Spieltheoretische Analyse von Blockchains

Schahed Hadawal
Betreuer: Heiko Niedermayer
Seminar: Future Internet SS18
Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: hadawal@in.tum.de

KURZFASSUNG

Die digitale Währung Bitcoin, welche auf Blockchain basiert, hängt bezüglich ihrer Korrektheit und Stabilität von einer Kombination aus Kryptographie, verteilten Algorithmen und anreizgesteuertem Verhalten ab. Dieses Paper untersucht Kryptowährungen bzw. das Minen von Kryptowährungen als ein Konsens-Spiel und stellt fest, dass das Minen (Generieren) von Bitcoins oder deren Handeln in volatilen Devisenmärkten nach der Spieltheorie eine Art von Spiel darstellt. Beim Mining-Mechanismus erhhält jeder Teilnehmer (Spieler bzw. Miner) Belohnungen in Form von Bitcoin oder Transaktionsgebühren. Dabei muss der Miner entscheiden, ob er sein Block an die längste Transaktionskette anhängt oder an einen anderen Zweig der Transaktionskette. In Anlehnung der Spieltheorie lässt sich dieses "Spiel" - wie jedes andere auch - in einer Entscheidungsmatrix (Bimatrix) runterbrechen. Analogien zwischen diesem Spiel und der Hirschjagd, Taube-Falke Spiel und das Chicken Spiel werden aufgezeigt. Des Weiteren wird begründet, weshalb sich ein Spieler an die vom *Proof-of-Work-Protokoll* festgelegten Regeln halten soll. Insgesamt geht das Paper also der Frage nach, ob sozialwissenschaftliche Probleme auf das Mining der Blockchain anwendbar ist.

Schlüsselworte

Bimatrix, Bitcoin, Blockchain, Chicken-Spiel, Dezentralisierung, Entscheidungsmatrix, Fork, Hash, Hirschjagd, Konsensbildung, Mining, Nash-Gleichgewicht, Nullsummenspiel, Proof-of-Work, Spieltheorie, Taube-Falke Spiel, Zentralisierung

1. EINLEITUNG

Bitcoin ist eine dezentrale elektronische Fiat-Währung[1], die auf Blockchain basiert und mittels Kryptographie und Peer-to-Peer-Technologie implementiert wird. Derzeit befinden sich ca. 17 Millionen Bitcoins im Umlauf[2], welche für eine Vielzahl von Waren und Dienstleistungen gehandelt werden können. Bitcoins werden auf volatilen Devisenmärkten gehandelt: Die globale Marktkapitalisierung beträgt ca. 108 Milliarden Euro (Stand: März 2018); das Handelsvolumen beträgt ca. 4 Milliarden Euro und ein Bitcoin kostet derzeit ca. 9.000 Dollar (Stand: März 2018)[3].[8]
Wie jede andere Währung auch, kann man Bitcoin für das Kaufen und Verkaufen von Waren und Dienstleistungen verwenden. Aber Bitcoin ist mehr als nur eine Währung. Bitcoin ist ein verteilter Algorithmus, der stets einwandfrei funktionieren muss, damit die Währung funktioniert, um beispielsweise einen Konsens darüber zu erzielen, wer welche Münzen besitzt. Der erfolgreiche Betrieb dieser Algorithmen beruht wiederum auf Annahmen, dass die Teilnehmer im System in bestimmter Weise kooperieren. Ob eine Zusammenarbeit sicher ist, hängt davon ab, ob die Anreize der Parteien sie zur Kooperation veranlassen.[5]

Dieses Paper untersucht, ob das Minen von Kryptowährungen mit Bitcoins als eine Art von Spiel hinsichtlich der Spieltheorie angesehen werden kann. Dabei werden in Kapitel 2 formale Definitionen über Blockchain geklärt. Des Weiteren wird u.a. die Funktionsweise von Blockchain erläutert und eine Methode zur Konsensbildung vorgestellt. Kapitel 3 befasst sich mit der Spieltheorie. In diesem Abschnitt werden grundlegende Definition der Spieltheorie erklärt und anhand von Beispielen untermauert. Außerdem wird ein Einblick in die 2x2-Bimatrix-Spiele gewährt, welche eine vereinfachte Darstellung jeglicher "Spiele" liefern kann. Diese Sektion soll zusammen mit Sektion 2 die Grundlage für die philosophische Frage klären, ob das Minen von Kryptowährungen als Spiel betrachtet werden kann. Diese Fragestellung wird in Kapitel 4 diskutiert. Im letzten Kapitel befindet sich eine kurze Zusammenfassung über dieses Paper und gibt ein kurzes Fazit zu dem Mining-Spiel ab.

2. BLOCKCHAIN

Seit Beginn der Digitalisierung von Geschäftsprozessen sind Verlässlichkeit und Vertrauen entscheidende Kernelemente der Digitalisierung. Gleichgültig, ob es sich um organisationsübergreifende Prozesse zwischen kooperierenden Geschäftspartnern in der Lieferkette oder zwischen Verkaufsportalen und Kunden handelt. Im heutigen Internet der Werte stellt sich die Frage nach dem Vertrauen in Transaktionen, die in verschiedene Formen von Werten abgebildet werden können. Traditionell setzen Datenbanken und Prozessmanagementsysteme auf einen zentralistischen Ansatz, der von einer autoritären Person mit einer zentralen Prozesssynchronisation verwaltet wird. Allerdings birgt die Zentralisierung eine beachtliche Anzahl an Risiken mit sich, die u.a. wären: "Leistungsengpässe, Ausfallsicherheit, Authentizität oder in-

[1]Als Fiat-Währung wird jedes Zahlungsmittel bezeichnet, welches keinen inneren Wert besitzt. Fiatgeld unterscheidet sich vom Warengeld wie z.B. Gold, Reis, Salz etc. - https://www.moneyland.ch/de/fiatgeld-definition
[2]https://de.statista.com/statistik/daten/studie/283301/umfrage/gesamtzahl-der-bitcoins-in-umlauf/
[3]https://coinmarketcap.com/de/currencies/bitcoin/

doi: 10.2313/NET-2018-11-1_03

terne und externe Angriffe auf die Integrität."[10]
Der Zentralisierung durch eine Autoritätsperson steht die Dezentralisierung durch die Blockchain gegenüber. Die Innovation von Kryptowährungen gewährleistet die Korrektheit von Transaktionen innerhalb eines Netzwerks und die gemeinsame Konsensfindung zwischen den Netzwerkpartnern. Die Einigkeit über die Transaktionskorrektheit findet nicht zentral, sondern durch eine Konsensfindung zwischen den Partnern statt. [10]

2.1 Definition

Die meisten Menschen kennen Blockchain als Basis von Kryptowährungen wie z.B. "Bitcoin" oder "Litecoin". Blockchain ist eine Datenbank, in der Daten angelegt werden, jedoch nicht mehr nachträglich verändert und gelöscht werden können. Dabei suggeriert der Begriff "Blockchain", dass die Datenbank aus mehreren aufeinanderfolgenden Blöcken besteht, welche Transaktions- bzw. Handänderungsdaten enthalten. Jeder dieser Blöcke wird zeitlich in eine Kette geordnet. Für jeden Block und dessen kompletten Inhalt wird ein Hash erzeugt, welcher eine eindeutige Referenz des Blocks darstellt. Der nächste Block verweist dann jeweils auf den Hash-Wert des vorgängigen Blocks und ein neuer wird jeweils immer vorne an eine bestehende Kette angehängt.[10]

