Die Blockchain-Technologie.
Von Kryptowährung zu verteilten Notarsystemen

Tom Zimmerling

Seminararbeit im Interdisziplinären Lehrangebot
des Instituts für Informatik

Leitung: Prof. Hans-Gert Gräbe, Ken Pierre Kleemann

`http://bis.informatik.uni-leipzig.de/de/Lehre/Graebe/Inter`

Leipzig, 31.09.2017

Inhaltsverzeichnis

1. Einleitung

Bei dem Wort Blockchain denken die meisten Leute an Kryptowährungen wie Bitcoin. Doch die Blockchain ist lediglich die Technologie, die hinter Bitcoin steckt. In dieser Arbeit werde ich mich mit dem Thema Blockchain und ihren Möglichkeiten beschäftigen.

BitCoin, eingeführt von Nakamoto[1], ist eine Art elektronisches Bargeld auf Basis eines Peer to Peer Netzwerkes. Es ist aber nicht nur als Geld zu sehen, denn durch die neue Technologie der Blockchain sind ganz neue praktische Anwendungen von Computersystemen entstanden. Das Bitcoin-System ist selbstorganisiert und besteht hauptsächlich aus drei Arten von Teilnehmern: Der Bitcoin Benutzer/Inhaber, den Handelsplattformen und den Bitcoin Minern. Die Teilnehmer können sich dem System anschließen oder es verlassen. Es ist keine Behörde für die Verwaltung oder Wartung des Systems nötig. Transaktionen werden mit Hilfe der Handelsplattformen getätigt. Diese erhalten für eine Transaktion eine Provision. Die Miner haben die Aufgabe neue Bitcoins zu produzieren, als Motivation bekommen sie selbst Bitcoin. All diese Prozesse werden in der Blockchain gesammelt und sind somit jederzeit nachvollziehbar. Die Gesamtmenge an Bitcoin nimmt nach und nach zu, bis die Menge von 21.000.000 erreicht ist. Dies wird ungefähr im Jahr 2140 erreicht sein. Bisher sehen viele Regierungen den Bitcoin kritisch, daher gibt es keinen offiziellen Rechtsschutz, dennoch gewinnt Bitcoin zunehmend an Popularität.

Doch wie Anfangs schon erwähnt, gibt es nicht nur den Bitcoin, der die Blockchain nutzt. Die bekannteste Entwicklung nach dem Bitcoin ist Ethereum. Ethereum ist wie Bitcoin eine dezentralisierte Plattform, welche unabhängig von Bitcoin arbeitet. Anders als bei Bitcoin geht es bei Ethereum vor allem um Smart Contracts. Durch Computeralgorithmen werden Vertragsbedingungen und Verhandlungen technisch gesteuert und machen Verschriftlichungen unter Umständen überflüssig. Diese Smart Contracts werden in der eigens entwickelten Programmiersprache Solidity geschrieben. Ethereum ist eine Entwicklung von Vitalik Buterin, Gavin Wood und Jeffrey Wilcke und wurde 2013 veröffentlicht.[2]

Ich werde mich im weiteren einige grundlegende Dinge zum Thema Blockchain und Bitcoin bearbeiten um dann zu erläutern warum Smart Contracts ihre Berechtigung haben und die Zukunft sein könnte.

---

[1] (Nakamoto, 2009)
[2] (Wikipedia, 2017)

2. Distributed Ledger und Blockchain

Ein Distributed Ledger (wörtlich „verteiltes Kontobuch“) ist ein öffentliches, dezentral geführtes Kontobuch. Es ist die technologische Grundlage virtueller Währungen und dient dazu im digitalen Zahlungs- und Geschäftsverkehr Transaktionen von Nutzer zu Nutzer aufzuzeichnen ohne, dass es einer zentralen Stelle bedarf, die jede einzelne Transaktion legitimiert. Die Blockchain ist das Distributed Ledger, welches der virtuellen Währung Bitcoins zugrunde liegt.

Kryptowährungen unterliegen allen Arten von ideologischen Kämpfen aber in einem sind die meisten Interessenten einverstanden: Dass das zugrundeliegende Konzept eines dezentralisierten öffentlichen Ledgers, das gemeinsam von einem Netzwerk von Teilnehmern gepflegt wird, sehr wichtig ist. Dies hat auch über die Devisentransaktionen hinaus zu einem großen Interesse an Blockchain Projekten geführt.[3]

Eine Blockchain ist als eine Datenbank zu sehen die inkrementell von einem Netzwerk von Nutzern aufgebaut wird, die dieselbe Software ausführen und die den Einschränkungen und Regeln der Software unterliegen. Es kann fast als eine Kalkulationstabelle gesehen werden, der sich allmählich neue Blöcke anketten. Eine Blockchain-Datenbank wird aufgebaut und gepflegt, solange die Software ausgeführt wird. Im Gegensatz zu einer zentralisierten Datenbank, die von einer einzigen Einheit gehalten wird, bleibt die Blockchain auch in Betrieb, wenn einzelne Teilnehmer austreten. Es schafft eine nahezu unauslöschliche Aufzeichnung, die resistent gegen Manipulation durch einzelne Parteien ist.

