Blockchain. Potentiale der Nachhaltigkeit

Florian Dähnert

Seminararbeit im Interdisziplinären Lehrangebot
des Instituts für Informatik

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

`http://informatik.uni-leipzig.de/~graebe/Lehre/Inter`

Leipzig, 31.03.2021

Inhaltsverzeichnis

1. Einleitung

Blockchain genießt derzeit einen Hype. Neugierde gegenüber der neuen Technologie überwiegt immer mehr der Skepsis. Unternehmen wenden sich an Experten, um mit dieser Entwicklung Schritt zu halten. Bitcoin, die Kryptowährung, die Blockchain erst ins Gespräch gebracht hat, erlangt neue Dimensionen, aber auch solche, in denen Bitcoin nicht als stabile Währung angesehen wird. Dennoch gibt es heute Möglichkeiten, Bitcoin so einfach wie Fiatgeld per PayPal zu transferieren. Genutzt wird diese Möglichkeit bisher lediglich von den Personen, die bereits einen Bezug zum Thema haben. Bis sich diese Neuerung grundlegend in unserer Gesellschaft durchsetzen kann, müssen Faktoren, wie Stabilität, White-Box-Modell und Akzeptanz geschaffen werden.

Die vorliegende Seminararbeit stellt den zweiten Teil des Informatikmoduls „Gesellschaftliche Strukturen im digitalen Wandel“ dar. Im Vorfeld wurde diesbezüglich bereits ein Referat zum Thema „Blockchain – Potentiale der Nachhaltigkeit“ ausgearbeitet. Die Intention der Seminararbeit ist folglich, das Referat und die anschließende Diskussion aufzuarbeiten und zu vervollständigen. Dazu wurden drei Themen ausgewählt, die nachfolgend, unter Berücksichtigung des aktuellen Stands, spezifiziert werden sollen. Dabei sollen keine vollumfänglichen Darstellungen erarbeitet werden, sondern es wird lediglich ein Einblick in die relevanten Themen gegeben.
In Absatz zwei sollen die Begriffe „zentral“, „dezentral“ und „distributed“ in einen Zusammenhang gesetzt werden. Anschließend wird ein Einblick in die rechtliche Umsetzung von Smart Contracts, einer Anwendung der Blockchain/Distributed Ledger Technologie, gegeben. Im vierten Absatz wird schließlich eine Anwendungsmöglichkeit für die Blockchain Technologie erläutert.

2. Zentral, dezentral, distributed – Spezifizierung der Begriffe

Vor allem der Begriff der Dezentralität wird häufig parallel zur Blockchain genannt. Nachfolgend soll - neben einer Einordnung der Begriffe - geklärt werden, warum moderne Blockchains immer mehr zur Zentralisierung neigen.

Die im Zusammenhang stehenden Begriffe, zentral, dezentral und distributed, sind in zwei Kategorien/ Ebenen einzuordnen. Dazu zählt einerseits die Kontrollebene und andererseits die Ebene der Standortunterschiede.

Zentralisierung und Dezentralisierung beziehen sich auf die Kontrollebene, die Verteilung (distribution) auf die Ebene der Standortunterschiede (vgl. (Poenitzsch, 2018)). Das heißt, der Begriff der Zentralisierung kann der Dezentralisierung und Verteilung gegenübergestellt werden.

Die Zentralisierung kann mit dem klassischen Client-Server-Modell erläutert werden. Der Server ist hier die einzige Instanz, die die Kontrolle über die anderen Knoten (Clients) ausübt. Jeder Nutzer muss sein Vertrauen in eine Entität, also eine natürliche oder juristische Person, übertragen. Um das Risiko eines Vertrauensbruchs zu minimieren, wird die Kontrolle stattdessen auf mehrere unabhängige Einheiten aufgeteilt. Dieser Eingriff in das System von einer oder wenigen verschiedenen Einheiten wird bei der Dezentralität unterbunden.

