Blockchain

Themenzeit

Erik Staas

14.05.2018

12a NaWi-Profil

Mentorierung: Herr Dittrich

Inhalt

Einleitung

In den letzten Jahren haben Kryptowährungen[1]*, allen voran *Bitcoin**, durch drastisch schwankende Wechselkurse in schwindelerregenden Höhen für Aufsehen gesorgt. Dabei wird in der allgemeinen Öffentlichkeit jedoch nur selten die diese Kryptowährung möglich machende Technologie, die *Blockchain*,* wahrgenommen. Doch immer mehr Unternehmen und Regierungen erwägen die Nutzung der *Blockchain,* und das nicht nur als Kryptowährungen. Dabei sind die Hoffnungen auf Innovationen mannigfaltig. Neben der Revolution des Finanzsektors durch Kryptowährungen wird auch der Einsatz zur "Krypto-Regierungsführung"[2] prophezeit. Auch Dubai möchte in die *Blockchain*-Technologie investieren und als erste Stadt die meisten Dienstleistungen der Stadt mithilfe einer *Blockchain* organisieren[5].

In meiner Hausarbeit im Rahmen der Themenzeit möchte ich mich mit der technischen Funktionsweise der *Blockchain* auseinandersetzen und darüber hinaus die gesellschaftlichen, wirtschaftlichen und ökologischen Auswirkungen und Möglichkeiten diskutieren. Des Weiteren möchte ich die Nachhaltigkeit der *Blockchain* insofern problematisieren, als dass beispielsweise die *Bitcoin-Blockchain* viel Energie verbraucht und potentielle Alternativen aufzeigen.

Technische Funktionsweise

Im Allgemeinen ist eine *Blockchain* ein öffentliches Register bzw. eine Datenbank, die von vielen verschiedenen Computern im Zusammenschluss geführt wird. Dabei ist sie durch kryptografische Mechanismen vor der Manipulation abgesichert. Dadurch müssen die Nutzer der *Blockchain* sich nicht gegenseitig vertrauen, um sicher zu sein, dass der Inhalt der *Blockchain* korrekt ist. Die Art des Inhalts hängt dabei vom Verwendungszweck der *Blockchain*-Implementierung ab. Dabei ist der Inhalt der *Blockchain* unveränderbar. Es können lediglich neue Blöcke* an das Ende der *Blockchain* angefügt werden, wodurch eine nachträgliche Fälschung bereits erzeugter Blöcke verhindert werden soll.

[1] * Wörter, die mit einen Stern (*) gekennzeichnet sind werden im Glossar auf Seite 18 erläutert.
[2] Engl: *Cryptogovernance*[4]

Zunächst einmal ist wichtig, dass die *Blockchain* nicht ausschließlich in Form einer Kryptowährung wie *Bitcoin* vorzufinden ist. Es sind auch andere Formen der *Blockchain* denkbar, jedoch sind die prominentesten Implementierungen der *Blockchain* nach heutigem Stand Kryptowährungen oder universelle *Blockchain* Plattformen, wie *Ethereum*.*

Der Grundbestandteil der *Blockchain* ist der *Block*. Ein *Block* besteht aus einem *Header** und dem *Body*.* Im *Header* werden Metadaten über den *Block* gespeichert, zu denen unter anderem der Erstellungszeitpunkt gehört. Ebenfalls beinhaltet der *Header* den *Hash*wert* des vorherigen *Headers* und eine mithilfe eines *Hash*-Baums* (siehe unten) erzeugte Repräsentation der Daten des Blockes, womit der Inhalt des Blockes mit dem Header des Blockes verbunden ist. Der *Body* entspricht dann dem tatsächlichen Dateninhalt der Blockchain, im Fall einer Kryptowährung wie *Bitcoin* wären dies die monitäre Transaktionen. Er kann aber auch andere Komponenten beinhalten.

Bei der Blockchain werden verschiedene Technologien, Algorithmen und Protokolle miteinander verbunden. Dabei sind vor allem die Bereiche der Kryptografie und der verteilten Netzwerke relevant, um die technische Funktionsweise der Blockchain zu verstehen. Im Nachfolgenden werden einige dieser Teilaspekte der *Blockchain,* die für sie essentiell und charakteristisch sind, näher erläutert.

Verteilte Netzwerke

Im Gegensatz zu zentralen Netzwerken ist eine verteilte Netzwerkarchitektur asymmetrisch. Das heißt, dass es keinen dedizierten *Server** gibt, von dem die *Clients** Informationen beziehen und der damit anders aufgebaut sein muss. Vielmehr übernehmen die sog. *Nodes** des verteilten Netzwerkes sowohl Aufgaben des *Clients,* als auch die des *Servers. Nodes* in diesem Sinne sind Computer, die die Software eines verteilten Netzwerkes, bzw. der *Blockchain* betreiben. Jede *Node* verfügt über eine interne Version der *Blockchain*.

