Zeitschrift für Praktische Philosophie
Band 11, Heft 1, 2024, S. 449–474
www.praktische-philosophie.org
https://doi.org/10.22613/zfpp/11.1.18

Blockchain statt Vertrauen?

Bedeutung der Blockchain-Technologie für Vertrauen und Sich-verlassen-auf

Blockchain statt Vertrauen?

Bedeutung der Blockchain-Technologie für Vertrauen und Sich-verlassen-auf

Ingrid Becker, St.Gallen

Zusammenfassung. Vertrauenslosigkeit und damit Vertrauen gelten als Kategorien, die Blockchain- und digitale Technologien über Fragen der bekannten Bitcoin-Anwendung hinaus theoretisch interessant machen. Es zeigt sich jedoch, dass es schwierig wird, wenn wir von „(Nicht-)Vertrauen in die Blockchain" sprechen. Ist es nicht oftmals eher Verlässlichkeit als Vertrauenswürdigkeit, auf deren Basis Bitcoin-Akteur:innen handeln? Ist Vertrauen in zwischenmenschlichen Beziehungen, das wir alltäglich konkret erleben und oft intuitiv verstehen, und das sich auf Institutionen und Professionen ausweiten kann, für die starre Blockchain-Technologie relevant? Und falls ja, auf welche Weise? Oder wird die Notwendigkeit für Vertrauen – wie es sich im Bitcoin-Whitepaper auf den ersten Blick lesen lässt – mit Bitcoin überflüssig? Sollten wir von einem Technologievertrauen sprechen, das, aufgrund der Unveränderlichkeit dessen, was in der Blockchain gespeichert ist, mit dem interpersonalen Vertrauensparadigma unvereinbar ist und damit eine tiefgreifende Transformation der sozialen Realitäten implizieren würde? Der hier unternommene Versuch, Vertrauen in Abgrenzung zu Sich-verlassen-auf, beide als philosophische Konzepte, im Blockchain-Kontext zu aktualisieren, bedeutet auch, Technologien in ihrer Verwobenheit mit sozial interpretierten Realitäten (des Vertrauens) zu verstehen.

Schlagwörter: Vertrauen, Vertrauenswürdigkeit, Sich-verlassen-auf, Blockchain-Technologie, Bitcoin

Abstract: Trustlessness and trust are considered essential categories that make Blockchain and digital technologies theoretically interesting beyond questions of the well-known Bitcoin application. However, it turns out to be difficult when we talk about the meaning of (non-)trust in Blockchain. Isn't it often reliability rather than trustworthiness that matters to Bitcoin actors? Is trust in interpersonal relationships, which we experience concretely and often intuitively in everyday life, and which can be extended to institutions and professions, relevant to the rigid blockchain technology? And if so, how? Or will the necessity for trust – as the Bitcoin Whitepaper suggests at first glance – become redundant with Bitcoin? Should we speak of technology trust that is incompatible with the interpersonal trust paradigm, due to the immutability of what is stored in the blockchain, and thus would imply a profound shift in social realities? The attempt made here to actualize trust in contrast to reliance, both as philosophical concepts, in the blockchain context also means understanding technologies in their interconnectedness with socially interpreted realities (of trust).

Keywords: Trust, Trustworthiness, Reliance, Blockchain technology, Bitcoin

1 Einleitung

Wir brauchen Geschichten darüber, wann Vertrauen, Misstrauen oder keines von beidem angemessen ist (Hawley 2014). Die Digitalisierung, neben Künstlicher Intelligenz (KI) auch die Blockchain-Technologie, lassen das Erzählen von Geschichten und das Verstehen durch Erzählungen nicht unberührt – doch sind es andere Erzählungen? Sollten es andere Erzählungen über Vertrauen und Verletzbarkeit sein? Vielleicht welche über Zweifel an Technologien und über ihre *Verlässlichkeit?* Ein Vertrauen, das als bedeutend für unsere Sozialität angenommen wird, hat Biss, wenn es nicht darum geht, es „billig [zu] erwerben" (Hartmann 2022, 15).

Bitcoin sticht als interessantes digitales Phänomen heraus, da es sich von digitalen Sicherheitsanwendungen und Organisationen abhebt, die Vertrauen auch in Verbindung mit Sicherheit als erforderlich erachten und dies im Sinne von „Sicherheit schaffe Vertrauen" (Hartmann 2022, 247) kommunizieren. Bitcoin hingegen zielt darauf ab, kompliziertes Vertrauen obsolet zu machen, wie es im Bitcoin-Whitepaper (Nakamoto 2008) zu lesen ist. Dieses beinhaltet den Programmkode der dezentralen Kryptowährung Bitcoin, die von einer, manche würden sagen robusten (Simser 2015, 156), Community in einem Peer-to-Peer-Netzwerk unterstützt wird. Vor dem Hintergrund der Finanzkrise will Bitcoin auf die Notwendigkeit von Vertrauen verzichten, während uns andernorts „ständig verfeinerte Methoden der Ver-

trauenswerbung“ (Frevert 2013, 10) umgeben. Mit einer engen Verbindung von „Credit“[1] und Vertrauen (Frevert 2013, 104) hat „Vertrauen“ eine lange Tradition in der Moderne. Es prägt (Erzählungen über) unsere Wirtschaftsweise, in die sich der „vertrauenslose Bitcoin“ scheinbar problemlos einfügt.

Wie im nachfolgenden Abschnitt gezeigt wird, ist umstritten, dass Bitcoin Vertrauen überflüssig macht. Gegenpositionen zur Annahme der Vertrauenslosigkeit gehen entweder davon aus, dass sich Vertrauen verlagert, das heißt, weiterhin über andere Ebenen realisiert wird, etwa über Vertrauen in Institutionen oder Professionen (Butler 2021, Jones 2004). Oder Vertrauen wird als Vertrauen in Programmkode oder in Algorithmen, allgemeiner in Technologien, verstanden. Mit dem Bitcoin-Projekt wird Vertrauen oder „Zuversicht in die Neutralität algorithmischen Handelns“ (Introna und Pecis 2020, 50) verbunden.

Algorithmen sind wesentlicher Bestandteil der Blockchain. Nur, was meinen wir, wenn wir sagen, wir vertrauen in die Blockchain, in Algorithmen, die in bestimmter Weise als neutral bewertet werden?[2] Wir können sagen, eine Community teilt bestimmte Werte, wie die Neutralität im Sinne einer Unparteilichkeit, und *verlässt* sich darauf, dass Blockchain-Technologie, beziehungsweise Bitcoin, Normen der Unparteilichkeit – potenzieller Zugang zum Netzwerk für alle – wie erwartet realisiert.[3] Doch können sich Sich-verlassen-auf und Vertrauen (ebenso wie Zuversicht und Vertrauen) wesentlich unterscheiden: Vertrauen ist „etwas“ mehr (Hawley 2014, 5).

Vertrauen und Sich-verlassen-auf sind als Begriffe und plurale Phänomene Teil unserer (sozialen) Lebenswelt. Theoretisch knüpft McLeod (2020) an eine entsprechend plurale Behandlung von Vertrauen und Sich-verlassen-auf in der Philosophie an. Dabei bleibt sie einem zwischenmenschlichen Vertrauensparadigma auch im Zusammenhang mit Technologien bzw. Robotern grundlegend verbunden (ähnlich auch Butler 2021). In diesem zwi-

1 „Von Campes Wörterbuch 1811 mit Vertrauen übersetzt und an die Geschäftstätigkeit eines Kaufmanns gebunden“ (Frevert 2013, 104).

2 Oft geht *neutral* im Falle von Bitcoin nicht über die implizite Bewertung hinaus, dass mehrere tausend Zeilen Programmkode als effizienter bewertet werden als bestehende Behörden und Organisationen, und mit „effizient“ gerade nicht neutral.

3 Wobei es problematisch werden kann, wenn das, was Blockchain ermöglicht, sich ausschließlich im Sinne dieser Maßstäbe zu rechtfertigen hat, beispielsweise einzig nach Effizienzgesichtspunkten.

schenmenschlichen Paradigma, wie es in Abschnitt drei zugrunde gelegt wird, ist „akzeptierte Verletzbarkeit“ (Baier 1986, 235, eigene Übersetzung) zentral, die Vertrauen abgrenzt von Vertrauen als allgemeine Abhängigkeit oder als Zweifel und insbesondere von Vertrauen als individuelle Risikovermeidung, und damit auch die Unterscheidung zwischen Sich-verlassen-auf und Vertrauen erklärt (McLeod 2020). Von Vertrauen im Zwischenmenschlichen nehmen wir grundlegend an, dass es möglichst vertrauenswürdigen Entitäten zugeschrieben werden sollte (Simon 2020, 1, O’Neill 2018), die ihrerseits Vertrauen benötigen, um sich als vertrauenswürdig erweisen zu können. Das bedeutet auch, dass Vertrauenswürdigkeit für die Philosophie ebenso wichtig sein sollte wie Vertrauen selbst (Simon 2013); gleiches gilt für Sich-verlassen-auf und Zuverlässigkeit. Mit derartiger begrifflicher Differenzierung lässt sich genauer verstehen, so zeigt es Abschnitt vier, welche der beteiligten Bitcoin-Akteur:innen sich kontextbedingt eher verlassen anstatt zu vertrauen, und ob ein gewisses „Vertrauen“ nicht doch angemessen ist, anstatt es als überflüssig zu konstruieren. Dabei impliziert mein Beitrag keine grundlegend anderen Bedeutungen von anspruchsvollem zwischenmenschlichem Vertrauen, wenn etwa konkrete Interaktionen zwischen Bitcoin-Entwickler:innen und die Rolle normativer Erwartungen betrachtet werden.