Simultan kann diese Erklärungsweise auf die Ebene der Standortunterschiede übertragen werden. Datenspeicherung und Datenausgabe werden bei der Zentralisierung von einer Instanz verwaltet. Das heißt wiederum, dass sie als einzige Entität die folgenden Schutzziele der Informationssicherheit garantieren sollte: Verfügbarkeit, Vertrauen und Integrität (vgl. (Eckert, 2018, S. 7ff.)).
Es besteht jedoch die Möglichkeit, mittels eines Hackerangriffes - beispielsweise mit einem Buffer-Overflow - das gesamte Netzwerk auszuschalten und den zentralen Server abzuschotten. Dadurch kann es weiterhin zu Datenverlust und -manipulation kommen.

Um dieses Risiko zu minimieren, geht der Trend immer mehr in die Richtung der Verteilung der Daten. Dabei werden Daten physisch, je nach Ressourcenverfügbarkeit und Ausfallssicherheit, auf verschiedenen Computern/Datencentern gemeinsam genutzt und repliziert.

Die in der Diskussion angesprochenen Cloud- und Mehrrechner-Dateisysteme sind hier der Kategorie des verteilten, aber zentralisierten Systems zuzuordnen. Die Datenspeicher erfolgen an vielen Standorten rund um den Globus. Dennoch kontrolliert beispielsweise ein Clouddienstanbieter als alleinige Einheit die Datenspeicherung und stellt diese durch Anwendungen bzw. Plattformen zur Verfügung.

Blockchain und Distributed Ledger Technologies sind auf Kontrollebene dezentralisiert und auf der Ebene der Standortunterschiede verteilt. Jedoch erfährt der Begriff der Dezentralisierung bereits erste Kritik.
Die University of Cornell spricht in diesem Zusammenhang in einer Studie davon, dass die eigentlich „dezentralisierten“ Blockchains einer „nicht besonders dezentralisierten“ Technik entsprechen würden (vgl. (Poenitzsch,2018).

Weiterhin wird von Monopolisierung der Blockchain durch das Konsensverfahren bzw. Mining gesprochen (vgl. (Eckert, 2018, S. 845ff.)). Das bedeutet, dass keine Dezentralisierung mehr zugesprochen werden kann, falls ein sogenannter Miner oder eine Gesellschaft von Minern einen Marktanteil von über 50 % erlangt.

Dies gilt weiterhin auch für private Blockchains, welche u.a. von Unternehmen unterhalten werden, die als zentrale Kontrolleinheit fungieren.

Zusammengefasst lässt sich sagen, dass die Ebene der Kontrolle und die der Standortunterscheidung immer einzeln auf die genannten Eigenschaften hin betrachtet und beurteilt werden muss. Der gewünschte Dezentralisierungs- und Verteilungsgrad hängt von den Zielen der Blockchain ab (vgl. (Poenitzsch, 2018). Durch den Trend zu privaten Blockchains und die Monopolisierung der Miner, entsprechen moderne Blockchains entgegen der eigentlichen Designziele eher der Zentralisierung.

3. Smart Contracts – Rechtlich umsetzbar?

Wer sich heute mit Themen wie Blockchain, Distributed Ledger Technologies, Ethereum und weiteren beschäftigt, muss sich zwangsläufig auch mit dem Thema Smart Contracts befassen.

Der Begriff Smart Contract geht auf den US-amerikanischen Informatiker und Juristen Nick Szabo zurück, der Konzepte rechtsrelevanter Computerprogramme bereits in den 90-igern beschrieben hatte.

„[...] A smart contract is a set of promises, specified in digital form, including pro- tocols within which the parties perform on these promises." (Szabo, 1996)

Die Thematik, die in der auf das Referat folgenden Diskussion über Smart Contracts aufgekommen war, beinhaltete die Frage um die rechtlichen Rahmenbedingungen eines Smart Contracts. Ist ein Smart Contract ein Rechtsgeschäft und gibt es Möglichkeiten der nachträglichen Modifikation, falls diese aufgrund von Programmierfehlern nötig wären? Auf diese Fragen wird im nachfolgenden Absatz eingegangen.