Darüber hinaus gibt es die Möglichkeit selbst eine Blockchain-Datenbank zu erstellen, die sämtliche Arten von Daten speichern kann, einschließlich Eigentums-Titeln, Verträgen, Aktien[4], Abstimmungsentscheidungen[5] oder sogar Reputationsbewertungen[6]. Gruppen wie Ethereum[7], Counterparty[8] und Blockstream[9]arbeiten an einer Software um es Personen oder Start-ups zu ermöglichen Blockchain-basierte Systeme zu implementieren. Zum Beispiel ist Provenance[10] ein Start-up, dass versucht das Ethereum-System zu verwenden, um ein hochtransparentes Ledger der globalen Daten der Unternehmenskette zu schaffen.

[3] (Swan, 2015)
[4] (Lee, 2015)
[5] (Noizat, 2015)
[6] (Scott, 2015)
[7] (www.ethereum.org, 2017)
[8] (www.counterparty.io, 2017)
[9] (www.blockstream.com, 2017)
[10] (www.provenance.org, 2017)

Zurzeit arbeitet die Szene daran intelligente Verträge auf eine Blockchain aufzuzeichnen, sodass die Teilnehmer mittels interaktiver Aufgaben zusammenarbeiten können, um einfache Aufgaben zu übernehmen.[11] Stellen Sie sich ein kodiertes Blockchain-basiertes Skript vor, das aktiviert wird, wenn zwei Parteien Bitcoins zu einem Treuhandel-Bitcoin-Konto senden. Dieses wird vom Skript gesteuert und gibt die Bitcoins in der Zukunft frei. Es kann sich zum Beispiel um eine Fußballwette handeln, bei der der Smart Contract automatisch den Gewinner ermittelt und die gewonnenen Bitcoins auf das Gewinnerkonto überweist.

Solche einfachen Verträge könnten zusammengefasst werden, um die Grundlage für komplexere mehrstufige oder multifunktionale Einheiten zu bilden, die von einigen als dezentralisierte autonome Organisationen (DAOs) bezeichnet werden.[12] Solche DAOs sind schwer zu verstehen, sind aber im Wesentlichen fortgeschrittene, mehrstufige Algorithmen, die auf einem dezentralen Netzwerk von Computern gehalten werden, anstatt von einem einzigen Management-Team oder einer Organisation gesteuert zu werden.

Für diejenigen mit einer marktwirtschaftlichen Orientierung sind Verträge um Eigentumsrechte besonders interessant. Ein häufig zitierter Anwendungsfall hierfür sind Landregister.[13] In Ländern mit schwachen Regierungs- und Organisationssystemen gibt es ein Problem der Doppelregistrierung von Land, Landtitelbetrug oder Titel zu ungewissem Land. Dies kann mit einem Blockchain-System möglicherweise behoben werden, um so Landtitel eindeutig zu bestimmen und öffentlich aufzuzeichnen. Im Jahr 2015 kündigte Honduras ein Geschäft mit dem amerikanischen Unternehmen Factom[14] an, um ein Blockchain-basiertes Grundbuch[15] zu entwickeln.

In einem Interview in dem Forbes Magazine heißt es "How Bitcoin will end world poverty“[16]. Brian Singer behauptet, dass die Blockchain-Technologie eine sehr gute Möglichkeit sei die Vision von Hernando de Soto, Eigentumsrechte in Volkswirtschaften zu integrieren, zu verwirklichen. Eigentumsrechte können so als Sicherheiten verwendet werden, sodass günstigere Bankkredite an Unternehmer vergeben werden können.

[11] (Wright, 2015)
[12] (Pangburn, 2015)
[13] (Williams, 2015)
[14] (www.factom.org, 2017)
[15] (Chavez-Dreyfuss, 2015)
[16] (Forbes, 2015)

Diese Analyse beruht auf der Behauptung, dass Markt- und Kapitalisierungsprozesse, sofern Vermögen und Vertrag gut geschützt sind, dazu beitragen werden, Menschen aus der Armut herauszuheben und den verborgenen Wert der Volkswirtschaften hervorzubringen.
Es ist jedoch unklar, ob die Blockchain solche Probleme lösen wird. An Orten, die Probleme mit Landtiteln haben, gibt es in der Regel schwache Institutionen, es bleibt also Ungewiss ob eine solch neuartige Technologie diese Länder erreichen wird. In einem solchen Kontext hat die Einführung einer Technologie, die zur Aufzeichnung von Forderungen verwendet werden kann, einen geringen Stellenwert, es sei denn, es gibt starke rechtliche Institutionen, die die aufgezeichneten Blockchain-Ansprüche erkennen und Ansprüche geltend machen. Hier herrscht eine gewisse Ironie. Die Blockchain-Technologie ist in Ländern, in denen es schwache Institutionen und Parteien gibt, die sich nicht vertrauen, zum Beispiel in einer Umgebung wie Afghanistan, mit geringer Staatskapazität und niedrigem Vertrauen, in Konflikt.

