

2. Hintergrundwissen

2.1 Warum Kryptowährungen (I): Vorspann

Feuerwehrleute, Systemrelevanz und SteuergelderEin Computer für 500 kg Kartoffeln, bitte!***Notenbanken und Inflation*** Die Aliens und das Fußballspiel***

2.1.1 Feuerwehrleute, Systemrelevanz und Steuergelder

Wer die Beliebtheit und den Hype um Kryptowährungen verstehen will, sollte zunächst in die Zeitmaschine steigen. Wir müssen aber nicht ins 17. Jahrhundert reisen, ein kurzer Flug in das zurückliegende Jahrzehnt genügt schon. Wir landen im Jahr 2007. Es gibt viele Wege, die damalige Finanzkrise zu erklären. Und mit wenigen Worten geht es meistens schwierig. Ich versuche es trotzdem mal und stelle Ihnen einen sympathischen jungen Feuerwehrmann vor. Er heißt Andrew, lebt im Bundesstaat New York, ist 26 Jahre alt und hat kürzlich geheiratet. Andrew isst gerne Burger und liebt die New York Yankees, aber das ist hier nicht so wichtig. Viel bedeuter ist, dass er vor dem Hintergrund der anstehenden Heirat seiner langjährigen Freundin Nancy denkt, dass die Zeit für einen Hauskauf reif ist. Deshalb macht er, was in dieser Situation viele tun. Er vereinbart einen Termin bei seiner Hausbank. Man redet dort über Einkommen, Zinsen und Sicherheiten, nimmt Prospekte mit und trifft sich noch zu einem zweiten und dritten Termin. Andrew und seine Frau planen mit 2 Kindern und verfügen über ein Haushaltseinkommen von 50 000 Dollar brutto. Wir wollen hier keine Rechenspiele veranstalten und machen es kurz und simpel: Die Bank finanziert Andrew und seiner Frau ein Haus, das sich die beiden eigentlich nicht leisten können. Denn die Zinsen sind in den ersten Jahren zwar sehr günstig, können langfristig aber nicht mehr bedient werden. Haus und Grundstück sind vom Kredit abbezahlt, das Darlehen können Andrew und seine Frau nicht tilgen. Die Bank hat das Haus, aber keinen getilgten Kredit. Sie kann versuchen, den ausstehenden Betrag über eine Zwangsversteigerung zu erlösen. Ein Geschäft mit Gewinn wird nur daraus, wenn jemand bereit ist, einen gewissen Preis für Haus und Grund zu zahlen. Wenn die Bank clever ist, verkauft sie das gesamte Darlehenspaket aber an einen Dritten, zum Beispiel an eine andere Bank. Diese andere Bank kauft die Forderung gegen Andrew und seine Frau samt Hypothek am Grundstück. Sie wird dafür den nominellen Wert der Darlehensforderung abzüglich eines Risikoabschlags zahlen. Sie fragen zu Recht: Welche Bank macht das? Das ist völlig richtig. Denn wenn die Bank sich Gedanken über die Höhe des Risikoabschlags macht, wird sie sich das Einkommen von Andrew und seiner Ehefrau ansehen. Und in der Folge das Angebot mit Dank ablehnen oder den Risiko-

abschlag so hoch beziffern, dass die andere Bank ihr den Kredit nicht mehr verkaufen will. Blöd. Die Bank, die das Kreditrisiko verkaufen will, überlegt sich, wie sie den Vertrag trotzdem los wird. Ganz einfach: Das Risiko fliegt nur dann auf, wenn sich die andere Bank dezidiert mit den Vermögensverhältnissen vom Feuerwehrmann und seiner Gattin auseinandersetzt. Was macht die andere Bank, wenn man ihr einfach einhundert solcher Darlehen im Paket verkauft? Oder tausend? Oder zehntausend? Sie ahnen es: Statt jedes Vertragsverhältnis durchzugehen, wird man einen pauschalen Risikoaufschlag wählen. Frei nach dem Motto: In den allermeisten Fällen wird schon alles gutgehen. Ein Fehler und ein gutes Geschäft für die Verkäuferbank. Das theoretische Problem: Wenn alle so handeln, sitzt irgendwann fast jede Bank auf zahlreichen Päckchen solcher „faulen Kredite“. Das praktische Problem: Genau so kam es. Wie gesagt, alles geht gut, solange die Hauspreise steigen. Denn so lange kann jede Bank bei einer Zwangsversteigerung genug Geld erlösen, um aus dem Kreditkauf ein Nullsummenspiel zu machen oder sogar einen Gewinn zu erzielen. Wir wissen jedoch alle, dass auch Immobilienpreise nicht ewig steigen und jede Blase irgendwann platzt.

