investitionen in die Technologie, aber das Potenzial wird erst aufgezeigt, wenn es einen guten Use Case gibt, an denen sich weitere orientieren können. Ich glaube stark an die Idee der Smart Contracts. Die Transaktion mit Blockchain jedoch nicht. Es gibt viele Technologien, welche eine sehr viel höhere Leistung aufweisen als die Blockchain. Aber Smart Contracts führen zu effizienteren Automatismen, welche einen grossen Vorteil für alle bringt. Man kann letztendlich auch einzelne technische Komponenten, welche der Blockchain zugrunde liegen, einsetzen, und schon einen grossen Mehrwert liefern. Dies trifft auch auf einen Smart Contract zu. Aber handelt es sich dann noch um eine Blockchain im eigentlichen Sinn?

Des Weiteren interessiert es mich stark, was passiert, wenn bei der Bitcoin alle Bitcoins geschürft wurden, es ist ja limitiert auf 21 Millionen Bitcoins. Die Theorie sagt, dass die Anzahl aller Transkationen in diesem Fall genug Bitcoins fliessen lassen, um die Miner weiterhin für ihre Aufwände zu vergüten und somit zu motivieren.

Master Thesis | **Die Blockchain Technologie und ihre Anwendungsfelder**

Autor: **Anand Paul Mooken**

Interviewleitfaden

Experteninterview mit Karin Frick

Zürich, den 10.05.2017

Vorname, Name	*Karin Frick*
Position	Leiterin Research und Mitglied der Geschäftsleitung
Unternehmen	Gottlieb Duttweiler Institute Langhaldenstrasse 21 Postfach 531 CH-8803 Rüschlikon/Zürich
Kontakt	Mail: karin.frick@gdi.ch Telefon: +41 44 724 62 40
Selektionskriterien	Analysiert Trends und Gegentrends in Wirtschaft, Gesellschaft und Konsum derzeit in Kollaboration mit IBM die Blockchain

Forschungsfragen:

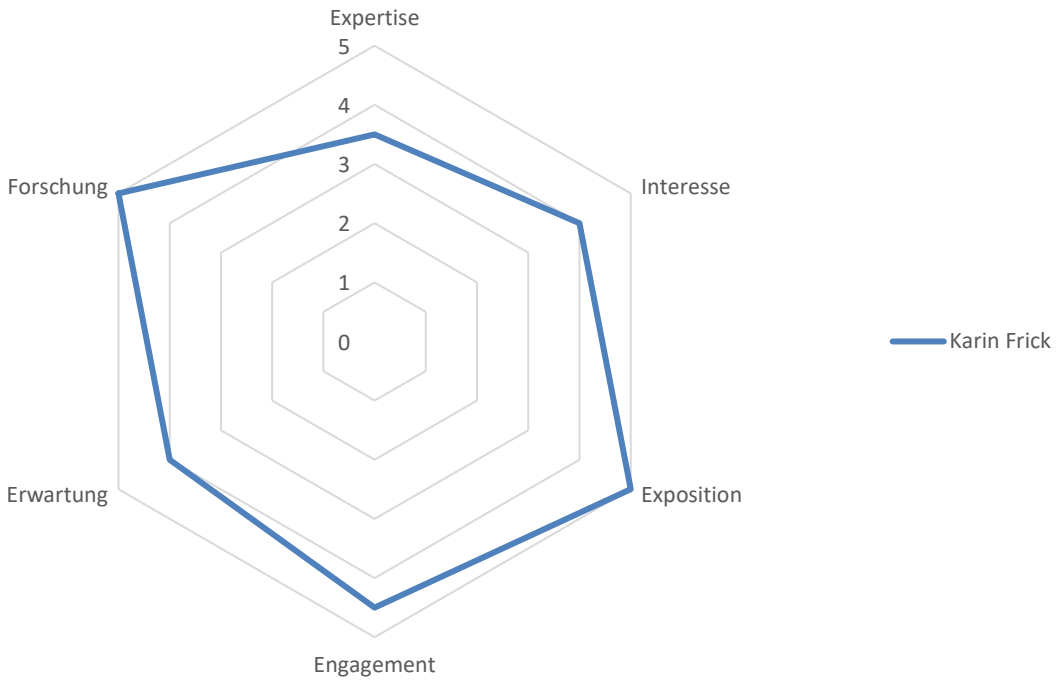
Was ist der Status Quo von Blockchain Technologie?

Wo liegen aktuell die Anwendungsfelder der Technologie?

Was sind mögliche Implikationen der Anwendung der Blockchain Technologie?

Wie können potenzielle Anwendungsfelder für die Blockchain Technologie systematisch identifiziert werden?

Profil der Interviewpartner im Kontext Blockchain:



Legende: Expertise = Wissen über Blockchain; Interesse = .. zum Thema Blockchain; Exposition = Aktivitäten zum Thema Blockchain; Engagement = Geschäftliche Interaktion mit Blockchain; Erwartungen = .. an Blockchain; Forschung = .. zum Thema

Karin Frick befasste sich seit mehr als 20 Jahrenin verschiedenen Funktionen mit Zukunftsthemen, gesellschaftlichem Wandel, Innovation und Veränderungen von Menschen und Märkten. Nach ihrem Studium an der Universität St. Gallen (HSG) war sie als Chef-Redaktorin der renommierten Vierteljahresschrift «GDI Impuls» und als Geschäftsführerin der Schweizerischen Vereinigung für Zukunftsforschung (swissfuture) tätig. Im Auftrag namhafter Firmen analysierte sie Trends im Konsumgüter- und Dienstleistungsbereich (Gottlieb Duttweiler Institute, 2017). Im Rahmen der im Juni 2017 stattfindenden Blockchain Valley Conference vom Gottlieb Duttweiler Institute ist sie selbst als Referentin neben Blockchain Experten wie Alex Tapscott auftritt und über die Blockchain spricht.

Das Interview fokussiert auf gesellschaftliche Implikationen der Blockchain.

Transkript:

Anand Mooken: Sehr geehrte Frau Frick, vielen Dank das Sie sich die Zeit nehmen, mit mir über die Blockchain Technologie zu sprechen. Können Sie mir etwas zu Ihrer Person und der Tätigkeit beim Gottlieb Duttweiler Institut sagen?

Karin Frick: Sehr gerne. Ich bin Karin Frick und mache schon seit vier Jahren Trend- und Zukunftsforschung. Das ist branchenübergreifend, es geht darum, wie sich gesellschaftliche Strukturen insgesamt verändern. Dabei betrachten wir die Wertvorstellungen und Verhaltensweisen von Menschen und wie sich diese durch verschiedene zukünftige Faktoren ändern könnten. Es ist insbesondere dort spannend, wo sich Gegebenheiten verändern und konvergieren.

AM: Was ist für Sie die Blockchain und wo sehen sie diese heute?

KF: Es ist eine Kommunikations- und Transaktionstechnologie. Dabei rede ich spezifisch von Blockchain und nicht von Bitcoin, welche mittels der Währungen noch viele weitere Definitionen benötigen würde. Blockchain ist also eine Technologie, die es ermöglicht, neue Transaktionen zu machen, ohne einen Mittelmann zu benötigen, wie man dies von traditionellen Transaktionen kennt. Dabei arbeitet es mit einem verteilten Netz, was ebenfalls eine andere Logik ist, die mitunter schwerfällt, zu verstehen. […] Es ist ein System ohne einen Chef. Dies kann man auch als eine soziale Innovation verstehen, denn es führt zu einer neuen Art der Denkweise. Heute hat sich ein gewisses Mass an hierarchischem Denken in unseren Köpfen manifestiert und wir handeln auch mehrheitlich danach.