2 Blockchain statt Vertrauen?

2.1 Blockchain-Technologie

Blockchain-Technologie gehört zu den digitalen Technologien, die als äußerst transformativ gelten. Als Möglichkeit eines unveränderbaren, dezentral gehaltenen Kassenbuchs, auch wenn es „vielleicht nicht sexy oder revolutionär klingen mag“ (The Economist 2015, eigene Übersetzung), ist Blockchain-Technologie auch eine Geschichte großer Umwälzungen. Blockchain wird angepriesen als neues Zeitalter (Tapscott und Tapscott 2018), als über-das-Internet-hinaus, da Blockchain-Technologie auf vernetzten Computern operiert (Davidson, De Filippi and Potts 2018), als „neues politisches Werkzeug […], dass das Potenzial hat, dort erfolgreich zu sein, wo das Internet versagt hat“ (De Filippi 2017, 60) oder als Projektionsfläche für nicht aufgegebene Visionen „vom egalisierenden Potential des Internets“ (Münker 2019, 117).

Davidson, De Filippi and Potts (2018) definieren (öffentliche) Blockchain-Technologie als „new digital technology that combines peer-to-peer

network computing and cryptography to create an immutable decentralised public ledger“ (Davidson, De Filippi and Potts 2018, 639). Blockchain-Technologie ermöglicht eine öffentliche gemeinsame Buchführung auf Basis der Erfüllung folgender fünf Kriterien:

(1) Die Blockchain kann als Datenbank verstanden werden. Sie validiert und speichert Datensätze (z. B. Transaktionen, Vermögenswerte), und zwar dezentral, das heißt,
(2) die Blockchain liegt nicht auf einem einzigen Rechner, sondern ist in identischer Form auf viele Rechnern verteilt, die miteinander vernetzt sind.
(3) Datensätze werden zu Blöcken zusammengefasst. Jeder Block wird mit einem Zeitstempel versehen und mit dem vorhergehenden Block kryptografisch verknüpft, wodurch eine chronologische, unveränderliche Reihenfolge der Datensätze entsteht.
(4) *Nodes*, mit dem Netzwerk verbundene Rechenknoten, übernehmen Prüfaufgaben (validieren Transaktionen) und fügen neue Blöcke auf Basis eines Konsensmechanismus hinzu.
(5) Die auf diese Weise akzeptierten Eingaben sind für alle im Netzwerk einsehbar.

Die Verknüpfung dieser Kriterien macht die Blockchain zu einem Instrument der Überprüfung von Transaktionen (Casino et al. 2019); genauer, der Überprüfung dessen, was eingegeben wurde, und der Überprüfung dessen in einem bestimmten Kontext. Auf die Frage, was die Blockchain ontologisch ausmacht, antworten Reijers und Coeckelbergh (2018, 107, eigene Übersetzung), indem sie auf die Blockchain-Technologie als „ständig wachsende digitale Kette von aufgezeichneten Transaktionen“ verweisen. Indem sich jeder neue Block (Datensatz) in linearer Ordnung auf den jeweils vorherigen Block bezieht (jeder Block stets den Hash-Wert des vorherigen Blocks enthält), entsteht eine fixe Reihenfolge, die als *eine* von Bitcoins verzahnten Sicherheitsmaßnahmen vor nachträglichen Änderungen schützen soll. Im Gegensatz zur Manipulation einer zentralen Datenbank würde das Ändern vorheriger Blöcke und damit ihrer Hash-Werte bedeuten, alle nachfolgenden Blöcke und deren Hash-Werte mit erheblichem Aufwand und durch Übernahme der Mehrheit der Rechenleistung im Netzwerk neu berechnen zu müssen („Proof-of-Work“, siehe Fußnote 7). In der Regel wird es als unrentabel angesehen, eine gefälschte Version der gesamten (Bitcoin-)Kette zu erstellen (Voshmgir 2016). Die lineare Ordnung der Blockchain stellt nach Mühlhoff (2018, 15) einen wesentlichen Unterschied zu vernetzten Websei-

ten dar, welche ohne Weiteres verändert, auf- und abgebaut, Informationen missbräuchlich verwendet werden können.

Durch die Blockchain-Technologie soll sich soziale Realität verändern (Tapscott und Tapscott 2018), über die Evolution digitaler Währungen und das Bitcoin-Projekt als prominenteste Anwendung der Blockchain hinaus.[4] Schon früh wurde Blockchain dabei mit „Vertrauen" und dessen Veränderung in Verbindung gebracht (Davidson, De Filippi and Potts 2018, De Filippi 2017, Werbach 2018). „Nicht digitale Münzen, sondern die Vertrauensmaschine, die diese Münzen prägt, ist die eigentliche Innovation", schreibt The Economist (2015, eigene Übersetzung). Gleichzeitig gewinnen „(Nicht-) Vertrauensbeziehungen" in Verbindung mit Blockchain insbesondere durch die Kryptowährung Bitcoin an Relevanz.

2.2 Bitcoin und Vertrauenslosigkeit?

Ein wesentlicher Bestandteil der Blockchain- und Bitcoin-Erzählungen ist, dass die Notwendigkeit von *Vertrauen* in zentrale intermediäre Organisationen sowie zwischen Transaktionsparteien überflüssig wird.[5] Auf Basis der Unveränderbarkeit gespeicherter Daten, validiert durch Konsens, soll Blockchain-Technologie auf Vertrauen verzichten können, dieses höchstens gegebenenfalls herstellen (Aste et al. 2017).

Das Bitcoin-Projekt startet, während der Finanzkrise 2008/2009, mit einer Kritik an (Zentral-)Banken und der finanziellen Blockade von Wi-

4 Das Spektrum der „erwünschten" Blockchain-basierten Veränderungen reicht vom inklusiveren Zugang zu globalen Finanzsystemen über die Erhöhung der Transparenz von Lieferketten bis hin zur digitalen Authentifizierung von Kunstwerken, Artefakten oder „The Second Era of Democracy" (z. B. Tapscott und Tapscott 2018, 211, Swan 2017, Swan 2015b). Kaum ein Bereich des gesellschaftlichen Lebens scheint für eine Optimierung durch die Blockchain ungeeignet (Tapscott und Tapscott 2018) – was auch für andere Versprechen gilt, die mit der Digitalisierung oder dem digitalen Kapitalismus aufkommen. (Wer dabei bestimmt, was als Problem gilt und bearbeitet werden soll, bleibt die interessantere Frage). Versprechungen wie diese fügen sich ein in eine vorherrschende technische Anwendungsorientierung in Wissenschaft und Gesellschaft im Gegensatz zu ebenso dringend benötigten überfachlichen und dialogischen Perspektiven (z. B. Swan und De Filippi 2017): zum Beispiel zum Verhältnis von Digitalisierung und Ethik, zum Verhältnis von Dezentralisierung und Macht oder zu Fragen konkreter Handlungsbedingungen.

5 Vertrauen soll überflüssig werden in einem Kontext, in dem Akteur:innen als Bitcoin-Miner, -Node, -Investor:in nicht ohne Risiken unterwegs sind.

kileaks durch mehrere Banken (Roio 2013).[6] Mit Veröffentlichung des Bitcoin-Whitepapers wird unter dem Pseudonym Nakamoto (2008) Vertrauenslosigkeit in den Mittelpunkt der Bitcoin-Architektur gestellt, ohne jedoch ein Verständnis von Vertrauen und dessen Überwindung oder Veränderung zu spezifizieren:

> What is needed is an electronic payment system based on cryptographic proof *instead of trust*, allowing any two willing parties to transact directly with each other without the need for a trusted third party. (Nakamoto 2008, 1, eigene Hervorhebung)
>
> We have proposed a system for electronic transactions *without relying on trust*. (Nakamoto 2008, 8, eigene Hervorhebung)
>
> The *root problem* with conventional currency is all the *trust* that's required to make it work. (Nakamoto 2009, Forumsbeitrag, eigene Hervorhebung)

Verstanden als sozial kompliziertes Vertrauen, so lassen sich die Zitate lesen, formuliert Nakamoto (2008, 2009) die Notwendigkeit, bisheriges Vertrauen durch Kryptographie – *nicht* etwa durch Vertrauen in Kryptographie – zu überwinden. Ein Nicht-Vertrauen-Müssen soll die Transaktionen zwischen (Transaktions-)Parteien kennzeichnen, die persönlich keine Bindung eingehen müssen (Nakamoto 2008, De Filippi 2017) und deren Transaktionen weder über vertrauenswürdige Dritte abgewickelt (Nakamoto 2008, 1, Swan 2015a) noch über digitale Reputationsmechanismen und stattdessen über Programmkode *abgesichert* werden.[7] „Vertrauenswürdige" Dritte werden ersetzbar: insbesondere Banken, die in der Regel Doppelausgaben verhindern und ein gewisses Maß an Privatsphäre sicherstellen, indem sie den Zugriff auf Transaktionsinformationen einschränken (Nakamoto 2008, 6). Auch Bitcoin löst das Problem der Doppelausgaben, ohne dabei auf die Öffentlichkeit der Transaktionen bei gleichzeitiger Wahrung einer gewissen

6 Losgelöst von der Finanzkrise gehen Bitcoin notwendige Entwicklungen in der Kryptographie mit einer älteren Geschichte voraus.

