Anonyme Datenkommunikation für Online-Plattformen –

Welche Elemente der Blockchain-Technologie lassen sich sinnvoll zur Unterstützung realer Geschäftsprozesse übernehmen?

Michael Merz, PONTON, 03.01.2023

1 Einleitung

Dieses Paper basiert auf Erfahrungen beider Welten –reale Geschäftsprozesse, wie wir sie als IT-Dienstleister seit Jahrzehnten analysieren, modellieren und umsetzen und der Welt der Blockchain-Technologie, bei der seit Jahren versucht wird, ebendiese Geschäftsprozesse neu zu gestalten.

Die „Blockchain“ existiert heute, am 3. Januar 2023, exakt 14 Jahre, und wir befinden uns mal wieder in einem Crypto-Winter – also einer Phase, in der das Vertrauen in die Anwendung der Technologie stark nachgelassen hat. Vielleicht ein guter Zeitpunkt, um zu resümieren, warum dies so ist und was die Welt dennoch vom Prinzip der Blockchain lernen kann.

Ich selbst habe mich über Jahre stark im Bereich Blockchain engagiert und verschiedene Projekte initiiert, die es ermöglichten reale Transaktionen dezentral, anonym, und durch einen Angreifer nicht korrumpierbar durchzuführen. Warum aber haben sich diese Projekte nicht zu einem schillernden Unicorn weiterentwickelt? Warum hat selbst Bitcoin heute Schwierigkeiten im Wettbewerb der Anlageklassen zumindest als Wertaufbewahrungsinstrument zu bestehen – und dies angesichts von Krieg, Krisen und Inflation? Wo ist endlich der erste Blockchain-Use Case, der auch ein Business Case ist?

Unsere Projekte waren durchaus erfolgreiche Use Cases, aber eben keine Business Cases. Am Ende waren es immer wieder die klassischen Plattformen, die das Rennen um die Kunden und branchenübergreifende Geschäftsprozesse gewannen.

Nachfolgend möchte ich daher einige Gedanken teilen, die über das Jahr 2022 aus einem Beratungsprojekt entstanden sind und die einige Monate brauchten, um soweit zu reifen, dass sie ein wenig strukturiert zu Papier gebracht werden können. Dazu werde ich

- kurz die Eigenschaften resümieren, die der Blockchain-Technologie zugeschrieben werden,
- anschließend sollen diesen reale Anforderungen gegenübergestellt werden. Liegt hier evtl. ein unüberwindlicher Graben, der verhindert, Blockchain einzusetzen?
- Anschließend möchte ich Synthesemöglichkeiten aufzeigen: Welche Blockchain-Eigenschaften kann man in die klassische Welt übernehmen und welche nicht?
- Schließlich folgt ein Beispiel, wie eine solche Komposition aus „klassisch“ und „Blockchain“ aussehen kann.

2 Was macht eine Blockchain aus?

Folgende Eigenschaften sind essenziell:

- **Dezentralisierung:** Ein Peer-2-Peer-Protokoll sorgt für Ausfallsicherheit, und bietet Schutz vor Angriffen Dritter bzw. sogar vor Angriffen aus den Reihen der Benutzer und Knotenbetreiber („byzantinische Fehlertoleranz“ bzw. „BFT“). Eine zentrale Kontrolle ist obsolet.
- **Mechanismen zur sicheren Protokollierung** (Hashing, elektronische Signaturen, Konsensprotokoll) sorgt für Immutabilität der Dateninhalte. „Sicher“ bedeutet also auch, dass die Daten nie wieder gelöscht werden können.

Dies waren bereits die zentralen Eigenschaften, mit denen Daten dezentral, sicher und permanent gespeichert werden können. Alle weiteren Eigenschaften sind anwendungsabhängig:

- **Pseudonymität** wie z.B. bei Bitcoin bzw. Ethereum oder **Anonymität** (zCash oder Monero) machen Sinn, um bei Kryptowährungen die Anonymität von Bargeld anzunähern[1].
- Über Daten hinaus kann man auch **Code** in der Blockchain speichern, den Knoten als Teil des Konsensprotokolls ausführen („Smart Contracts“).
- Grundsätzlich ist eine Blockchain **transparent**, d.h., jeder (auch Außenstehende) können den Inhalt des Ledgers lesen. Entsprechend kann man Block-Explorern die Inhalte der gängigen Chains durchforsten. Verschlüsseln von Inhalten ist also keine inhärente Blockchain-Eigenschaft.
- Eine Blockchain kann bzgl. **Zugriff** eingeschränkt sein (konsortiale Blockchains).
- Eine Blockchain kann Anreize bieten, sich am Konsensprotokoll zu beteiligen („**Block Reward**“). Dies gilt vor allem für öffentliche Blockchains im Bereich der Kryptowährungen.