AM: Wie schätzen Sie den Einfluss der Blockchain in unserem Leben heute ein (1-5, wobei 5 stark ist)?

KF: Heute hat die Blockchain noch keinen Einfluss auf unser Leben, somit würde ich hier auf eine eins gehen. […] Es ist wie bei den Computern. Wir haben erst nach und nach den Einsatz von diesen Hilfsmitteln angenommen und bestehende Aktivitäten dadurch effizienter gestaltet. Und die Blockchain befindet sich am Anfang seiner Entwicklung und muss sich erst noch beweisen.

AM: Wie schätzen Sie den Einfluss der Blockchain in unserem Leben in 5 und 10 Jahren ein (1-5, wobei 5 stark ist)? Und weshalb?

KF: In fünf Jahren wird die Blockchain sicher einen Einfluss auf unser Leben haben. In diesem Zeitraum wird die Technologie definitiv in manchen Bereichen einen disruptiven Einfluss nehmen und befindet sich in der heissen Phase. Da passiert etwas. Aber in zehn Jahren wird die Technologie ihren Platz in unserer Umwelt gefunden haben und nicht wirklich weiter auffallen, wie dies schon vielen technologischen Innovationen wiederfahren ist. Die Menschen werden nicht mehr darüber nachdenken, ob sie mit der Blockchain in Berührung kommen oder nicht. Es wird sich nach ihrer

Etablierung wohl einfach wie vieles in unserem Leben als selbstverständlich einordnen. Es ist jeweils aufregend, wenn etwas abgelöst wird, aber nachdem sich das Neue etabliert hat, lässt das Interesse entsprechend nach.

AM: Blockchain als Begriff ist derzeit in aller Munde. Sehen Sie diesen Hype als berechtigt an?
KF: Das ist eine sehr interessante Frage. Das gesamte Potenzial der Blockchain leitet sich daraus, dass es gewisse Prozesse sicherer, kosteneffizienter und schneller machen kann. Es wird jedoch dort interessant, wo die Technologie bestehende Prozesslandschaften verändern kann. Beispielsweise gibt es heute eine Plattform namens Open Bazaar. Es handelt sich um eine Handelsplattform, in dem die Produzenten die Ware direkt an den Endverbraucher verkaufen können, ganz ohne Mittelmann. Im Gegensatz zu den klassischen eCommerce Plattformen fehlen viele Prozesse zwischen den einzelnen Intermediären wie Zwischenhändler oder Bank, womit es nur noch zwei Partner im Geschäft gibt: Der Produzent und der Verbraucher. Die Aktivitäten der Intermediäre gehören zum Selbstverständnis der heutigen Gesellschaft. Doch neue Formen werden entstehen, an welche sich die Gesellschaft aber zunächst noch gewöhnen muss. Ein System ohne Zentralorgan, wie es heute Banken wie auch staatliche Institutionen bilden, ist heute noch schwer vorstellbar.
AM: Viele Drittanbieter wie Banken wie auch Bösen könnten durch Blockchain obsolet werden. Sehen Sie dies als mögliches Szenario an?
KF: Also rein vom Mechanismus her ist dies sehr gut möglich. Letztendlich aber geht es um Organisationsprinzipien und es gibt schon Systeme, welche ganz ohne Chef und Zentralorgan auskommen. Und wir denken ja auch so. Denn es gibt im menschlichen Gehirn nicht eine Zellenhoheit, welche letztinstanzlich über unsere Gedanken verfügt. Das Gehirn ist auch ein Netzwerk, welches seine Gedanken über mehrere Nervenzellen ordnet und organisiert. Gedanken entstehen demnach auch durch die Verknüpfung aller Bereiche und hier gibt es keine übergeordneten Neurone – quasi eine Chef-Neurone, welche als zentrale Institution handelt. Und der Ansatz von selbstgesteuerten Systemen erleben wir auch in der Natur im Allgemeinen. Nehmen wir einen Ozean. Dieses Ökosystem funktioniert trotz Fehlen einer zentralen Steuerung und ganz ohne Chef.
AM: Sie sprechen hier von einer der disruptiven Eigenschaften der Blockchain oder einer disruptiven Entwicklung, welche durch die Blockchain verstärkt wird?
KF: Sie kennen ja die Darstellung mit dem Netzwerk, dem verteilten Netz. Und dann stellt sich die Frage, wie sich das Netz steuert. Es steuert sich selbst. Das heisst, Selbstorganisation ist auch kein neues Thema. Aber mittels der Blockchain lässt sich dieses System technisch implementieren. Und wenn dies möglich wird, dann wird auch der Mensch möglicherweise seine Denkweise neu ausrichten. Es entstehen neue Ordnungsformen und das finde ich sehr spannend. Als Beispiel dafür

lässt sich der Wandel der Kommunikationsform erwähnen. Früher haben wir alles über Papier gemacht, da gab es die elektronischen Formen noch nicht. Dabei haben wir uns auch an den Postträger gewöhnt. Doch mit den heutigen technologischen Mitteln können wir eine direkte Kommunikation aufrechterhalten und sind nicht weiter angewiesen auf einen Intermediär, wie es in diesem Beispiel die Post ist. Doch die Post gibt es noch immer. Also kann man nicht unbedingt sagen, dass wir ganz auf Drittanbieter wie Banken und Börsen in Zukunft verzichten müssen bzw. können, nur werden die Aufgabengebiete solcher Drittanbieter zukünftig mit der Anwendung der Blockchain Technologie wohl ein wenig anders ausfallen. Und auch die Post hat letztendlich viele Filialen bereits geschlossen. Die Frage ist wohl eher, ob die Gesellschaft die neuen Muster auf gewisse gesellschaftliche Systeme übertragen kann, wo dann anders funktionieren zu dem was wir heute kennen.

AM: Was Sie sagen, klingt aber nach einer sehr utopischen Vorstellung.

KF: Ganz klar, es ist utopisch. Man muss aber bedenken, dass die Leute, welche die Innovation erfunden haben, eben nicht Banken oder andere zentrale Institutionen waren. Es sind Menschen, die einen revolutionären Charakter haben und damit einen solchen Umbruch verwirklichen wollen. Die Banken haben da nur die Entwicklungen gesehen und sind auf den Zug mitgesprungen, natürlich mit ihren eigenen Intentionen.

AM: Gehen wir mal von der Hypothese aus, dass sich die Blockchain durchgesetzt hat. Wo sehen Sie potenzielle Probleme, die sich dadurch ergeben könnten?