Diese Art der Netzwerkarchitektur wird auch als *Peer-to-Peer** Netzwerk bezeichnet. *Peer-to-Peer* Netzwerken haftet aufgrund ihrer Verwendung bei illegalen Internet-Musiktauschbörsen eine negative Konnotation an, obwohl die Technologie an sich legitim ist. Ein Vorteil dieses Systems ist es, dass es keinen zentralen *Server* gibt, der funktionsunfähig oder kompromittiert werden könnte. Dies kann das Risiko eines Datenverlustes deutlich verringern [16]

Die *Nodes* einer *Blockchain* kommunizieren ständig miteinander. Dabei tauschen sie Informationen über den Status ihrer internen *Blockchain* aus. Hat eine andere *Node* eine neue Version der *Blockchain,* gibt es einen Algorithmus, mit dem bestimmt wird, ob die *Node* die andere Version der *Blockchain* akzeptiert. Dazu ist das wichtigste und erste Kriterium die Validität der *Blockchain.* D.h. es wird überprüft, ob die *Hashes* der *Header* eine kontinuierliche Kette ergeben und, ob die Blöcke in sich schlüssig sind. Danach werden die Längen der *Blockchains* miteinander verglichen. Dabei gibt die *Node* immer der längeren Kette den Vorzug, sofern beide *Blockchains* valide sind. Sollten zwei *Nodes* gleichzeitig erfolgreich einen neuen *Block* erschaffen und ihn über das Netzwerk verteilen, nimmt jede *Node* des Netzwerkes die zuerst erhaltene *Blockchain* als korrekt an. Zu diesem Zeitpunkt existieren dann also zwei, oder sogar mehrere verschiedene *Blockchains,* über die bei Teilen des Netzwerkes Konsens herrscht. Der Konflikt zwischen diesen beiden *Blockchains* wird gelöst, wenn ein neuer Block gefunden wird. Jede *Node* versucht einen Block zu finden, der an die *Blockchain* passt, die sie als die Konsens-*Blockchain* betrachtet. Sobald also ein neuer Block gefunden wurde, weist die *Blockchain* mit dem neuen Block eine größere Länge auf, womit sie als Konsens-*Blockchain* von allen Mitgliedern des Netzwerkes akzeptiert wird.

*Hash*funktionen

*Hash*funktionen sind Algorithmen, die aus einem beliebigen Datensatz einen *Hash* berechnen, der den Datensatz zweifelsfrei identifiziert. Daher werden *Hashes* häufig auch als “Fingerabdruck” der Daten bezeichnet, da sie die Daten eindeutig kennzeichnen, ohne dass sich die Daten aus dem *Hash* reproduzieren lassen.

Damit eine *Hash*funktion kryptografisch sicher ist, muss es unmöglich sein, gezielt Hashkollisionen zu erzeugen. Eine *Hash*kollisionen entsteht, wenn zwei unterschiedliche Datensätze den gleichen *Hash*wert erzeugen. Dies ist insofern problematisch, da der *Hash*algorithmus damit nicht mehr seine eigentliche Funktion der zweifelsfreien Identifizierung eines Datensatzes erfüllt und seine Nutzung in der *Blockchain* Fälschungen zulassen würde.

Konsens in verteilten Netzwerken

Um zu verhindern, dass kompromittierte *Nodes*, d.h. solche, die absichtlich oder unabsichtlich versuchen falsche Informationen in die *Blockchain* einzuspeisen[3], eine gefälschte Version der *Blockchain* verbreiten, muss es ein Verfahren bzw. Protokoll geben, um zu Konsens über den rechtmäßigen Zustand der *Blockchain* zu gelangen. *Nodes* sind im Konsens, wenn sie die gleiche interne *Blockchain* besitzen.

Diese Problemstellung ist auch unter dem Namen “Problem der byzantinischen Generäle” bekannt. Bei der Belagerung von Konstantinopel im Jahr 1453 mussten die byzantinischen Heerführer, der Legende nach, die Stadt von mehreren Stellen aus angreifen, um die starken Befestigungen zu durchbrechen. Das Problem dabei war allerdings, dass es sich bei einigen der byzantinischen Generäle vermutlich um Verräter handelte. Wenn sich die Generäle auf einen Zeitpunkt zum Angriff hätten verständigen wollen, hätte ein Verräter einen falschen Zeitpunkt weiterleiten können. Dadurch wären die Angriffe zeitversetzt geschehen, wodurch eine Eroberung Konstantinopels nicht möglich wäre. *[15]*

Bezieht man dieses Problem der byzantinischen Generäle wieder auf die *Blockchain,* so entsprechen die *Nodes* in der *Blockchain* dabei den Generälen und der Konsens über den Inhalt der *Blockchain* entspricht dem Zeitpunkt des Angriffes. Die Lösung dieses Problems ist die grundlegende Aufgabe und die eigentliche Innovation der *Blockchain*, die sie zu etwas Neuem und Besonderem macht.

[3] Dies wäre z.B. dann der Fall, wenn der Betreiber einer *Node* von einer Kryptowährung versucht sich selbst zu bereichern, indem er seinen eigenen Kontostand erhöht.

Die im Folgenden beschriebenen Konsensprotokolle sind jene, die am häufigsten in *Blockchains* verwendet werden und auch am verbreitetsten sind. Durch die Notwendigkeit eines Konsensprotokolles lässt sich begründen, warum alle großen, praktisch bereits verwendeten *Blockchains* zumindest auch eine Kryptowährung beinhalten. Diese Konsensprotokolle, brauchen nämlich stets Mitglieder, die beispielsweise Rechenleistung zur Verfügung stellen. Durch eine in die jeweilige *Blockchain* integrierte Kryptowährung ist es möglich diese Mitglieder für ihre Arbeit zu belohnen und ihnen so einen Anreiz zur Mitarbeit zu bieten. Theoretisch ist demnach aber auch eine *Blockchain* denkbar, die versucht ohne eine Kryptowährung auszukommen.