3. Ist Bitcoin eine Währung?

Währung oder Geld im Allgemeinen ist in der Regel durch drei Hauptfunktionen definiert: Ein Medium der Börse, eine Rechnungseinheit auf dem Konto und ein Vermögenswert. [17]Unter den verschiedenen Währungsarten unterscheiden sich virtuelle Währungen eindeutig von Fiat-Währungen (d.h. "reale Währung", "echtes Geld", "nationale Währung" oder "Standardwährung"), die im Münz- und Papierformat als gesetzliches Zahlungsmittel bezeichnet wird. Diese werden von der Zentralbank reglementiert und im Ausstellungsland verwendet und akzeptiert (Abbildung 1).[18] Nach der von der EZB vorgeschlagenen Definition ist eine virtuelle Währung eine Art von unreguliertem, digitalem Geld, das ausgestellt und in der Regel von seinen Entwicklern kontrolliert und unter den Mitgliedern einer bestimmten virtuellen Gemeinschaft verwendet und akzeptiert wird.[19] Ähnlich sind nach der EBA virtuelle Währungen als eine digitale Wertdarstellung definiert, die weder von einer Zentralbank oder einer öffentlichen Behörde ausgestellt wird, noch notwendiger weise an eine konventionelle Währung gebunden ist, sondern nur von natürlichen oder juristischen Personen als Austauschmittel, gelagert oder gehandelt werden. [20]

[17] (Mankiw, 2007)
[18] (FATF, 2014)
[19] (ECB, 2012)
[20] (EBA, 2014)

Table 1
Type of currencies

	Money (currency) format	
	Physical	**Digital**
Legal status		
Unregulated	Certain types of local currencies	Virtual currency
Regulated	Banknotes and coins	E-money
		Commercial bank money (deposits)

Abbildung 1 – ECB (2012)[21]

Die beliebteste virtuelle Währung ist BitCoin, die 2009 von dem japanischen Programmierer Satoshi Nakamoto erstellt wurde.[22] Es war die erste virtuelle Open-Source-Währung. BitCoin wird von einem Open-Source-Software-Algorithmus, der das globale Internet verwendet, verwaltet. Als Digitale Währung verwendet BitCoin die Prinzipien der Kryptographie, um die Erstellung und den Austausch von BitCoins zu steuern. BitCoins können in lokalen Brieftaschen (z. B. PC, Smartphone), unter Verwendung einer Open-Source-Software, oder in einer Online-Brieftasche[23]gespeichert werden.

Im Vergleich zu Standard-Fiat-Währungen wie US-Dollar oder Euro ist ein Merkmal von BitCoin, dass die Menge der im Umlauf befindlichen Einheiten nicht von einer Person, einer Gruppe, einer Firma, einer zentralen Behörde oder einer Regierung kontrolliert wird, sondern von einem Software-Algorithmus reguliert wird. BitCoins werden in einem Mining-Prozess erstellt, in dem Netzwerkteilnehmer, die ihre Rechenleistung bereitstellen, die Zahlungen in der BlockChain verifizieren und aufzeichnen. Als Gegenleistung für diesen Service erhalten sie Transaktionsgebühren und neu geprägte BitCoins. Eine feste Menge an BitCoins wird als eine konstant definierte und öffentlich bekannte Menge ausgegeben, wonach der Bestand an BitCoins mit abnehmender Rate zunimmt. Im Jahr 2140 wird die Wachstumsrate von BitCoin

[21] (ECB, 2012)
[22] (Nakamoto, 2009)
[23] (Brito, 2013)

gegen null konvergieren. Dann ist die maximale Menge an BitCoins, 21 Millionen, im Umlauf. Nach dem aktuellen Algorithmus wird es sich nach 2140 nicht ändern.

BitCoin hat keine physische Darbietung. Stattdessen wird es entweder auf elektronischen Geräten (z. B. Personal Computer, Mobile, Tablette) gespeichert oder einem Online-Service anvertraut und wird über das Internet übertragen. BitCoins können sowohl für Waren als auch für Dienstleistungen ausgegeben werden, wenn sie vom Händler akzeptiert werden. Benutzer interagieren direkt und zum großen Teil anonym. Es gibt weder eine zentrale Stelle, noch eine andere Vermittlerinstitution, die an den Transaktionen beteiligt ist. Derzeit können BitCoins entweder (1) erworben werden indem sie Fiat-Geld (z,B, US-Dollar, Euro) auf einer BitCoin-Börse oder von einem BitCoin-Händler austauschen (2) oder indem sie sie aus dem Verkauf von Waren oder Dienstleistungen erhalten. Die 3. Möglichkeit ist es die BitCoins selbst zu minen (ein Prozess um BitCoins herzustellen).[24]