2.1.1 Öffentliche und Private Blockchain

Blockchains können privat oder öffentlich zur Verfügung stehen, wobei der Unterschied darin besteht, welcher Nutzer neue Transaktionen jener Blockchain hinzufügen und validieren darf. Bei einer öffentlichen Blockchain hat jeder Nutzer das Recht, neue Informationen zur Blockchain hinzuzufügen und zu validieren. Bei privaten Blockchains ist der Nutzer auf die Erlaubnis einer Organisation oder Konsortiums angewiesen, erst dann darf er Informationen auf die Blockchain schreiben bzw. validieren. Diese Arbeit beschäftigt sich ausschließlich mit öffentlicher Blockchain, da andernfalls der Rahmen dieser Arbeit gesprengt wird.[10]

2.1.2 Was ist ein Block?

Jeder Block besitzt jeweils einen Header, der aus einer ID, einem Zeitstempel, der Difficulty, der Nonce (number used only once), dem Hash-Wert des vorgängigen Blocks und dem Hash des aktuellen Blocks besteht. Außerdem enthält ein Block ein Datenfeld, das für die Transaktionsdaten reserviert ist. Eine Blockkette wird ungültig, sobald man versucht, die Daten auf einem Block zu verändern. Denn eine Änderung des Blocks führt zur Änderung des Hash-Werts des gesamten Blocks, wodurch die Referenz zum nachfolgenden Block nicht mehr stimmt. Um die Kette wieder gültig zu machen, müsste man für jeden Block in der Kette einen neuen Hash-Wert erzeugen bzw. generieren (Mining), welches allerdings sehr zeit- und rechenintensiv ist.[10]

2.1.3 Was ist ein Hash?

Ein Hash ist eine Zahl, die einer beliebigen Zeichenkette einen eindeutigen Wert zuordnet, d.h. ein beliebiger Datenraum wird auf Daten fester Größe mittels Hashfunktion abgebildet. Wird ein Zeichen in der Zeichenfolge verändert oder hinzugefügt, sei es auch nur ein einzelnes Zeichen, so führt das zu einem neuen Hash-Wert, der durch einen beliebigen Computer sehr schnell erzeugt werden kann. Auf diese Weise kann man prüfen, ob ein Hash-Wert zu einer bestimmten Zeichenkette gehört oder nicht.[6]

2.1.4 Was bedeutet Mining?

Es sind die Miner, die entscheiden, zu welchem vorherigen Block ein neuer Block verkettet wird uns somit eine einzelne Kette oder Fork (Spaltung der Transaktionskette in mehreren Ketten) entstehen lässt. Miner sind an das *Proof-of-Work*-Protokoll (Abschnitt 2.3) gebunden und sie versuchen zu jedem Zeitpunkt, einen neuen Transaktionsblock zu generieren und zu validieren. Dieses Konzept der Validierung nennt man Mining. Derjenige Miner, der den nächsten Block vorschlagen darf, wird ausgelost, somit wird gewährleistet, dass alle Miner sich beim Validieren der Blöcke abwechseln und zu keinem Zeitpunkt ein bestimmter Miner den gesamten Verifizierungsprozess unter seine Kontrolle bringt.[4]
Welcher Anreiz wird den Minern geboten? Jeder Miner, der dabei hilft ein *Proof-of-Work*-Problem (z.B. in der Handelsfinanzierung) zu lösen, indem er erfolgreich einen Transaktionsblock generiert und validiert, wird mit neu geschaffenen Einheiten der Währung belohnt (z.B. 12.5 Bitcoin pro Block - Stand: 2018 [4]). Des Weiteren erhält jeder Miner eine *Transaction fee*, welche mit dem Block generiert wird.[4]

Im folgenden wird die Funktionsweise der Blockchain bzw. das Mining genauer betrachtet.

2.2 Funktionsweise

Wie bereits oben erwähnt, gibt es zwei Kernelemente der Technologie, nämlich die Codierung von Transaktionen durch Hashing und die Konsensfindung über die Korrektheit von Transaktionen. Beim ersten Kernelement ist eine Abbildung unterschiedlicher Zeichenketten auf denselben Code ausgeschlossen (Kollisionsfreiheit). Nach einer formalen Überprüfung der Transaktion versuchen die Netzwerkpartner über die Transaktion einen Konsens zu finden. Falls die Partner für die Transaktion einen Konsens gefunden haben, so wird sie im Netz verteilt und in die globale Blockchain aufgenommen. Abbildung 1 zeigt eine vereinfachte schematische Darstellung von der Iniitierung bis zum Abschluss der Transaktion.[5]

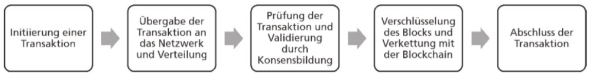

Abb.1: Funktionsweise einer Blockchain (Fraunhofer FIT)[10]

Zuerst wird jede Transaktion von einem Sender generiert und digital signiert (Initiierung). Eine Transaktion kann dabei z.B. die Überweisung einer Kryptowährung oder die Registrierung eines Dokuments sein. Anschließend wird die Transaktion an das Netzwerk übermittelt und an die beteiligten Knoten im Netz verteilt. Dabei überprüft jeder Knoten im Netzwerk die Gültigkeit der Transaktion und versucht dadurch einen Konsens zu finden. Bevor es zum Abschluss der Transaktion kommt, wird die Transaktion in einem Block

doi: 10.2313/NET-2018-11-1_03

gespeichert und durch Hashfunktionen in ein standardisiertes Format überführt, d.h. jede einzelne Transaktion wird in Hashwerte codiert und hierarchisch zu einer Blockkette verdichtet (Hash oder Merkle-Baum). Diese Codierung ist sicher gegenüber Manipulationsversuchen, da mögliche Änderungen der Transaktionen den Hashwert des Blocks ändern würden. Dadurch wäre der Hashbaum nicht mehr konsistent. Abbildung 2 verdeutlicht den vorherig genannten Ablauf der Transaktion mit Hilfe eines konkreten Beispiels, in der Partner A Geld an Partner B überweisen möchte. Mittels eines Computers überweist Partner A einen Geldbetrag an Partner B. Dabei wird die Transaktion einem Block angefügt und an beide Netzwerkteilnehmer weitergeleitet. Anschließend wird die Transaktion von beiden Netzwerkteilnehmern ge-nehmigt und validiert, so dass dieser Block an die bereits bestehende Blockkette (Blockchain) angehängt wird. Wie gewünscht wird das Geld am Ende überwiesen und die Transaktion erfolgreich abgeschlossen.[9]

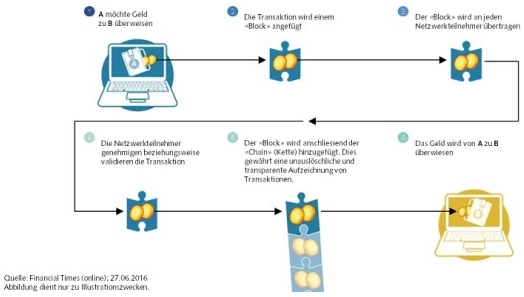

Abb.2: Beispiel für die Funktionsweise einer Blockchain

Damit ein Block in die Blockkette (Blockchain) aufgenommen werden kann, muss ein Verfahren zur Konsensbildung absolviert werden.