Proof-of-Work*

Bei einem *Proof-of-Work* Protokoll müssen die *Miner** eine bestimmte schwer zu berechnende Aufgabe lösen, die i.d.R. nur durch ein *Trial-and-Error*[4] Verfahren gelöst werden kann. Ein *Miner* muss den *Hash* des gegenwärtigen Blockes berechnen. Dies ist zunächst eine für einen Computer triviale Aufgabe. Deshalb wird zusätzlich die Anforderung an den *Miner* gestellt, dass er einen *Hash* berechnen muss, der unter einem bestimmten Wert, der *Difficulty** liegt. Dazu darf er ein Attribut des *Block-Headers*, den *Nonce*,* frei wählen und so den endgültigen *Hash* verändern. Da *Hash*funktionen pseudozufällig sind, kann man nur durch Herumprobieren einen passenden Block finden. *[12] [13]*

Der *Proof-of-Work* Mechanismus sorgt für die Unveränderlichkeit der *Blockchain*, indem jeder *Block* zur Erstellung ein recht großes Stück Arbeit benötigt. Je weiter man in der Historie zurückgeht, desto schwieriger wird es, diese Blöcke zu fälschen, weil man für eine erfolgreiche Fälschung den Block und alle seine nachfolgenden Blöcke neu berechnen müsste. Andernfalls hat die gefälschte *Blockchain* eine geringere Länge als die wahre *Blockchain* und wird somit von nicht kompromittierten *Nodes* zurückgewiesen.

[4] Lösungsstrategie, bei der durch willkürliches Probieren eine Lösung gesucht wird.

Im allgemeinen gibt es hauptsächlich zwei verschiedene Anforderungen an ein *Proof-of-Work* Protokoll. Zum einen muss der Schwierigkeitsgrad[5], der zu lösende Aufgabe variabel sein, um sich an die *Hashpower* der *Blockchain* anpassen zu können. Zum anderen muss es trivial sein, die richtige Lösung zu verifizieren.

Ein Nachteil des *Proof-of-Work* Verfahrens ist die große Menge an Rechenressourcen, die für die Berechnung der *Hashes* verwendet werden muss. Dadurch können in einer *Blockchain,* die mit einem *Proof-of-Work* Protokoll betrieben wird, Probleme mit einem hohen Stromverbrauch entstehen.

Proof-of-Stake*

Das *Proof-of-Stake* Verfahren ist eine Alternative zu dem von der Bitcoin genutzten *Proof-of-Work,* das bald von Bitcoin-Konkurrenten wie *Ethereum* ergänzend zum *Proof-of-Work* eingesetzt werden soll. Anders als beim *Proof-of-Work* hat nicht derjenige, der am meisten Arbeit verrichtet, die höchste Chance auf die Erschaffung eines neuen Blockes, sondern derjenige, der über die größte Menge von Einheiten der jeweiligen Kryptowährung verfügt. Der Erschaffer eines neuen Blocks wird bei *Proof-of-Stake Blockchains* als *Validator* bezeichnet, anders als beim *Proof-of-Work*. Bei der Verwendung eines *Proof-of-Stake* Protokolls ist die maximale Anzahl an Währungseinheiten bereits von vorneherein verfügbar, sodass die Validatoren lediglich durch Transaktionsgebühren bezahlt werden. *[12]*

Hash-Baum

Hash-Bäume werden in der *Blockchain* dazu verwendet, die Integrität des *Bodies* eines Blockes zu sichern. Ein *Hash*-Baum sorgt hier für eine schnelle Überprüfbarkeit der Transaktionen eines Blockes, wodurch es möglich ist festzustellen, ob eine gegebene Transaktion in einem Block eingebettet ist. Eine *Blockchain* ist grundsätzlich auch ohne *Hash*-Bäume umsetzbar, sie dienen hauptsächlich der Zeitersparnis bei der Überprüfung und bieten auch die Möglichkeit der Reduzierung der Speichergröße*[13].*

[5] Wird auch als *Difficulty* (dt: Schwierigkeit) bezeichnet.

Ein *Hash*-Baum besteht auf der untersten Ebene aus den Transaktionen, die in einen Block aufgenommen werden sollen. Aus zwei dieser Transaktionen wird dann der *Hash* H gebildet, indem die *Hash*funktion f auf die Summe zweier aufeinanderfolgenden Transaktionen A und B angewendet wird: $H = f(A + B)$. Dadurch wird es unmöglich die Transaktion A oder B zu verändern, ohne dass sich auch H ändert. Das gleiche Verfahren wird nun solange rekursiv auf die aus den Transaktionen gebildeten *Hashes* angewendet, bis ein einziger *Hash* übrig bleibt, der als Wurzel oder *Root* des *Hash*-Baums bezeichnet wird. Durch diesen *Hash* kann man nun einen beliebigen Satz an Transaktionen mit einem anderen vergleichen, während es nicht nötig ist, die *Hashes* jeder Transaktion einzeln miteinander zu vergleichen.[1][13]

Sicherheit

51%-Angriff

Bei einem 51% Angriff wird mehr als die Hälfte der gesamten *Hashpower* des Netzwerkes kompromittiert. Dadurch kann der Angreifer eine beliebige Version der *Blockchain* im Netzwerk verteilen. Im Fall einer Kryptowährung kann sich der Angreifer selbst bereichern. Allerdings ist dies nur in einem bestimmten Rahmen möglich. Sollte der Angreifer beispielsweise die gesamte Kryptowährung auf ein von ihm kontrolliertes Konto überweisen, so hätte er davon keinen direkten Mehrwert, weil Kryptowährungen keinen inhärenten Wert besitzen und sich ihr Preis aus dem Zusammenspiel aus Angebot und Nachfrage bildet. Ist also eine Kryptowährung gänzlich kompromittiert, so würde sie vermutlich jeglichen Wert verlieren. Außerdem kann der Angreifer seinen eigenen Kontostand nicht beliebig verändern, weil ehrliche *Nodes* eine *Blockchain* nur akzeptieren, sofern sie den Regeln der *Blockchain* entsprechen, die eine solche plötzliche Bereicherung nicht vorsehen.