BitCoins können verwendet werden um Waren oder Dienstleistungen weltweit zu kaufen, vorausgesetzt der Transaktionspartner akzeptiert BitCoin als Mittel der Zahlung. Eine Transaktion impliziert, dass der derzeitige Eigentümer der BitCoins das Eigentum an einer bestimmten Anzahl von BitCoins an einen anderen Marktteilnehmer im Austausch für andere Währungen, Waren oder Dienstleistungen überträgt. Eine kontinuierlich wachsende Zahl von Unternehmen akzeptiert BitCoins als Zahlungen für ihre Waren und Dienstleistungen, zu Beginn des Jahres 2015 gab es mehr als 100.000 Shops, die BitCoins akzeptierten.[25] Im April 2017 sind es alleine in Japan, dem Land mit dem weltweit größten Handelsvolumen von BitCoin, 260.000[26] Shops.

Es gibt zwei konkurrierende Ansichten in der Literatur darüber, ob BitCoin die drei Kriterien einer Währung (ein Medium der Börse, eine Rechnungseinheit auf dem Konto und ein Vermögenswert) erfüllt. Ein Teil der Literatur argumentiert, dass BitCoin sich nicht weitgehend wie eine echte Währung verhält, da es nicht die Hauptfunktionen einer Währung erfüllt, sondern eher als Objekt für spekulative Investitionen dient.[27] Andere

[24] (Plassaras, 2013)
[25] (www.coindesk.com, 2015)
[26] (Helms, 2017)
[27] (Velde, 2013)

Forschungsrichtungen betonen das Potenzial von BitCoin und sehen es als globale Währung mit starkem Zukunftspotential an.[28]

4. Smart Contracts

Die Idee eines Peer-to-Peer-Systems von Verträgen die kryptographisch erstellt werden geht mindestens 20 Jahre zurück.[29] Aber es war weitgehend der Erfolg von Bitcoin, der den Impuls gab, die Idee in die Praxis umzusetzen. Das erfolgreichste Projekt zum Thema Smart Contract ist Ethereum[30].

Der Ethereum Gründer ist Vitalik Buterin, ein Mitbegründer des Bitcoin Magazins. Ethereum hat seine eigene Währung, genannt "Ether"[31] und wird mit ETH abgekürzt. Allerdings spielt die Währung nur eine Nebenrolle und dient nicht dem Selbstzweck. Ethereum bietet eine Plattform und eine Programmiersprache, die genügend ausdrucksstarke Flexibilität hat um einen kryptographisch durchsetzbaren Vertrag zu beschreiben (der Fachausdruck ist "Turing complete"). Eine Transaktion, die einen Teil Code enthält, muss eine Gebühr enthalten, die proportional zur Anzahl der Computeranweisungen, die ausgeführt werden, berechnet wird. (Dies verhindert der Code, der unendliche Schleifen hat.) Darüber hinaus, kann ETH wie Bitcoin auch versendet und empfangen werden, wenn man im Besitz der Software ist. Ein einfaches Beispiel dafür wie Etherum-Verträge funktionieren können lautet wie folgt:

Angenommen, zwei Benutzer A und B, die in verschiedenen Teilen der Welt leben, wollen 1000 ETH auf das Ergebnis der Fußball Weltmeisterschaft wetten. Sie einigen sich auf ein Ethereum Smart Contract und stellen 1000 ETH zur Verfügung, die unter der Bedingung des Vertrages eingefroren werden. Während die WM läuft, haben Sie keinen Zugriff zu diesem Ether. Sobald der Sieger der WM feststeht, konsultiert der Smart Contract mehrere Webseiten um festzustellen welches Team gewonnen hat und überträgt dem Gewinner automatisch die eingefrorenen Ether auf die digitale Brieftasche des Gewinners.

[28] (Plassaras, 2013)
[29] (Szabo, Formalizing and securing relationships on public networks, 1997)
[30] (www.ethereum.org, 2017)

[31] Im Folgenden als ETH abgekürzt

4.1 Use Cases zu Smart Contracts

4.1.1 Smart Contracts für digitale Identität

Nicht nur bei Sportwetten haben Smart Contracts Vorteile. Durch sie kann es der Einzelperson auch ermöglicht werden digitale Ausweise zu besitzen. Bestandteile dieser könnten zum Beispiel personenbezogene Daten, Vermögenswerte oder die eigene Identität sein. Hierzu gilt es aber zunächst einige Herausforderungen zu meistern. Die wohl größte Herausforderung ist, Akzeptanz der Bevölkerung in eine digitale und sichere Identität zu schaffen. Außerdem fehlen hierzu bis heute in den meisten Ländern die technischen Voraussetzungen. In Estland ist die Regierung hier schon etwas weiter. Den Bürgern wird es dort schon jetzt ermöglicht sämtliche Behördengänge online zu erledigen. [32]