2.3 Methoden der Konsensbildung - Proof-of-Work

Ein wesentlicher Grundpfeiler des Blockchains-Konzepts ist die Konsensbildung. In der Konsensbildung werden Transaktionen so validiert, dass eine Übereinstimmung über die als gültig anzuerkennende Transaktion gefunden werden kann. Die Konsensbildung sorgt dafür, dass die gespeicherte Aussage anerkannt wird und zukünftig nicht mehr veränderbar ist.[9]
Das bekannteste Verfahrung zur Konsensbildung ist der Proof-of-Work der Bitcoin Blockchain. Dieses Verfahren basiert auf einen asymmetrischen Ansatz, bei dem ein Dienstnutzer Arbeit leisten muss, die von einem Dienstanbieter ohne große Mühe überprüft werden kann.[6] Im Kontext der Blockchain entsprechen die Nutzer den Minern, welche den Prof-of-Work aufwändig berechnen. Demenstprechend stellen die Anbieter alle Knoten dar, die ohne großen Aufwand prüfen, ob der Miner den Proof-of-Work ordnungsgemäß berechnet hat.[9]
Wie bereits in Kapitel 2.1.4 erwähnt, ist das Ziel des Proof-of-Work-Algorithmus, eine Zahl (Nonce = number used only once) zu finden, die in Kombination mit dem neu generierten Block, welcher an die bestehende Blockchain angehängt wird, einen Hashwert ergibt, der eine bestimmte Bedingung erfüllt. Eine solche Bedingung könnte sein, dass der zu findende Wert aus einer bestimmten Anzahl an führenden Nullen besteht (Kapitel 2.1.4). Hashfunktionen sind Einwegfunktionen, daher kann diese Zahl nur durch Brute-Force (Ausprobieren) gefunden werden.[10]
Beim Proof-of-Work-Verfahren steht die Rechenleistung der Knoten im Vordergrund, wenn es darum geht, einen passenden Nonce-Wert zu finden. Jeder Miner wird für das Finden eines solchen Wertes mit Bitcoins (Kryptowährung - virtuelle Währ-ung) belohnt, daher entsteht ein Wettbewerb, bei dem jeder Miner versucht, seine Rechenleistung zu verbessern bzw. zu erhöhen. Dies hat zur Folge, dass die Zeitdauer für das Auffinden von gültigen Nonce-Werten reduziert wird. Würden sich die Zeitintervalle verkürzen, in denen neue Blöcke erzeugt werden, dann würde sich die Geldmenge zu schnell erhöhen. Daher wird die Schwierigkeit des Auffindes von jenen Werten erhöht, wenn sich die Rechenkapazität verkürzt. Für die Miner bedeutet das: erhöhter Aufwand für geringe Erfolgsaussichten.[9]
Neben der Rechenleistung gibt es auch speicher- oder netzwerkbasierte Proof-of-Work-Verfahren. Beim speicherbasierten Proof-of-Work-Verfahren wird das Finden von Nonce-Werten durch eine entsprechende Anzahl von Speicherzugriffen gelöst [3]. Beim netzwerkbasierten Proof-of-Work-Verfahren wird das Rätsel durch Kommunikation mit anderen Netzknoten gelöst. Zum Beispiel werden Informationen gesammelt, die für das Auffinden des Wertes notwendig sind.[2]
Das Proof-of-Work verfahren eignet sich insbesondere für öffentliche Blockchain-Netzwerke, da es keiner Zugangsbeschränkung unterliegt. Für private Blockchains eignet sich das Proof-of-Stake-Verfahren, bei dem die Knoten, welche einen neuen Block validieren können, nach ihren Anteilen an der Kryptowährung oder über ein Zufallsverfahren ausgewählt werden.[1]

2.4 Was ist ein Fork?

Ein Fork in der Blockchain beschreibt ein Vorgang in der Kryptowährung, bei dem ein Projekt durch Modifikation des Quellcodes die ursprüngliche Blockchain in eine neue Blockchain abspaltet. Graphisch gesehen entwickelt sich aus der Transaktionskette ein "Transaktionsbaum". In Abb. 3 entwickeln sich ab dem Block X parallel zwei Blockchains. Die ältere Blockchain wird weiterhin von einigen Benutzern der älteren Version mit Mining versorgt. Dabei ignorieren die älteren Clients den neuen Block X. Neue User widerum versorgen die abgespaltene Blockchain X mit weiteren Blöcken, sodass sie wächst. Unabhängig davon, wie lange die einzelnen Transaktionsketten werden können die neuen User zwischen den Blöcken hin und her wechseln (minen).[4]

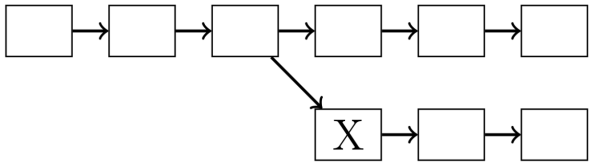

Abb.3: Fork in der Blockchain[4]

[4]https://bitcoinblog.de/2015/06/15/was-passiert-bei-einem-hard-fork/

doi: 10.2313/NET-2018-11-1_03

2.4.1 Warum treten Forks in der Blockchain auf?

Bei einem Fork treten immer wieder Änderungen in der Blockchain auf, die nicht kompatibel mit den alten Blöcken sind. Dies führt hin und wieder dazu, Erweiterungen an den Protokollen vorzunehmen. Die Änderungen können verschiedener Natur sein: Von kleinen Ergänzungen bis hin zu neuen Features, wie z.B. die Blockgrößenerweiterung. Da die Blockchain ein Open-Source Projekt ist und für jeden frei zugänglich ist, kommt es häufig zu Uneinigkeiten in der Community. Falls die Community zu keiner Einigung gelangt, so entstehen zwei Gruppen, die unterschiedliche Ziele erreichen wollen und somit zu einer Blockchainspaltung. Dies kann mitunter zur Entstehung neuer Kryptowährungen führen. Ein bekanntes Bespiel hierfür ist das Bitcoin Gold[6], welches sich von der Bitcoin Blockchain abgespalten hat, um eine eigenständige Kryptowährung zu werden.[4]

2.4.2 Welche Konsequenzen resultieren aus den Forks?

Viele Parteien sind an der Blockchainentwicklung und -benutzung beteiligt. Dies erfordert ihre Teilnahme an allen Änderungen der Blockchain.[4]

1. Szenario: die neue Software wird bei vielen Endnutzern, Börsenbetreibern und Händlern verwendet. Allerdings weigern sich die Miner die neuen und größeren Block zu veröffentlichen und verhindern die Transaktionsbestätigung.

2. Szenario: Alle Miner benutzen die neueste Version der Blockchain. Die Endnutzer, Börsenbetreiber und Händ-ler sind aber noch nicht auf die neue Version umgestiegen, nutzen noch die alte Version und ignorieren die großen Blöcke. Dies führt dazu, dass keine weiteren Transaktionen mehr bestätigt werden können, da keine neuen Blöcke mehr gefunden werden können. Für die Miner ist dieses Szenario ebenso ungünstig, da sie ihre Belohnung nicht erhalten würden. Die Miner sind dementsprechend daran interessiert, diese Situation zu vermeiden und sollten sich mit den Endnutzern abstimmen.

3. Szenario: In diesem Szenario wird die neue Version nur von wenigen Usern und Minern verwendet. Die generierten Blöcke werden zwar innerhalb dieser "Gruppe" anerkannt und validiert, aber vom restlichen Netzwerk ignoriert. Die Belohnung wird dementsprechend klein ausfallen, da es sich um kleine Gruppen handelt.

4. Szenario: Analog zum vorherigen Szenario ist die umgekehrte Variante ebenfalls möglich, dass eine große Mehrheit die neue Version benutzt. Die erste Blockchain wird von den Usern der alten Version ignoriert. Dies würde allerdings keine größeren Konsequenzen zur Folge haben, da alle Endnutzer, Händler und Börsen ebenso die neue Version nutzen würden.

5. Szenario: In diesem Szenario sind beide Blockchains nach der Abspaltung aktiv. Dies hat zur Konsequenz, dass beide Blockchains unterschiedliche Informationen enthalten, da Miner frei entscheiden können, welche Transaktionskette verlängert werden soll. Die eine Blockchain könnte das Geld für ein gekauftes Auto enthalten während in der anderen Blockchain das Geld noch in der Wallet[7] des Käufers steckt. Durch geschickte Manipulationen kann man so ein Szenario nach einem Fork auch erzwingen.