Man könnte jetzt weitere Details hinzufügen, aber für die grobe Argumentationslinie dieses Papers reichen die oben genannten Eigenschaften. Diese erscheinen alle sinnvoll, warum also muss man heute einen Blockchain-Business-Case immer noch mit dem Mikroskop suchen?

Es ist eben nicht alles Gold, was glänzt. Zu jeder der o.g. Eigenschaften lässt sich zeigen, dass sie nicht uneingeschränkt gilt. Hier in Kürze einige Entwicklungen der letzten Jahre:

- **Dezentralisierung:** Auch wenn die Anzahl der Knoten bei Bitcoin und Ethereum immer weiter steigt, so hat sich über die letzten Jahre deren Konzentration der Miner auch immer weiter erhöht: Am 27.12.2022 wurden über 51% aller Blöcke durch zwei Mining Pools erzeugt: Foundry USA und AntPool[2]. Auch bei Ethereum zeichnet sich eine wachsende Konzentration der sog. Stakers ab. Nur diese sind berechtigt, neue Ethereum-Blöcke zu generieren, weil sie einen höheren ETH-Betrag hinterlegt („gestaked“) haben. Insofern finden wir uns tendenziell beim Konsensprotokoll bzgl. der Anzahl an Validatoren dort wieder, wo auch sog. Konsortial-Blockchains liegen. Bei letzteren sind es 4-10 Validatoren. Diese überschaubare Zahl war bei den PoW-Befürwortern vor wenigen Jahren noch als nahezu zentralisiert verschrien.
  Während die „Carrier-Blockchains“ wie Bitcoin, Ethereum etc. immerhin noch dezentralisiert sind, gilt dies keineswegs für die meisten Anbieter von Tokens, die z.B. auf Ethereum aufsetzen: Hier steht und fällt der Wert eines Tokens mit der Glaubwürdigkeit des einen, zentralen Herausgebers. Zu viele Scams und Skandale haben über die letzten Jahre die Glaubwürdigkeit solcher Herausgeber untergraben. Am Ende gilt genau das, was die

[1] Satoshi Nakamotos Paper lautet schließlich „Bitcoin: A Peer-to-Peer Electronic Cash System“
[22] Vgl. https://www.blockchain.com/explorer/charts/pools, die Konzentration lässt sich für den aktuerllen Tag anzeigen.

Blockchain verhindern soll: Teilnehmer sind den de-facto zentralisierten Betreibern von Börsen, ICOs, oder Smart Contracts für das Management von Tokens hilflos ausgeliefert.

- Zur **sicheren Protokollierung in der Blockchain**: Ein Ethereum Archive Node, der die gesamte Blockchain-Historie vorhält, benötigt heutzutage über 13 TB an Plattenplatz[3]. Das ist kein Pappenstiel, zumal die Blockchain jährlich um mehr als 3 TB wächst. 2030 muss ein Knotenbetreiber möglicherweise eine 40-80 TB große Datenbank verwalten. Folglich schrumpft die Zahl derer, die das historische Erbe der Blockchain verwalten, auch hier erleben wir also eine zunehmende Konzentration.
  Was die Verwendung **asymmetrischer Verschlüsselung** betrifft, ist eine Bitcoin-Adresse immer mit exakt einem Paar aus privatem und öffentlichem Schlüssel verbunden. Im praktischen Leben sieht die Welt anders aus: Hier kann man heute einen privaten Schlüssel P1 verwenden, verbunden mit dem öffentlichen Schlüssel Ö1 und später auf P2 und Ö2 wechseln. Bei Bitcoin ist dies mit dem Wechsel der Bitcoin-Adresse verbunden. Dies mag ja noch erträglich sein – man muss dann sein Geld von Adresse 1 auf Adresse 2 übertragen, aber bei Ethereum ist dies nahezu unmöglich: Wenn ein Smart Contract vom Konto K1 auf K2 wechselt, dann müssen alle damit verbundenen Daten bzw. Zustände übertragen werden – ein nicht jedem zumutbarer Aufwand.
- Ein **Smart Contract** ist also mitsamt seiner Logik und seinem Datenbestand fest mit einem Ethereum-Konto verbunden. Sollte einmal ein Update der Software erfolgen, dann ist die Hölle los: Was im normalen Leben zentralisierter Anwendungssysteme mit einem Patch erledigt ist, bedeutet bei Ethereum: Hochladen des neuen Codes, umkopieren der Daten von der früheren Version des Smart Contract auf den neuen und ggf. dabei auch eine Transformation der Daten. Denn bei einer zentralen Internetplattform legt man ja auch hin und wieder neue Datenfelder an oder erzeugt einen neuen Index.
  Heute ist das Deployment regulärer Software bereits eine Wissenschaft für sich: Mit viel Aufwand und Parametrisierung lässt sich Anwendungscode in die Cloud laden, testen, duplizieren, skalieren, verschieben, aktualisieren, analysieren, etc. Dies alles klappt nur in vergleichsweise primitiver Form auf der Blockchain. Folglich sind Blockchain-Anwendungen per se begrenzt und gelangen daher in der Praxis über eine logisch zentralisierte Audit-Trail-Funktion nicht hinaus.
- **Verschlüsseln**. Dies ist wie gesagt eine Nicht-Eigenschaft der Blockchain. Erst auf einer höheren Ebene – also bei den Client-Systemen, die auf die Blockchain zugreifen – werden Daten verschlüsselt, in die Blockchain geschrieben und ggf. von anderen Teilnehmern wieder entschlüsselt. Ob sich als Medium „unten drunter“ eine Blockchain, eine zentrale Datenbank oder ein USB-Stick befindet, ist – funktional betrachtet – egal! Siehe auch das Anwendungsbeispiel weiter unten.