7 Für Sicherheit sorgt etwa der Proof-of-Work, ein Ausführungsnachweis, der regelt wie im Konsens neue Blöcke zur Blockchain hinzugefügt werden und mit erheblichem Rechenaufwand einhergeht. Nach Nakamoto (2008, 1): „The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work".

Privatheit verzichten zu müssen (Nakamoto 2008, 6). Begrenzung von Unsicherheit wird neben der Vermeidung von Doppelausgaben auch darin gesehen, dass bitcoins „mit einer *vorhersehbaren* Rate produziert werden und die Geldmenge vorbestimmt ist“[8] (Christopher 2016, 172, eigene Übersetzung und Hervorhebung). Es ist also relevant, wie sich Vorhersage und Vertrauen verhalten, und ob das Verhältnis zwischen Sicherheit und Vertrauen nicht vielschichtiger ist als die Annahme, dass sich Vertrauen mit Sicherheit (durch Algorithmen) erübrigt.

Auch De Filippi (2017, 59) stellt die „vertrauenslose Infrastruktur“ als bemerkenswerte Eigenschaft der Blockchain heraus; als eine für das Eingehen sozialer Bindungen bedrohliche Eigenschaft. Institutionell abgesichertes Vertrauen gerät laut Glaser (2017, 1543) mit Bitcoin unter Beschuss. Die Bezeichnung der „trustfree setups“ (Glaser 2017, 1543) entsteht: die Möglichkeit, institutionelles und persönliches Vertrauen zu umgehen oder durch „etwas“ zu ersetzen. „Anspruchsvollere“ Formen der Kooperation werden auf Basis indirekter Reziprozität mit Blockchain als möglichem Mittel erhofft (van den Hoven et al. 2019, Teng 2023). Ob die Person oder Organisation, die partizipiert und insbesondere Transaktionen abwickelt (Nakamoto 2008), vertraut oder vertrauenswürdig ist, soll vernachlässigbar sein. Relevant ist, dass möglichst viele Nodes an der Validierung *zuverlässig* beteiligt sind und die erforderlichen Rechenoperationen ohne konkreten Bezug zur Person ausgeführt werden.[9] Dazu passt der Bitcoin-Gründungsmythos, dass bis heute verborgen bleibt, welche Person oder Gruppe hinter dem Pseudonym Nakamoto steckt.

Die Frage nach Vertrauenswürdigkeit stellt sich im Verständnis eines vollkommen vertrauensfreien Setups nicht: Vertrauenswürdigkeit entspräche grob einem aktiven Umgang mit Erfahrungen, Personen und Ereignissen, die den Bitcoin-Kontext ausmachen und Vertrauen einladen können.

2.3 Bitcoin und Vertrauen?

Nicht immer wird davon ausgegangen, dass Vertrauen im Blockchain-Kontext überflüssig wird, also ganz darauf verzichtet werden kann. Entweder wird dann angenommen, (1) dass Vertrauen weiterhin realisiert wird, d. h.

8 Die maximale Anzahl an bitcoins wurde durch das Protokoll auf knapp 21 Millionen Einheiten festgelegt und kann von einzelnen Akteur:innen nicht beeinflusst werden.

9 Zu Problemen der Bitcoin-Anonymität siehe Maurer et al. (2013).

andere Entitäten die Vertrauenslast übernehmen (Butler 2021) und sich diese teilen (Werbach 2018), oder es wird deutlich weitergegangen und angenommen, (2) dass Vertrauen anders hervorgebracht wird: als „Vertrauen" in Algorithmen oder Kode (van Lier 2017, Velasco 2017).

(1) Im Falle von Vertrauen auf weiteren Ebenen werden Bitcoin-Akteur:innen nicht isoliert betrachtet, sondern als über Bitcoin hinausgehend (normativ) eingebunden: in soziale, partizipative (Open-Source-) Gemeinschaften, Rechtsverhältnisse und wirtschaftliche Systeme. Sie geben ihr Vertrauen Expert:innen oder Professionen (der Kryptographie), dem breiteren Rechtssystem (Butler 2021), oder sie *verlassen sich* auf etablierte Marktpraktiken, die auch Bitcoin ausmachen (Mining-Wettbewerb). Mit weiteren Vertrauensebenen ist meist (vertikales) Vertrauen in Institutionen gemeint, die uns auch „in Form von Mensch-zu-Mensch-Kontakten" begegnen (Hartmann 2022, 127). Vertrauen bleibt außerdem relevant in Ansätzen, in denen sich die Perspektive auf die entscheidenden Vertrauensakteur:innen weitet: Es werden nicht hauptsächlich User berücksichtigt, die Transaktionen (Zahlungen) über Bitcoin durchführen (Nakamoto 2008 kann so eng gelesen werden). Stattdessen werden für Vertrauensfragen verschiedene und vielleicht relevantere Entitäten betrachtet – Entwickler:innen, Core-Maintainer, die für die Pflege und Aktualisierung des Bitcoin-Quellkodes verantwortlich sind, und mit dem Netzwerk verbundene Rechenknoten (Teng 2023, Bundesamt für Sicherheit in der Informationstechnik 2019). Es wird gefragt, auf wen oder was die Akteur:innen vertrauen und wann sie misstrauen (sollten), oder was sie zuversichtlich macht, statt von Vertrauenslosigkeit auszugehen.

Für die Vorstellung, dass sich Vertrauen verlagert und weiterhin stattfindet, sind Rückbezüge auf zwischenmenschliche Interaktionen und soziale Normen entscheidend. Nach Teng (2023, 147, 153) verkörpern Technologien wie die Blockchain moralische Standards, die ein breites Spektrum an normativen Erwartungen einladen und gerade auch emotionale Enttäuschungen (Wut etc.) nachvollziehbar machen. Von den Beteiligten sind moralische Standards in ihrem Anwendungskontext zu interpretieren: Je nach Bedeutung können unterschiedliche Vertrauensbeziehungen entstehen oder auch nicht. Zudem ist nicht auszuschließen, dass sich normative Erwartungen mit Technologien verschieben und Blockchain-Technologien Vertrauen vermitteln können (Reijers und Coeckelbergh 2018).

(2) Weiter als (1) gehen Ansätze, die Vertrauen grundsätzlich(er) in einem Wandel sehen und ein „technisches Vertrauen" konzeptualisieren. Dann

ist die Rede von einer Revolution des Vertrauens, von Vertrauen, das sich mit der Blockchain verändert oder verändern kann (van Lier 2017, Velasco 2017). Beispielsweise spricht Velasco (2017, 722, eigene Übersetzungen) im Falle von Bitcoin[10] von einer instrumentellen oder „computergenerierten funktionsfähigen Version von Vertrauen". Diese computergenerierte Version von Vertrauen wird damit erklärt, dass „die institutionelle Aufzeichnung und Überprüfung [etwa durch Banken, IB] zur rechnergestützten Aufzeichnung und Überprüfung übergeht" (Velasco 2017, 721). Velasco (2017, 722) adressiert die „Vorherrschaft der computergenerierten Elemente" für ein bestimmtes Funktionieren (von Blockchain): Dass neue bitcoins durch Berechnung erzeugt werden, führt nach Velasco (ebd.) zur „Verschiebung oder gar Verdrängung [displacement] des gemeinsamen Vertrauens – verkörpert durch Institutionen und soziale Interaktionen". Velascos Ansatz oder auch van Liers (2017, 703) „Vertrauen in Informationen oder Transaktionen, die von vernetzten Systemen autonom durchgeführt werden" deuten darauf hin, dass es für die Analyse von „neueren" Vertrauensformen relevant ist, auf wen oder was vertraut wird. Unter anderem können neuere Vertrauensformen „nicht mehr vollständig von bisherigen Akteur:innen (Staat, Entwickler:innen, etc.) definiert werden" (Velasco 2017, 724). Zu diskutieren wäre, ob van Lier (2017) mit dem Fokus auf Vorhersagen nicht eher ein Sich-verlassen-auf meinen könnte und welchem Vertrauensverständnis Velascos (2017) *Kontrolle* von Vertrauen (durch staatliche Autoritäten oder „computing ledgers") genauer entspricht. Solche Fragen sind zu stellen, da Vorstellungen von Vertrauen nicht zwingend unberührt bleiben von „computergeneriertem Vertrauen", von neuen Entitäten, die uns die Last des Vertrauens (vermeintlich) abnehmen. Die Eigenschaften der Blockchain-Technologie berühren in besonderer Weise Fragen zum Verhältnis von Vertrauen und Sicherheit, von Vertrauen und Kontrolle.