[6]https://bitcoingold.org

Diese Szenarien verdeutlichen, wie wichtig es ist, einen Konsens zu erzeugen. Wie erzeugen alle Beteiligten einen Konsens?

2.4.3 Konsensbildung

Kroll et al (2013) definiert drei Typen von Konsens:

1. Konsens über Regeln: Alle Miner müssen sich auf Kriterien einigen, um zu bestimmen, welche Transaktionen gültig sind. Nur gültige Transaktionen sollten im Bitcoin-Protokoll vermerkt werden. Jedoch erfordert dies eine Übereinstimmung darüber, wie die Gültigkeit zu bestimmen ist.

2. Konsens über den Status: Die Miner müssen sich darauf einigen, welche Transaktionen tatsächlich stattgefunden haben, d.h. sie müssen ein gemeinsames Verständnis dafür haben, wer zu welcher Zeit welche Münzen besitzt.

3. Konsens über den Bitcoinwert: Außerdem müssen alle Beteiligten akzeptieren, dass Bitcoins einen Wert besitzen, so dass Endnutzer bereit sind, Bitcoins in Zahlungen zu akzeptieren und zu verwenden.

Jeder dieser Punkte ist abhängig von den jeweils anderen. Diese Konsensprozesse sind ein sozialer Prozess in denen die Teilnehmer sich darüber einig werden müssen, was erlaubt ist und was nicht. Die Regeln müssen dann in der Software, die jeder Teilnehmer verwendet, kodiert werden können.

Bevor der Frage nachgegangen werden kann, ob es sich bei Mining von Bitcoins um ein Spiel im Sinne der Spieltheorie handelt, müssen ersteinmal die Begriffe rund um die Spieltheorie näher betrachtet werden.

3. SPIELTHEORIE

Damit der Mensch seine Handlungsoptionen und die daraus resultierenden Folgen im Voraus analysieren kann, muss er mit Hilfe eines im Geist konstruierten Abbildes der realen Umgebung arbeiten. Alle Spieltheorien basieren auf dieser Tatsache. Nur Dank dieser Planungsfähigkeit ist ein soziales Miteinander auf unterschiedlichen Ebenen (z.B. in polit. Verhandlungen oder wirtschaftlichen Systemen wie Märkte etc.) möglich. Eine weitere Grundlage dieser Theorien ist die Annahme, dass alle Teilnehmer eines Spiels ein möglichst gutes Ergebnis für sich selbst erzielen wollen, d.h. jeder Spieler (Player) ist daran interessiert, sein Gewinn zu maximieren.

Im folgenden wird die Spieltheorie im Allgemeinen definiert.

[7]Eine Wallet ist eine virtuelle Geldbörse, in der man seine Kryptowährung anlegen kann

doi: 10.2313/NET-2018-11-1_03

Anschließend werden einige Begriffe wie z.B. die Entscheidungsmatrix, Bimatrix und einige global anwendbare Spiele vorgestellt.

3.1 Definitionen

Spieltheorie ist eine Theorie sozialer Interaktion, d.h. ein Spiel ist nichts anderes als eine soziale Interaktion zwischen n Spielern (n-Personen Spiele). Im Vordergrund der Spieltheorie steht die Entscheidungssituation, bei dem das Ergebnis einer Entscheidung nicht nur von dem Entscheider (Spieler), sondern auch von dem Verhalten der anderen Entscheider (Gegenpieler) abhängt. Solche Entscheidungssituationen sind beispielsweise in Gesellschaftsspielen wieder zufinden. Allerdings hat die Spieltheorie weniger mit Gesellschaftsspielen zu tun, sondern ist lediglich im übertragenen Sinn eine Basis für jedes Spiel und relevant für Entscheidungen im täglichen Leben.[11]
In der Spieltheorie spielt man immer gegen die Natur, die in unterschiedlichen Formen z.B. konkurrente Mitspieler oder Zufall, aber auch als die Natur selbst auftreten kann. Ein Beispiel, in der die Natur als Gegenspieler im Spiel dargestellt wird, ist die landwirtschaftliche Produktion, in der das Wetter viele Umweltzustände bestimmen kann.[11]
Spieltheorien betrachten ebenfalls strategische Spiele, die wiederum auch Zufallselemente enthalten können. Dabei ist ein strategisches Spiel, auch strategische Interaktion/Konflikt genannt, eine Entscheidungssituation, in der mehrere vernunftbegabter Entscheider Einfluss auf das Resultat haben und ihre eigenen Interessen verfolgen. In erster Linie wird dabei versucht, für ein Problem (gegebenes Spiel), das als strategisches Konflikt abgebildet ist, eine Lösung zu ermitteln. Dabei ist die Lösung des Spiels ein Vorschlag bzw. Anleitung, wie das Spiel zu spielen sei. Die Lösung eines Spiels wird aus den Eigenschaften des Spiels hergeleitet und nicht aufgrund von psychologischer Überlegungen. Im Zusammenhang mit strategischen Spielen kann eine Strategie auch mit Entscheidungsalternative übersetzt werden. [7]

In der Spieltheorie lässt sich ein Spiel in *kooperative* und *nicht-kooperative* Spiele unterteilen. Diese Begrifflichkeiten werden im folgenden Abschnitt erklärt.

3.1.1 Kooperative und nicht-kooperative Spieltheorie

In der *kooperativen Spieltheorie* wird versucht, Situationen zu untersuchen, in denen sich Spieler mittels natürlicher Sprache verständigen. Bei einem Spiel hat jeder einzelne Spieler einen Einfluss auf den Spielausgang, daher verhandeln die Spieler zusammen darüber, welches Spielergebnis gemeinsam realisiert werden soll. Um das gemeinsam vereinbarte Spielergebnis zu gewährleisten, können die Spieler einen Vertrag abschließen, der jeden Spieler dazu verpflichtet, sich auch so zu entscheiden, wie abgesprochen. Die Einhaltung des Vertrages ist also im Rahmen der Spielregeln gesichert und extern vorgegeben. In dieser Form der Spieltheorie wird der Gewinn für alle beteiligten umso größer, je besser die Player zusammenarbeiten.[11]
In der *nicht-kooperativen Spieltheorie* wird versucht, Situationen zu untersuchen, in denen die Spieler vollkommen getrennt voneinander sind und nicht in natürlicher Sprache miteinander kommunizieren und bindende Verträge eingehen können. Die einzige Möglichkeit miteinander zu kommunizieren sind die Entscheidungen, die jeder Spieler während dem Spiel trifft. Dabei stellen die Züge eine Art stilisierterSprache dar. Des Weiteren hat keiner der Spieler einen Einblick über die Psychologie des Gegenspielers. Die Rationalität ist also die einzige psychologische Komponente, von der jeder Spieler ausgehen kann, dass der Gegenspieler sie besitzt. In dieser Form der Spieltheorie versucht jeder Player das bestmögliche Ergebnis für sich selbst zu erhalten, auch auf Kosten der Gegenspieler. Daneben zielen sie darauf ab, nicht nur den absoluten, sondern auch den relativen Gewinn - d.h. den Gewinn im Verhältnis zu den Ergebnissen der anderen - zu maximieren.[11]
Eine weitere Form, die aber eigentlich Teil der vorher genannten Formen bildet, ist das Nullsummenspiel. Nullsummenspiel ist ein Spiel, in dem einige der Player das gewinnen, was andere verlieren. Dabei addiert sich die Gesamtsumme aus Gewinn und Verlust aller Spieler immer zu null.[11]

Eine einfache und wohlbekannte Methode, mit dem ein Problem bzw. gegebenes Spiel strukturiert werden kann, ist die Entscheidungsmatrix, die im nächsten Abschnitt anhand eines Beispiels erläutert wird.