KF: Naja, wenn sie ein altes System durch ein neues ablösen, kann oder wird dies fast immer zu Problemen führen. Das neue System ist dann wohl noch nicht unbedingt das perfekte System, aber es kann sich zu solch einem entwickeln. Als Beispiel kann man hier die Digitalfotografie und Kodak nehmen. Da kam es zunächst auch erst zu einer sehr langsamen Transformation mit vielen Kinderkrankheiten doch letztendlich konnte sich die neue Form des Fotografierens behaupten. So wird es auch mit der Blockchain sein. Man wird sehen, dass Prozesse gestützt durch Blockchain kosteneffizienter und schneller arbeiten und dabei weniger Ressourcen benötigen. In dieser Entwicklung gibt es dann erste etablierte Unternehmen, welche dieser Entwicklung unterliegen und vom Markt verschwinden werden. Dies ist sozusagen der erste Stress der Einführung von Blockchain. Jedoch entstehen auch neue, effizientere Unternehmen am Markt. Dabei wird man die gleichen oder ähnlichen Probleme sehen, die man ganz im Allgemeinen mit der Digitalisierung bereits erlebt. Es ist einfach eine weitere Fortsetzung dieser Entwicklung. Es gibt immer eine Transformation, denn es gibt immer bessere Wege, wie man ein Geschäft betreibt. Und neue Firmen sind dabei immer schneller und flexibler, auf solche Entwicklungen zu reagieren und diese zu adaptieren. Bei einer Transformation kommt es fast immer zu Verschiebungen und diese verlaufen nicht immer reibungslos aber beruhigen sich dann auch wieder. Eben nicht viel dramatischer, als wir es bereits

mit der vorhergehenden Digitalisierung erlebt haben. […] Und dann gibt es natürlich ein ganz neues Problem, sobald alles mittels Blockchain umgesetzt wird. Wer wird zukünftig meine Rechte durchsetzen? Heute haben wir zentrale Institutionen wie Polizei und Gerichte, die ich zur Durchsetzung meiner Rechte einberufen kann. Doch wie funktioniert das in einer Gesellschaft ganz ohne solche «Hilfsmittel»? Bei einfachen Anwendungsfällen ist das ja noch vorstellbar, aber wie verhaltet es sich beispielsweise mit komplexeren Fällen, in denen ich meine Bürgerrechte durchsetzen muss? Wie wäre es zum Beispiel, wenn ich über ein Blockchain-gestütztes Zahlungssystem auf einer Plattform eine Ferienwohnung miete? Da bezahle ich dafür im Voraus und stehe dann davor, ohne dass ich reinkomme. Hier wird heute eine Vertragsverletzung begangen, welche ich vor einem Gericht geltend machen kann. Also eben einer der zentralen Institutionen, welche nach den Prinzipien der Blockchain nicht mehr notwendig wären. Wie würde ich dann die Vertragsverletzung geltend machen? […] Man könnte das zwar, wie es heute schon gelöst wird, mittels Bewertungsmöglichkeit etwas verbessern, aber auf dem Schaden bleibe ich dann wohl sitzen. Das Prinzip des Zero-Trust ist technisch sehr wohl umsetzbar, doch Menschen verhalten sich nicht immer so berechenbar, wie es dies ein Algorithmus tut. […] Hier stossen wir auf gewisse Limitationen bzw. einer hohen Komplexität der Materie, welche uns wohl zukünftig noch häufiger beschäftigen werden.

AM: Blockchain wurde mit Open-Source Gedanke eingeführt. Nun versuchen insbesondere Banken, sich des Systems zu ermächtigen, in dem proprietäre Lösungen entwickelt werden. Wie stehen Sie dieser Entwicklung gegenüber?

KF: Ich glaube, dass es verschiedene Blockchains geben wird, welche jeweils ein wenig anders aufgebaut sind und sich für spezifische Anwendungsfälle eignen. Als Beispiel möchte ich hier den Vergleich zwischen Apple als geschlossenes System und Google mit Android als offenes System erwähnen. Beides kann sehr gut koexistieren. Dabei gibt es viele mächtige Interessenparteien. Und je nachdem, welches System dabei von Vorteil ist – geschlossen oder offen – wird entsprechend genutzt. Es ist auch verständlich, dass Banken nun versuchen, eine virtuelle Mauer zum Schutz ihrer Interessen aufzubauen. Und ich denke auch, dass es möglich ist, dass solch verschiedene Ansätze der Blockchain miteinander existieren können. Dabei möchte ich darauf hinweisen, dass Apple mit ihrem geschlossenen System natürlich auch eine für den Nutzer bequeme Lösung anbietet, die zugleich sicher ist. In offenen Systemen ist es meist nicht so einfach und vor allem auch nicht unbedingt sicher. Banken könnten hier auf eine geschlossene Blockchain setzen und dem Kunden eine bequeme Zahlungsmöglichkeit anbieten, die zugleich sicher ist. In diesem Anwendungsfall ist es für den Kunden nicht mehr so relevant, ob es sich um eine geschlossene Blockchain handelt, solange es schnell, bequem und sicher abläuft. Somit entscheidet letztendlich der Nutzer,

welches System sich durchsetzen wird, wobei, wie gesagt, beide Arten – offen wie auch geschlossen – parallel existieren können.

AM: Sehr interessant, bleiben wir noch kurz bei den Banken und beleuchten mal deren Vorgehensweise. Die Banken versuchen zurzeit, die Blockchain zu nutzen, um bestehende Prozesse zu optimieren. Daneben gibt es natürlich den Ansatz, bestehende Prozesse ganz neu zu definieren und mit Blockchain umzusetzen. Welcher Ansatz sehen Sie als den richtigen an?

KF: Ganz klar den letzteren. So wird auch der revolutionäre Gedanke der Technologie umgesetzt. Aber klar sehe ich die Vorgehensweise der Banken nicht als den falschen Weg an. Denn wie jede innovative Technologie muss man zunächst deren Einsatzmöglichkeiten prüfen. Und es ist hier einfacher, bestehende Prozesse mittels der Blockchain zu verbessern, als ganz neu zu erfinden. […] Daneben gibt es aber auch andere Unternehmen wie beispielsweise Paypal, welches sich die Vorgehensweise der Banken zu Nutzen macht und in dieser Zeit einen ganz neuen Geschäftsprozess erarbeitet. Wenn man mitten im System ist, ist es jeweils nicht mehr so einfach, sich neuen Einflüssen zu öffnen und es braucht dementsprechend auch länger. Man glaubt sich sicher, mit den bestehenden Prozessen noch lange am Markt zu überleben. Da insbesondere in der Finanzbranche auch die Gesellschaft noch sehr traditionell agiert, werden neue Anwendungsfälle gestützt durch die Blockchain noch schwierig haben, sich durchzusetzen. Daneben geht es hier natürlich auch um eine Vielzahl von Regulatorien, die den Transformationsprozess ausbremsen. Man kann nicht gegen Regulatorien agieren und ist an deren Entwicklung gebunden.

AM: Was wären den Anwendungsfälle, welche die Blockchain in einem grösseren Umfang etablieren können?

KF: Internet der Dinge, ganz klar. Die Kombination dieser beiden Bewegungen hat das Potenzial, dass sich die Blockchain schneller etablieren könnte. Und löst gleichzeitig auch mögliche Probleme, die sich aus der Nutzung der Blockchain alleine ergeben könnten. Wenn zwei Unternehmen gemeinsam Geschäfte machen, so wird – nicht nur aus rechtlicher Sicht – immer eine gewisse hierarchische Ordnung explizit oder auch implizit erwirkt. So ist einer der Zulieferer, einer der Hersteller, einer der Sender und einer der Empfänger. Somit hat man auf jeden Fall implizit einen Chef. Durch das Internet der Dinge kann man diese Rolle auf einen physischen Gegenstand transferieren, beispielsweise einem Tracker. Intelligente Systeme [inklusive IoT Geräte] könnten miteinander kommunizieren und die Transaktion mittels künstlicher Intelligenz steuern. Wenn man alles miteinander vernetzt, so hat man eine Schwarmintelligenz, die Prozesse ohne direkte Hierarchie steuern kann. Dabei braucht das Internet der Dinge das Konzept der Smart Contracts, was wiederum durch die Blockchain geliefert wird.