3 Was also bedeutet „Sicherheit“ bei der Blockchain?

Sicherheit meint bei Blockchain etwas ganz anderes als die Sicherheit, die man im Zusammenhang mit der Entwicklung und dem Betrieb von Software benötigt. „Sicherheit“ ist abhängig vom Use-Case:

- Sind es Personen, die sich Geld übertragen wollen? Dann liegt die Sicherheit darin, dass ein übergriffiger Staat ihrer nicht Habhaft werden kann. Wer also aus einem diktatorischen Staat flieht und seines Bargelds nicht beraubt werden will, benutzt Bitcoin. Die Bedroher sind hier Staaten und Banken.

[3] Vgl. https://etherscan.io/chartsync/chainarchive

- Ist es ein Staat, der eine Wahl fälschen will, dann braucht es einen Algorithmus, der diese „trustless“ ermöglicht und einen Speicherort, von dem jederzeit das Wahlergebnis unverfälscht hervorgeholt werden kann. Dies Antwort könnte hier ein „Smart Contract“ sein in Verbindung mit Ethereum oder ähnlichen Blockchain-Umgebungen.
- Ist es aber eine zentrale Plattform im Internet, die einen Geschäftsprozess hosten soll, dann kann der Bösewicht der Betreiber selber sein oder einer vierter, der per Cyber-Attacke Daten stiehlt (oder per Ransomware-Attacke verschlüsselt).

Warum aber gibt es angesichts dieser vielen Bedrohungsszenarien heute immer noch keine Blockchain-Anwendung, die nicht nur technisch, sondern auch wirtschaftlich funktioniert? Vermutlich liegt es daran, dass folgende Aspekte bei der Entwicklung Blockchain-basierter Anwendungen nicht ausreichend gewürdigt werden:

- **Technisch:** Die Entwicklung einer „klassischen“ Online-Plattform ist erheblich einfacher (will heißen kostengünstiger) als die eines Blockchain-basierten Prozesses. Einen Smart Contract kann nicht bzgl. Performanz, Datenvolumen, Wartbarkeit, Rechtemanagement etc. mit einer professionellen Plattform mithalten, die Prozesse für Kunden zentral abwickelt. Man stelle sich ein Flugbuchungssystem auf der Blockchain vor…
- **Soziologisch:** Irgendwie haben wir es gelernt, uns mit vertrauenswürdigen Dritten zu arrangieren. Diese kosten Geld und sie sind durchaus potenzielle Betrüger, aber unterm Strich ist die Wahrscheinlichkeit des Fehlverhaltens in einer zivilisierten Gesellschaft akzeptabel.

Im Folgenden soll nun insbesondere dieser soziologische Aspekt genauer untersucht werden.

4 Vertrauenswürdige Dritte in unserer Gesellschaft

Im Zuge unserer Arbeit bei PONTON haben eine ganze Reihe zentralisierter Plattformen entwickelt und auch eine Reihe von Blockchain-Anwendungen. Die Plattformen sind durchweg Systeme zur Abwicklung von Handelsgeschäften oder auch solche, die von Strom- und Gasnetzbetreibern eingesetzt werden. Kritische Infrastruktur also soweit das Auge reicht! Die zentralisierten existieren seit fast 20 Jahren, die dezentralen haben das PoC-Stadium nicht verlassen. Warum?

Am Ende stehen hinter jeder Geschäftsbeziehung Verträge, die Fehlverhalten sanktionieren. Dies gilt für Softwareunternehmen als Entwickler bzw. Betreiber, es gilt für unsere Kunden, die Abrechnungssysteme für Dritte betreiben, es gilt aber auch für Zulieferer und alle sonstigen Dritten bis Dreißigsten: Banken, Notare, Versicherungen, KfZ-Leasinggesellschaften, Reisebuchungssysteme, Behörden, den Staat im Allgemeinen etc.