3.1.2 Entscheidungsmatrix

Angenommen ein Geschäftsführer (erster Spieler) eines Unternehmens muss für das folgende Geschäftsjahr festlegen, wie stark sein Unternehmen sich auf dem Markt engagieren will. Dafür muss er das Marketing- und Investitionsbudget im Vornherein festlegen. Dem Geschäftsführer stehen vier Engagement-Stufen zur Verfügung, nämlich von 1 (geringes Engagement) bis 4 (sehr starkes Engagement). Der Erfolg seines Unternehmens hängt von der Konkurrenzlage (zweiter Spieler) ab, die entweder günstig, normal oder ungünstig sein kann. Abbildung 4 zeigt die bisher aufgezählten Daten, die in der Matrix eingetragen sind. Die darin enthaltenen Zahlen stellen den Gewinn für das Unternehmen dar, sind frei erfunden und dienen zur Veranschaulichung des Beispiels. Die Zeilen der Matrix repräsentieren das Engagement des Unternehmens auf dem Markt, während die Spalten die Konkurrenzlage widerspiegelt.[11]

Konkurrenzlage: Engagement auf dem Markt:	günstig	normal	ungünstig
1 (gering)	5	3	1
2 (mittel)	14	10	0
3 (stark)	30	5	-5
4 (sehr stark)	12	9	-9

Abb.4: Darstellung einer Entscheidungsmatrix[11]

Die zentrale Frage, die sich hier der Geschäftsführer (Spieler) stellt, ist wie er sich verhalten muss, damit er seinen Gewinn maximieren kann. In der Entscheidungstheorie gibt es zahlreiche Strategien (Lösungsvorschläge), um dieses Ziel zu erreichen.
Im folgenden werden zwei davon aufgelistet. Der Geschäftsführer kann u.a. von den folgenden zwei Strategien eine auswählen:

doi: 10.2313/NET-2018-11-1_03

1. Der Unternehmer könnte die Eintrittswahrscheinlichkeiten für die verschiedenen Konkurrenzlagen schätzen und die Handlungsalternative wählen, für die der Erwartungsgewinn maximal ist.
2. Er wählt das Maximal-Prinzip, bei der der schlechteste mögliche Gewinn maximal ist.

Angenommen das Unternehmen agiert gering auf dem Markt und die Konkurrenzlage ist hoch, sprich ungünstig, dann erwirtschaftet das Unternehmen einen Gewinn von einer Einheit. Auf der anderen Seite erwirtschaftet der Geschäftsführer für sein Unternehmen einen Gewinn von 30 Einheiten, wenn er sich am Markt stark beteiligt und die Konkurrenzlage günstig steht.

Anmerkung: Logischerweise müsste der Unternehmer einen höheren Gewinn erzielen, falls er sich "sehr stark" am Markt engagiert und die Konkurrenzlage günstig steht (hier Gewinn von 12 Einheiten, Maximum liegt aber bei 30 Einheiten). Jedoch wurden hier bewusst die Zahlen so eingetragen, dass dieser "logische" Fall nicht eintritt, um zu veranschaulichen, dass ein Spiel immer noch Regeln definiert und unabhängig von Logik und Rationalität agiert.

Wie sollte sich der Geschäftsführer nun entscheiden?

Für den Spieler ist es nicht leicht, sich für eine Alternative zu entscheiden, jedoch lassen sich Alternativen leicht aussondern. Der Gewinn bei Alternative 4 (sehr starkes Engagement) ist bei jedem Umweltzustand, also bei jedem Verhalten des Gegenspielers, schlechter als der Gewinn bei Alternative 2 (mittleres Engagement). In anderen Worten: Egal was passiert, Alternative 2 schüttet - aus Sicht des Geschäftsführers - einen höheren Gewinn aus, als Alternative 4. Somit wird Alternative 4 aus der Matrix gestrichen, da es für den Geschäftsführer keinen Grund gibt, sich jemals "sehr stark" zu engagieren. Die selbe Entscheidungsregel gilt auch für Alternative 1, die von Alternative 2 überboten und somit dominiert wird. Daher wird auch Alternative 1 von der Entscheidungstheorie eliminiert.

Wie der Spieler (Geschäftsführer) sich letztendlich im weiteren Verlauf entscheidet, hängt von seiner Strategie (Lösung) bzw. Ziel und von den Regeln, die das Spiel definiert, ab. Auf die Lösung wird nicht eingegangen, da der Rahmen dieser Arbeit gesprengt wird.

3.1.3 Dominierte Strategien und Nash-Gleichgewicht

Wenn es für einen Spieler vorteilhaft ist, immer die selbe Strategie zu wählen, unabhängig davon, welche Strategie die anderen Spieler wählen, dann spricht man von einer dominanten Strategie.[11] Damit eng verknüpft ist das Nash-Gleichgewicht.
Das Nash-Gleichgewicht (NGG) beschreibt in nicht kooperativen Spielen eine Kombination von Strategien, bei denen es für keinen der Spieler sinnvoll ist, von seiner Strategie als einziger abzuweichen, um seinen Gewinn zu maximieren. D.h. in einem NGG bereut jeder Spieler auch im Nachhinhein seine Strategiewahl nicht und würde seine Entscheidung wieder genau so treffen.[11]

3.2 2 x 2 - Bimatrix Spiele

Eine Reduktion der Entscheidungsmatrix (Kapitel 3.1.2) ist die 2x2-Bimatrix, in der zwei Spieler ein Spiel spielen, wobei jeder der Player jeweils zwei Handlungsmöglichkeiten hat.[11] Wie man diese Form der Matrix liest und anwendet, wird anhand folgender Grafik (Abb. 5) welche das Beispiel verdeutlichen soll, erläutert.

		Spielerin B(erta): links	rechts
Spieler A(nton):	oben	(2, 1)	(9, 0)
	unten	(1, -1)	(9, 8)

Abb.5: Darstellung einer Bimatrix[11]

Wie bereits oben erwähnt, stellt die Bimatrix zwei Player auf, die jeweils zwei Handlungsmöglichkeiten haben. Die Player können nicht kontrollieren, welche Strategie sein Gegenüber wählt. Die Lösung eines Spiels ist dabei eine Kombination von Verhaltensweisen der Spieler, die als rational gerechtfertigt werden kann [11]. Spieler A (Anton) und Spieler B (Berta) befinden sich in einer Quizsendung und müssen unabhängig voneinander und gleichzeitig auf einen Knopf drücken. Player A hat die Möglichkeit zwischen den Knöpfen *oben* und *unten* zu drücken, während Player B zwischen den Knöpfen *links* und *rechts* drücken kann. Der jeweilige Gewinn bzw. Verlust beider Spieler ist in einem Tupel (a,b) in der Matrix eingetragen. Dabei steht a für den Gewinn/Verlust von Spieler A. Das selbe gilt analog für Spieler B. Wenn Anton beispielsweise den Knopf *unten* drückt und Berta auf *links*, dann gewinnt er in dem Spiel eine Einheit und sie verliert eine Einheit. Die Player erfahren die Knopfwahl des Gegenübers erst nachdem beide unanbhängig und gleichzeitig auf einen Knopf gedrückt haben.[11]

Für welche Alternative sollten sich die Spieler entscheiden?

In der Spieltheorie gilt generell die Annahme, dass jeder Player nur an seinem Gewinn interessiert ist [11]. Betrachtet man die Entscheidungsalternativen, die sich für Berta ergeben, so sieht man folgendes:

1. Sollte Anton *oben* wählen, so wäre es für Berta am gewinnbringendsten den *linken* Knopf zu betätigen
2. Wählt Anton *unten*, so sollte sich Berta für den *rechten* Knopf entscheiden, da dieser - hinsichtlich des Gewinns - am sinnvollsten erscheint.