Die Banken machten große Verluste und einige große Bankenhäuser standen vor der Insolvenz. Mit Zahlungsunfähigkeit ist das so eine Sache. Im Normalfall geht ein zahlungsunfähiges oder überschuldetes Unternehmen insolvent. Die Lage der Banken ist aber sehr stark mit dem Schicksal der einzelnen Menschen verquickt. Der Wegfall der eigenen Vermögensanlage tut sehr weh. Die Pleite einer großen Bank kann zehntausende Sparer arm machen und wegen der wechselseitigen Abhängigkeit der Banken untereinander auch weitere Bankeninsolvenzen nach sich ziehen. Deshalb entschieden sich Staaten zur Rettung dieser Banken. Schulden der Banken bezahlte man mit Geld aus Staatseinnahmen. Dazu gehörten auch Boni von Entscheidungsträgern der Banken aus vorangegangenen Jahren, teils in schwindelerregender Höhe. Das trug nicht unbedingt dazu bei, die Liebe zu und das Vertrauen in Banken zu steigern. Nicht nur bei Andrew und seiner Frau und nicht nur in den USA.

Immer mehr Menschen fragten sich: Geht „Geld“ auch anders?

2.1.2 Ein Computer für 500 Kg Kartoffeln, bitte!

Historisch war Geld in erster Linie ein Tauschmittel. Nehmen wir an, Sie wollen Ihr Handy verkaufen und einen neuen Computer erwerben. Sie können Ihr Handy bei Herrn T. gegen 500 kg Kartoffeln tauschen. Dann stellen sich mehrere Fragen: Wo lagern Sie die Kartoffeln? Wie transportieren Sie die Kartoffeln? Und vor allem: Wer isst die Kartoffeln? Selbst wenn bei den ersten beiden Fragen keine Probleme auftauchen, wollen Sie doch eigentlich

einen Computer. Und vielleicht haben Sie schon 50 kg Kartoffeln in Ihrem Keller liegen, der Bedarf ist gedeckt. Ein universales Tauschgut, das noch dazu wenig wiegt und leicht zu transportieren ist, wäre hier von Vorteil. Deswegen gibt es Geld. Und wenn z. B. ein Händler in früherer Zeit von Italien nach Deutschland über die Alpen reiste, um Waren auf einer Messe zu verkaufen, gab es bei der Bezahlung auch eine Absicherung gegen Raubüberfälle: Der Verkäufer bekam einen auf ihn ausgestellten Wechsel, das Geld gab es bequem gegen Einlösung dieses Wechsels bei der Bank in Italien. Alles gut, oder?

2.1.3 Notenbanken und Inflation

Die Einführung und Lenkung von Geld ist aber komplex. Die Geldmenge will gesteuert sein, damit zu viel Geld nicht eine übermäßige Inflation mit stets steigenden Preisen auslöst. Dafür gibt es Zentralbanken. Sie sehen: Die Lösung eines Problems führt zum nächsten und jede neue Herausforderung erfordert eine neue (zentrale) Stelle, eine neue Institution, einen neuen Player.

Traditionelle Bezahlmethoden leiden nun an zwei Mängeln: Der Gefahr der Geldentwertung und der Bedeutung der Banken. Dass Banken für das Funktionieren einer Volkswirtschaft unentbehrlich sind, ist völlig in Ordnung, aber muss ich wirklich eine hohe Bearbeitungsgebühr zahlen, wenn ich Geschäfte mit US-Amerikanern mache und diese in Dollar bezahle, obwohl ich nur Euros habe? Hinzu kommt die Gefahr von Geldfälschung. Das betrifft zwar nicht mein Guthaben auf dem Bankkonto, aber die Frage, ob ich den neuen Computer mit dem Bargeld für das Handy bezahlen kann. Denn auf die halbe Tonne Kartoffeln möchte ich ungern zurückgreifen...

Lange Rede, kurzer Sinn: Kryptowährungen lösen diese Probleme. Zum mindest auf den ersten Blick und wenigstens teilweise. Dass hier keineswegs alles Gold ist, was glänzt, werden wir noch sehen. Kryptowährungen sind also ein alternativer Zahlungsweg, aber beileibe nicht alternativlos.