Jeder kann als einseitiger Verwahrer von Daten, als Erbringer einer Dienstleistung, als Vertrauensträger versagen oder betrügen. Und dennoch funktioniert unsere Gesellschaft einigermaßen gut. Jedenfalls so gut, dass nur in seltenen Fällen auftretendes Fehlverhalten sanktioniert werden muss. Betrug vs. vertrauensvoller Umgang stehen also in einem ökonomisch „gesunden“ Verhältnis. Eine solche wirtschaftliche und gesellschaftliche Ordnung braucht keine Blockchain.

Natürlich mag dies in anderen Gesellschaften anders aussehen. Natürlich kann auch unsere zivilisierte Gesellschaft in X Jahren aus dem Ruder laufen. Aber was nützt dann Blockchain, wenn die Schergen vor der Tür stehen und die Verbannung nach Sibirien droht? Was nützt der Grundbucheintrag unserer Immobilie in der Blockchain, wenn der Notar gezwungen wurde, einen Schenkungsvertrag mit wem

auch immer als Begünstigten aufzusetzen? Die Blockchain kann nicht reparieren – und auch nicht verhindern – dass Unrecht geschieht. Sie kann nur funktionieren, wenn es Anwender gibt, die die Daten der Blockchain auch im Sinne der Anwender benutzen können.

Solange aber unsere Gesellschaft intakt ist, impliziert dies, dass wir mir vertrauenswürdigen Dritten leben können. In diesem Fall können wir uns dann aber auch für die zentralisierte Softwareanwendung entscheiden und in Kauf nehmen, dass es sehr selten zu Fehlverhalten kommen kann.

Apropos „Fehlverhalten“: Wo gab es über die letzten Jahre Fehlverhalten quasi als Massenbewegung? In der Kryptowelt. Und warum? Weil es dort nicht die sozialen, juristischen und ökonomischen Konventionen gibt, die gerade Fehlverhalten eindämmen. In der Anonymität der Blockchain stehen offensichtlich Kriminellen Tür und Tor offen. Zumindest zu einem höheren Prozentsatz als im Falle einer intakten Gesellschaft mit „klassischem“ Umgang.

Dennoch finden sich seit etwa acht Jahren immer wieder Begeisterte, die in der Nutzung der Blockchain Erlösung suchen. Ganze Generationen von Start-Ups hangeln sich von Finanzierung zu Finanzierung, überleben mit dem rasanten Wertzuwachs ihrer Krypto-Portfolios oder setzten öffentliche Fördergelder als lebensverlängernde Elixier ein. Am Ende beginnen Sie dann einen Neustart als „erfahrene Krypto-Unternehmer“, sodass der Zyklus von vorne beginnen kann.

Gibt es aber möglicherweise eine Synthese aus Blockchain und non-Blockchain? Gibt es Blockchain-Eigenschaften (und Nichteigenschaften), die auch im klassischen Kontext eine sinnvolle Ergänzung darstellen? Dann müsste man sich nicht einen technologischen Maximalschritt gehen, sondern nur solche Komponenten verwenden, die für eine gegebene Anwendung sinnvoll sind.

5 Wieviel Sicherheit braucht eine Online-Plattform?

Sicherheitsanforderungen skalieren zwischen Extrema, die man als „niedrig“ und „wasserdicht“ bezeichnen kann. Man stelle sich vor, mit der Technik von vor 25 Jahren eine heutige Anwendungsplattform zu entwickeln: Die primitive Front-End-Technologie der Neunziger würde bereits zur Cyberattacke einladen. Die Datenbank würde Daten nicht verschlüsseln, die gespeichert werden. Jeder Anfänger könnte die Anwendung per SQL-Injection zu Fall bringen und keine der Datenverbindungen wäre verschlüsselt. Außerdem hätte keiner der Entwickler einen Überblick, wie die Anwendung in der Cloud installiert ist. Ach ja, und eine AVV (Auftragsdatenverarbeitungs-vereinbarung) gäbe es natürlich auch nicht – schöne, einfache Welt von gestern! Diese Extremvariante kann man heute getrost als **„naiv“** bezeichnen. Sie soll lediglich das schwache Ende eines Sicherheitsspektrums markieren.

Heute ist das übliche Sicherheitsniveau bei Online-Anwendungen von diesem primitiven Ende ganz weit in die andere Richtung verschoben. Neben den oben genannten Aspekten gibt es eine riesige Anzahl an Maßnahmen, die essenziell sind, um Software, die der Öffentlichkeit ausgesetzt ist, sicher zu betreiben. Nennen wird dies die Stufe **„State-of-the-Art“**.