Aus den zwei genannten Punkten lässt sich nur eines rückschließen: Spielerin B hat keine dominierte Strategie und muss rational handeln. Spieler A muss sich logischerweise und unabhängig von der Wahl, die Spieler B trifft, für den Knopf *oben* entscheiden, da dieser Knopf den *unteren* Knopf dominiert, d.h. der Gewinn von Knopf *oben* ist mindestens

doi: 10.2313/NET-2018-11-1_03

gleichbringend wie der Knopf *unten*. Daher kann Spieler A die zweite Zeile aus der Matrix streichen und somit seine Entscheidungsalternative festlegen. Berta handelt rational und erkennt diese Strategie, womit sie nur noch ihre Wahl auf die reduzierte Matrix anwenden muss. Folglich fällt ihre Wahl selbstverständlich auf den Knopf *links*. Damit ist die Lösung nach dem Dominanzkriterium klar, die Spieler müssen sich für die Kombination (*oben*, *links*) entscheiden. Jeweils beide Player würden einen höheren Gewinn erwirtschaften, sofern sich beide auf die Kombination (*unten*, *rechts*) einigen könnten. Jedoch treten in solchen Spielen meist immer Komplikationen auf: Die Player können nicht kontrollieren, welche Strategie sein Gegenüber wählt.

Im folgenden werden drei Spiele vorgestellt, die in der Sozialwissenschaft häufig verwendet werden. Diese Spiele werden später einen Bezug zu Kapitel 4 darstellen und dort wieder aufgegriffen.

3.2.1 Hirschjagd (Stag Hunt)

Die Hirschjagd geht auf J.J. Rousseau zurück und beschreibt ein Spiel, bei dem es um eine *win-win* Situation geht. In erster Linie beschreibt das Spiel einen Konflikt zwischen Sicherheit und soziale Kooperation, indem die Widersprüche des individuellen Handelns innerhalb der Gemeinschaft aufgezeigt werden, welche letztendlich zur Einrichtung von sozialen Zwangmitteln führt, die eine Kooperation der Mitglieder erfordert und sichert.[12]
Rousseau lässt zwei Spieler (Jäger 1, Jäger 2) auf die Jagd gehen. Im Jagdgebiet kann man zwei Tiere jagen: Hirsche (stag) und Hasen (rabbit). Dabei ist folgendes zu beachten:

1. Beide Spieler müssen unabhängig voneinander entscheiden, welches Tier sie jagen
2. Den Hirsch können nur beide gemeinsam erlegen bzw. jagen, einen Hasen kann jeder alleine jagen. Falls einer der beiden einen Hasen jagen sollte, so entkommt der Hirsch.
3. Beide Tiere gleichzeitig zu jagen ist unmöglich

Das zugehörige Spiel sieht in 2x2-Bimatrix-Form folgendermaßen aus:

		Jägerin 2:	
		Hirsch	Hase
	Hirsch	(5, 5)	(0, 1)
Jäger 1:	Hase	(1, 0)	(1, 1)

Abb.6: Gewinne und Verluste im Hirschjagdspiel in 2x2-Bimatrix-Form[9]

[9]http://www.spieltheorie.de/spieltheorie-grundlagen/win-win-hirschjagd/)

Wie man an Abbildung 6 sehen kann, ergibt sich ein Nullsummenspiel, wenn einer der beiden einen Hasen und der andere jeweils einen Hirsch jagt. Auf der anderen Seite entsteht ein Nash-Gleichgewicht (Kap. **??**) wenn beide Spieler den Hirsch jagen, als auch wenn beide einen Hasen jagen. Allerdings gewinnen beide Spieler beim Hirsch eine Auszahlung von 5 Einheiten, beim Hasen dagegen nur eine Auszahlung von einer Einheit. Die Zusammenarbeit lohnt sich also für beide und es gibt eigentlich gar keinen Grund für einen Interessenkonflikt.
Jedoch gibt es einen Haken: jeder Spieler versucht in erster Linie seinen Gewinn zu maximieren. Allerdings achtet der Spieler auch darauf, sein Minimum zu maximieren. In diesem Spiel beträgt das Minimum null, falls man einen Hasen jagt und eins, falls man einen Hirsch jagt, vorausgesetzt, der Mitspieler jagt das jeweils andere Tier. Rational empfiehlt es sich hier, den Hasen zu jagen, weil man da gegen leere Taschen abgesichert ist. Diese Strategie ist aber nur sinnvoll, wenn es sich um ein Nullsummenspiel handeln würde. In diesem Spiel ist aber die Zusammenarbeit und Kommunikation möglich, daher sollten beide Parteien den Hirsch jagen.[12]

3.2.2 Taube-Falke Spiel (Hawk Dove Game)

In diesem Spiel gelangen zwei Tiere gleichzeitig zu einer Ressource, z.B. ein günstiges Gebiet für ein Revier. Dieses Revier kann allerdings nur von einem der beiden genutzt werden. Hier repräsentieren die Tiere die Spieler A und B und haben zwei Auswahlmöglichkeiten: Flucht (Taube) oder Kampf (Falke). Jedes Tier nimmt zu Beginn eine Drohposition ein, damit der Mitspieler nicht sofort erkennt, ob sein Gegenüber kämpfen oder flüchten will. Wenn ein Tier sich entscheidet, die Strategie Taube (dove) zu wählen, so flüchtet es sofort. Entscheidet das Tier sich für den Falken (hawk), so nimmt es nicht nur die Drohposition ein, sondern kämpft - falls das andere Tier sich auch für den Falken entscheidet - bis aufs Blut.[11]
Die Tiere müssen sich wegen der Eingangssituation (Drohposition) sofort und unabhängig von der Strategie des Gegenspielers entscheiden. Dadurch kann sich keiner der Player auf das Verhalten des anderen einstellen.[11]

Das zugehörige Spiel sieht in 2x2-Bimatrix-Form folgendermaßen aus:

		Tier B:	
		Taube	Falke
Tier A:	Taube	(1,1)	**(0,2)**
	Falke	**(2,0)**	(-10,-10)

Abb.7: Gewinne und Verluste im Taube-Falke-Spiel in 2x2-Bimatrix-Form[11]

Treffen zwei Tauben aufeinander, so erhält jeder der beiden Tauben das Revier mit einer Wahrscheinlichkeit von $\frac{1}{2}$:

doi: 10.2313/NET-2018-11-1_03

damit beträgt die erwartete Auszahlung: $\frac{1}{2} * 2 = 1$. Treffen zwei Falken aufeinander, so erleiden beide einen Verlust von -10 Einheiten und sterben. Diese zwei Fälle sind dem Nash-Gleichgewicht zugeordnet.[11]
Stößt eine Taube auf einen Falken, so geht die Taube leer aus (0 Einheiten) und der Falke enthält 2 Einheiten (Nullsummenspiel).
Wie löst ein Spieler dieses Spiel zu seinen Gunsten? In diesem Spiel wäre es ratsam nach dem Prinzip *"der Klügere gibt nach"* zu handeln. Man geht zwar nach dem Nullsummenspiel eventuell das Risiko ein, leer auszugehen, jedoch hat man vielleicht Glück und der Gegenspieler wählt ebenfalls die selbe Strategie, sodass man immerhin noch eine Einheit erhält. Andernfalls kommt es zu einem bitteren Kampf, in dem im schlimmsten Fall beide -10 Einheiten verlieren.[11]
Aus diesem Modell geht hervor, dass Tiere derselben Art sich nicht zerfleischen. Dies liegt aber nicht an der inneren Harmonie der Natur, sondern aus Angst, dass der Gegner auch *Falke* spielen könnte und es somit zu einem Zweikampf kommt, der einen immensen Schaden verursacht. In der realen Welt könnte dieses Modell vielleicht erklären, warum der Kalte Krieg nicht in einen Atomkrieg geendet hat.[11]