Bei Smart Contracts handelt es sich um eine Überschneidung von IT und juristischer Vertragsgestaltung. Dabei wird Leistung und Gegenleistung durch die Programmlogik vorgegeben. Laut Kaulartz (2016, S.2) müssen als eine Voraussetzung für den Abschluss schuldrechtlicher Verträge, folgende Merkmale in einem Geschäft durch Smart Contracts enthalten sein:

Beispiel: Parken – automatisches Bezahlen der Parkgebühr beim Verlassen des Parkplatzes

1. *digital prüfbares Ereignis: Bezahlung der Parkgebühr*
2. *Programmcode, welcher das Ereignis verarbeitet: Boardsoftware im Auto*
3. *Rechtlich relevante Handlung, welche auf Grundlage des Ereignisses ausgeführt wird: Freigabe zum Verlassen des Parkplatzes bei Bezahlung*

Anhand dieser Merkmale lässt sich schlussfolgern, dass ein Smart Contract eine Software ist, welche rechtlich relevante Handlungen in Abhängigkeit prüfbarer Ereignisse steuert, kontrolliert und dokumentiert (vgl. (Kaulartz et al., 2016, S.2)). Im Umkehrschluss können hier nur schuldrechtliche Verträge in Form der Mithilfe durch Smart Contracts geschlossen werden.

Daher benutzen Juristen häufig den Begriff „selbstdurchsetzend" in Bezug auf Smart Contracts. Sie sollen also verdeutlichen, was in einem schuldrechtlichen Vertrag vereinbart wurde (vgl. (Daniels, 2017)).

Rechtlich gesehen würde der Vertragsschluss bereits vor einem erfolgten definierten Ereignis stattfinden, allerdings kann der endgültige Vertragsabschluss erst beim Eintreten des Ereignisses vollzogen werden. Auf das Beispiel bezogen würde es also einen „Vorvertrag" mit dem Parkplatzbetreiber geben, wobei eine Transaktion in Form einer Währung erst dann erfolgt, wenn man vom Parkplatz fahren möchte (Ereignis). Die Prüfung des Ereignisses erfolgt durch die im P2P-Netzwerk beteiligten Rechner.

Hierbei besteht jedoch die Schwierigkeit, natürliche Ereignisse auf digitale Umgebungen abzubilden. Daher werden Smart Contracts in der Regel in ihrer Anwendbarkeit auf digital prüfbare Ergebnisse als *beschränkt* bezeichnet (vgl. (Kaulartz et al., 2016, S. 4)). Um die Ereignisse aus der realen Welt für die Blockchain zu übersetzen und eine Kompatibilität herzustellen, benötigt es sogenannte Oracles (vgl. (Fridgen et al., S. 112). Diese IT-Schnittstellen gelangen aber spätestens dann an ihre Grenzen, wenn das zu prüfende Ereignis mit unbestimmten Rechtsbegriffen, wie „Ablauf einer angemessenen Frist", verknüpft ist. Um dieser Anforderung gerecht zu werden, liefert Kaulartz den Vorschlag, zentrale Stellen zu nutzen, welche die Transaktionen kontrollieren und das Monitoring von Vertragsbedingungen und der Durchführung übernehmen. In den klassischen Blockchainsystemen ist eine solche zentrale Stelle nicht vorgesehen. Hingegen agieren die meisten Distributed Ledger Technologies bereits mit einer zentralen Stelle, um Smart Contracts einbinden zu können.

So eine zentrale Stelle bzw. hier Schiedsstelle, benötigt man, wenn Smart Contracts mit Programmierfehlern versehen sind. Falls ein Ereignis versehentlich falsch definiert wurde, kann es

aufgrund seiner Garantie der Auslösung bei einem definierten Ereignis, zu einer ungewollten Vermögenstransaktion kommen. Ein schuldrechtlicher Rückübertragungsanspruch kann an dieser Stelle auch ausgeschlossen werden, da die Namen der Beteiligten unter der Anonymisierung bzw. Pseudonymisierung verwahrt werden (vgl. (Fridgen et al., S. 120). Die Anpassung oder Löschung eines Smart Contracts ist in erster Linie nicht möglich. Daher wird empfohlen eine programmierte Schiedsstelle in einen Smart Contract zu implementieren (vgl. (Kaulartz et al., 2016, S. 10f)). Das kann ein unabhängiges Institut, eine natürliche Person oder eine juristische Gesellschaft sein. Somit kann bei Fehlern im Smart Contract über eine unabhängige Instanz entschieden werden, ob an dieser Stelle dem rechtlichen Vertrag widersprochen werden kann.