AM: Sie haben die Smart Contracts angesprochen, welche die Funktionalität der Blockchain vergrössert. Damit könnte man aber auch gewisse Betrügereien, wie Sie diese bereits zuvor erwähnt haben, einschränken, oder nicht?

KF: Kommt drauf an. Man müsste sich genau überlegen, wie man dann so einen Smart Contract [mit IoT Geräten] programmiert. Denn nur, weil ein Smart Contract genutzt wird, impliziert dies nicht ein betrugssicheres System. Es ist der Inhalt auf den es ankommt. Und je komplexer der abzubildende Prozess ist, desto schwieriger ist es, einen stich- und hiebfesten Smart Contract zu schreiben. Um auf mein Beispiel mit dem Betrug bei Ferienhäusern zurückzukommen, gibt es so viele Möglichkeiten, wie man dabei betrügen kann. Beispielsweise kann ja das Objekt extrem von dem im Internet abgebildeten Ferienhaus abweichen. Sobald ich dann dort die Türe öffne, wird das Geld überwiesen, obwohl es sich nicht um das abgebildete Ferienhaus handelt. […] Umgekehrt kann ich die Zahlung auch nicht auslösen, indem ich die Aktivität zur Auslösung der Zahlung erst gar nicht ausführe. […] Wenn mir das einfach so einfällt, ohne dass ich eine Expertin für Betrügereien bin, wie viele Möglichkeiten wird es dann effektiv geben, um so ein System auszutricksen.

AM: Gibt es denn weitere Anwendungsfälle, mit denen sie Blockchain in Verbindung bringen würden?

KF: Also ganz klar natürlich Zahlungen. Mit Bitcoin hat man ja bereits eine Währung, welche die Vorteile der Blockchain gut aufzeigen. Daraus können sich neue Zahlungsformen und -systeme ergeben. Ich glaube aber nicht, dass es zukünftig Bitcoin sein wird, welches sich als neues Zahlungsmittel durchsetzen wird. Dafür bietet die Währung noch zu viele Einschränkungen. Danach natürlich auch die ganze Thematik der Mobilität, was viele Elemente beinhaltet, welche sich für die Anwendung von Blockchain eignet. Letztendlich kann man sich die Anwendungsfelder der Blockchain durch dessen Eigenschaften ableiten.

AM: Wir kommen nun langsam zum Ende des Interviews. Gibt es Punkte, welche Sie noch gerne zur Thematik Blockchain und Anwendungsfelder erwähnen möchten? Persönliche Sichtweisen, Favorisierte Anwendungsfelder etc.

KF: Ich denke, dass wir uns heute noch mit Anwendungsfällen beschäftigen, welche zukünftig nicht primär die Möglichkeiten der Blockchain ausnutzen. Es werden darum in Zukunft wohl völlig andere Anwendungsfälle sein, welche durch die Blockchain ermöglicht werden, als wir es uns heute vorstellen können. Unter Berücksichtigung der sich nur langsam verändernden Gesellschaft denke ich, dass zunächst privatrechtliche Thematiken durch die die Blockchain beeinflusst werden, bevor es die öffentlich-rechtlichen werden. Privatrechtlich wären es dann die Transaktionsverträge. Dabei kann man auch die Komplexität reduzieren, denn es sind meist nur zwei Parteien involviert.

Master Thesis | **Die Blockchain Technologie und ihre Anwendungsfelder**

Autor: **Anand Paul Mooken**

Interviewleitfaden

Experteninterview mit Stipe-Mate Brkljacic

Zürich, den 12.05.2017

Vorname, Name	*Stipe-Mate Brkljacic*
Position	Programmleiter UBS, Start-up-Gründer
Unternehmen	UBS Schweiz AG Flurstrasse 70 8048 Zürich
Kontakt	Mail: stipe-mate.brkljacic@ubs.com
Selektionskriterien	Mitgründer eines eigenen Start-up-Unternehmens zur Blockchain und Verfasser einer Masterarbeit zum Thema Blockchain

Forschungsfragen:

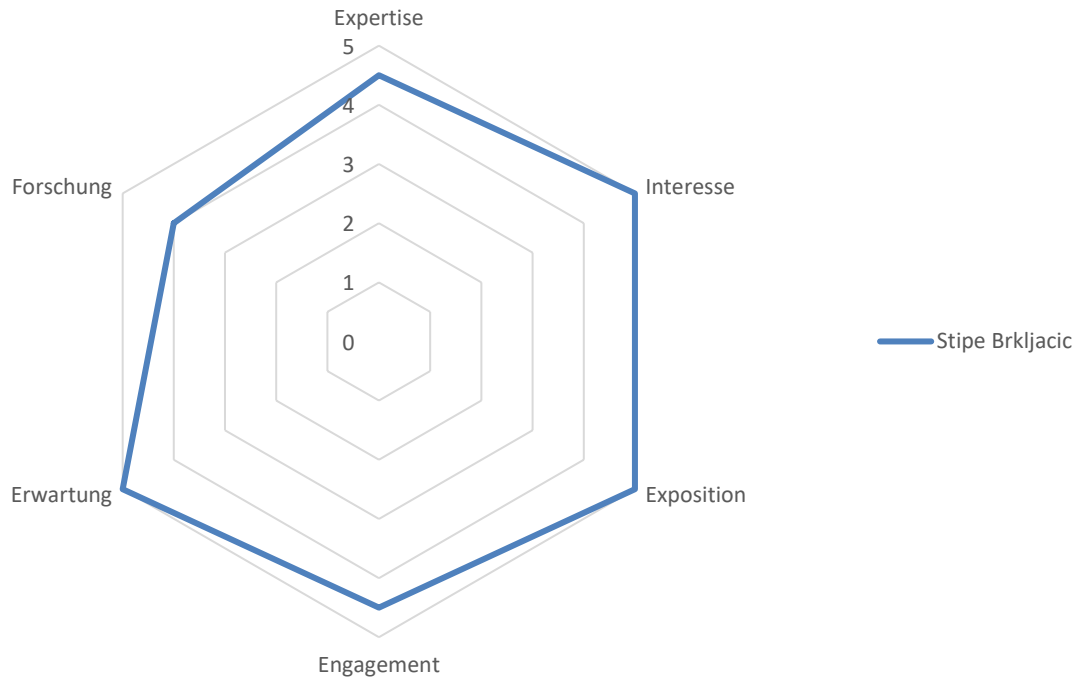
Was ist der Status Quo von Blockchain Technologie?

Wo liegen aktuell die Anwendungsfelder der Technologie?

Was sind mögliche Implikationen der Anwendung der Blockchain Technologie?

Wie können potenzielle Anwendungsfelder für die Blockchain Technologie systematisch identifiziert werden?