Für viele steht **„Blockchain“** am oberen Endpunkt des Sicherheitsspektrums insbesondere weil sie gegen den (nicht mehr vorhanden) zentralen Betreiber und gegen andere Teilnehmer schützt. Man stelle sich entsprechend eine Bank vor, die nicht mehr auf die Daten ihrer eigenen Transaktion zugreifen kann. Dies klingt absurd, denn sie muss ja in Zeiten überbordender Regulierung alle erdenklichen Details für Prüfzwecke bereithalten. Zu behaupten, dass ein Kunde einem anderen Kunden Geld überwiesen hat, aber nicht bestimmen zu können, wer diese waren oder wie hoch der Betrag war, erscheint als „zu sicher“ – auch für die sicherheitsgeplagte Finanzbranche.

Aber es gibt Szenarien im Grenzbereich zwischen Blockchain und klassischer Umsetzung, in denen letztere etwas von ersterer übernehmen kann. Zum Beispiel kann es Sinn machen, **dass der Betreiber einer zentralen Plattform nicht wissen soll, wer mit wem in einer Geschäftsbeziehung steht**, aber andere Teile der Transaktion verarbeiten können soll. Ein Beispiel dazu lernen wir gleich kennen. Bei dieser Klasse von Anwendungen könnte der Betreiber damit werben, dass er die von ihm verwalteten Daten nachweislich nicht missbrauchen kann, weil ihm ein dafür erforderlicher Teil fehlt.

Oder der Betreiber nutzt eine sichere Protokollierung, wie sie bei Blockchains in Form von **Hash-Ketten** (Merkle-Tree und Verkettung von Blöcken) verwendet wird. Diese Verkettung kann man Teilnehmern offenlegen, sodass für jeden nachvollziehbar ist, dass Daten nicht eingefügt, verändert oder gelöscht wurden.

Wir betrachten „Blockchain“ hierbei also als Baukasten, der die anfangs genannten Eigenschaften bietet, komponieren die Anwendung allerdings nicht als vollwertige Blockchain-Lösung, sondern picken uns solche Eigenschaften heraus, die für eine gegebene Anforderung sinnvoll ist. So nähern wir die „State-of-the-Art-Anwendung“ ein wenig dem Blockchain-Profil an. Aber wir verzichten auch bewusst auf eine der wichtigsten Eigenschaften – die der byzantinischen Fehlertoleranz – also den Schutz vor Angreifern auch aus dem Kreis der Teilnehmer.

Macht das Sinn? Rekapitulieren wir: Dezentralität im Sinne der Blockchain schützt vor Ausfällen und vor byzantinischen Angriffen. Technische Ausfälle sind heute auch mit Standardtechnologien wie Kafka und Deployment-Technologien wie Kubernetes zu erreichen. Bleibt also „nur“ die BFT. Wir verzichten also einerseits auf dieses wesentliche Blockchain-Element, erreichen aber andererseits durch die technische Zentralisierung des Betriebs eine erhebliche Vereinfachung und Aufwandsreduktion gegenüber der Blockchain.

Die These dieses Beitrags ist nun, dass dieser Verzicht angesichts der o.a. gesellschaftlichen Rahmenbedingungen tragbar ist, bestimmte Anwendungen sicherer macht und schließlich auch zu Blockchain-nahen Business Cases führen kann. Bezeichnen wir diese Ausprägung also als **„Blockchain-orientiert“**.