2.1.4 Die Aliens und das Fußballspiel

Die Beliebtheit von Kryptowährungen in manchen Kreisen hat auch etwas mit einer Geschichte um Aliens und einem Fußballspiel zu tun, jedenfalls im weitesten Sinne. Ob sich diese so zugetragen hat oder zutragen wird, wissen wir nicht. Drei Außerirdische – selbstverständlich mit in die Breite gezogenem grünen Kopf, fragiler Statur und großen Augen – fliegen in einer Welt Raumkapsel im All umher und machen kurz bei der Erde halt, wo sie menschliches Leben beobachten wollen. Für zwei Stunden schauen sie durch ein Fernrohr und betrachten eine mitteleuropäische Stadt in der Abendsonne.

Insgesamt drei unterschiedlichen Männern wird dabei zugesehen, wie diese abends alleine zuhause essen, als nächstes zur U-Bahn laufen, mit dieser Bahn einige Stationen fahren, um sich anschließend in einer Kneipe zusammen mit Freunden ein Fußballspiel zu Gemüte zu führen. Dann drehen die außerordentlichen Außerirdischen wieder ab und fixieren ihre Beobachtungen der Menschheit auf einem Notizzettel: „Die Menschen leben alleine in übersichtlichen Räumen und nach jeder Mahlzeit fahren sie in einem langen Gefährt auf Schienen namens U-Bahn an einen geselligen Ort und schauen dort auf einem Bildschirm mit anderen Menschen, wie wiederum andere Menschen einem Ball hinterherrennen. Sollten wir die Erde je angreifen wollen, könnten wir gezielt diese U-Bahnen attackieren, nachdem wir den Menschen etwas zu essen gegeben haben. Denn nach dem Essen steigen die Menschen in diese Bahnen, wie unsere Beobachtungen ergeben haben.“

Wie naiv, denken wir Menschen. Denn schon die Annahme, alle Menschen würden alleine leben, ist falsch. Außerdem ist das Essen nicht die Ursache für eine Fahrt mit der Bahn und die Bahnfahrt auch nicht der Grund dafür, Fußball zu schauen. Die eben genannten Tätigkeiten tauchten in den wenigen Beobachtungen von außen zufällig zeitlich hintereinander auf, verursachen einander aber nicht. Die Außerirdischen gelangen zu falschen Schlussfolgerungen, weil ihre Stichprobe zu klein ist. Hätten sie unterschiedliche Gegenden der Erde und mehrere Haushalte über einen längeren Zeitraum beobachtet, wären ihnen ihre fehlerhaften Schlussfolgerungen schnell aufgefallen. Sie hätten Ihre Annahmen korrigiert und nicht Korrelation, das zufällige, aber ohne Ursachenzusammenhang miteinander Auftreten von Ereignissen, mit Kausalität verwechselt. Aber was hat das mit Kryptowährungen zu tun? Eine Vielzahl an Menschen hält den durch gezielte Maßnahmen in die Wirtschaft eingreifenden Staat gewissermaßen für einen der eben beschriebenen Außerirdischen. Staat und Wirtschaftswissenschaft hätten angesichts der zahlreichen die Wirtschaft beeinflussenden Faktoren zu wenig Informationen über das Verhältnis dieser Faktoren zueinander, um lenkend in wirtschaftliche Abläufe eingreifen zu können.

Auch die Geldmenge staatlicher Währungen wird von Zentralbanken kontrolliert und zur Erreichung von Stabilitätszielen vermeintlich effizient gesteuert. In Wahrheit regiere hier der Zufall, der Beobachter könne nicht zwischen Kausalität und Korrelation unterscheiden und maße sich Wissen an, was er nicht habe.

Die verfügbare Datenmenge sei schlicht zu gering, um einigermaßen verlässliche Vorhersagen über die Folgen spezifischer staatlicher Handlungen zu treffen. Die Mechanismen freier Märkte würden von alleine zur für alle besten Lösung führen, Marktversagen am besten durch das zufällige und unkoordinierte Zusammenspiel freier privater Interessen vermieden und

geheilt. Deshalb sei ein Wettbewerb privater Währungen ökonomisch betrachtet besser als die zentrale Steuerung einer einzigen Währung mit Monopolstellung. Der Aufstieg von Kryptowährungen wird deshalb von diesen Denkern mit Applaus begleitet, Vertreter des kritischen Rationalismus oder des Liberalismus erfreuen sich prinzipiell an dem neuartigen Wettbewerb, den Kryptocoins im Währungskontext entfachen.