Profil der Interviewpartner im Kontext Blockchain:



Legende: Expertise = Wissen über Blockchain; Interesse = .. zum Thema Blockchain; Exposition = Aktivitäten zum Thema Blockchain; Engagement = Geschäftliche Interaktion mit Blockchain; Erwartungen = .. an Blockchain; Forschung = .. zum Thema

Stipe-Mate Brkljacic ist Programmleiter bei der UBS Schweiz AG und arbeitet gemeinsam mit weiteren Partnern im eigenen Start-up, welches mittels Blockchain und Smart Contracts in der Versicherungsbranche Produkte entwickelt. Er war seit der Einführung von Bitcoin stets interessiert an der Kryptowährung und der darunterliegenden Blockchain. Neben seinem Start-up hat er im vergangen Jahr 2016 seinen Master of Science in Wirtschaftsinformatik an der Zürcher Hochschule für Angewandte Wissenschaften erlangt. Mit der Masterthesis «Blockchain: Chancen und Risiken für die Schweizer Finanzindustrie» hat er seine Kompetenzen zur Thematik eindrücklich bewiesen. Seither verfolgt er aktiv die Entwicklungen der Blockchain und daraus resultierender Produkte.

Transkript:

Anand Mooken: Hallo Stipe, vielen Dank das du dir die Zeit nimmst, mit mir über die Blockchain Technologie zu sprechen. Kannst du mir etwas zu deiner Person und deiner beruflichen Tätigkeit bei der UBS sowie deinem eigenen Start-up sagen?

Stipe-Mate Brkljacic: Grundsätzlich arbeite ich bei der UBS als Programm Manager. Was für dich aber sicher viel interessanter ist: Mit zwei Freunden vom Studium arbeiten wir seit ungefähr einem Jahr an einem Blockchain Projekt. Mit grosser Sicherheit werden wir in diesem Jahr versuchen, bei verschiedenen Schweizer Firmen unser Produkt zu platzieren. Das Produkt ist somit bereits marktreif. Und natürlich habe ich meine Masterthesis auch zur Blockchain geschrieben, womit ich über eine gewisse Expertise verfüge.

AM: Was ist für dich die Blockchain und wo siehst du sie heute?

SMB: Blockchain ist für mich vieles. Grundsätzlich ist es eine Technologie. Es stecken sehr viele Algorithmen dahinter. Für sehr viele Investoren ist es aber eine Währung. Es ist ein Investment. Aber für mich ist es vor allem ein Neubeginn des Verständnisses vom Internet, d.h. man demokratisiert etwas, wo bisher sehr zentral funktioniert hat, wie beispielsweise ein Payment System, bei dem du irgendwelche Intermediäre benötigt hast, wird demokratisiert und jeder kann ein Teilnehmer des Netzwerks werden. Auf der anderen Seite ist es auch ein Instrument zur Optimierung der bestehenden Welt – Prozesse zu optimieren. Du hast also ein breites Band. Die Blockchain Technologie kann also als Enabler die bisherigen Prozesse verbessern und für bisherige Anwendungsfälle genutzt werden, es kann aber das bestehende System auch komplett als disruptive Technologie verändern. Es gibt verschiedene Ausprägungen, wie man die Blockchain sehen kann.

AM: Blockchain als Begriff ist derzeit in aller Munde. Siehst du diesen Hype als berechtigt an?

SMB: Klar, ich sehe den Hype immer noch als berechtigt an. Er hält sich ja schon seit mehreren Jahren. Man muss aber ganz klar differenzieren. Es gibt ältere Blockchain Derivate wie die Bitcoin, welche für mich die Blockchain 1.0 ausmacht. Dann gibt es neuere Projekte wie Ethereum, welche erst vor wenigen Jahren aus der Betaphase produktiv geworden sind. Du hast neue Blockchain Projekte, die dazukommen. Grundsätzlich finde ich, dass der Hype absolut gerechtfertigt ist. Man muss einfach differenzieren und insbesondere nicht wie es die Investoren machen, nur auf die Zahlen schauen, sondern auf die Technologie, welche dahintersteckt. […] Die Sicht der Investoren ist ebenfalls begründet durch den derzeitigen Hype. Und dieser Teil des Hypes erachte ich als sehr schädlich für die Technologie und sollte meiner Meinung nach vermieden werden. Auch wenn dies wohl kaum möglich ist. Aber für die Technologie könnte dieser Hype eine positive Wirkung haben.

AM: Neben den Projekten, die sich vollkommen der Blockchain verschrieben haben, starten nun auch traditionelle Unternehmen mit Integrationsversuchen. Dabei wählen sie den von dir beschriebenen Ansatz, die Blockchain als Prozessoptimierer zu nutzen. Findest du dies einen gangbaren Weg oder sollen zuerst die Prozesse an sich neu definiert werden?

SMB: Nein, ich finde den Ansatz der traditionellen Unternehmen sehr gut. So kommt es zu einer schnelleren Implementation der Technologie. An neuralgischen Punkten kann die Blockchain durch ihre positiven Eigenschaften einen grossen Mehrwert für diese Unternehmen bieten. Denn ich sehe die Blockchain nicht nur als grosse disruptive Technologie an. Sie kann auch im kleinen Umfeld eingesetzt werden und dort gut funktionieren. Ohnehin erachte ich es als sinnvoll, die neue Technologie zunächst auf kleine Bereiche zu testen, bevor man einen Big Bang Ansatz wählt. Die Technologie muss sich ja noch beweisen – beispielsweise, dass sie wirklich sicher ist - und sich so ein Vertrauen erarbeiten. Kleinere Anwendungsfälle wie beispielsweise der postalische Briefverkehr mit eingebetteter Personenidentifikation bilden für mich eine gute Basis, um die Technologie langsam einzuführen und gleichzeitig zu testen. Dabei hat man im Vergleich zu heutigen Prozessen bereits einen grossen Mehrwert generiert.

AM: Das Potenzial der Blockchain als Prozessoptimierer ist demnach bereits sehr gross?

SMB: Ganz genau. Man nimmt es zwar nicht so wahr [ist im Hype auch kein Thema]. Die Blockchain wird mit einem revolutionären Gedanken verknüpft, aber rational betrachtet kann man wirklich sehr viele Prozesse von heutigen Unternehmen optimieren.

AM: Blockchain wurde mit Open-Source Gedanke eingeführt. Nun versuchen insbesondere Banken, sich des Systems zu ermächtigen, in dem proprietäre Lösungen entwickelt werden. Wie siehst du diese Entwicklung?

SMB: Grundsätzlich finde ich das sehr gut. Wir [Start-up] nutzen beispielsweise Quorum von JP Morgan. Das ist ja eigentlich nichts Anderes als ein Permissioned-Blockchain basierend auf Ethereum. Ich finde das als Anwendungsfall im kleinen Rahmen viel effizienter und viel logischer als eine public Blockchain, in welcher du eigentlich alles transparent abbildest. Der Vorteil bei einer geschlossenen Blockchain ist zum einen, dass du bestimmen kannst, wer in so einem Netz teilnehmen kann und insbesondere, wer dieser Teilnehmer genau ist [Identifikation] und die mögliche Implementation eines Regulators. Du kannst dich viel leichter mit den heute gegebenen Organisationsformen markttechnisch positionieren. Auf der anderen Seite bin ich auch absoluter Fan von der public Blockchain. Ich finde es genial, habe auch Geld investiert [Bitcoin]. Es kann viele Prozesse revolutionieren. Zum einen das Payment System aber man kann heute auch schon ganze Filesysteme in der Blockchain abbilden. Bitcoin mit der Blockchain Version 1.0 hat noch viele Schwach-

stellen. Beispielsweise den Proof-of-Work Mechanismus. Dann hat man auch ganz viele chinesische Farmen, welche das Mining implizit wieder zentralisieren. Das wiederum wird wieder einene [negativen] Einfluss auf das Vertrauen in so eine public Blockchain haben.