3.2.3 *Chicken Spiel (Game of Chicken)*

Bei einer Mutprobe fahren Spieler A und Spieler B mit ihren Autos direkt aufeinander zu. Dabei hat jeder der beiden Spieler zwei Optionen zur Auswahl: Kurs halten oder ausweichen. Derjenige Fahrer, der zuerst ausweicht, ist das "Chicken", bleibt aber am Leben. Der andere Spieler gilt dann als "Held".[11]

Das Spiel sieht in 2x2-Bimatrix-Form folgendermaßen aus:

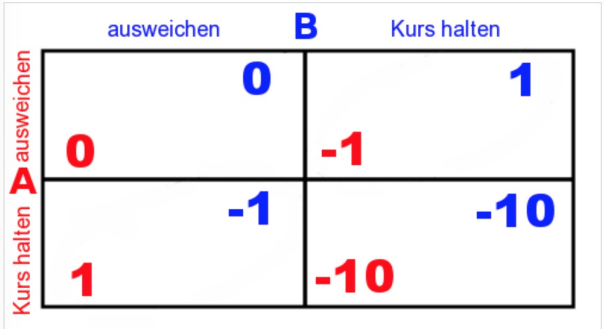

Abb.8: Gewinne und Verluste im Chicken-Spiel in 2x2-Bimatrix-Form[13]

Erweisen sich beide Player als irrational stur, so kommt es zu einer Kollision und beide sterben (-10 Einheiten). Dies steht nicht im Interesse beider Spieler. Wenn beide Fahrer entweder Kurs halten oder ausweichen, so entsteht hier wieder ein Nash-Gleichgewicht (Kap. **??**). Falls einer der Fahrer kurs hält und der andere ausweicht, so verliert der eine einen Minuspunkt (Chicken), der andere gewinnt einen Punkt (Held) und beide überleben.[11]
Hier existiert keine dominante Strategie, da Weiterfahren zum bestmöglichen, aber auch zum allerschlechtesten Ergebnis führen kann. Wiederum besteht Unsicherheit über das Verhalten des anderen, weswegen auch Wahrscheinlichkeitsüberlegungen in die Entscheidung einfließen können. Für beide Spieler ist klar, dass sie es doch bevorzugen als Feigling dazustehen. Weichen beide gleichzeitig aus, gibt es weder Gewinner noch Verlierer.[11]

Im nächsten Kapitel werden die im Kapitel 3 gennanten Spiele hinsichtlich der Blockchain aufgearbeitet, gedeutet und versucht einen Zusammenhang bzw. Parallele zwischen der Blockchain und der Spieltheorie herzustellen. Dabei wird zuerst ein Spiel beschrieben und anschließend die Relation zur Spieltheorie herangezogen.

4. INTERPRETATION

Angenommen es gibt einen Spieler A, der sich überlegt in das Mininggeschäft einzusteigen. Der Spieler kann helfen, jedes Projekt, das auf Blockchain basiert, zu entwickeln, indem er einen Block generiert und validiert (Mining). Für jeden Miningvorgang erhält der Spieler im Gegenzug ein Honorar in Form von Bitcoin oder Transaktionsgebühr. Für das Minen muss der Spieler Ressourcen (z.B. technische Ausrüstung und Strom) zu einem bestimmten Preis investieren. Es wird angenommen, dass jeder Spieler dieselben technischen Voraussetzungen besitzt.
Im Mining gibt es unterschiedliche Möglichkeiten für einen Miner zu minen. Damit dieses Spiel nicht in der Komplexität ausartet, gehen wir jedoch von dem einfachsten Fall aus: der Spieler hat zwei Alternativen, von denen er eine auswählen muss. Nachdem der Spieler einen Block generiert hat, muss dieser Block an die bestehende Blockkette angehängt werden (vgl. 2.2):

1. Strategie 1 (*monotone Strategie*[14]): Spieler A könnte die längste Kette verlängern, indem er eine Belohnung von 5 Einheiten erhält. Der nächste Miner (Spieler B), der einen Block mined, erhält dann auch 5 Einheiten.

2. Strategie 2: Spieler A lässt den Transaktionsbaum spalten (Fork) bzw. hängt seinen Block irgendwo an einer anderen Verzweigung der Kette und nicht an der längsten Transaktionskette. Er erhält dafür eine Belohnung von 55 Einheiten.

Abbildung 9 zeigt das Spiel in der 2x2-Bimatrix. Dabei repräsentiert Spieler B nicht nur einen anderen Mitspieler, sondern alle anderen Miner. Die Einheiten sind willkürlich gewählt.

Die Spielregeln der Miner werden in den großen öffentlichen Blockchains durch das *Proof-of-Work*-Protokoll (vgl. Kap. 2.3) festgelegt. Diese Bitcoin-Dokumentation besagt, dass Miner die monotone Strategie wählen sollten. Jedoch ignorieren einige Spieler diese Regeln, um aus ihrem Nutzen ein Maximum zu ziehen. In diesem Spiel gehen wir genau diesem Beispiel nach und gehen davon aus, dass Spieler A genau so handeln wird, um seinen Nutzen zu maximieren, unanbhängig davon, was das *Proof-of-Work*-Protokoll vorschreibt.[8]

[10] http://scienceblogs.de/zoonpolitikon/2008/04/24/spieltheorie-einfach-erklart-ii-feiglingsspiel-chicken/

[14] Eine Strategie ist monoton, wenn der längste Block um eine neuen Block ergänzt wird.

doi: 10.2313/NET-2018-11-1_03

	Spieler B (alle anderen Miner)		
		Längste Block	Fork
Spieler A	Längste Block	(5,5)	(5,55)
	Fork	(55,5	(55,55)

Abb.9: Mining-Game in 2x2-Bimatrix-Form - Eigene Darstellung

4.1 Analogie zur Spieltheorie

Welche Option ist die bessre Alternative für Spieler A? Um dies herauszufinden, muss man überlegen, welche Strategie die anderen Miner anwenden würden. Dazu betrachtet man die Spiele, die in Kapitel 3 vorgestellt wurden.

Hirschjagd (vgl. Kap. 3.2.1)

Sowohl Spieler A, als auch alle anderen Spieler (Miner) müssen wie bei der Hirschjagd unabhängig voneinander entscheiden, welche Strategie Sie wählen. Beide Player können gemeinsam dafür sorgen, dass der längste Block noch länger wird. Somit sollte es keinen Interessenskonflikt geben. Es kann aber auch sein, dass einer der Spieler an seinen maximalen Gewinn denkt und deshalb seinen Block auf dem Fork aufbaut. Nur wenn beide Miner "kooperieren" im Sinne der Hirschjagd, können Forks verhindert werden und sichern so, dass ihre Blöcke in der Konsens-Kette landen, um dann honoriert zu werden. Da aber beim Minen keine klassische Kooperation möglich ist, bleibt nur noch die Rationalität und das *Proof-of-Work* als Wegbegleiter.[8]

Taube-Falke Spiel (vgl. Kap. 3.2.2)

Nach dem Taube-Falke Spiel "gibt der Klügere nach" und jeder Spieler sollte nach Nakamoto (2008) und dem *Proof-of-Work* die monotone Strategie wählen. Dadurch hat jeder Spieler kurzfristig gesehen einen niedrigeren Gewinn erzielt, aber langfristig gesehen landet sein Block möglicherweise in der Konsens-Kette, wodurch er einen höheren Nutzen erreicht. In Anlehnung an das Taube-Falke Spiel würden seine Blöcke somit in der Blockchainkette "überleben" und einen Gewinn honorieren.