Damit gibt es zwei plausible Szenarien, die ein Angreifer verfolgen kann. Zum einen könnte er die Kryptowährung komplett entwerten. Zum anderen könnte er sich in kleinem Rahmen selbst bereichen, sodass andere Mitglieder des Netzwerkes nicht darauf aufmerksam werden.

Generell ist ein 51%-Angriff umso schwerer, je größer das *Blockchain*-Netzwerk ist, weil dementsprechend mehr Rechenleistung verwendet werden muss, um mehr als 50 Prozent der *Hashpower* zu besitzen. Tendenziell ist diese Art des Angriffs nur bei kleineren Netzwerken problematisch, da sie über eine vergleichsweise kleine Gesamt-*Hashpower* verfügen.

Ausfalltoleranz

Aufgrund der verteilten Natur der *Blockchain* lässt sich auf jeder *Node* des Netzwerkes stets eine volle Kopie der *Blockchain* finden. Diese Redundanz sorgt für eine beträchtliche Ausfalltoleranz von *Blockchain* Systemen. Sollte eine einzelne *Node* funktionsunfähig werden, spielt dies für das Netzwerk als solches keine Rolle. Diese Ausfalltoleranz geht durch die Konsensmechanismen der *Blockchain* sogar so weit, dass bewusst irreführendes Verhalten einzelner kompromittierter *Nodes* toleriert werden kann. Verglichen mit zentralen und herkömmlichen dezentralen Netzwerken, aber auch mit normalen *Peer-to-Peer* Netzwerken, bei denen nicht jede *Node* über eine vollständige Kopie des Inhalts verfügt, ist die *Blockchain* also wesentlich ausfalltoleranter.

Implementierungen

Bitcoin

Die bislang größte und populärste öffentliche *Blockchain* ist *Bitcoin*, die eine prototypische Kryptowährung darstellt. Die Blöcke ihrer *Blockchain* enthalten eine Art Liste aller Kontostände der Mitglieder der *Bitcoin-Blockchain*. Diesen ist es möglich Transaktionen anzustoßen, durch die ein bestimmter Betrag an *Bitcoins*[6] an ein anderes Konto überwiesen wird. So kann die *Bitcoin* als eine Währung verwendet werden. Sobald der nächste Block erzeugt wurde, werden diese Transaktionen gültig. Was die *Bitcoin* vom herkömmlichen *Online-Banking* unterscheidet, ist das Fehlen einer zentralen Instanz, die das mehrfache Ausgeben von dem Geld aus einem Konto verhindert. In der *Bitcoin* tritt an diese Stelle das Vertrauensnetzwerk der *Blockchain*, in dem der Konsens eine doppelte Ausgabe verhindert. Damit verhält sich die *Bitcoin* insofern eher wie eine herkömmliche Papierwährung, indem es keine zentrale Instanz gibt,

Geschichte

Bitcoin wurde 2008 durch eine Person oder eine Gruppe mit dem Pseudonym Satoshi Nakamoto veröffentlicht*[13].* Dieser war es auch, der die ersten *Bitcoins* erzeugte und die ersten Transaktionen durchführte. Die Erfindung der *Bitcoin* durch Nakamoto ist gleichzeitig auch die erstmalige Konzeptionierung und Implementierung einer *Blockchain*. Die technische Funktionsweise der *Bitcoin-Blockchain* beschreibt Nakamoto in einem 2008 veröffentlichten Artikel (vgl. *[13])*

[6] In diesem Fall die Währung innerhalb der *Bitcoin-Blockchain,* abgekürzt mit BTC. Dabei entspricht 1BTC 100.000.000 Satoshis.

Technische Besonderheiten

Als Konsensprotokoll wird der *Hashcash* Proof-of-Work* Algorithmus verwendet. Dieser dient gleichzeitig dazu, neue *Bitcoins* in Umlauf zu bringen, indem derjenige dem es gelingt einen validen *Proof-of-Work* zu finden, mit einer festgelegten Menge an Bitcoins belohnt wird. Zu Beginn der *Bitcoin-Blockchain* betrug diese Belohnung 50 Bitcoins, wobei sie sich nach 210.000 generierten Blöcken halbiert. Ab einem bestimmten Zeitpunkt werden dann keine Bitcoins mehr für das erfolgreiche Erstellen eines *Blocks* vergeben. Ab diesem Zeitpunkt ist die absolute Menge an *Bitcoins* erreicht und es kann keine weiteren mehr geben. Damit das Bereitstellen von Rechenleistung durch die Verringerung der in Aussicht stehenden Gewinne nicht unattraktiv wird, darf der erfolgreiche *Miner* ebenfalls eine Gebühr für die in dem von ihm generierten *Block* getätigten Transaktionen erheben. *[14]*

Als *Hash*funktion findet der SHA256[7] Algorithmus aus der SHA2-Familie Verwendung, der von der NSA[8] entwickelt wurde. Die *Hash*größe beträgt 32 Bytes, was 256 Bits entspricht. Die *Hash*größe gibt an, welche Anzahl an Bits bzw. Bytes für den *Hash*wert verwendet werden. Bei einer *Hash*größe von 256 Bits entspricht das 2^{256} verschiedenen möglichen *Hash*werten, die generiert werden können. Momentan gilt der Algorithmus als kryptografisch sicher. Dies kann sich allerdings durch anwachsende Rechenleistung von Computern ändern, da es so einfacher wird, schnell *Hashes* mit dem Algorithmus zu berechnen und es so möglich werden kann, in endlicher Zeit *Hash*kollisionen zu erzeugen. In der *Bitcoin* wird der SHA256 Algorithmus in verschachtelter Form verwendet. D.h. der *Hash* der Daten wird noch einmal an die *Hash*funktion übergeben. Der so entstehende *Hash*wert wird dann genutzt, um über eine Referenz auf den vorherigen *Block* zu verfügen. Außerdem findet die SHA256 *Hash*funktion in dem *Hashcash Proof-of-Work* Konsensprotokoll Anwendung.