AM: Somit würdest du sagen, dass beides verfolgt werden soll; eine geschlossene wie auch offene Blockchain. Es wird also für beide Formen eine Zukunft geben?

SMB: Genau, die einzige Instanz die allem einen Riegel vorschieben kann, ist der Regulator. Also wenn gewisse, vor allem westliche Nationen finden, dass es Zeit wird, die ganze Entwicklung zu regulieren, dann kommt es zu einer Kräfteverschiebung zwischen einer private und einer public Blockchain, denn dann sind die bisher mehrheitlich nicht regulierten Anwendungen, welche mit einer public Blockchain aktuell umgesetzt werden [Stichwort Darknet, Silkroad, illegale Finanzierungen] nicht mehr möglich, denn es wird so auch eher Richtung permissioned-Blockchain gehen. Aber auf der anderen Seite sieht man in Ländern wie China und Venezuela ganz klare Tendenzen dazu, dass man den Regierungen, also dem Regulator, nicht mehr traut, und Menschen in diesen Ländern in Kryptowährungen wie Bitcoin oder Ether flüchtet. Man kann solche globalen Trends und Entwicklungen nicht blockieren; es sei denn, man sperrt gleich das ganze Internet aus – und somit wären wir wieder beim Regulator.

AM: Greifen wir das Stichwort Regulator auf. Es bildet eine zentrale Autorität, welche bei einer Blockchain nicht notwendig ist. Wie lässt sich dieser Konflikt lösen?

SMB: Es ist noch schwierig. Auf der einen Seite hast du zentrale Staaten, die ihre Gesetze entsprechend zentral erlassen und auch durchsetzen, ebenso wie ihre Interessen. Du hast Regierungen, die interessiert daran sind, dass die Arbeitsplätze erhalten bleiben. Trotz allem musst du den aktuellen Entwicklungen, wie Blockchain eine ist, folgen und diese auch umsetzen. Doch Blockchain ist global und kennt entsprechend keine Grenzen. Die Blockchain ist weder zentral kontrolliert, noch hast du Instanzen, welche über anderen stehen. Man kennt hier keine Gewaltentrennung, wie wir sie beispielsweise von der Schweiz kennen. Es ist eine Demokratisierung von allem. Hier frage ich mich, wie man mit diesem Fakt zukünftig umgehen will.

AM: Ein Ansatz wäre die Differenzierung zwischen öffentlicher und geschlossener Blockchain.

SMB: Klar, aber was macht man dann mit der public Blockchain? Soll diese durch ein internationales Gremium reguliert bzw. standardisiert werden? Dann nimmst du aus der heutigen Welt das hierarchische Denken mit in die Blockchain und hast wiederum eine zentrale Instanz, die Auflagen generiert und die Revolution versucht, zu zähmen. Ich wüsste nicht mal, wie man das so umsetzen möchte. Es gibt immer mehr Interessierte, die sich dem Thema widmen und aktiv partizipieren. Auch von nicht mehr so technikaffinen Bereichen. So auch Investoren, die bereits stark spekulieren.

AM: Stichwort Standard und Regulatorien. Du hast dich in deiner Masterthesis stark mit dieser Frage auseinandergesetzt. Wie siehst du dies heute?

SMB: Ich würde sagen, dass Regulatoren ziemlich reaktiv arbeiten. Es hat auch seine berechtigten Gründe, oder aber historischen Gründe. Ich finde jedoch, dass es einfach eine offene Art gegenüber disruptiven Technologien braucht. Man sollte ganz ohne Vorbehalt an solche Themen herangehen. Und natürlich muss man auch Zeit investieren, um sich mit der Thematik auseinanderzusetzen. Dies, damit man auch die richtigen Auflagen verabschiedet. In der Schweiz wurde vor kurzem eine revidierte Verordnung zugunsten von Start-ups in Kraft gesetzt. Das ist der richtige Ansatz. Aber sind wir ehrlich, die Regulatoren können mit der Entwicklung einfach nicht Schritt halten. Beispielsweise prüft das SEC [Amerikanische Börsenaufsichtsprüfung] die Zulassung von ETFs, welche auf Bitcoin basieren. Während dieser langwierigen Prüfung kommen immer weitere Anfragen hinzu, die sich bereits weiterentwickelt haben. So kann man natürlich auch nicht schritthalten. Ein anderes Beispiel findet sich hier in der Schweiz. Du kannst hier bei keiner Bank ein Konto eröffnen, wenn du irgendwas mit der Blockchain [oder Kryptowährung] zu tun hast, da der Handel damit immer noch unter das Geldwäschereigesetzt geht. In Grossbritannien gibt es deshalb ein Unternehmen namens Coinbase, welches dir in Estland ein Bankkonto eröffnet. Denn die Regulatoren von Estland haben hier bereits reagiert und die generelle Verknüpfung mit der Geldwäscherei gelöst.

AM: Aber ist es denn nicht verständlich, dass die Regulatoren noch vorsichtig sind, wenn man die negativen Schlagzeilen von Silkroad und Darknet berücksichtigt?

SMB: Absolut, da schlagen jetzt zwei Herzen in mir. Ich bin jemand, der an diese Technologie glaubt. Wenn du die Technologie kommerzialisieren willst, dann musst du all die illegalen Machenschaften aus diesem Netzwerk verbannen. Ansonsten kannst du es nicht kommerziell nutzen. Vertrauenswürdige Unternehmen wie die UBS, Credit Suisse, Zürich Versicherungen etc. können nicht in einem Netzwerk teilnehmen, dass auch illegale Aktivitäten unterstützt.

AM: Hier brauchst du also auch zukünftig eine Drittpartei, die absichern kann, dass die Teilnehmer der Blockchain vertrauenswürdig sind?

SMB: Absolut. Aber da müsste man das auch ein wenig innovativer sehen oder einfach anders. Man kann heutzutage ja schon Instrumente nutzen, um die Teilnehmer zu kontrollieren, jedoch bevor sie überhaupt Teil des Blockchain Netzwerks werden. Wie wäre es beispielsweise, wenn man beim Passbüro nicht nur einen Personalausweis beantragt, aber gleich dazu noch eine digitale Identität, welche durch das Passbüro verifiziert ist und entsprechend in die Blockchain reingeladen wird. Dann sind die Voraussetzungen völlig anders. Plötzlich hast du eine Blockchain, deren Teilnehmern du vertrauen kannst. Ich glaube, dass dies ein gangbarer Weg ist, aber hier wären wir dann bei einer hybriden Blockchain oder gar wieder bei einer geschlossenen. Auf der anderen Seite

gibt es auch heute schon solche Angriffe und den illegalen Handel. Somit verlagern sich bestehende Probleme womöglich nur in die neue Technologie. Ich bin aber der Meinung, je mehr Menschen sich in die Blockchain wagen, desto mehr Menschen hat man, die eine positive Intention und Einstellung zur Technologie haben.

AM: Die zuvor erwähnte Bitcoin geniesst in diesem Zusammenhang einen verhaltenen Ruf und ist zuletzt mit negativen Schlagzeilen aufgefallen. Siehst du dies als negatives Vorzeichen für die Blockchain Technologie?