Die Frage nach einem angemessenen Vertrauensverständnis im Zusammenhang mit Technologien weiter zu diskutieren, beinhaltet in diesem Beitrag (1) eine kontextuelle Aktualisierung des Vertrauenskonzepts in Abgrenzung zu Sich-Verlassen und damit verbunden, (2) den Vertrauensgegenstand, das heißt auch die Vertrauenswürdigkeit in Abgrenzung zur Verlässlichkeit, zu betrachten. Die einzelnen Fragen lauten: Zu (1) Sollten wir von „Vertrauen" absehen, wenn ausschließlich gemeint ist, sich (berech-

10 Beziehungsweise im Falle von „computing ledgers", also „Computerbüchern" oder „Computerbuchführung" (Velasco 2017).

nend) risikominimierend zu verhalten, was dann zu Kooperation führen kann (Gambetta 1988)? Welche Bitcoin-Akteur:innen treten bei einem Vertrauenskonzept, das über Sich-verlassen-auf hinausgeht, hervor? Wer muss Verletzbarkeit bis zu einem gewissen Grad akzeptieren? Zu (2) Wenn von Vertrauen gesprochen werden kann, was macht die Eigenschaft der Vertrauenswürdigkeit aus? Welche Qualitäten haben Bitcoin-Entitäten, um Vertrauen einzuladen oder dessen Bildung anzustoßen?

Je nach zugrunde liegendem Ansatz und Verständnis von Vertrauen fallen Antworten auf Vertrauensfragen im Zusammenhang mit (Blockchain-)Technologien unterschiedlich aus. Wie sich zeigen wird, haben die Antworten auch unterschiedliche normative Relevanz. Für die Nutzung und Regulierung von Anwendungen wie Bitcoin sollte von Bedeutung sein, unter welchen Bedingungen und in welchen Kontexten (auch ethisch) angemessen von Vertrauen, Sich-Verlassen oder Misstrauen gesprochen werden kann. Dies gewinnt nicht zuletzt aufgrund der Beobachtung an Relevanz, dass auch in dezentralen Architekturen wie Bitcoin mächtige Akteur:innen und Mechanismen entstehen, die Vertrauensbeziehungen zwischen bekannten und unbekannten Anderen beeinflussen können.

3 Vertrauen und Sich-verlassen-auf als philosophische Konzepte

Vertrauen ist ein oft positiv besetzter Begriff, insbesondere im alltäglichen Gebrauch, und wird gerade in (technik)philosophischen Ansätzen wieder aufgegriffen und mitunter kritisch (unterscheidend) analysiert (Hartmann 2022, Jacobs 2021, Reinhardt 2023, Teng 2023). Als Begriff und Phänomen durchdringt Vertrauen zwischenmenschliche Beziehungen, angefangen von der (Vertrauens-)Beziehung zu uns selbst, über Vertrauen in Freundschaften, Gemeinschaften und Familien, in alltäglichen Interaktionen und spontanen Begegnungen bis hin zu einer Relevanz für Gesellschaften. Fast *selbstverständlich* wenden wir „Vertrauen“ auf verschiedenartige Phänomene an.

Dabei ergibt sich die Schwierigkeit, Vertrauen zu konzeptualisieren, auch aufgrund eines zwiespältigen Ursprungs (Simon 2020, 1–2): Vertrauen wird nicht allein als Chance begriffen, sondern mit Gefahren verbunden – darin überschneiden sich ansonsten gegensätzliche Vertrauensverständnisse, wenn sie diese Gefahren auch unterschiedlich spezifizieren: manchmal enger als Risiko oder, wie in diesem Aufsatz übernommen, als „Moment der Unsicherheit und Unverfügbarkeit“ (Frevert 2013, 33) und als „akzeptierte

Verletzbarkeit“ (Baier 1986, 235). Verletzbarkeit macht auch verständlich, warum Hartmann (2022, 94) Vertrauen nicht einfach als „weiches Phänomen“ versteht. Er nimmt Bezug auf Probleme, wie Ungleichheit in der Ehe, die dazu geführt hat, dass sich überhaupt mit Vertrauen in feministischer Philosophie beschäftigt wurde (Baier 1986, Baier 2001).

Auch weil Vertrauen allgegenwärtig erscheint, und um der Komplexität von Vertrauen gerecht zu werden, schlägt Simon (2020, 2) vor, Vertrauen innerhalb konkreter Vertrauensbeziehungen kontextbedingt zu verstehen und vielschichtige Perspektiven zuzulassen. Dabei fällt auf: Oft führt die Analyse unterschiedlicher Vertrauensverhältnisse, etwa in Bezug auf digitale Technologien, wiederum zum Paradigma zwischenmenschlicher Beziehungen zurück oder zumindest nicht daran vorbei (McLeod 2020, Butler 2021, Hartmann 2022); ein Paradigma, das Vertrauen und Vertrauenswürdigkeit insbesondere in Abgrenzung zu Sich-verlassen-auf und Verlässlichkeit bestimmt.

3.1 Vertrauen und Verletzbarkeit

Die Bedeutung von Vertrauen wird in diesem Beitrag im *Dazwischen* verortet, das heißt, die Beteiligten müssen eine Haltung zueinander haben, die Vertrauen ermöglicht (McLeod 2020). Vertrauen wird sich angenähert als eine *Einstellung* gegenüber Personen, oder Entitäten, von denen wir hoffen, dass sie vertrauenswürdig sind (ebd.); oder, von denen wir – über das Hoffen hinaus – aus normativen Gründen erwarten, dass sie vertrauenswürdig sind. Vertrauen wird von Hartmann (2022, 103) als eine praktische „Einstellung zum anderen“ bezeichnet, und zwar eine Einstellung, die mit Erfahrung, Reflektion und geteilten Gründen korrespondiert und deren Kontext sie letztlich sinnvoll und nachvollziehbar macht (Hartmann 2022, 125 f.). Vertrauenswürdigkeit versteht McLeod (ebd.) als eine *Eigenschaft*, die im besten Falle zu Vertrauen führt, mangelnde Vertrauenswürdigkeit respektive zu Misstrauen.

Vertrauen, so die Annahme bei McLeod (ebd.), ermöglicht, sich ganz oder partiell mindestens auf andere zu *verlassen*, in dem Wissen, dass keine äußere Macht Vertrauen oder Vertrauenswürdigkeit erzwingen kann – gäbe es Garantie, müssten wir nicht vertrauen. Vertrauen ist relevant, „bevor man die Handlungen anderer nachverfolgen kann“ (Dasgupta 1988, 51, eigene Übersetzung), wenn es „in gewisser Weise schon zu spät ist“ (Hartmann 2011: 16) oder das Nachverfolgen auch einfach nicht gewollt ist wie beispielsweise in Freundschaften. Auch wenn bestimmte Gründe für Vertrauen vor-

ab bestehen, braucht es den Vertrauensvollzug, der die guten und anderen Gründe vervollständigt (ebd.).

Insbesondere Baier (1986) geht es bei Vertrauen nicht allein um die Einstellung im Sinne eines Daran-glaubens, dass die Vertrauensempfänger:innen das tun werden, was wir ihnen zu- oder anvertrauen. Vertrauen umfasst auch mehr als die bloße Erwartung, dass viele Dinge in unserer Umgebung regelmäßig geschehen, und dass diese Erwartung enttäuscht werden kann. Mit Baier (ebd.) betonen auch Jones (2004) und Hartmann (2022) Verletzbarkeit in Vertrauensbeziehungen. Sie verstehen diese als eine *akzeptierte Verletzbarkeit,* die nicht vermieden werden kann, um Vertrauen selbst und das, was uns wichtig ist, realisieren zu können. Mit Verletzbarkeit ist nicht gemeint, dass wir etwa einen Mangel an Wohlwollen uns gegenüber erwarten (Baier 1986, 235) oder dass wir verletzt werden wollen (Hartmann 2022, 92). Wir sind aber bereit, bestimmten anderen *Möglichkeiten* (Hunziker 2010, 187) offen zu lassen und nehmen eine begrenzte Kontrollierbarkeit beim Vertrauen in Kauf (Hartmann 2022).

3.2 Vertrauen und normative Erwartungen

Wenn wir vertrauen, *verlassen* wir uns darauf, dass andere kompetent und auch bereit sind, das für uns zu tun, was wir von ihnen erwarten (McLeod 2020). Vertrauen wird in diesem Beitrag zudem als normative Haltung betrachtet, die der anderen Entität entgegengebracht wird (Walker 2006, Jones 2004): dass man ihr auf eine (für sie) normativ verständliche Weise vertraut. Die Grundlage eines umfänglichen Konzepts normativer Erwartungen (Jones 2004) geht über Erwartungen hinaus, die sich vorrangig auf Vorhersehbares und damit auf vergangene Beobachtungen und Erfahrungen beziehen. Auch normative Erwartungen haben dabei die Konsequenz zwischen Vertrauen und Sich-verlassen-auf zu unterscheiden (Walker 2006, Jones 2004). Insbesondere Sich-zu-verlassen wird im Zusammenhang mit (digitalen) Technologien diskutiert (Pettit 2004), unter anderem als *Handlungsweise*, die Nickel (2013) nach einer Entsprechung zur *Einstellung* des Vertrauens fragen lässt.