Seit Neuestem besteht dem entgegen die Möglichkeit, Smart Contracts über Umwege zu verändern. Dazu benötigt ein Smart Contract eine Verlinkung zu einem Dispatcher. Dieser wiederum muss auf Bibliotheken (libraries) verweisen (vgl. (Wilkens et al., 2019, S. 12)). Die Bibliotheken sind hier die Schlüsselstellen, denn diese sind veränderlich und anpassbar. Durch das Verweisen werden die Smart Contracts gemeinsam mit den Bibliotheken über den Dispatcher gelesen und Änderungen berücksichtigt.

Welche Variante sich durchsetzen wird, kann zum dem jetzigen Zeitpunkt noch nicht beurteilt werden. Abschließend kann jedoch gesagt werden, dass der rechtliche und technische Rahmen noch Lücken aufweist, die vor der Nutzung als alltägliche Anwendung geschlossen werden müssen.

4. Wahlen mit Blockchain – Sierra Leone geht als Beispiel voran

Abschließend soll mit diesem Absatz eine mögliche Umsetzung der Blockchain-Technologie vorgestellt werden, wie sie im März 2018 in Sierra Leone umgesetzt wurde.
Anlässlich der fortwährenden Kritik an analogen Wahlen, wie sie bis zum heutigen Tag durchgeführt werden, soll die Blockchain Möglichkeiten gegen Korruption und Manipulation von Wahlergebnissen bieten. Sierra Leone startete am 7. März 2018 erste Tests, um digitale Wahlen mittels Blockchain umzusetzen (vgl. (Perper, 2018)).
Hierbei wurde die Blockchain vorerst jedoch nur für die Protokollierung und Verifikation von Papierstimmen genutzt. Die Mitarbeiter des schweizer Blockchain-Unternehmens Agora übernahmen während des Projektes lediglich eine Beobachterrolle, während die Stimmzettel von Mitarbeitern der Agora, unter Beobachtung der internationalen Wahlkommission (NEC) manuell übertragen wurden (vgl. (Houser, 2018)). Außerdem wurden nur Teilgebiete des westafrikanischen Staates erfasst.

Das Konzept, welches mit diesem Versuch überprüft werden sollte, kann also eine Möglichkeit für zukünftige Wahlen in anderen Ländern darstellen. Betrachtet man beispielsweise die US-Wahlen von 2020, so würde man mit der Blockchain-Technologie mögliche Manipulationen durch Wahlhelfer oder bei Briefwahlen umgehen können. Der Vorwurf der veralteten Wahlmethoden existiert jedoch auch über die US-Grenzen hinaus. Daher stellt sich nun die Frage, inwiefern das Pilot-Projekt Vorteile bietet und wo seine Grenzen zu verorten sind.

Die wesentliche Chance, die die Blockchain mitbringt, stellt die fehlende übergeordnete Instanz dar. Dadurch bietet sich vor allem in Ländern, in denen Korruption und Konflikte vorherrschen die Möglichkeit, die Wahl unabhängig von politischen oder sozialen Mächten durchzuführen, um Meinungsfreiheit und Demokratie zu ermöglichen (vgl. (o.V., 2020)).
Da die Methode jedoch noch nicht ausgereift ist, gehen mit ihr auch verschiedene Probleme einher. Dazu zählt einerseits die mögliche Monopolisierung von Minern (bei öffentlichen Blockchains) und andererseits die fehlende Aufklärung, welche die Grundlage für die Akzeptanz und Verbreitung darstellt (vgl. (Eckert, 2018, S. 845ff.)).
Unabhängig von diesen entwicklungsbedingten Schwächen bietet die Blockchain jedoch eine gute, ausbaufähige Grundlage für faire und transparente Wahlen, sofern entsprechende politische Voraussetzungen in den Ländern erfüllt sind.