SMB: Nein, das ist nur eine Ausprägung. Die Blockchain ist ja viel mehr als nur ein einziger Anwendungsfall [Kryptowährung]. Die Bitcoin Blockchain ist die Mutter aller Blockchains, es ist die erste Blockchain überhaupt. Es handelt sich um einen guten Ansatz, aber es ist natürlich die Blockchain 1.0 und heute weiss man, dass diese Blockchain 1.0 seine Schwächen und Limitationen hat. Ich erachte es als sehr wahrscheinlich, dass die Bitcoin irgendwann das Vertrauen verlieren wird und an Wert verlieren wird. Aber es kann auch sehr gut sein, dass die Bitcoin aufgrund ihres grossen Marktvolumens weiterentwickelt wird oder sich als Standardwährung für Internettransaktionen anbieten wird. Man muss berücksichtigen, dass die Hackerangriffe und andere Limitationen in der Bitcoin Community immer aufgenommen wurden und an besseren Lösungen gearbeitet wird. Bitcoin ist von Wert und Marktvolumen ja heute so stark wie noch nie. Das überrascht mich ein bisschen, denn Ethereum bietet viel mehr Funktionalitäten als Bitcoin.

AM: Interessantes Stichwort, kommen wir nun zu Ethereum. Hier konnte man ebenfalls einen Vorfall beobachten, der kontrovers diskutiert wurde. Nämlich der Hard Fork nach einem Exploit eines Hackers, welcher zu einem kritischen Verlust geführt hätte [ohne Hard Fork]. Findest du die Vorgehensweise als richtiger: Weg von Ethereum?

SMB: Das ist eine sehr kontroverse Entscheidung. Ich persönlich finde es eine sehr gute Entscheidung zugunsten des Vertrauens in Ethereum, dass man sich zu diesem Entscheid bewegt hat. Es ging um sehr viel Geld. Es ging um Geld für die Organisation selber. Es ging dabei vor allem um die Weiterentwicklung des Systems. Aber trotzdem… Wir haben nun genau diese Situation, dass eine zentrale Institution die Macht hat und bestimmt hat, wie sich diese Blockchain entwickelt und somit eigentlich eine Manipulation dieser vorgenommen hat. Man hat hierbei wie einen Schritt rückwärts gemacht, um die reine Ausgangslage wiederherzustellen. Es ist sehr kontrovers. Zum einen finde ich es gut für das Vertrauen. Zum anderen ist es aber auch wiederum schlecht für das Vertrauen. Es handelt sich hierbei um eine Glaubensfrage. Wenn man eine Schwäche vom System ausnutzen kann, dann kann man das. Dann ist dies passiert und man sollte aus diesem Fehler lernen und entsprechend verbessern. Es handelte sich meines Wissens nach ja um einen ganz kleinen Fehler in einem Smart Contract, wobei die Konsequenzen viel schlimmer gewesen wären. Wiederum schlagen hier zwei Herzen in mir. Zum einen hat der Entscheid einen faden Beigeschmack,

denn das Prinzip des Zero-Trust-Networks wurde gravierend verletzt. Andererseits respektiere ich den Entscheid zugunsten des Projekts und des Vertrauens für Ether und Ethereum als Organisation. Im Sinne von: Hey, schaut her, wenn es wirklich mal so einen extremen Fall eines Missbrauchs gibt, dann können wir dies auf eine rationale Art und Weise lösen. […] Insgesamt kann man aber sagen, dass dieser Vorfall wirklich sehr früh in der Entwicklung von Ethereum stattgefunden hat. Dabei befand man sich noch in einer recht jungen Phase und da kann man Kinderkrankheiten nicht ganz ausschliessen. Somit könnte man ein Auge zudrücken und davon absehen. Die Organisation dahinter hat ja eine positive Intention und das sollte man nicht ganz ausser Acht lassen. […] Man kann es vergleichen mit der Frage, ob man jetzt ein Land einfach bankrott gehen lässt, oder es wie im Fall von Griechenland einfach durchfüttert und hofft, dass es bald wieder von alleine funktioniert. […] Ich finde es nach wie vor gut, dass sie einen Hard Fork gemacht haben, erachte aber jedes Argument dagegen als gerechtfertigt. Es ist eher eine Glaubensfrage.

AM: Ok, gehen wir mal von den negativen Schlagzeilen weg und schauen auf ein weiteres Prinzip der Blockchain, die folgendes besagt: Es braucht zukünftig keine Drittpersonen mehr. Du arbeitest ja in einer Bank, kannst du hinter diesem Prinzip stehen? *(Abgeleitet von der Frage vom Leitfaden: 16. Viele Drittanbieter wie Banken wie auch Bösen könnten durch Blockchain obsolet werden. Sehen Sie dies als mögliches Szenario an?)*

SMB: Ich bin der Meinung, dass Drittanbieter nicht verschwinden werden. Bezogen auf Banken glaube ich, dass die heute etablierten Unternehmen mit all dem erarbeiteten Vertrauen die Blockchain so einsetzen werden, dass vor allem die Hintergrundprozesse viel effizienter und effektiver ausgeführt werden, wodurch die Preise für ihre Dienstleistungen gesenkt werden können. […] Ich glaube nicht, dass somit bei der UBS zum Beispiel gute 50 bis 60'000 Arbeitsplätze durch die Blockchain verschwinden werden. Nicht in den nächsten 20 Jahren. Und auch ich als doch innovative Person bin froh, wenn ich bei einer Hypothek beispielsweise eine kompetente Ansprechperson habe. All das basiert ja auf langfristigem Vertrauen […] Allgemein auf Intermediäre bezogen, kann es aber gut sein, dass diese verschwinden könnten. Denn es gibt Drittanbieter, welche auf keine langfristige Vertrauensbasis angewiesen sind und nur vermittelnd auftreten. In diesem Rahmen kann man diese auch durch die Blockchain ersetzen und den Prozess somit effizienter gestalten. Wieso brauchst du beispielsweise als Bank einen Infrastrukturanbieter wie die SIX Group, welche das Settlement im Zahlungsverkehr leistet und für diesen Prozess eine Tagesendverarbeitung benötigt, wenn du dies über die Blockchain sicher, transparent und in Echtzeit abwickeln könntest? Solche Intermediäre sind in diesem Kontext zu unterscheiden von Banken. Denn bei einer Bank kannst du auch den persönlichen Kontakt suchen und entsprechend das Vertrauen abholen. Dies ist bei den anderen Intermediären nicht der Fall.

AM: Jetzt war der Fokus aber insbesondere auf der Finanzbranche. Öffnen wir mal diese Sicht. Fallen dir mögliche Anpassungen des Markts ganz allgemein ein?