4.1.2 Smart Contracts für den Wertpapierhandel

Der Wertpapierhandel kann vereinfacht werden und Vermittler können umgangen werden. Bei dem Handel mit Wertpapieren kann ein digitaler Vertrag dafür sorgen, dass Zahlungen von Dividenden oder Haftungen automatisiert werden. Dies verringert nicht nur den Arbeitsaufwand, es vermindert auch Risiken. Auch dieser Use Case benötigt noch mehr Vertrauen in die Technologie. [33]

4.1.3 Smart Contracts für Kaufverträge sämtlicher Art

Ein weiteres Beispiel entsteht durch den Verkauf von Häusern oder Grundstücken. Angenommen, Partei A ist damit einverstanden ein Haus von Partei B zu kaufen, vorausgesetzt, dass er alle Reparaturen, die vom Ingenieurbüro empfohlen werden erledigt.
B stimmt zu, sie beschließen, eine Summe von 10.000 ETH[34]. An einem gewissen Datum D1 wird B 5 ETH an E zahlen, der die Reparaturen am Haus durchführt. E wird daraufhin A und B einen Bericht zum Datum D2 zustellen. Danach haben der Käufer A und der Verkäufer B die Sicherheit, dass zum Schlussdatum D3 der Kaufvertrag zu aller Zufriedenheit abgeschlossen werden kann. Der Smart Contract, welcher durch die 3 Parteien digital signiert ist, friert die Summe von 10.000 ETH vom Konto der Partei A ein.
Am Datum D1 geht der Smart Contract durch das Netzwerk, dort wird überprüft ob Partei E 5 BTC von Partei B erhalten hat. Am Datum D2 wird überprüft ob es eine signierte Nachricht

[32] (Szabo, Smart Contracts: 12 Use Cases for Business and Beyond, 2016)
[33] (Szabo, Smart Contracts: 12 Use Cases for Business and Beyond, 2016)
[34] Abkürzung für Bitcoin

von E an A und B gibt. Am Datum D3 wird von B bestätigt, dass alle Reparaturen von E erledigt sind. Wenn alle Bedingungen erfüllt sind, werden 10.000 ETH an B überwiesen, falls eine der Bedingungen nicht erfüllt wird, wird die eingefrorene Summe wieder freigegeben.
Auch hier sind die Vorteile gegenüber den notariellen Verträgen eindeutig. Die Abwicklung von Zahlungen und Verpflichtungen geschieht praktisch automatisch und macht Drittparteien überflüssig. Größte Herausforderung ist hier das Erstellen einer Blockchain, der die Leute vertrauen. Papierbasierte Vereinbarungen können so überflüssig werden.

4.1.4 Smart Contracts für Besitztitel

Wie einem vorherigen Kapitel schon beschrieben, ist die Ordnung des Landbesitzes nicht in allen Regionen der Welt so gut geführt wie in Deutschland. Durch digitale Verträge lässt sich Betrug verringern und Vertrauen in den eigenen Besitz deutlich steigern. Außerdem werden Kosten reduziert, welches zur verbesserten Liquidität der einzelnen Länder führt. Zudem kann durch solch einen Vertrag die Transparenz erhöht werden. Größte Herausforderung hierbei ist die Schaffung einer Infrastruktur, die in dieser Größenordnung Grundbesitz verwaltet.[35]

4.1.5 Smart Contracts für Internet of Things[36]

Durch Smart Contracts kann es ermöglicht werden Dinge in Echtzeit zu erhalten.

Amazon[37] machte hier den Anfang. Sie haben 2014 den sogenannten Dash Button[38] veröffentlicht. Dieser ermöglicht Kunden durch das Betätigen eines Knopfes eine Bestellung auszulösen. Dies ist von Vorteil, wenn es um Bestellungen geht, die man regelmäßig benötigt, wie z.B. Waschmittel. Durch einen Knopfdruck wird automatisch neues Waschmittel bestellt. Durch Smart Contracts und Internet of Things lässt sich dieses Verfahren weitestgehend automatisieren. Man kann sich heute schon vorstellen, dass die Waschmaschine selbst weiß wann sie neues Waschmittel benötigt und dieses selbstständig bestellt. Die größte Herausforderung in diesem Use Case ist die noch nicht vorhandene Technologie. Es ist also notwendig sämtliche Geräte mit einem gewissen Maß an Intelligenz auszustatten, damit dadurch selbstständig entschieden wird wann welche Aktionen nötig sind.

[35] (Szabo, Smart Contracts: 12 Use Cases for Business and Beyond, 2016)
[36] (www.wikipedia.org, 2017)
[37] (www.amazon.de, kein Datum)
[38] (https://www.amazon.de/Amazon-Dash-Button/b?ie=UTF8&node=10852572031, 2017)

4.2 Unterschiede zum Bitcoin Netzwerk

Der wichtigste Unterschied zum Bitcoin Netzwerk ist, dass die Menge an ETH nicht durch den Algorithmus begrenzt ist, somit ist der Ether nicht deflationär. Neue ETH werden mit einer konstanten Rate von 15625576 pro Jahr erstellt.[39] Im Jahr 2014 gab es einen Vorverkauf von ETH, dieser hatte einen Wer von 31.531 BTC, welches dem damaligen Wert von ungefähr 18.438.086 $ entsprach.