[7] SHA steht für *Secure Hashing Algorithm* (dt: Sicherer *Hash*algorithmus). 256 bezieht sich auf die Größe des entstehenden *Hashes*, angegeben in Bits.
[8] NSA steht für *National Security Agency* (US-Amerikanischer Geheimdienst).

Ethereum

Ethereum ist als zum heutigen Stand zweitgrößte *Blockchain* Implementierung der mächtigste Konkurrent der *Bitcoin.* Gehandelt wird in ihr mit der Kryptowährung *Ether.* Besonders interessant wird *Ethereum* durch zwei Faktoren: *Smart Contracts** und ein geplantes *Proof-of-Stake* Konsensprotokoll.

Smart Contracts

Ethereum ist mehr als eine reine Kryptowährung. Es bietet Nutzern der *Blockchain* die Möglichkeit durch die sog. *Smart Contracts* selbst Verhalten der *Blockchain* zu definieren. *Smart Contracts* sind im Grunde Kodierungen eines bestimmten Verhaltens beim Auftreten bestimmter Bedingungen. Damit ist es flexibler als herkömmliche Kryptowährungen, da es über den durch die Implementierung der *Blockchain* vorgeschriebenen Regelsatz möglich ist, weitere Verträge zu formulieren. *Smart Contracts* erlauben es also, das Vertrauen in die *Blockchain* auf beliebiges selbst-definiertes Verhalten in Form von Verträgen auszuweiten, weshalb *Ethereum* auch als *Blockchain*-Plattform bezeichnet wird. [3]

Konsens

Zum anderen soll die *Ethereum* Plattform von dem bisher verwendet *Proof-of-Work* Mechanismus auf ein *Proof-of-Stake* Protokoll umgestellt werden, welches eine immense Energieersparnis im Vergleich zu der bislang genutzten Methode in Aussicht stellt.

Nachhaltigkeit

Gerade vor dem Hintergrund der *Sustainable Development Goals (SDGs)* der Vereinten Nationen sollte man die *Blockchain*-Technologie auf ihren Nutzen für nachhaltige Entwicklung untersuchen. Einerseits ist ein großes Potenzial zur Nachhaltigkeit vorhanden.

Chancen

Die herausragende Leistung der *Blockchain*-Technologie ist die Entfernung eines Vermittlers. Diesem Vermittler müssen alle Kunden eines herkömmlichen Dienstes Vertrauen schenken. Ein Beispiel hierfür ist eine Bank mit Internetpräsenz, die intern die Kontostände ihrer Kunden verwaltet. Wenn nun ein Kunde dieser Bank jemandem eine Überweisung von seinem Konto machen möchte, müssen beide Parteien darauf vertrauen, dass die dritte Partei, also die Bank, die Transaktionen ordnungsgemäß durchführt und ebenfalls nicht kompromittiert ist. Im Gegensatz dazu gibt es bei einer *Blockchain*-Kryptowährung keine Notwendigkeit einem Dritten zu vertrauen. Stattdessen vertraut der Nutzer einer solchen Kryptowährung dem Verfahren der *Blockchain*, also den Protokollen, die für Konsens innerhalb der *Blockchain* sorgen. Diese Eigenschaft der *Blockchain* eröffnet einige nachhaltige Nutzungsszenarien, die mit herkömmlicher Technologie kaum oder nur indirekt umsetzbar gewesen werden. Beispielsweise kann in Ländern mit instabilen oder unterentwickelten Infrastruktur die *Blockchain* Lösungsansätze liefern, auch ohne den Aufbau von Rechenzentren vor Ort.

Pobleme

Das offensichtlichste Problem der Blockchain ist der enorme Energieverbrauch, der durch die Nutzung in großem Maßstab entsteht. So verbraucht z.B. die Bitcoin-Blockchain mittlerweile große Mengen an Strom. Die Ursache dafür liegt in dem verbreiteten *Proof-of-Work* Algorithmus (s.o.). Die Lösung dieses Problems kann in der Verwendung von alternativen Konsensverfahren wie z.B. dem *Proof-of-Stake* liegen, die das Potenzial haben, wesentlich weniger Strom zu verbrauchen. [6]

Daneben gibt es auch noch ein Problem, das man als nachträgliche Zentralisierung bezeichnen könnte. Obwohl *Blockchains* wie *Bitcoin* zunächst absolut dezentral sind, kann es durch äußere Faktoren dazu kommen, dass die *Hashpower* sich zentralisiert. Ein Beispiel dafür ist eine geographische Zentralisierung aufgrund von Stromkosten. Da der Gewinn, der sich aus der Tätigkeit als *Bitcoin-Miner* generieren lässt, die Differenz von erhaltenen Prämien und den Stromkosten ist, lohnt sich *Bitcoin-Mining* besonders in Regionen mit niedrigen Stromkosten. Dadurch stammt in der *Bitcoin-Blockchain* 71% der *Hashpower* aus China, worauf Indien mit lediglich 4% als zweites folgt[6]. Da China mittelfristig aus dem *Bitcoin-Mining* aussteigen möchte[9], könnte dies zu Problemen für das *Blockchain*-Netzwerk führen. Weil der *Mining*-Ausstieg Chinas allerdings nicht abrupt ist, sondern über einen längeren Zeitraum erfolgen soll, hat das *Bitcoin*-Netzwerk Zeit die *Difficulty* anzupassen und so auf die insgesamt geringere *Hashpower* zu reagieren[8]. Trotzdem ist diese dramatische Verringerung nicht gänzlich ungefährlich, da somit ein 51%-Angriff, aufgrund der drastisch sinkenden Netzwerkleistung, tendenziell einfacher wird.