Chicken Spiel (vgl. Kap. 3.2.3)

Ähnlich zum Taube-Falke Spiel verhält sich in diesem Fall das Chicken Spiel, bei dem derjenige Miner, der die monotone Strategie wählt, möglicherweise zwar als "Chicken" degradiert wird, dessen Block allerdings nachhaltig in der Transaktionskette landet, die am längsten ist, welche seine Honorierung absichert.

In allen drei Spielformen ist zu beobachten, dass falls Spieler A die monotone Strategie wählt, ein Nash-Gleichgewicht existiert, da alle Player ebenfalls die erste Strategie wählen. Falls Spieler A in der nächsten Transaktionsrunde zu einer anderen Strategie wechseln würde, so hätte er keinen höheren Nutzen (Gewinn) davon, da sich die Rate für die Blockerstellung nicht beschleunigen würde.[8]. Falls Spieler A einen Fork wählt und Spieler B die monotone Strategie oder umgekehrt, dann erhält man ein Nullsummenspiel.

Reale Lösung

Spieler A kann nicht kontrollieren, welche Strategie die anderen Miner wählen. Wenn alle anderen Miner der Heuristik des Mining auf dem Block folgen, der am längsten ist und wenn es im Netzwerk keine Latenz gibt, so ist Forking ineffektiv und Strategie 1 ist eindeutig überlegen. Auf der anderen Seite werden sie sich vielleicht dafür entscheiden, auf dem Fork statt auf dem längsten Block zu bauen, da Option 2 eine höhre Belohnung (55 Einheiten) ausgibt. Diese Belohnung ist jedoch nur wertvoll, wenn der neue Block in der langfristigen Konsens-Kette endet. Wenn ständig neue Forks entstehen, dann hat man langfristig gesehen keinen Nutzen aus den Blöcken, da jede Kette unterbrochen wird. Des Weiteren gelten in der Realität Forks als gefährlich für Bitcoin, da sie mehrere konkurrierende Versionen der Transaktionsgeschichte erstellen und somit Zweifel darüber aufkommen lassen, wem welche Münzen gehören.[8] Tatsächlich nimmt der Spieler rational an, dass jeder Block, der aus dem Gleichgewichtspfad gelöst wird, von anderen Minern nicht akzeptiert wird und die entsprechende Belohnung bzw. dieser Zweig wertlos sein wird. Folglich hat ein Miner, der Belohnungen gesammelt hat, indem er mehrere Blöcke auf einer gegebenen Kette gelöst hat, ein Interesse daran, dass diese Kette aktiv bleibt. Insbesondere würde der Wert dieser Belohnungen sinken, wenn er in eine andere Kette wechseln würde.[4] Jeder Miner sollte sich also an das *Proof-of-Work*-Protokoll halten.

5. ZUSAMMENFASSUNG/FAZIT

Dieses Paper hat gezeigt, dass das Minen von Kryptowährungen, als ein Konsens-Spiel im Sinne der Spieltheorie betrachtet werden kann. Beim Mining-Mechanismus erhält jeder Teilnehmer (Spieler bzw. Miner) Belohnungen in Form von Bitcoin oder Transaktionsgebühren. Im Gegenzug muss Spieler A Ressourcen - wie z.B. Strom - investieren um "Rechenpuzzle" zu lösen. In Anlehnung der Spieltheorie lässt sich dieses "Spiel" - wie jedes andere auch - in einer Entscheidungsmatrix (Bimatrix) runterbrechen. Dabei werden die Regeln von einem *Proof-of-Work*-Protokoll definiert, welche allerdings von den Spielern (Minern) möglicherweise ignoriert werden, um ihren Gewinn zu maximieren. Damit jeder Miner seine Rechenleistung honoriert bekommt, muss er sich vereinfacht für eine Strategie entscheiden. Dabei gibt es zwei Optionen zur Auswahl. Entweder der Miner mined die Transaktionsblöcke und hängt sie, damit sie validiert werden, an den längsten Block der Transaktionskette (monotone Strategie) oder er hängt seinen Transaktionsblock an einer anderen Verzweigung in der Transaktionskette (Fork). Ersteres wird vom *Proof-of-Work*-Protokoll empfohlen, da Forks mehrere konkurrierende Versionen der Transaktionsgeschichte erstellen und somit Zweifel darüber aufkommen lassen, wem welche Münzen gehören. Entscheidet sich Spieler A für die monotone Strategie, so erhält er einen bestimmten Betrag. Fällt seine Wahl allerdings auf den Fork, so erhält er eine höhere Gage. Auf dem ersten Blick liegt die Wahl, für die sich der Miner entscheiden

doi: 10.2313/NET-2018-11-1_03

sollte, auf der Hand. Doch bei genauerer Betrachtung ist ersichtlich, dass es für ihn doch nicht so einfach ist, seine Strategie zu wählen. Wie bereits erwähnt, birgen Forks einige Gefahren. Des Weiteren erhält ein Miner nur dann seinen Gewinn, wenn sein Block langfristig in der Konsens-Kette landet. Dies bedeutet intuitiv: wenn alle anderen Spieler die längste Transaktionskette anvisieren und Miner A seinen Block an den Fork anhängt, er möglicherweise seinen Gewinn nicht einstreichen kann, da sein Block langfristig aus der Konsens-Kette verschwindet. Das optimale Ergebnis nach der Hirschjagd scheint in diesem Fall ein unsicheres Ergebnis zu sein. Nach dem Taube-Falke Spiel "gibt der Klügere nach" und jeder Spieler sollte nach Nakamoto (2008) und dem *Proof-of-Work* die monotone Strategie wählen. Ähnlich zum Taube-Falke Spiel verhält sich in diesem Fall das Chicken Spiel, bei dem derjenige Miner, der die monotone Strategie wählt, möglicherweise zwar als "Chicken" degradiert wird, dessen Block allerdings nachhaltig in der Transaktionskette landet, die am längsten ist, welche seine Honorierung absichert. Folglich sollte sich also jeder Miner an das *Proof-of-Work*-Protokoll halten.

6. LITERATUR

[1] Whitepaper: Nxt: https://nxtwiki.org/wiki/whitepaper:nxt.

[2] M. Abliz and T. Znati. A guided tour puzzle for denial of service prevention. In *Proceedings of the 2009 Annual Computer Security Applications Conference*, ACSAC '09, pages 279–288, Washington, DC, USA, 2009. IEEE Computer Society.

[3] A. Back. Hashcash - a denial of service counter-measure. September 2002.

[4] B. Biais, C. Bisiere, M. Bouvard, and C. Casamatta. The blockchain folk theorem. January 2018.

[5] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan. On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 154–167, New York, NY, USA, 2016. ACM.

[6] S. King and N. S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake; https://peercoin.net/assets/paper/peercoin-paper.pdf. 2012.

[7] P. D. W. Krabs. *Spieltheorie - Dynamische Behandlung von Spielen*. G. Teubner Verlag - Springer Science+Business Media, Stuttgart, 2005.

[8] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. 2013.

[9] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system; http://bitcoin.org/bitcoin.pdf. 2008.

[10] W. Prinz, T. Rose, T. Osterland, C. Putschli, T. Osterland, and C. Putschli. *Blockchain*, pages 311–319. Springer Berlin Heidelberg, Berlin, Heidelberg, 2018.

[11] C. Rieck. *Spieltheorie - Einführung für Wirtschafts- und Sozialwissenschaftler*. Dr. Th. Gabler GmbH Verlag - Bertelsmann International, Wiesbaden, 1993.

[12] R. v. Rooij. The stag hunt and the evolution of social structure. *Studia Logica*, 85(1):133–138, Feb 2007.