Ein weiterer Unterschied ist, dass die Verschwendung von Strom und Rechenressourcen durch die große Anzahl von Hash Berechnungen, deren einziger Zweck es ist, eine willkürliche mathematische Ungleichung zu erfüllen, umgangen wird. Dies geschieht dadurch, dass vorzugsweise Berechnungen im Zusammenhang mit wissenschaftlichen Arbeiten stehen. Beispielweise beinhaltet die Sloan Digital Sky Survey[40] eine systematische Suche nach bestimmten Arten von astronomisch interessanten Objekten. Es lassen sich so ETH in Verbindung mit nützlichen Berechnungen erstellen. Dies spart Rechenenergie und Strom.

In einem gewissen Maße werden Smart Contracts die gleichen Widersprüche wie Bitcoin haben. Strafverfolgung und nationale Sicherheitsbehörden zum Beispiel weisen darauf hin, dass Ethereum illegales Glücksspiel erleichtere und die Möglichkeiten für grenzüberschreitende kriminelle Gruppen und terroristische Netzwerke größer würden.

Es gibt eine Gruppe die sich von Smart Contracts bedroht fühlt, das sind die Anwälte, Notare und Broker, die durch diese Technologie wohlmöglich nicht mehr die Bedeutung in unserer Gesellschaft haben könnten, die sie heute besitzen.

5. Kritik

Im April 2017 sind die Preise von Ether und Bitcoin regelrecht explodiert. Von dort an bis jetzt ist ein Wachstum von bis zu 1000% zu verzeichnen[41]. Das Wachstum entstand vor allem durch die stark steigende Nachfrage an Bitcoin und Co. Doch bis jetzt werden Bitcoin und andere Kryptowährungen zumeist als Spekulationsobjekt genutzt. [42]

Weitere Kritik entsteht vor allem an sogenannten ICO's. Initial Coin Offering ist eine Art Crowdfunding, welches von Firmen benutzt wird, welche die Blockchain nutzen. Solche

[39] (www.kryptocoins.net, 2016)
[40] (www.sdss.org, 2017)
[41] (www.coinmarketcap.com, 2017)
[42] (www.heise.de, 2017)

Firmen können so schnell weltweit an neue Investoren gelangen um ihr Projekt umzusetzen. Dies stößt auf heftige Kritik, denn nicht alle dieser Firmen sind seriös. Anleger können schnell um ihr Geld gebracht werden. Wie das Handelsblatt berichtet, verbietet China, der bis dahin größte Markt für Kryptowährungen und ICOs, am 04.09.2017 diese Art von Crowdfunding. [43]

Außerdem gibt es weitere Kryptowährungen, die nicht auf die ursprüngliche dezentralisierte und organisationsfreie Lösung der Blockchain setzen. Eines der bekanntesten Beispiele ist Onecoin[44]. Onecoin hat eine Kryptowährung entwickelt und bewirbt diese massiv. Die Bundesfinanzaufsicht warnt ausdrücklich vor dieser Firma.

Auch bekannte Bänker wie Jamie Dimon verrufen Bitcoin als Betrug. Laut einem Bericht von BTC-Echo, kauft seine Bank JPMorgan dennoch Bitcoin.[45]

Auch die IT Sicherheit ist ein großer Kritikpunkt, auch wenn das Blockchain Prinzip als sehr sicher gilt, treten immer wieder Fehler in kleineren Skripten und Applikationen auf. Dazu kommen Fehler in der Smart Contract Implementierung, die großen Schaden, bis hin zu Vermögensverlust, für die Nutzer bedeuten können.

Ein weiterer wichtiger Punkt ist die Frage nach der rechtlichen Lage. Bis heute gibt es für die Blockchain Technologie keine Rechtslage, da sich das Netzwerk weitestgehend selbst steuert. Außerdem kann eine Blockchain länderübergreifend sein, was die Rechtszuständigkeit unklar lässt.

Trotz all der Kritik sind sich bekannte Personen wie Bill Gates oder John McAfee einig. Die Blockchain Technologie wird Bestand haben und unser Leben revolutionieren. John McAfee wettete am 17.07.2017 auf Twitter, dass ein Bitcoin in 3 Jahren 500.000 $ Wert sei, er sagte: „if not, I will eat my dick on national television“.[46]

[43] (www.handelsblatt.com, 2017)
[44] (www.onecoin.eu, 2017)
[45] (www.btc-echo.de, 2017)
[46] (www.twitter.com, 2017)