Eine geographische Zentralisierung von vielen *Minern* ist immer dann ein Problem für die Nachhaltigkeit in einer Region, wenn durch das *Mining* so viel Energie beansprucht wird, dass es zu infrastrukturellen Problemen kommen kann. Ein Beispiel hierfür ist Island, das über günstigen Wasserkraft- und Geothermiestrom verfügt. Diese Gegebenheit hat einige *Bitcoin-Miner* dazu veranlasst, sich in Island niederzulassen und Rechenzentren aufzubauen. Obwohl der Strom in Island recht einfach zu produzieren und damit günstig ist, sind die Kapazitäten begrenzt, weshalb es bei einem Anstieg des Stromverbrauchs in kurzer Zeit durch *Bitcoin-Miner* zu einer Stromknappheit führen könnte. Dies würde dann zu einem Anstieg der Strompreise führen mit potentiell weitreichenden Folgen für die isländische Wirtschaft. [17]

[9] Dieser Ausstieg lässt sich u.a. mit dem großen Stromverbrauch des Betriebs dieser *Blockchain,* vor allem in China, erklären.

Neben der geographischen Zentralisierung von *Hashpower* gibt es noch das Problem der Zentralisierung in *Mining-Pools.* Diese sind Zusammenschlüsse von mehreren *Minern.* Als einzelner *Miner* mit vergleichsweise winziger *Hashpower* ist die Wahrscheinlichkeit in einer *Proof-of-Work Blockchain* erfolgreich den nächsten Block zu berechnen verschwindend gering. Daher schließen sich *Miner* zu einem sog. *Pool* zusammen und verbinden so ihre *Hashpower*. Erschafft der *Mining-Pool* den neuen Block, so teilt er die Belohnung dafür unter seinen Mitgliedern anteilig nach ihrer individuellen *Hashpower.* Problematisch kann dies werden, wenn ein *Mining-Pool* über die Mehrheit der *Hashpower* der *Blockchain* verfügt. So wäre er in der Lage einen 51%-Angriff durchzuführen und damit die Kryptowährung zu destabilisieren. Allerdings muss hierbei auch die Wirtschaftlichkeit in Betracht gezogen werden. Aufgrund des zu erwartenden Wertverlustes einer so angegriffenen Kryptowährung brächte ein solcher Angriff dem *Mining-Pool* keinen ökonomischen Vorteil ein. *[10]*

Hard Fork

Ein grundlegendes Problem von *Blockchain*-Projekten ist das Unvermögen große Veränderungen im Nachhinein problemlos durchzuführen. Der technische Hintergrund dieses Problems liegt in der Art und Weise wie neue Versionen der *Bitcoin-Software* bereitgestellt werden. Gibt es solch eine neue Version mit schwerwiegenden Veränderungen, die zu einer Inkompatibilität zwischen der neuen und der alten Version der *Blockchain* führt, können die Mitglieder des Netzwerkes die neue Version herunterladen, um sie zu nutzen. Es liegt aber in der Natur der *Blockchain,* dass es keine zentrale Instanz gibt, die die Mitglieder des Netzwerkes dazu zwingen könnte, die neue Version der *Blockchain* zu verwenden oder die alte Version der *Blockchain* für ungültig erklären könnte. Daher existiert die alte *Blockchain* weiterhin und kann problemlos weiter genutzt werden, solange genügend Mitglieder an der *Blockchain* teilnehmen, um sie zu betreiben. Da es bei einer ausreichend großen *Blockchain* immer Mitglieder geben wird, die aus unterschiedlichen Gründen die alte Version der *Blockchain* weiterhin betreiben, wird die Nutzerbasis fragmentiert, sodass zwei unterschiedliche Versionen der *Blockchain* existieren. Dieses Phänomen wird auch als *Hard Fork* bezeichnet.

Ein Beispiel für eine hypothetische Änderung wäre die Einführung einer neuen *Hash*funktion. Dies könnte beispielsweise dann notwendig sein, wenn die zuvor verwendete *Hash*funktion nicht mehr sicher genug ist.

Lokale Nutzungsmöglichkeiten und Zukunftsperspektiven

Blockchain-Technologie bietet auch lokale Nutzungsmöglichkeiten in der Region Kiel. Die Landeshauptstadt versucht schon seit Längerem digitale Entwicklung und Innovation im Raum Kiel zu fördern. So fand im September 2017 die erste “Digitale Woche Kiel” statt und eine weitere ist für September 2018 geplant[11]. Auch sind Kiel und San Francisco, das mit dem *Silicon Valley* als weltgrößte digitale Innovationsstätte gilt, in 2017 eine Städtepartnerschaft eingegangen[18]. Kiel bringt damit einige Bedingungen mit, die es Kiel erlauben könnten, in der digitalen Entwicklung eine führende Rolle innerhalb von Deutschland einzunehmen. Die *Blockchain*-Technologie wird dabei vermutlich eine wichtige Rolle spielen und kann auch bereits auf lokaler bzw. regionaler Ebene verwendet werden. In der Verwaltung kann die *Blockchain* beispielsweise viele verschiedene Dienstleistungen des Verwaltungsapparates abbilden, bei denen Besitzverhältnisse dargestellt werden. Konkret könnte dies z.B. die Organisierung von Grundstücks-Eigentumsverhältnissen mithilfe der *Blockchain* bedeuten. Dies hätte im Bezug auf die nachhaltige Entwicklung im Rahmen der *SDGs* verschiedene Vorteile. Der Verwaltungsaufwand kann reduziert werden, indem Prozesse digitalisiert werden. Dies würde bei der Umsetzung des 9. Entwicklungsziels der UN, welches u.a. belastbare Infrastruktur fordert, hilfreich sein. Hier kann die *Blockchain* für eine sichere digitale Infrastruktur sorgen, indem nicht auf eine zentrale Instanz vertraut wird, die unter Umständen kompromittiert werden könnte.