SMB: Wie bereits erwähnt, du kannst mittlerweile ganze Filesysteme in der Blockchain abbilden. Dies konkurrenziert die Dienstleistungen von Dropbox oder iCloud [Cloud Storage Dienstleister]. Und man kennt es ja von iCloud. Die Online Speicher werden gehakt und plötzlich zirkulieren private Bilder im Netz. Die Blockchain könnte dies um einiges sicherer umsetzen. Die Entwicklung ist dabei noch spannend. Vor einigen Jahren hätte man sich nie denken können, dass man die Blockchain als Filesystem nutzen kann. Und heute gibt es solche Anwendungen. Und wenn man eine permissioned-Blockchain nutzt, so kann man auch sehr viele Prozesse und Dienstleistungen von Versicherungen, Krankenkassen usw. ersetzen. Die Thematik der eingeschriebenen Briefe lässt sich transformieren. Und auch das ganze Vertragswesen lässt sich revolutionieren. Denn die Signatur lässt eindeutig klarstellen, dass die richtige Person den Vertrag digital unterzeichnet hat. Und solche Anwendungsfälle müssen in den nächsten ein bis zwei Jahren kommen. Doch dies ist natürlich auch wieder sehr abhängig von den Regulatoren. Die tun sich ja zurzeit schon alleine schwer mit der Thematik der digitalen Identität. Aber trotz allem, solche Anwendungsfälle sollte man möglichst schnell umsetzen zugunsten der Blockchain. Rein die Kostenersparnis wäre riesig. Dann gibt es natürlich Inhouse-Transaktionen und Prozesse. Ganze Prozesslandschaften lassen sich effizienter gestalten. Und was ich ganz besonders gut finde, ist die Kombination der Blockchain mit künstlicher Intelligenz. So kann sich ein Prozess selbst verwalten. Es gibt also sehr viele Anwendungsfälle. Und ich selbst bin deshalb bereits vor über einem Jahr von der Zentrierung auf den Payment Markt weggekommen und habe meine Sichtweise verbreitert. Alles was heutzutage mit einem Prozess erstellt wird, könnte womöglich seinen Weg in die Blockchain finden.

AM: Die Frage, die sich stellt: Kann man nicht auch andere gleichwertige Technologien verwenden, um gewisse von dir beschriebenen Anwendungsfälle umzusetzen?

SMB: Natürlich. Die Blockchain ist ja eigentlich nur eine Verbindung von verschiedenen bereits existierenden Technologien. Doch die Kombination ist ausgeklügelt. Dies macht den Einsatz einiges einfacher als ein heterogen zusammengestelltes System.

AM: Für meine Methode habe ich auch Bereiche inkludiert, welche Vertrauen benötigen, diese jedoch jetzt noch nicht aufweisen. Beispielsweise Wählersysteme oder Rohstoffhandel. Wie siehst du diese Bereiche für die Blockchain?

SMB: Da kann ich gleich noch was Aktuelles dazu berichten. Ich war vor drei Wochen an einem eVoting Podium und habe dort selbst den Vorschlag gebracht, dass man Blockchain hier sehr gut nutzen könnte. Und da sass jemand neben mir, der genau dies mit dem Bund in der Schweiz als Option prüft. Das ist also ein Thema das aktuell sicher Beachtung findet. Ich weiss nicht, wo genau

sie stehen, aber da wird sicher bald was kommen. […] Und beim Rohstoffhandel sehe ich das gleiche Potenzial. […] Und dann haben wir noch das Konzept der Asset Tokenization. Man nimmt einen Asset, sei dies ein Diamant oder eine Banane, ein Kleidungsstück oder gar ein Haus, und integriert diese aufgrund von eindeutigen Kriterien in die Blockchain. So erhältst du eine transparente Kette der Verwertung. Das eindeutige Identifikationsmerkmal kann ja auch ein RFID Chip sein. Da ist auch die UBS der Meinung, dass dies sicher ein viel grösserer disruptiver Prozess sein wird, als wir es heute im Zahlungsverkehr sehen.

AM: Wir kommen langsam zum Ende unserer Zeit. Ich würde gerne noch ein Thema ansprechen, nämlich die Volatilität, die man bei den heutigen Blockchain-basierten Anwendungsfällen beobachten kann. Wie kann man dieser unberechenbaren Entwicklung entgegenwirken?

SMB: Das ist effektiv noch ein grosses Problem. Zwar sieht man das auch heute ausgelöst durch die herrschende Fisaklpolitik. Doch wenn man sich die Kursschwankungen von Bitcoin mal anschaut, sind diese sehr viel stärker als bei traditionellen Währungen. Ein Kollege von mir ist mal auf mich zugekommen und hat gefragt, ob ich Bitcoin kennen würde. Er würde gerne investieren, ist ja eine grandiose Asset Class. Solche Investoren und Spekulanten haben dann eine sehr grosse Wirkung auf den Kursverlauf von Kryptowährungen. Der Kollege hat dann auch gleich mal 20'000 Schweizer Franken darin investiert. Der Chart sieht ja auch sehr surreal aus und animiert viele Investoren zum Kauf der Kryptowährung. Zum einen ergibt sich daraus eine Spekulationsblase. Man kann nicht mehr genau einschätzen, wo der realistische Wert der Währung liegt. Man muss aber wissen – und das sage ich allen, die mich fragen – dahinter steckt eine Technologie. Dahinter stecken aber auch Produktionskosten. Denn neben Bitcoin basiert auch Ethereum noch auf dem Proof-of-Work. Man muss also diejenigen bezahlen, welche die technische Arbeit verrichten. Man befindet sich sozusagen in einem Hamsterrad. […] Diese Entwicklung finde ich persönlich nicht gut. Es geht ja um eine Technologie und nun kommen irgendwelche Investoren und Spekulanten, die nicht wirklich eine Ahnung davon haben und wollen mitspielen und ihren kurzfristigen Gewinn abziehen. Dies schadet dem Netzwerk eher, als das es eine positive Wirkung darauf hätte. Es könnte dazu kommen, dass innerhalb einer Kettenreaktion die Blase platzt und letztendlich das Vertrauen in die Technologie erlischt.

AM: Ein sehr interessanter Aspekt. Wir sind aber nun leider bereits am Ende des Interviews. Abschliessend: Gibt es Punkte, welche du noch gerne zur Thematik Blockchain und Anwendungsfelder erwähnen möchten? Persönliche Sichtweisen, Favorisierte Anwendungsfelder etc.

SMB: Ich habe mir da vor kurzer Zeit mal eine interessante Frage gestellt. Was passiert, wenn man seine Währungsreserven in Bitcoin zurückführen und gegen traditionelle Währungen eintauschen möchte. Du hast plötzlich Euros auf einem Bankkonto einer estnischen Bank und möchtest dieses Geld ja in die Schweiz zurückführen. Ich glaube nicht, dass eine UBS das Geld ohne Bedenken oder

überhaupt annehmen würde. Das wäre ja nach geltendem Recht in der Schweiz unter Geldwäscherei fallen. Und dieser Fakt haben sich, glaube ich, noch nicht so viele bei der ganzen Sache überlegt. Grundsätzlich finde ich das Thema Anwendungsfelder noch sehr schwierig. Es gibt so viele Möglichkeiten, die Blockchain einzusetzen. Und ob dann auch wirklich was wird aus einem rein hypothetisch gezeichneten Anwendungsfall, das ist eine ganz andere Frage. Im Verlauf des letzten Jahres hat sich bereits so vieles verändert, da sind so viele neue Projekte initiiert worden… Unter solchen Umständen lässt sich eine Prognose über die zukünftige Entwicklung nur sehr schwer abgeben. Ich würde mich persönlich auf einige wenige Anwendungsfälle konzentrieren.

Eidesstattliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit respektive die von mir ausgewiesene Leistung selbstständig und ohne Mithilfe Dritter verfasst habe, dass ich alle verwendeten Quellen sowie alle verwendete Literatur angegeben habe, dass ich das Vertraulichkeitsinteresse der Auftraggeber wahren und die Urheberrechtsbestimmungen der Zürcher Hochschule für Angewandte Wissenschaft respektieren werde.

Ort, Datum: Zürich, 26.05.2017

Unterschrift: 

Anand Paul Mooken