2.2 Warum Kryptowährungen (II): Die Macht der Mittelsmänner

Vertrauen ist gut, zu dritt ist es besser?**2 > 3 ?!*****

2.2.1 Vertrauen ist gut, zu dritt ist es besser?

Eben ging es um Banken und Sie haben es gleich gemerkt: Banken sind die Mittler zwischen zwei Parteien und fungieren als Zahlstelle für einen davon. Ich kann mein Handy an jemanden auf der Straße gegen Bargeld verkaufen, ich kann es aber auch an einen Käufer aus Wanne-Eickel an selbigem Ort verschicken und dafür Geld überwiesen bekommen. Meine Bank hält eine Art virtuellen Geldbeutel für mich. Wenn ich zu ihr gehe und es von ihr verlange, leert sie diesen für mich. Natürlich macht sie das nicht umsonst und erst recht nicht kostenlos. Ich zahle eine Verwaltungsgebühr und Bearbeitungsgebühren für besondere Überweisungen. Brauche ich das?

Nun gut, in der Vergangenheit sind Mittler zwischen zwei Vertragsparteien regelrecht aufgeblüht: Ebay und Airbnb sind nur zwei Beispiele für Internetplattformen, deren Nutzen sich darin erschöpft, als Intermediär aufzutreten; sie vermitteln Vertragsschlüsse. Banken sind damit aber nicht vergleichbar. Denn zum einen bringen Ebay und Airbnb Personen zusammen, die sonst gar nicht in Kontakt getreten wären. Zum anderen betrifft der Zahlungsvorgang nur die Vertragserfüllung einer Partei, nämlich die Zahlung, nicht aber den Vertragsschluss. Sind Banken vielleicht trotzdem entbehrlich?

2.2.2 2 > 3?

Nun ja, wenn man die Bank als Dritte aus dem Zahlungsvorgang herausnehmen und die Zahl der Beteiligten auf zwei senken möchte, dann müsste ein Anderer die Funktion der Bank einnehmen. Das scheint schwierig bis unlösbar zu sein! Denn es geht ja um die Überweisung von Geld. Und mein Geld (ausgenommen von den Münzen und Scheinchen im Geldbeutel) liegt ja irgendwo. Eben. Die Bankfunktion muss jemand anderes übernehmen. Aber dann wäre auch wieder ein Dritter im Spiel. Ohne einen Dritten müsste jeder seine eigene Bank sein, sein virtuelles Geld selbst verwalten.

Aber wo zahle ich dann ein, wer zahlt mir Geld aus? Ich bräuchte ein Programm. Irgendeine computertechnisch aufbereitete Infrastruktur, die mein Geld von A nach B bringt und alle Bankfunktionen erfüllt. Und zwar ohne dass ein anderes Unternehmen diese Infrastruktur stellt. Im klassischen Bankverkehr sind drei Parteien in einen Zahlungsvorgang involviert. Meistens sogar vier, wenn Empfänger- und Versenderbank nicht übereinstimmen. Können wir aus vier auch zwei oder aus drei zwei machen? Das klingt nach einer feinen Sache, einer Win-win-Situation, aber funktioniert das auch? Zwei ist also beileibe nicht größer als drei (oder vier), auch im 21. Jahrhundert gelten die ewigen Wahrheiten der Mathematik. Aber vielleicht sind zwei besser als drei. Wir werden sehen...

2.3 Warum Kryptowährungen (III): Alles wird leicht

Flow & growSmart solutions & big business***

2.3.1 Flow and grow

Wenn Zahlungsvorgänge einfacher und weniger Parteien daran beteiligt wären, würde das einem allgemeinen Trend entsprechen. Denn immer mehr Unternehmen versuchen, dem menschlichen Hang zur Trägheit gerecht zu werden, indem sie alles simpler und smarter machen (oder dies zumindest versprechen). Weil das Erfolg bringt.

In einem angesehenen Blog eines Professors für VWL erzählte dieser vor einigen Jahren eine hochinteressante Anekdote von den täglichen Busfahrten mit seiner Tochter. Er begleitet sie täglich auf dem Schulweg und die beiden steigen zunächst in eine U-Bahn, bevor sie diese verlassen und an einer vollgepackten Bushaltestelle auf die zehnminütige Weiterfahrt warten. Etwa fünfzig Menschen stehen, schwitzen und schnattern dort. Wenn der Bus ankommt, sind maximal zehn Sitzplätze frei. Das bedeutet: Die Fahrt wird zur Hölle, Entspannung zum Fremdwort. Irgendwann fällt dem klugen Geist auf, dass die vorherige Haltestelle nur ca. 200 m entfernt und in Sichtweite liegt. Dort steht niemand an. Von da an läuft er mit seiner Tochter stets dort hin, der Sitzplatz ist sicher, Entspannung und Komfort garantiert. Doch warum kam offenbar niemand der anderen Fahrgäste auf diese Idee? Nun ja, der Mensch ist träge.¹