Auch im Bereich des Klimaschutzes und der erneuerbaren Energien kann die *Blockchain* neue Möglichkeiten schaffen. So gibt es bereits Projekte, bei denen erneuerbarer Strom mithilfe der *Blockchain* unter extrem geringen Transaktionskosten direkt zwischen Verbraucher und Erzeuger gehandelt wird. Dies kann gerade bei einer dezentralen Stromproduktion, wie sie etwa bei Solarstrom der Fall ist, große Vorteile bringen. [7]

Fazit

Wie bei fast jeder neuen Technologie gibt es auf der einen Seite die Fortschrittsoptimisten, die die *Blockchain* für das Allheilmittel halten. Auf der anderen Seite gibt es die Skeptiker, die die Nachteile der neuen Technologie für so schwerwiegend halten, dass sie längerfristig nicht Fuß fassen würde. Die Wahrheit liegt vermutlich zwischen den beiden Extremen. Zum einen gibt es einige Anwendungsszenarien, die durch die durchdachte Verwendung der *Blockchain* verbessert, oder sogar revolutioniert werden könnten. Zum anderen gibt es aber auch Probleme und Risiken, die sich in den bereits vorhandenen Projekten niederschlagen. Ob und inwiefern Lösungen für diese Probleme gefunden werden können, kann nur die Zukunft zeigen. Gerade die ökologischen Nachhaltigkeitsprobleme, die sich aus der gezielten Energieverschwendung von *Proof-of-Work* Protokollen ergeben, könnten sich im Licht der globalen Erwärmung als fatales Problem der *Blockchain* herausstellen.

Fraglich ist außerdem, ob die *Bitcoin* ihren heutigen Status als größte und beliebteste Kryptowährung beibehalten kann und ob dies überhaupt positiv für die Weiterentwicklung der *Blockchain* Technologie wäre. Im Hintergrund dieser Fragestellung steht die Überlegung, dass *Blockchain*-Projekte aufgrund ihres Aufbaus unflexibel sind und sich damit möglicherweise nicht schnell genug an neue Situationen, aber auch an neue Entdeckungen und Entwicklungen in der Kryptographie anpassen kann.

Insgesamt lässt sich zum heutigen Stand also nicht endgültig feststellen, ob die *Blockchain* jene weitreichenden Konsequenzen haben wird, die ihr einige Enthusiasten prophezeiten.

Glossar

Bitcoin	dt. etwa: Bitmünze. Hier: erste Kryptowährung, die auf einer Blockchain basiert.
Block	Grundbaustein einer Blockchain. Besteht aus einem Header und einem Body. Dieser kann je nach dem Anwendungsgebiet der Blockchain Verschiedenes beinhalten. Im Fall einer Kryptowährungen wären dies z.B. die Transaktionen.
Blockchain	dt. etwa: Blockkette. Hier: Blöcke, die durch kryptografische Verfahren miteinander verkettet sind.
Body	dt: Körper. Hier: Teil eines Blockes, in dem der tatsächliche Inhalt gespeichert wird.
Client	dt: Kunde. Hier: Computer, der Daten von einem Server erhält.
Difficulty	dt. Schwierigkeit. Hier: Maß für der Aufwand, der betrieben werden muss, um einen neuen Block in einer Proof-of-Work Blockchain zu finden.
Ethereum	Zweitgrößte öffentliche Blockchain, die sowohl eine Kryptowährung als auch eine universelle Blockchain Plattform mithilfe von Smart Contracts bietet.
Hash	Wert, der mithilfe einer *Hash*funktion berechnet wird.
Hash-Baum	Methode für eine effiziente Intigritätsüberprüfung von großen Datensätzen.
Hashcash	*Proof-of-Work* Implementierung, die u.a. von der *Bitcoin* verwendet wird.
Header	dt: Kopfzeile oder Dateikopf. Hier: Teil eines Blocks, in dem Metadaten sowie die Root des *Hash*-Baums der Transaktionen gespeichert wird.
Kryptowährung	Eine digitale Währung, die durch kryptografische Verfahren funktioniert und die nicht durch eine Instanz wie eine Zentralbank abgesichert ist.
Miner	dt: Bergbauarbeiter. Hier: eine Node, die Rechenleistung zur Erzeugung eines Blockes einer Proof-of-Work Blockchain zur Verfügung stellt.
Node	dt: Knoten. Hier: Computer, der ein Mitglied eines Peer-to-Peer Netzwerkes, bzw. einer Blockchain ist.
Nonce	Abk. für Number used only once (dt: Nummer, die nur einmal genutzt wird). Sie ist ein Attribut eines Block-Headers, das der Miner frei wählen kann und damit den *Hash*wert des Headers ändert.
Peer-to-Peer	dt. etwa: Gleichgestellter zu Gleichgestelltem. Hier: Eine Form des Netzwerk, die ohne zentrale Instanz und dedizierten Server arbeitet.
Proof-of-Stake	dt: etwa: Beteiligungsnachweis. Kurz: PoS. Hier: Ein Konsensprotokoll.
Proof-of-Work	dt. etwa: Arbeitsnachweis. Kurz: PoW. Hier: Ein Konsensprotokoll.
Server	dt: Kellner. Hier: Computer, der dafür verantwortlich ist Daten auf Anfrage zur Verfügung zu stellen.