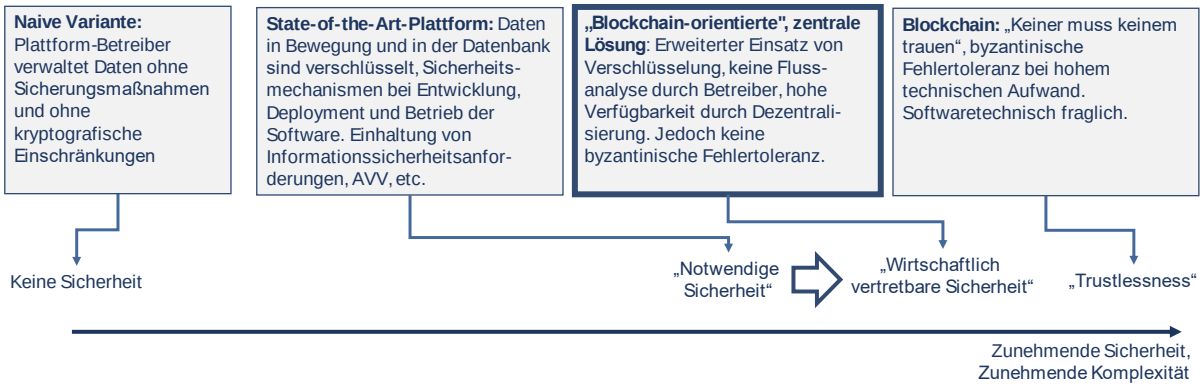

Abbildung 1: Software-Sicherheitsskala mit vier Ausprägungen

6 Eine Registeranwendung mit Blockchain-Eigenschaften

Man stelle sich folgende Situation vor: Für das Verfolgen von Herkunftsdaten in Lieferketten ist das Speichern von Chargeninformation nötig, um zu verstehen, welches Produkt zu welchem Zeitpunkt geliefert wurde. Es geht hierbei um den Herkunftsnachweis gegenüber den Konsumenten, die am Ende der Lieferkette stehen. Bei Kaffee könnte dies „Guatemala“ sein, bei Fleisch „Irland“ und bei Blumenerde „Estland“. Von Stufe zu Stufe der Lieferkette wird also diese Information weitergegeben. Ggf. können auch Produkte aus vorherigen Chargen kombiniert oder modifiziert werden – man denke an das Raffinieren von Rohöl.

Die Anforderungen der Konsumenten liegen also in der Identifikation des Herkunftslandes und die des Initiators einer solchen Online-Plattform in der Verkettung der einzelnen Chargeninformation. Aber es gibt noch weitere Stakeholder zu berücksichtigen: Die Lieferanten und Kunden entlang der Lieferkette. Wenn diese nicht mitspielen, dann bricht das Kartenhaus der Registeranwendung zusammen. Teilnehmer der Lieferkette, sind möglicherweise bereit, Herkunftsdaten ihrer Produkte einzutragen, aber nicht ihre direkten Lieferbeziehungen.

Das Vertrauen in die Registerplattform, dass sie diese Daten nicht an Dritte weitergibt, ist hier also ein essentieller Faktor. Nun könnte man, der Argumentation weiter oben folgend, behaupten, dass juristische, wirtschaftliche und soziale Regeln den Registerbetreiber schon hinreichend einschränken. Aber aus wettbewerblicher Sicht könnte er bei den unterschiedlichen Teilnehmern besser punkten, wenn er bei seinen Sicherheitsmaßnahmen freiwillig noch ein, zwei Schritte weiter geht in Richtung Blockchain – also seine Plattform „Blockchain-orientiert“ entwickelt.

Dies macht z.B. Sinn bei folgenden Blockchain-Eigenschaften:

- **Anonymität**. Dies ist die Forderung der Lieferketten-Teilnehmer – und zwar in solch einer Form, dass auch der Registerbetreiber die Zusammenhänge der Lieferbeziehungen nicht erschließen kann.
- **Immutabilität**. Auch wenn heute Datenbanken bei „State-of-the-Art“-Anwendungen eine Audit-Trail-Funktion anbieten, bei der das Erzeugen, Ändern und Löschen von Daten protokolliert wird, so gibt es am Ende immer noch irgend einen zentralen Administrator oder eine Gruppe von ihnen, die das Protokoll und die Daten möglicherweise löschen können. Stattdessen könnte man aus der Blockchain-Welt das Hashing von Transaktionen übernehmen, Transaktionen explizit mit einem Hash versehen und mit der Vorgängertransaktion verketten. Dies ist kein Block und somit auch keine Blockchain, aber eine Übernahme des Nötigsten. Dritte können dabei die Transaktionsdaten und die darauf basierende Hash-Kette überprüfen – möglicherweise sogar andere Nutzer. Auf diese Weise wird sichergesellt, dass keine nachträgliche Manipulation der Daten erfolgt.

Für unsere Registeranwendung passt eine Erweiterung um diese zwei Eigenschaften:

Anonymität lässt sich herstellen, indem die Identität des Senders einer Chargeninformation verschlüsselt wird. Dabei verschlüsselt der Lieferant seinem Kunden die Lieferanten-ID unter Verwendung des öffentlichen Schlüssels des Kunden. So kann nur der Kunde herausfinden, wer der Lieferant der Daten war. Er könnte sogar diese Charge mit denen, die er an seine Kunden liefert, öffentlich verbinden, ohne dass ein Dritter irgendeinen Teilnehmer identifizieren kann. Andere, weniger kritische Daten wie z.B. das Herkunftsland des Produkts lassen sich unverschlüsselt als Teil der Chargeninformation transportieren.

Allerdings ist der Registerbetreiber jetzt immer noch in der Lage, Lieferant und Kunde einer Charge zu identifizieren, da die API-Aufrufe des Registers verbindbar sind mit der Identität des Lieferanten („Flussanalyse“).