Es macht einen konzeptionellen Unterschied, ob Vertrauen mit normativen Erwartungen in bestimmten Kontexten und Beziehungen verbunden wird. Beruht Vertrauen auf normativen Erwartungen und wird gebrochen, führt dies eher zu Verletzungen und Wut (Baier 1991) als zu Enttäuschungen über bloße Unzuverlässigkeit. Vertrauen auf Basis normativer Erwartungen geht darüber hinaus, dass etwas vorhersehbar sein soll und

dass wir uns verlassen wollen, zum Beispiel auf ein Funktionieren. Wenn es bei normativen Erwartungen verständliche Gründe für Vertrauen gibt, wird eine Reaktion auf die Gründe erwartet, beziehungsweise es wird erwartet, dass (auch) die Gründe dazu beitragen, dass auf Vertrauen angemessen reagiert wird (McLeod 2020).

Zu Vertrauenswürdigkeit ist im Unterschied zu Verlässlichkeit anzunehmen, dass wir andere mit Vertrauen auf Basis normativer Erwartungen einer Belastung aussetzen (ebd.), wenn sie etwa Vertrauen trotz normativer Konflikte erfüllen oder wenn sie es (berechtigt) verletzen müssen. Unangemessenes Vertrauen kann Erwartungen auf der vertrauensempfangenden Seite verletzen. An die unterschiedlichen normativen Erwartungen der Bitcoin-Communities auch gegenüber den Core-Maintainern ist hier etwa zu denken. Doch was kann Vertrauenswürdigkeit ausmachen in ungewissen Situationen? Auf alle Fälle kann der Versuch, die Verletzbarkeit durch Überlegungen gänzlich auszuräumen, Vertrauen, und das, was durch Vertrauen ermöglicht wird, gerade gefährlich werden (ebd.). Die eigene Haltung kann auf ein bloßes Sich-Verlassen-Wollen zurückfallen, sich also mehr auf das Erwarten und verlässliche Erfüllen einer Rolle oder Funktion beschränken.

Vertrauen ist, wie in diesem Aufsatz angenommen, relevant in sozialen Interaktionen, in denen Erwartungen über Vorhersagen und die Erfüllung von Vorgaben oder Verträgen hinausgehen. Geht es primär darum, vorzugeben, was andere Entitäten zu tun haben, und sie erfüllen diese Vorgabe, zeigt das vor allem, dass sie *verlässlich* Vorgaben erfüllen können, nicht zwangsweise, dass sie vertrauenswürdig sind, d. h. Vertrauen auf die ein oder andere Weise erfüllen. Wie würden sie sich den Vertrauenden gegenüber verhalten, wenn konkrete Vorgaben oder Sanktionsmöglichkeiten fehlen?[11] Geht es primär um Vorhersagen, kann es passieren, dass es letztlich um das *Zutreffen* von Erwartungen geht (Hunziker 2010, 188–189). Auch ein bestimmtes rationales Akteur:innenverständnis ist mit Vorhersagen verbunden (siehe Abschnitt 4.1). Gerade aber die vielfältigen normativen Ansprüche an andere, die mit ihnen verbundenen Formen der Verletzbarkeit und die Annahme, dass Vorhersagen und Vorgaben nicht immer gewollt sind oder mit ihnen etwas anderes verloren ginge, sind jedoch Aspekte, die in diesem Beitrag als entscheidend für Vertrauensanalysen angesehen werden.

11 Wenn wir kaum Erfahrung darüber haben, ob und wie eine Entität derartige Aufträge erfüllt, könnten wir noch davon sprechen, dass wir ihr vertrauen.

4 Blockchain-Technologie und zwischenmenschliches Vertrauensparadigma

Obwohl die Perspektive zur Eigenschaft der Vertrauenswürdigkeit in diesem Beitrag bisher offengehalten und bewusst von Vertrauen in andere „Entitäten" gesprochen wurde, wurde und wird das zwischenmenschliche Vertrauensparadigma (McLeod 2020) nicht verlassen: Einerseits, weil Verletzbarkeit im zwischenmenschlichen Paradigma zentral ist und sich damit die Unterscheidung zwischen Vertrauen und Sich-verlassen-auf erklären lässt, die für Technologiebetrachtungen als relevant angesehen wird. Mit dem zwischenmenschlichen Paradigma im Hintergrund wird im Blockchain-Kontext ein Vertrauensverständnis angewandt, das über Vorhersage und Risikoabschätzungen, also über Sich-verlassen, hinausgeht. Es wird ein Vertrauen zugrunde gelegt, bei dem es nicht nur darauf ankommt, dass Erwartungen zutreffen, sondern auch betrachtet, inwiefern normative Erwartungen eine Rolle spielen. Es wird für Vertrauen mehr vorausgesetzt als funktionierende Blockchain-Spezifikationen oder -Operationalisierungen, die sich für Vorhersagen eignen. Andererseits wird das zwischenmenschliche Paradigma zugrunde gelegt, weil der Bitcoin-Kontext nicht ohne zwischenmenschliche Interaktionen verstanden wird. Bitcoin vermittelt diese Interaktionen nicht ausschließlich, so als könne Bitcoin als isoliertes, „freistehendes Vertrauensobjekt" (Nickel 2013, 225) betrachtet werden. Zwischenmenschliche Interaktionen finden statt, wenn wir etwa an die aufwendigen Beiträge von Bitcoin-Developern denken, an die „Prosa und Poesie, die von Bitcoin-Usern produziert werden" (Maurer et al. 2013, 262f., eigene Übersetzung). Wie auch McLeod (2020) annimmt, wird in diesem Beitrag davon ausgegangen, dass Vertrauen in soziotechnischen Kontexten (wie Blockchain) mit zwischenmenschlichem Vertrauen gewisse Merkmale teilt, das heißt, dass für gewisse Bitcoin-Akteur:innen und -Zusammenhänge zwischenmenschliches Vertrauen relevant bleibt.

4.1 Sich auf Bitcoin verlassen und zweifeln können

Unproblematisch kann von Vertrauen in Bitcoin-Kode oder -Kryptographie gesprochen werden, vergleichbar mit Vertrauen in Maschinen oder allgemeiner in Artefakte, wenn Verlässlichkeit als hinreichende Bedingung für Vertrauen angenommen wird; wenn Vertrauen grundsätzlich mit Sich-verlassen-auf gleichgesetzt wird (vgl. Simon 2013). Sich-verlassen bedeutet ein Handeln, unter der Annahme, dass Bitcoin funktioniert (und das tut Bitcoin bisher). Bestimmtes Handeln der Bitcoin-Akteur:innen impliziert ihr

Verlassen auf Bitcoin (vgl. Goldberg 2020). Sich-verlassen setzt dabei nicht voraus, dass eine hundertprozentige epistemische Gewissheit besteht (Coeckelbergh 2012).

Sich-verlassen und Zuverlässigkeit wurden in Abschnitt 3.2 bereits mit Vorhersageerwartungen (Jones 2004) in Verbindung gebracht. Erwartungen, die sich auf Vorhersagen beziehen, sind dabei für Akteur:innen wichtig, die als rational verstanden werden, häufig im Sinne von risikominimierend. Bekannte Vertrauensansätze gehen von rationalen Akteur:innen und Risikoabwägungen aus. Sie sind als Rational-Choice- oder Cognitive-Trust-Ansätze bekannt (Gambetta 1988). In diesen Ansätzen ist für Zuverlässigkeit hinreichend, dass Vorhersageerwartungen möglichst zutreffen; in den Hintergrund können die Gründe dafür geraten.

Die Tatsache, dass beteiligte Akteur:innen sich auf Bitcoin verlassen, muss ihnen nicht zwangsläufig bewusst sein; ebenso muss sich die Entität, auf die sich verlassen wird, des Verlassens nicht bewusst sein, so entspricht es Goldbergs (2020, 97f.) Verständnis von Sich-verlassen-auf. Goldberg definiert Verlass als eine „Annahme oder Vermutung, auf deren Basis man bereit ist, zu handeln“ (2020, 97, eigene Übersetzung). Sofern Akteur:innen nicht gezwungen werden, sich zu verlassen, und sie auch Alternativen hätten, resultiert ihr Sich-verlassen, dass also angenommen wird, dass Bitcoin morgen noch funktioniert, hinreichend aus ihrer Handlung (ebd.): aus dem Mining, Investieren, Handeln oder Programmieren.

Von Sich-auf-etwas-verlassen wird auch in der Kryptographie gesprochen, die sich mit der Verschlüsselung oder dem Verbergen befasst. Verschlüsselung zielt auf die Sicherheit von Daten; dass sich Bitcoin-User unter anderem auf Anonymität verlassen können. Dabei schließt Sich-verlassen-auf einen bestimmten Zweifel nicht aus (Goldberg 2020, 97f.), der nicht gleichbedeutend ist mit Verletzbarkeit in Vertrauensbeziehungen; eine Unterscheidung, die nachfolgend wieder aufgegriffen wird. Grenzen der Sicherheit und konkrete Zweifel an kryptographischen Funktionen gehen in Vorhersageerwartungen ein. Zweifel sind im Bitcoin-Kontext nicht unwahrscheinlich und auch bekannt. Nehmen wir kryptografische Schlüssel oder den „Private Key“, dessen Besitz den Zugriff und damit die Kontrolle über das Bitcoin-Guthaben sichert und fester Bestandteil von Bitcoin ist, um Benutzer:innen vor Diebstahl ihrer Coins zu schützen. Die Verschlüsselung basiert auf kryptografischen Funktionen. Mit Unterstützung der kryptografischen Wissenschaft und ihrer Verfahren wird kritisch geprüft und prognostiziert, wie wahrscheinlich es ist, dass Hintertüren in diese Funktionen

eingebaut wurden (Kroll et al. 2013), die Diebstahl zum Beispiel doch ermöglichen könnten. Die Bitcoin-Community, zumindest ein Teil der Mitglieder, verlässt sich nicht darauf, dass Hintertüren nicht vorhanden sind, wenn sie versuchen, das Risiko zu minimieren und sich auf das Auffinden von Fehlern konzentrieren. So wurden auch nach Veröffentlichung des Bitcoin-Whitepapers zahlreiche Fehler des Bitcoin-Protokolls identifiziert und durch Softwareupdates behoben.