5. Fazit

Auch wenn die vorangegangenen Ausführungen nicht vollumfänglich dargestellt werden konnten, so bieten sie dennoch einen Einblick in mögliche Potenziale von Blockchain für die Nachhaltigkeit und vertiefen die in der Diskussion angeschnittenen Inhalte.
Zum einen wurde dargestellt, wie Cloud-Anbieter und Mehrrechner-Dateisysteme in Bezug auf die Begriffe - zentral, dezentral und verteilt – einzuordnen sind.
Weiterhin wurde der rechtliche Rahmen von Smart Contracts hinsichtlich der Anwendbarkeit bei Programmierfehlern beschrieben. Schließlich wurde eine konkrete Möglichkeit der Umsetzung von Blockchain aufgezeigt, welche eine Grundlage für weitere Auseinandersetzungen bietet und das Thema damit auf theoretischer Ebene abschließt.

Da die Thematik rund um Blockchain einer stetigen Weiterentwicklung unterliegt, sind die angeführten Vertiefungs- und Anwendungsmöglichkeiten lediglich als einzelne Aspekte einer Bewegung zu verstehen, die auch in Zukunft einen wesentlichen Trend in der IT-Branche verzeichnen wird.

6. Literaturverzeichnis

(1) Julia Poenitzsch: What's the difference between Decentralized and Distributed?, medium.com, 2018, URL: https://medium.com/nakamo-to/whats-the-difference-between-decentralized-and-distributed-1b8de5e7f5a4, gelesen am 05.03.2021.

(2) Prof. Dr. Claudia Eckert: IT-Sicherheit: Konzepte-Verfahren-Protokolle, Walter de Gruyter GmbH, 2018, 10. Auflage, Berlin/Bosten.

(3) Markus Kaulartz, Jörn Heckmann: Smart Contracts – Anwendung der Blockchain Technologie, Verlag Dr. Otto Schmidt, 2016, Köln.

(4) Robert Wilkens, Richard, Falk: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Springer Gabler, 2019, Berlin.

(5) Nick Szabo: Smart Contracts: Building Blocks for Digital Markets, fon.hum.uva.nl, 1996, URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html, gelesen am 20.03.2021.

(6) Arnold Daniels: Smart Contracts 3 – limitation of self-enforcment agreement, medium.com, 2017, URL: https://medium.com/ltonetwork/smart-contracts-3-limitations-of-a-self-enforcing-agreement-257cfbabeff5, gelesen am 20.03.2021.

(7) Prof. Dr. Gilbert Fridgen Prof. Dr. Nikolas Guggenberger Prof. Dr. Thomas Hoeren Prof. Wolfgang Prinz (PhD) Prof. Dr. Nils Urbach: Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, Bundesministerium für Verkehr und digitale Infrastruktur, 2019, Berlin.

(8) Kristin Houser: Hold up: What actually happened in Sierra Leone´s Blockchain Election?, futurism.com, 2018, URL: https://futurism.com/sierra-leone-election-blockchain-agora, gelesen am 21.03.2021.

(9) Rosie Perper: Sierra Leone just became the first country in the world to use blockchain during the election, businessinsider.com, 2018, URL: https://www.businessinsider.com/sierra-leone-blockchain-elections-2018-3?r=DE&IR=T, gelesen am 21.03.2021.

(10) o.V.: Nach US-Wahldebakel: Ist digitales Wählen auf Blockchain eine Alternativ, finanzen.net, 2020, URL: https://www.finanzen.net/nachricht/devisen/wahlsysteme-in-der-kritik-nach-us-wahldebakel-ist-digitales-waehlen-auf-blockchain-eine-alternative-9495507, gelesen am 23.03.2021.