Erst durch einen weiteren Schritt ist hier vollständige Anonymisierung möglich: Wenn die Chargeninformation in einen Transaktionspool eingestellt wird, bei dem alle Teilnehmer regelmäßig abfragen, ob für sie Transaktionen eingegangen sind, entscheidet sich erst nach Herunterladen aller Transaktionen durch einen Teilnehmer, ob für ihn etwas dabei ist. Ist dies der Fall, entscheidet sich dies lokal beim Teilnehmer, der Registerbetreiber erhält keine Information darüber, dass dieser Teilnehmer Kunde einer Charge ist. Dieses Verfahren der anonymen Kommunikation über eine zentrale Plattform lässt sich verallgemeinern, z.B. für Bestätigungen, die ein Kunde dem Lieferanten zurücksendet.

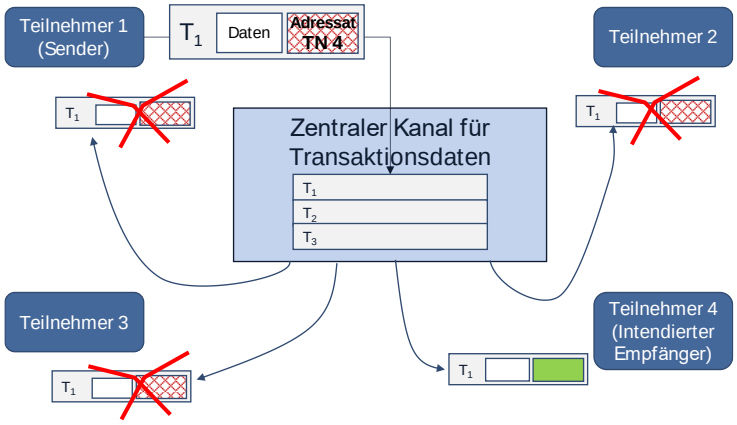

Abbildung 2: Anonymer Datenaustausch über eine zentrale Plattform

Natürlich ist dieses Verfahren aufwändig, und die Notwendigkeit, auch Transaktionen zu prüfen, die anderen Teilnehmern zugeordnet sind, wächst quadratisch mit der Anzahl an Teilnehmern. Es gibt sicherlich Anwendungsfälle mit hoher Teilnehmer- oder Transaktionszahl, bei denen dieses Verfahren nicht mehr effizient ist. Aber es ist ja auch eine optionale Entscheidung, die Blockchain-Eigenschaft der Anonymität zu verwenden.

Im Umkehrschluss zeigt dieses Verfahren übrigens auch, wie ineffizient Blockchains sind: Hier werden ebenfalls alle Transaktionen allen Teilnehmer zugänglich gemacht – und dies bei allen Anwendungen[4], die in Form von Smart Contracts auf der Blockchain sitzen.

Die andere Blockchain-Eigenschaft, die wir für die Registeranwendung einführen wollen, ist **Immutabilität**, realisiert durch das Verketten von Transaktionen per Hash-Kette. Da in unserem Anwendungsbeispiel die Chargendaten des Registers ohnehin öffentlich sind, können diese auch um zusätzlich erzeugte Hashwerte ergänzt werden. Auf diese Weise kann jeder Teilnehmer (ggf. auch jeder Dritte) die Korrektheit der Transaktionen überprüfen, indem ein Validierungslauf über sämtliche Transaktionen durchgeführt wird:

- Für die erste Transaktion T_1 ist zu prüfen: Ist der Hashwert H_1 ihrer Daten korrekt?
- Für jede nachfolgende Transaktion T_n ($n > 1$): Ist für der Hashwert H_n korrekt, der sich aus dem Hashwert H_{n-1} von T_{n-1} in Verbindung mit dem Hashwert aus Transaktion T_n ergibt?

[4] Man könnte jetzt einwenden, dass das mit Ethereum 2.0 einzuführende Sharding hier Abhilfe schafft, aber dies gilt nur für den Gesamtdatenbestand. Je Shard oder spätestens je Smart Contract wiederholt sich Problem für die Teilnehmer und Knotenbetreiber.