Geht es um Vorhersageerwartungen, kommen oft andere Handlungsoptionen ins Spiel. Optionen werden relevant, wenn etwa Bitcoin-Akteur:innen wie beispielswiese mächtige kommerzielle Mining-Organisationen auf individuellen Output abzielen: auf neu geprägte bitcoins als Blockbelohnung, die Bitcoin-Miner erhalten, wenn sie erfolgreich einen neuen Block zur Blockchain hinzufügen. In diesen Fällen ist die Entität, auf die sich verlassen wird, in ihrem Mittel zur „rationalen" Optimierung – dass sich zum Beispiel der Einsatz von Rechenleistung möglichst noch mehr auszahlt – austauschbar. Es gibt keine Gründe, bei risikoärmeren Investitionsmöglichkeiten, auch von Rechenkapazitäten, oder bei vielversprechenderen (spekulativen) Investitionsobjekten nicht zu wechseln.

Auch die Bitcoin-Anwendung selbst hat Payoff-Strukturen zentral integriert, die kritisiert werden. Nach De Filippi (2017, 84–88) ist Bitcoin-Dezentralität nicht hinreichend für Zusammenarbeit und „kollaborative Ökonomie" nach Botsman und Rogers (2010). Auf der einen Seite wird die gemeinsame Bereitstellung von Rechenkapazitäten für das Netzwerk vorausgesetzt (De Filippi 2017, 86). Auf der anderen Seite sind die spieltheoretischen Annahmen des Bitcoin-Protokolls, die den eingebauten Wettbewerbsmechanismus beim Hinzufügen neuer Blocks erklären (ebd.) – dass dabei eher nicht kooperiert wird –, für die Verwendung in einem gemeinschaftlichen Kontext nicht ausgelegt (Kroll et al. 2013). Nur diejenige Akteur:in, die als erste die Lösung der mit dem Block verknüpften Rechenaufgabe findet, erhält eine Belohnung. Mit anderen Worten kann es sich für Einzelne lohnen, die Entscheidung über den eigenen Beitrag (im Mining) auf den *einen* Gesichtspunkt des individuellen Payoffs und damit eine Vorhersageerwartung zu reduzieren (De Filippi 2017, 87). Das Interesse besteht dann an einer verlässlichen Vorhersage. Wie De Filippi (2017) schreibt, kann unter Reduktion auf Payoff-Gesichtspunkte der eigene Beitrag ohne größere Sorgen aus dem Gemeinschaftsprojekt zurückgezogen werden, was die Organisation als Ganzes gefährdet.

Werden die Rechenkapazitäten nicht länger in Bitcoin investiert, kann das ein Zeichen sein, dass sich nicht mehr verlassen wird. Aufgrund

der Möglichkeit des Zweifels im Sich-verlassen-auf und der Möglichkeit unterschiedlicher Erwartungen ist zu empfehlen, die (Un-)Zuverlässigkeit von Bitcoin, etwa von bestimmten Sicherheitselementen, als eigenständiges Thema zu behandeln und kritisch zu begleiten, anstatt von Vertrauenslosigkeit zu sprechen. Doch geht es Bitcoin-Akteur:innen nicht ausschließlich darum, sich zu verlassen oder sich nicht zu verlassen, so die Annahme in Abschnitt 4.2. Auch wenn Bitcoin auf Basis der Kryptographie eine gewisse Sicherheit versprechen kann, ist unter anderem Folgendes zu diskutieren. Ist ein grundlegendes Vertrauen erforderlich, in das, woraus die Sicherheit erwächst? Wenn Sicherheit etwa auch aus gemeinschaftlichen Praktiken, wie der Überprüfung von Hintertüren, hervorgeht? *Sicherheit durch Kryptographie statt Vertrauen* könnte gewisse Bitcoin-Grundlagen verdecken, etwa bestimmte Normen der Zusammenarbeit in Open-Source-Communities und des uneingeschränkten Zugangs zum Netzwerk („permissionless" Bitcoin).

4.2 Bitcoin und Vertrauen: Verletzbarkeit

Vertrauen geht weiter als Sich-verlassen-auf (Hawley 2014, Walker 2006), insbesondere in Verbindung mit normativen Erwartungen, die für Jones (2004) Bestandteil eines Erwartungskonzeptes sind, das über Vorhersagen oder Prognosen hinausgeht. Mit normativen Erwartungen (Jones 2004, Baier 1986) lassen sich insbesondere Erwartungen hervorheben, die im konkreten Austausch zwischen Personen entstehen: aus den Erfahrungen und Einsichten dieses Austausches, in dem die Möglichkeit spontaner Momente besteht, in dem sich gegenseitige Ermessenspielräume eingeräumt werden. Akzeptierte Verletzbarkeit (Baier 1986) ergibt sich konkret aus der Beziehung zu der Entität, auf die sich das Vertrauen bezieht (oder Verletzbarkeit wird im Falle von Misstrauen nicht akzeptiert).

Nehmen wir etwa an, dass für die Beteiligung im Bitcoin-Netzwerk, die von Nakamoto (2008) proklamierten Werte und Normen der Dezentralität[12] oder der „permissionless Blockchain"[13] für persönliche Erwartungen eine Rolle spielen, auch für die Erwartung, dass andere Bitcoin Akteur:innen sie teilen. Dann sind es auch gute Gründe, die sie (als Personen) über

12 Wobei zu klären ist, was mit Dezentralität erreicht werden soll. Dazu unter anderem „dezentrale Governance-Struktur", also Dezentralisierung auf Ebene der *Governance*, s. De Filippi (2017, 61).

13 Als öffentliche, „permissionless" Blockchain steht die Teilnahme am Bitcoin-Netzwerk prinzipiell für alle offen.

Normen der Dezentralisierung oder die „Erlaubnislosigkeit“ vertrauen lassen. Personen müssen sich in dem Maße als verletzbar akzeptieren, indem ihre sozialen Normen auch von konkreten Personen(gruppen) verraten werden können. Mit geteilten Werten sind soziale Beziehungen verbunden, die zwischen Bitcoin Entwickler:innen oder Core Maintainern entstehen können, in denen sich vertraut wird. Bei Betrug kann es dazu kommen, dass nicht Vertrauen allein, sondern auch die soziale Beziehung in und zur Community, in der sich die Personen sehen, geschädigt wird (vgl. Coeckelbergh 2012, 54) – und sie auch in dieser Hinsicht verletzbar sind. Aus phänomenologisch-sozialer Sicht, wie Coeckelbergh (2012) sie im Zusammenhang mit Technologien vertritt, haben wir nicht nur eine begrenzte individuelle Kontrolle über Vertrauen, das zu sozialen Beziehungen gehört, sondern über die soziale Beziehung selbst.

Es ist anzunehmen, dass die Möglichkeit der Verletzung insbesondere dann eine Rolle spielt, wenn sich Erwartungen auf konkrete Expert:innen und auf die Normen und Werte beziehen, die ihrem Handeln zugrunde liegen (sollten). Anders gewendet, als vertrauenswürdig können sich zum Beispiel Entwickler:innen als Personen und Gruppe mit der gemeinsamen Überprüfung und Verbesserung von Bitcoin-Programmkode erweisen, indem sie Fehler finden. Ebenso kann Vertrauen in und unter den Bitcoin Core Maintainern eine Rolle spielen, die letztlich die Entscheidungsbefugnis über eingehende Pull-Requests tragen, bei denen es darum geht, Programmkode mit Erläuterung der Gründe hinzuzufügen oder zu verändern. Wird angenommen, dass sich wie im Falle von Ärzt:innen Vertrauen auf Professionen oder Institutionen ausdehnen kann (Jones 2004) und sich Entwickler:innen und Maintainer als vertrauenswürdig erweisen, kann auch im Falle von Bitcoin angenommen werden, dass ein gewisses Vertrauen besteht, das zusammenhängt mit informellen Normen der Open-Source-Community (mit dem Bitcoin-Whitepaper).

Gehen wir von Vertrauen in (Programmkode-)Entwickler:innen und ihre Profession aus, sind nach wie vor konkrete Personen und Gemeinschaften, die Normen befolgen, oder sich entscheiden, diese nicht zu befolgen, involviert. Vertrauen in eine künstliche Entität – in die computergenerierte Blockchain –, dass diese statt den entscheidenden Personen(gruppen) Vertrauen einlädt und verändern kann, ist von dem, was in diesem Aufsatz unter Vertrauen verstanden wird, jedoch zu trennen. Vertrauen wie hier analysiert gewinnt seine Stärke durch den Bezug auf Personen und konkrete Erfahrungen, wenn auch in anonymerer Form. In einem Vertrauensverhältnis wie hier

verstanden beziehen sich die Beteiligten aufeinander, es besteht eine normative Haltung gegenüber einer anderen Entität, von der erwartet wird, dass sie auf die Haltung eingeht.