Literaturverzeichnis

[1] Antonopoulos, Andreas M.: Bitcoin & Blockchain - Grundlagen und Programmierung. Die Blockchain verstehen, Anwendungen entwickeln. 2. Auflage. Heidelberg: O'Reilly 2018.

[2] Arab, Adrian; Zschäpitz, Holger (2018): Deutschland verpass schon wieder eine Internetrevolution (WWW-Seite, Stand: 26.02.2018). Internet: https://www.welt.de/wirtschaft/article173946251/Blockchain-Deutschland-verpasst-die-naechste-Internetrevolution.html (Zugriff: 13.05.2018, 15:40MEZ)

[3] Atzei, Nicola; Bartoletti, Massimo; Cimoli, Tiziana: A Survey of Attacks on Ethereum Smart Contracts. International Conference on Principles of Security and Trust. Springer, Berlin, Heidelberg, (2017). S. 164-186.

[4] Chapron, Guillaume: The environment needs cryptogovernance.Nature, London, 545, (2017) S.403.

[5] D'Cunha, Suprana Dutt (2017): Dubai Sets Its Sights On Becoming The World's First Blockchain-Powered Government (WWW-Seite, Stand: 18.12.2017) Internet: https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/ (Zugriff: 12.05.2018 23:10MEZ)

[6] Delahaye, Jean-Paul: Die Welt des Bitcoin. Die wichtigsten Fragen zur ersten großen digitalen Währung. Spektrum der Wissenschaft, Heidelberg, 4.18, (2018) S.26-28.

[7] Diermann, Ralph (2016): Energie - Wie Blockchain-Technik das Energiesystem revolutionieren kann (WWW-Seite, Stand: 14.08.2016). Internet: http://www.sueddeutsche.de/wissen/energie-wie-blockchain-technik-das-energiesystem-revolutionieren-kann-1.3117309 (Zugriff: 13.05.2018, 16:18MEZ)

[8] Dölle, Mirko: Chinas Brexit. Warum Chinas Mining-Ausstieg keinen Untergang der Bitcoin bedeutet. c't Magazin für Computertechnik, Hannover, 7/18, (2018) S.6-8.

[9] Graf, Hagen (2018): Blockchain. Byzantnische Generäle und das CAP Theorem (WWW-Seite, Stand: 22.01.2018). Internet: https://blog.novatrend.ch/2018/01/22/blockchain-byzantinische-generaele-und-das-cap-theorem/ (Zugriff: 11.05.2018, 09:05MEZ)

[10] Kannenberg, Axel (2014): Bitcoin: Erstmals gefährliche Konzentration der Mining-Leistung (WWW-Seite, Stand: 16.06.2014). Internet: https://www.heise.de/newsticker/meldung/Bitcoin-Erstmals-gefaehrliche-Konzentration-der-Mining-Leistung-2224113.html (Zugriff: 13.05.2018 14:00MEZ)

[11] Landeshauptstadt Kiel (Hrsg.) (2018): Digitale Woche Kiel - Digitalisierung erleben in Kiel (WWW-Seite, Stand: 13.05.2018) Internet: https://digitalewochekiel.de/ (Zugriff: 13.05.2018, 15:40MEZ)

[12] Lang, Mirco; Karlsletter, Florian (2017): Concensus-Modelle in der Übersicht (WWW-Seite, Stand: 11.08.2017). Internet: https://www.dev-insider.de/consensus-modelle-in-der-uebersicht-a-631671/ (Zugriff: 12.05.2018, 22:52MEZ)

[13] Nakamoto, Satoshi (2008). Bitcoin. A Peer-to-Peer Electronic Cash System. (PDF, Stand: 2008). Internet:https://bitcoin.org/bitcoin.pdf (Zugriff: 24.3.2018, 19:00MEZ)

[14] Pavlus, John: Die Welt des Bitcoin. Die wichtigsten Fragen zur ersten großen digitalen Währung. Spektrum der Wissenschaft, Heidelberg, 4.18, (2018) S.12-20.

[15] Schmidt, Jürgen (2016): Kryptographie in der IT - Empfehlungen zu Verschlüsselungen und Verfahren (WWW-Seite, Stand: 17.06.2017) Internet: https://www.heise.de/security/artikel/Kryptographie-in-der-IT-Empfehlungen-zu-Verschluesselung-und-Verfahren-3221002.html?seite=all (Zugriff: 11.05.2018, 11:38MEZ)

[16] Schoder, Detlef u. Fischbach, Kai: Peer-to-Peer. Anwendungsbereiche und Herausforderungen. Wirtschaftsinformatik, München, Vol.44, (2002) No.6, S.587-589.

[17] Seidler, Christoph (2.4.2018): Islands Geldschürfer. (WWW-Seite). Internet: http://www.spiegel.de/wissenschaft/technik/bitcoin-boom-der-kryptowaehrungen-in-island-kann-das-gutgehen-a-1199460.html (Stand: 12.05.2018, 19:30MEZ)

[18] Wolf, Christian (2017): San Francisco und Kiel besiegeln Partnerschaft (WWW-Seite, Stand: 24.09.2017). Internenet: https://www.ndr.de/nachrichten/schleswig-holstein/San-Francisco-und-Kiel-besiegeln-Partnerschaft,sanfrancisco118.html (Zugriff: 13.05.2018, 15:50MEZ)