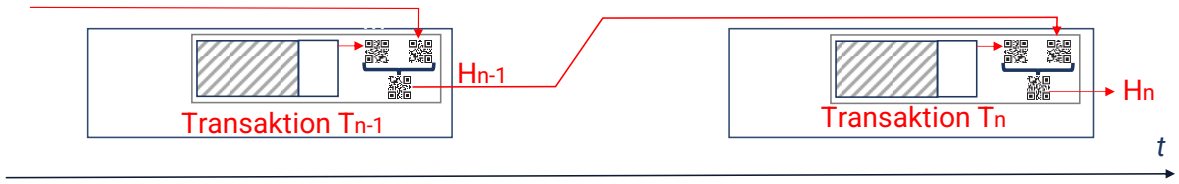

Abbildung 3: Transaktions-Hashkette

Sollte die Kette durch Löschen / Ändern / Erzeugen von Transaktionen durchbrochen werden, ist dies für alle erkennbar. Nicht erkennbar ist, wer sie durchbrochen hat und heilbar ist dies auch nicht (diese Möglichkeit bleibt nur einer dezentralen, „echten" Blockchain vorbehalten). Aber es geht hier ja eben um die Annährung der Sicherheit in Richtung Blockchain, nicht um deren Einsatz.

Das Vertrauen in den Betreiber ist nach wie vor höher als bei einer „State-of-the-Art"-Anwendung: Er muss den Betrieb technisch am Laufen halten und er muss fachlich die von ihm erwartete Logik erbringen. Bei der Einführung einer neuen Anwendung mag es also Sinn machen, die o.g. Eigenschaften zu unterstützen. Ggf. kann man später, wenn das Vertrauen gewachsen ist, die Anwendung auch wieder auf den Umfang einer „State-of-the-Art"-Umsetzung zurückführen[5].

7 Zusammenfassung

In diesem Paper wurden typische Blockchain-Eigenschaften identifiziert und analysiert. Für viele stellen diese eine Grundlage zu Entwicklung besonders sicherer Anwendungen dar. Außerhalb der Welt der Kryptowährungen haben sich bisher aber bestenfalls nur sporadisch kaufmännisch sinnvolle Anwendungsfälle gefunden, die mit Hilfe der Blockchain-Technologie besser umsetzbar sind als mit State-of-the-Art-Technologie.

Dennoch lassen sich Eigenschaften finden, die bei passenden Anwendungsfällen die Sicherheit für Teilnehmer auch bei einer zentralen Online-Plattform erhöhen und die Möglichkeit zur Einflussnahme durch deren Betreiber reduzieren. Am Beispiel der Registeranwendung zur Ermittlung der Herkunftsländer von Produkten wurde aufgezeigt, welche Blockchain-Eigenschaften als Ergänzung einer zentralisierten Anwendung sinnvoll erscheinen, aber auch, wo deren Grenzen liegen.

Die These dieses Beitrags ist folglich, dass die Blockchain-Technologie grundsätzlich zu fordernd ist für die meisten Anwendungsfälle, die auch zentralisiert sinnvoll realisierbar sind. Man beachte hierbei auch die vielen Flussdiagramme, die schon vor Jahren entwickelt wurden, um durch eine Staffelung von Ausschlusskriterien den sehr kleinen Residualraum für Blockchain-Anwendungen zu bestimmen.

Aus dem Beispiel der Registeranwendung ist erkennbar, dass die Ausprägung „Blockchain" in der Sicherheitsskala eine Extremstellung einnimmt, die technische Vorteile mit hohem äußerst hohem Aufwand erkauft. Zudem scheint die Art des juristischen, wirtschaftlichen und persönlichen Umgangs innerhalb unserer Gesellschaft einen Rahmen zu schaffen, der eine Abweichung vom Maximalmaß der Blockchain-Sicherheit in Verbindung mit der Toleranz weniger Verfehlungen ermöglicht.

Wir streben folglich als Gesellschaft immer wieder ein neues Optimum auf der Sicherheitsskala an, dass sich jederzeit verschieben kann. Ransomware-Attacken und andere Formen von Cyberkriminalität verursachen eine Verschiebung des Optimums in Richtung „Mehr Sicherheit bei höheren Kosten", aber

[5] Wir sind bei der Handelsplattform für Wälzlager „Bearing X" so vorgegangen: Zunächst wurde der Handel dezentral per Blockchain organisiert, aus Performancegründen war es jedoch später sinnvoll, statt einer Blockchain Kafka einzusetzen. Siehe auch weitere Details im PONTON-Whitepaper.

dies muss nicht bedeuten, dass wir das maximale Ende der Skala für alle Anwendungsfälle technisch einfordern müssen.

Im Beitrag wurde deutlich gemacht, dass die Entscheidung „Blockchain oder nicht Blockchain“ keine Binäre ist. Die „Blockchain“ lässt sich zerlegen und in einigen funktionalen Bestandteilen wiederverwenden. Selbst die Ausfallsicherheit durch Dezentralisierung lässt sich durch nachrichtenbasierte Kommunikationsinfrastrukturen wie Kafka erreichen. Was als residuale Eigenschaft der Blockchain einzig bleibt, ist die byzantinische Fehlertoleranz. Ist diese erforderlich, sind wir tatsächlich am Blockchain-Ende des Spektrums angekommen.