5 Fazit

Mit akzentuierten Elementen eines interpersonellen Vertrauensparadigmas – Verletzbarkeiten im menschlichen, sozialen Miteinander verbunden mit normativer Erwartung – wurde gezeigt, welche Überlegungen sich zur Bedeutung der Blockchain-Technologie für Vertrauen und Sich-verlassen-auf, speziell in Bezug auf die Bitcoin-Anwendung, anstellen lassen. Blockchain-Technologie sollte ohne genauere Kontextualisierung nicht als vertrauenswürdig oder „vertrauenslos" betrachtet werden. Vertrauen in unterschiedliche Technologien, beziehungsweise in unterschiedlichen technologischen Kontexten, variiert. Auch ist es nicht nachvollziehbar, was Vertrauenslosigkeit bei Nakamoto (2008) meint; ob sie sich in erster Linie auf einen bestimmten Bereich oder bestimmte Akteur:innen beschränkt, wie zum Beispiel auf diejenigen, die mit Bitcoin Zahlungen ausführen. Dennoch kann Vertrauen relevant sein für Bitcoin-Akteur:innen und über ein Sich-verlassen-auf hinausgehen. Es ist nicht auszuschließen, dass gewisse Praktiken, die zum Entstehen und Verbleib von Bitcoin beitrugen, auf Vertrauensbeziehungen und -normen (der Open-Source-Community) gründeten und die Verlässlichkeit von Bitcoin-Operationen auch mit ihnen zu tun hat.

In diesem Beitrag habe ich argumentiert, dass Vertrauen gewisser Akteur:innen im Bitcoin-Kontext weder von zwischenmenschlichem Vertrauen gänzlich entkoppelt ist, noch von Vertrauen in Professionen oder Institutionen. Es finden immer noch konkrete Interaktionen unter und mit Entwickler:innen statt, die den Bitcoin-Programmkode pflegen, auf Basis geteilter normativer Erwartungen. Insbesondere die Beziehungen von Entwickler:innen zur Gruppe der Core Maintainer und die Beziehungen zwischen letzteren sind für praktisches Vertrauen relevant. Wir können annehmen, dass Entwickler:innen mit ihren freiwilligen Beiträgen zur Kodepflege einen gewissen Vertrauensvorschuss geben. Für sie steht etwas auf dem Spiel, wenn sie erwarten, dass ihre Beiträge langfristig eine bestimmte Akzeptanz oder Anerkennung durch andere und letztlich durch die Gruppe der Core Maintainer finden – vielleicht in einer Kombination aus Sich-Verlassen-auf und Vertrauen, die genauer zu analysieren wäre.

Die Blockchain nimmt den Verantwortlichen der sozialen Welt die Vertrauenslast längst nicht aus der Hand. Auch ein Sich-verlassen-auf ist relevant und kann auf verschiedene Weise mit Vertrauen in Verbindung gebracht werden. So verstehe ich auch Butlers (2021) Schlussfolgerung, der die Vertrauenslast noch immer im Sozialen verortet, indem er unter anderem auf die menschlichen Akteur:innen und ihre Institutionen verweist, auf die wir uns spätestens dann beziehen (wollen), wenn Probleme mit Bitcoin auftauchen.

Vertrauen ist nicht ohne eine gewisse Erfahrung zu haben und beinhaltet ein kritisches Prüfen, wie es etwa von Expert:innen der Kryptographie geleistet wird. Zum kritischen Prüfen gehört allerdings nicht allein eine technische Prüfung von Sicherheitsaspekten. Dazu gehört auch ein Interesse dafür, was digitale Technologien wie die Blockchain und ihre Anwendungen für unser Aufeinanderbezogensein und für unsere gegenseitige Abhängigkeit bedeuten. Wie – auch mit welchen Gründen – können wir über den Einsatz der Blockchain in Verbindung kommen und wie wollen wir es nur bedingt oder gar nicht? Sich auf „etwas" und unbestimmte andere verlassen zu können ist dabei nicht wenig. Gewisse Elemente sind aus Sicht eines praktischen Vertrauens vielversprechende normative Potenziale der Blockchain. Beispiele sind der *permissionless* und dezentrale Charakter des Bitcoin-Projektes, die sich für künftiges Ausprobieren und Erfahrungen in verschiedenen Bereichen lohnen. Im Falle von Bitcoin wird die Kritik immer lauter, dass das Fortbestehen des Systems von nur wenigen einflussreichen Playern abhängt und Bitcoin für illegale oder illegitime Zwecke verwendet wird. Dennoch haben die Beteiligten trotz und mit den bestehenden Abhängigkeitsverhältnissen einen gewissen Spielraum zur Verfügung, um zuverlässig zu handeln, und, weil gewisse Normen auf dem Spiel stehen und sich mit Technologien verschieben können, auch Vertrauenswürdigkeit zu demonstrieren.

Danksagung

Mein herzlicher Dank gilt der Gastherausgeberin Karoline Reinhardt und Johanna Sinn für ihre besondere Aufmerksamkeit sowie den beiden anonymen Gutachter:innen für ihre konstruktiven Kommentare, die mich über diesen Aufsatz hinaus beschäftigen werden. Auch wohlwollend-prüfende Gespräche mit Roger Wattenhofer (ETH Zürich) und Stefan Münker (Humboldt-Universität Berlin) begleiteten diesen Aufsatz. Nicht zuletzt bin ich dankbar, dass der Grundlagenforschungsfonds (GFF) der Universität St.Gal-

len diese Forschung zu Vertrauensfragen im Zusammenhang mit Technologien unterstützt.

Literatur

Aste, Tomaso, Paolo Tasca und Tiziana Di Matteo. 2017. „Blockchain Technologies: The Foreseeable Impact on Society and Industry". *Computer* 50 (9): 18–28. https://doi.org/10.1109/MC.2017.3571064.

Baier, Annette. 1986. „Trust and Antitrust". *Ethics* 96 (2): 231–260. https://doi.org/10.1086/292745.

Baier, Annette. 1991. „Trust". In *Tanner Lectures on Human Values* (Volume 13): 109–174. Salt Lake City: University of Utah Press.

Baier, Annette. 2001. „Vertrauen und seine Grenzen". In *Vertrauen. Die Grundlage des Sozialen Zusammenhalts*, herausgegeben von Martin Hartmann, 37–84. Frankfurt: Campus Verlag.

Botsman, Rachel, und Roo Rogers. 2010. *What's Mine Is Yours: The Rise of Collaboration Consumption*. New York: HarperCollins.

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2019. „Blockchain sicher gestalten: Konzepte, Anforderungen, Bewertungen". Zugriff am 15. Januar 2024. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.html.

Burr, Christopher, Jessica Morley, Mariarosaria Taddeo und Luciano Floridi. 2020. „Digital Psychiatry: Ethical Risks and Opportunities for Public Health and Well-Being". *IEEE Transactions on Technology and Society* 1 (1): 21–33. https://10.1109/TTS.2020.2977059.

Butler, Aaron. 2021. „Preliminary Reflections on the Ontological Significance of Blockchain Technology for Trust and Trustworthiness". In *Digitalisierung Aus Theologischer Und Ethischer Perspektive: Konzeptionen – Anfragen – Impulse*, herausgegeben von Gotlind Ulshöfer, Peter Kirchschläger und Markus Huppenbauer, 211–225. Zürich, Baden-Baden: Nomos.

Casino, Fran, Thomas K. Dasaklis und Constantinos Patsakis. 2019. „A systematic literature review of blockchain-based applications: Current status, classification and open issues". *Telematics Informatics 36: 55*–81. https://doi.org/10.1016/j.tele.2018.11.006.

Christopher, Catherine Martin. 2016. „The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking Bitcoin and the Blockchain". *Nevada Law Journal* 17 (1): 139–180. https://paperity.org/p/83729488.

Coeckelbergh, Mark. 2012. „Can We Trust Robots?" Ethics and Information Technology 31: 9–14. https://doi.org/10.1007/s10676-011-9279-1.

Coeckelbergh, Mark, und Wessel Reijers. 2016. „Cryptocurrencies As Narrative Technologies“. *Acm Sigcas Computers and Society* 45 (3): 172–178. https://doi.org/10.1145/2874239.2874264.

Dasgupta, Partha. 1988. „Trust as a Commodity“. In *Trust: Making and Breaking Cooperative Relations, herausgegeben von Diego Gambetta,* 49–72. New York: Basil Blackwell.

Davidson, Sinclair, Primavera De Filippi und Jason Potts. 2018. „Blockchains and the Economic Institutions of Capitalism“. *Journal of Institutional Economics* 14 (4): 639–658. https://doi.org/10.1017/S1744137417000200.

De Filippi, Primavera. 2017. „‚In Blockchain We Trust‘: Vertrauenslose Technologie für einevertrauenslose Gesellschaft“. In *Reclaim Autonomy. Selbstermächtigung in der digitalen Weltordnung*, herausgegeben von Jakob Augstein, 53–81. Berlin: Suhrkamp.