6. Fazit

Das kleine Land Estland ist im Bereich Blockchain Vorreiter in der EU. Insbesondere die Hauptstadt Tallin ist ein Paradebeispiel für eine digitale Gesellschaft. Sigmar Gabriel sagte nach einem Besuch in Estland im Februar 2017: „Ich muss zugeben, dass wir Deutschen uns dabei ein bisschen wie ein Entwicklungsland gefühlt haben.“ [47] Die Bürger aus Estland, die sich selbst als E-Estonia bezeichnen, können seit Ende 2014 sämtliche Behördengänge online erledigen. Angela Merkel bremste die Hoffnung auf Ähnliches in Deutschland allerdings schnell. Sie sagte: „Natürlich ist es manchmal in einem größeren Land, in einem föderalen Land, in einem Land, das einen langen Entwicklungsprozess schon ohne das digitale Zeitalter hinter sich hat, nicht ganz so einfach, die Dinge zu verändern.“. Estland versuchte in diesem Jahr sogar selbst eine eigene Kryptowährung zu entwickeln, dies wurde von der EU allerdings untersagt, da der Euro das einzige Zahlungsmittel in der Euro-Zone sein darf. [48] Dennoch arbeiten Forscher in Tallin an dem Projekt Agrello[49], welches durch ein ICO finanziert wurde und sich mit Smart Contracts beschäftigt sodass Bürger diese in Zukunft werden nutzen können.

In Deutschland wurde am 29.06.2017 der Bundesverband Blockchain[50] gegründet. Der Verband hat sich zur Aufgabe gestellt, die Blockchaintechnologie zu fördern und fordern.

Mit der FDP wurde zu der Bundestageswahl 2017 eine Partei in den Bundestag gewählt, die in ihrem Parteiprogramm folgende Ziele zur Digitalisierung beschreibt: „

- Eine flächendeckend leistungsfähige digitale Infrastruktur
- Den Abbau von bürokratischen Barrieren für Startups und Innovationen
- Mehr Offenheit gegenüber neuen Technologien und Geschäftsmodellen, wie zum Beispiel der sogenannten Share Economy
- Den Einsatz digitaler Technologien und entsprechend ausgebildeter Lehrer an den Schulen
- Eine flexible Arbeitskultur, die Freiräume für die Vereinbarkeit von Familie und Beruf schafft
- Wirksame internationale Datenschutzstandards und starke Verschlüsselungstechnologien
- Verwaltungsvorgänge durch E-Government beschleunigen“[51]

[47] (www.heise.de, 2017)
[48] (www.btc-echo.de, 2017)
[49] (www.agrello.org, 2017)
[50] (www.bundesblock.de, 2017)
[51] (www.fdp.de, 2017)

Von Smart Contracts ist hier nichts zu lesen, dennoch ist besonders die flächendeckende Infrastruktur ein wichtiger und längst überflüssiger Schritt in Richtung Blockchain Technologie.

Es bleibt insgesamt also abzuwarten wie die Welt mit dem Thema Bitcoin, Blockchain und Smart Contracts umgehen wird. Die Möglichkeiten dieser neuen Technologie sind herausragend. Trotzdem ist es schwer vorstellbar, dass Plattformen wie Etherum unsere Versicherungsverträge oder auch Testamente umgehen wird.

„Smart Contracts stecken noch in den Kinderschuhen und sind erst in wenigen Bereichen vernünftig einsetzbar. Richtig ausgereift werden sie wohl erst in 10 Jahren sein. Aber richtig "smart" sind sie auch dann nicht.“[52]

[52] (Jaggi, 2016)

7. Literaturverzeichnis

Brito. (2013). *Bitcoin: a primer for policymakers.* Arlington: George Mason University.

Chavez-Dreyfuss. (2015). *reuters.com.* Abgerufen am 01. 10 2017 von http://in.reuters.com/article/usa-honduras-technology/honduras-to-build-land-title-registry-using-bitcoin-technology-idINKBN0O01V720150515

EBA. (2014). *https://www.eba.europa.eu.* Abgerufen am 01. 10 2017 von https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

ECB. (2012). *https://www.ecb.europa.eu.* Abgerufen am 01. 10 2017 von https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

FATF. (2014). *http://www.fatf-gafi.org.* Abgerufen am 01. 10 2017 von http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Forbes. (2015). *www.forbes.com.* Abgerufen am 01. 10 2017 von https://www.forbes.com/sites/steveforbes/2015/04/02/how-bitcoin-will-end-world-poverty/#553b64ec2a5a

Helms. (04. 05 2017). *www.news.bitcoin.com/bitcoin-accepted-260000-stores-summer*. Abgerufen am 01. 10 2017 von (https://news.bitcoin.com/bitcoin-accepted-260000-stores-summer/)

https://www.amazon.de/Amazon-Dash-Button/b?ie=UTF8&node=10852572031. (2017). Abgerufen am 01. 10 2017 von https://www.amazon.de/Amazon-Dash-Button/b?ie=UTF8&node=10852572031

Jaggi. (14. 07 2016). *www.inside-it.ch.* Abgerufen am 07. 10 2017 von http://www.inside-it.ch/articles/44468

Lee. (11 2015). *New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market.* Von www.the-blockchain.com: http://www.the-blockchain.com/docs/New%20Kids%20on%20the%20Blockchain%20How%20Bitcoin%20Technology%20Could%20Reinvent%20the%20Stock%20Market.pdf abgerufen

Mankiw. (2007). *Macroeconomics.* New York.