DuPont, Quinn. 2014. „The Politics of Cryptography: Bitcoin and The Ordering Machines“. *Journal of Peer Production* 1 (4): 1–10.

Frevert, Ute. 2013. *Vertrauensfragen. Eine Obsession Der Moderne*. München: Beck.

Gambetta, Diego. 1988. „Can We Trust Trust?“ In *Trust: Making and Breaking Cooperative Relations,* herausgegeben von Diego Gambetta, 213–237. New York: Basil Blackwell.

Glaser, Florian. 2017. „Pervasive Decentralisation of Digital Infrastructures a Framework for Blockchain Enabled System and Use Case Analysis“. *Proceedings of the 50th Hawaii International Conference on System Sciences:* 1543–1552. Zugriff am 15. Januar 2024. http://scholarspace.manoa.hawaii.edu/handle/10125/41339.

Goldberg, Sanford C. 2020. „Trust and Reliance“. In *The Routledge Handbook of Trust and Philosophy*, herausgegeben von Judith Simon, 97–108. New York, NY: Routledge.

Hartmann, Martin. 2011. *Die Praxis des Vertrauens*. Berlin: Suhrkamp.

Hartmann, Martin. 2022. *Vertrauen – Die unsichtbare Macht*. Frankfurt am Main: Fischer.

Hawley, Katherine. 2014. „Trust, Distrust and Commitment“. *Noûs* 48 (1): 1–20. doi:10.1111/nous.12000.

Hunziker, Andreas. 2010. „Vertrauen Verstehen – nach Wittgenstein“. *Hermeneutische Blätter 16: 179–203*.

Ihde, Don. 2009. Postphenomenology and Technoscience: The Peking University Lectures. Albany: State University of New York Press.

Introna, Lucas, und Lara Pecis. 2020. „Bitcoin as a mediating technology of organization“. In *The Oxford Handbook of Media, Technology, and Organization Studies*, herausgegeben von Timon Beyes, Robin Holt und Claus Pias, 43–53. Oxford, United Kingdom: Oxford University Press.

Jacobs, Mattis. 2021. „ How Implicit Assumptions on the Nature of Trust Shape the Understanding of the Blockchain Technology“. *Philosophy & Technology* 34: 573–587. https://doi.org/10.1007/s13347-020-00410-x.

Jaeggi, Rahel. 2018. „Ökonomie als soziale Praxis“. *Zeitschrift für Wirtschafts- und Unternehmensethik* 19 (3): 343–361. https://doi.org/10.5771/1439-880X-2018-3-343.

Jones, Karen. 2004. „Trust and Terror“. In *Moral Psychology: Feminist Ethics and Social Theory*, herausgegeben von Peggy Des Autels und Margaret Urban Walker, 3–18. Lanham, MD: Rowman & Littlefield.

Kroll, Joshua A., Ian C. Davey und Edward W. Felten. 2013. „The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries“. *Proceedings of WEIS*: 1–21. Zugriff am 15. Januar 2024. https://www.utwente.nl/en/ces/sal/exams/digital-exams/Blockchain-and-Distributed-Ledger-Technology-test/1-Bitcoin/bitcoin-in-the-presence-of-adversaries.pdf.

Maurer, Bill, Taylor C. Nelms und Lana Swartz. 2013. „‚When perhaps the real problem is money itself!‘: the practical materiality of Bitcoin“. *Social Semiotics* 23 (2): 261–277. https://doi.org/10.1080/10350330.2013.777594.

McLeod, Carolyn. 2020. „Trust“. In *The Stanford Encyclopedia of Philosophy* (Fall 2021 Edition), herausgegeben von Edward N. Zalta, https://plato.stanford.edu/archives/fall2021/entries/trust/.

Mühlhoff, Birthe. 2018. „Die Ontologie der Blockchain“. *Philosophie Magazin* Nr. 38, Februar/März. https://www.philomag.de/artikel/die-ontologie-der-blockchain.

Münker, Stefan. 2019. „Freiheit, die in Ketten liegt. Zur Philosophie der Blockchain“. *ZMK Zeitschrift für Medien- und Kulturforschung. Blockchain* 10 (2): 117–126. https://doi.org/10.25969/mediarep/18742.

Nakamoto, Satoshi. 2008. „Bitcoin: A peer-to-peer electronic cash system“. Zugriff am 22. September 2023. https://bitcoin.org/bitcoin.pdf.

Nakamoto, Satoshi. 2009. „Bitcoin open source implementation of P2P currency“. *P2P foundation*. 11. Februar 2009. Zugriff am 22. September 2023. https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

Nickel, Philip J. 2013. „Trust in Technological Systems“. In *Norms in Technology*, herausgegeben von Marc J. De Vries, Sven-Ove Hansson und Anthonie W. M Meijers, 223–237. Dordrecht: Springer. https://doi.org/10.1007/978-94-007-5243-6.

O’Neill, Onora. 2018. „Linking Trust to Trustworthiness“. *International Journal of Philosophical Studies* 26 (2): 293–300. https://doi.org/10.1080/09672559.2018.1454637.

Pettit, Philip. 2004. „Trust Reliance and the Internet“. *Analyse & Kritik* 26: 108–121. https://doi.org/10.1515/auk-2004-0106.

Reijers, Wessel, und Mark Coeckelbergh. 2018. „The Blockchain As a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies“. *Philosophy & Technology* 31: 103–130. https://doi.org/10.1007/s13347-016-0239-x.

Reinhardt, Karoline. 2023. „Trust and Trustworthiness in AI Ethics“. *AI and Ethics* 3: 735–744. https://doi.org/10.1007/s43681-022-00200-5.

Ricoeur, Paul. 1983. *Time and Narrative – Volume 1*. Herausgegeben von Kathleen McLaughlin und David Pellauer. Chicago: The University of Chicago Press.

Roio, Denis. 2013. „Bitcoin, the End of the Taboo on Money“. *Dyne.org Digital Press*, April 2013: 1–17. Zugriff am 15. Januar 2024. https://files.dyne.org/readers/Bitcoin_end_of_taboo_on_money.pdf.

Simmel, Georg. 1992 [1908]. *Soziologie. Untersuchungen über die Formen der Vergesellschaftung*. Frankfurt am Main: Suhrkamp.

Simon, Judith. 2013. „Trust“. In *Oxford Bibliographies in Philosophy,* herausgegeben von Duncan Pritchard. Oxford University Press. Zugriff am 22. September 2023. https://doi.org/10.1093/OBO/9780195396577-0157.

Simon, Judith. 2020. „Introduction“. In *The Routledge Handbook of Trust and Philosophy*, herausgegeben von Judith Simon, 1–13. New York, NY: Routledge.

Simser, Jeffrey. 2015. „Bitcoin and Modern Alchemy: In Code We Trust“. *Journal of Financial Crime* 22 (2): 156–169. https://doi.org/10.1108/JFC-11-2013-0067.

Swan, Melanie. 2015a. *Blockchain: Blueprint for a new economy*. Beijing: O'Reilly.

Swan, Melanie. 2015b. „Blockchain thinking the brain as a decentralized autonomous corporation“. *IEEE Technology and Society Magazine* 34 (4): 41–52. https://doi.org/10.1109/MTS.2015.2494358.

Swan, Melanie. 2017. „Anticipating the economic benefits of Blockchain“. *Technology Innovation Management Review* 7 (10): 6–13. https://doi.org/10.22215/timreview/1109.

Swan, Melanie, und Primavera De Filippi. 2017. „Toward a philosophy of Blockchain: A symposium: Introduction“. *Metaphilosophy* 48 (5): 603–619. https://doi.org/10.1111/meta.12270.

Tapscott, Don, und Alex Tapscott. 2018. *Blockchain revolution: How the technology behind Bitcoin is changing money, business and the world*. London: Portfolio Penguin.

Teng, Yan. 2023. „What Does It Mean to Trust Blockchain Technology?“ *Metaphilosophy* 54 (1): 145–160. https://doi.org/10.1111/meta.12596.

The Economist. 2015. „The Trust Machine“. 31. Oktober 2015. https://www.economist.com/leaders/2015/10/31/the-trust-machine.

van den Hoven, Jeroen, Johan Pouwelse, Dirk Helbing und Stefan Klauser. 2019. „The Blockchain Age: Awareness, Empowerment and Coordination“. In *Towards Digital Enlightenment,* herausgegeben von Dirk Helbing, 163–166. Cham: Springer.

van Lier, Ben. 2017. „Can Cyber-Physical Systems Reliably Collaborate Within a Blockchain?“ *Metaphilosophy* 48 (5): 698–711. https://doi.org/10.1111/meta.12275.

Velasco, Pablo R. 2017. „Computing ledgers and the political ontology of the Blockchain“. *Metaphilosophy* 48 (5): 712–726. https://doi.org/10.1111/meta.12274.

Voshmgir, Shermin, 2016. *Blockchains, Smart Contracts, und das Dezentrale Web*. Berlin: Technologiestiftung Berlin.

Walker, Margaret Urban. 2006. *Moral Repair: Reconstructing Moral Relations After Wrongdoing*. Cambridge UK: Cambridge University Press.

Werbach, Kevin. 2018. *The Blockchain and the New Architecture of Trust*. Cambridge MA: MIT Press.