Nakamoto. (09. 10 2009). *bitcoin.org.* Von http://bitcoin.org/bitcoin.pdf abgerufen

Noizat. (2015). Blockchain Electronic Vote. In D. L. Chuen, *Handbook of Digital Currency, edited* (S. 453-461). San Diego : CA: Academic Press.

Pangburn. (2015). *fastcompany.com*. Abgerufen am 01. 10 2017 von https://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them

Plassaras. (2013). Regulating digital currencies: bringing Bitcoin within the reach of the IMF.

Scott. (2015). Blockchain Technology for Reputation Scoring of Financial Actors. *Finance and the Common Good / Bien Commun*, No. 42 and 43.

Swan. (2015). *Blockchain: Blueprint for a New Economy* . Sebastopol: CA: O'Reilly Media.

Szabo. (1997). Formalizing and securing relationships on public networks. *First Monday*.

Szabo. (2016). *Smart Contracts: 12 Use Cases for Business and Beyond.*

Technology, N. I. (2013). *Digital Signature Standard.* Gaithersburg.

Velde. (2013). Bitcoin: a primer. *Chicago fed letters no. 317.*

Wikipedia. (09. 10 2017). *wikipedia.org*. Von https://de.wikipedia.org/wiki/Ethereum abgerufen

Williams. (2015). *www.williamsassociates-ltd.com.* Abgerufen am 01. 10 2017 von http://williamsassociates-ltd.com/articles/Are_Notaries_an_Endangered_Species_by_Steven_E_Williams.pdf

Wright, A. a. (23. 09 2015). *papers.ssn.com.* Von https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 abgerufen

www.agrello.org. (2017). Abgerufen am 5. 10 2017 von https://www.agrello.org/

www.amazon.de. (kein Datum). Abgerufen am 01. 10 2017 von www.amazon.de

www.bitcoinmagazine.com. (2014). Abgerufen am 5. 10 2017 von https://bitcoinmagazine.com/articles/web-3-0-chat-ethereums-gavin-wood-1398455401/

www.blockstream.com. (2017). Abgerufen am 01. 10 2017 von https://blockstream.com/

www.btc-echo.de. (2017). Abgerufen am 05. 10 2017 von https://www.btc-echo.de/jp-morgan-kauft-bitcoin-obwohl-ceo-jamie-dimon-bitcoin-als-betrug-bezeichnet/

www.btc-echo.de. (2017). Abgerufen am 05. 10 2017 von https://www.btc-echo.de/estland-gelingt-es-nicht-seine-eigene-kryptowaehrung-rauszubringen

www.bundesblock.de. (2017). Abgerufen am 01. 10 2017 von http://bundesblock.de/

www.coindesk.com. (19. 10 2015). Abgerufen am 01. 10 2017 von http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

www.coinmarketcap.com. (2017). Abgerufen am 01. 10 2017 von https://coinmarketcap.com

www.counterparty.io. (2017). Abgerufen am 01. 10 2017 von https://counterparty.io/

www.ethereum.org. (2017). Abgerufen am 01. 10 2017 von www.ethereum.org

www.factom.org. (2017). Abgerufen am 01. 10 2017 von www.factom.org

www.fdp.de. (2017). Abgerufen am 1. 10 2017 von https://www.fdp.de/position/digitalisierung

www.handelsblatt.com. (2017). Abgerufen am 05. 10 2017 von http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/nein-zu-icos-chinesische-zentralbank-verbietet-krypto-boersengaenge/20279068.html

www.heise.de. (2017). Abgerufen am 5. 10 2017 von https://www.heise.de/newsticker/meldung/Neues-Kurshoch-beim-Bitcoin-Bundesbank-warnt-vor-Spekulationsobjekt-3705965.html

www.heise.de. (2017). Abgerufen am 01. 10 2017 von https://www.heise.de/newsticker/meldung/Gabriel-Deutschland-bei-Digitalisierung-wie-ein-Entwicklungsland-3639900.html

www.kryptocoins.net. (2016). Abgerufen am 1. 10 2017 von http://kryptocoins.net/2016/02/ethereum-entwicklung-anzahl-der-ether-einheiten/

www.onecoin.eu. (2017). Abgerufen am 05. 10 2017 von https://www.onecoin.eu/de/

www.provenance.org. (2017). Abgerufen am 01. 10 2017 von https://www.provenance.org/

www.provenance.org. (2017). Abgerufen am 01. 10 2017 von https://www.provenance.org/

www.sdss.org. (2017). Abgerufen am 1. 10 2017 von http://www.sdss.org

www.twitter.com. (2017). Abgerufen am 05. 10 2017 von https://twitter.com/officialmcafee/status/887024683379544065?lang=de

www.wikipedia.org. (2017). Abgerufen am 2017. 10 10 von https://de.wikipedia.org/wiki/Internet_der_Dinge