¹ http://freakonomics.com/2007/03/21/herd-mentality-the-freakonomics-of-boarding-a-bus/?c_page=9

2.3.2 Smart solutions & big business

Was meinen Sie, warum sich heute Touchscreens auf unseren Handys befinden oder wir Anrufe über Spracherkennung auslösen? Die Antwort ist simpel: Weil es weniger Anstrengung kostet, weil es leichter von der Hand geht. Produktentwickler fragen sich täglich, wie Nutzer in der Phase zwischen dem ersten und letzten Kontakt mit dem Produkt glücklicher gemacht werden können, die Produktnutzung angenehmer gestaltet werden kann. Denn der Mensch denkt und kauft effizient, jedenfalls meistens. Erstrebenswert ist alles, was intuitiv(er) und locker-leicht abläuft, Design Thinking nennt sich ein Teilbereich dieser Denkrichtung. Übersetzt als Handlungsanweisung für Unternehmen: Flowing is growing. Aus diesem Grund gibt es smart phones, smart homes und smart solutions. Alles soll weniger Anstrengung erfordern, schlanker und deshalb smarter sein.

2.4 Was ist die Blockchain (I): Der Autokauf

*****Was die Blockchain mit dem PKW-Kauf zu tun hat ***Zwei minus Eins ist nicht gleich Eins*****

2.4.1 Was die Blockchain mit dem PKW-Kauf zu tun hat

Was hat die Blockchain mit dem Kauf eines Gebrauchtwagens zu tun? Nicht so viel, könnte man meinen. Ziemlich viel, meinen andere. Nehmen wir an, Sie stöbern im Inseratsbereich einer Zeitung und stoßen auf ein interessantes Angebot. Ein dunkelblauer Mittelklassewagen, 1 Jahr alt, 3000 km, scheckheft gepflegt etc. pp., 2/3 des Originalpreises. Das weckt Ihre Neugier und Sie rufen den Händler an. Zwei Tage später: Sonnenschein im sommerlichen Feierabend, Sie sitzen im gewünschten Fahrzeug und bewegen das dynamisch-komfortable Gefährt. Fahrgefühl, Beschleunigung, Bequemlichkeit, Sicherheit, Straßenlage – alles bestens. Bei der Probefahrt ist ein Freund von Ihnen dabei, Martin. Mit dem vertrauenerweckenden Verkäufer sind Sie sich schnell einig: Sie zahlen sofort in bar und sollen drei Tage später das Auto samt Papieren abholen, ein Kaufvertrag wird in zweifacher Ausfertigung noch an Ort und Stelle unterzeichnet.

2.4.2 Zwei minus Eins ist nicht gleich Eins

Sie nehmen den Vertrag mit und verwahren ihn in einer Schublade. Was passiert, wenn Sie drei Tage darauf auf einen verkaufsunwilligen Verkäufer stoßen, der in der Zwischenzeit ein anderes Angebot bekommen hat? Es ist simpel: Sie drohen mit einer Klage, denn Sie haben mit dem Verkäufer einen Vertrag geschlossen und im Übrigen auch schon bezahlt. Vor Gericht haben

Sie nun Beweisprobleme: Denn entgegen anderslautenden Gerüchten zählt ein Richter nicht einfach schematisch die Zahl der Zeugen und Parteien und schaut dann, wer mehr Stimmen auf seiner Seite hat. Es nützt also oftmals nichts, mehr Zeugen als die Gegenseite zu haben.

Sie haben zwar ein Schriftstück, welches den Vertragsschluss mit dem Verkäufer dokumentiert, eine Quittung für die Zahlung besitzen Sie jedoch nicht. Und selbst wenn Sie eine bekommen hätten, so hätten Sie diese sorgfältig abheften müssen: Wenn in der Zwischenzeit Ihre Wohnung abbrennt oder ein Dieb Wertsachen und den Ordner mit dem Vertrag stiehlt, hilft Ihnen auch Ihre Ordnung nicht. Aber vielleicht hätte Sie eine Dokumentation des Zahlungsvorgangs auf einer Blockchain gerettet? Wie das funktioniert, wird sogleich näher erklärt. Aber die Charakteristika der Blockchain erklären sich auch durch ein wenig Nachdenken von alleine. Nehmen wir einmal an, zwei Unternehmen möchten die Dokumentation bestimmter wiederkehrender Vorgänge untereinander wie z.B. Zahlungen kontinuierlich aktualisieren. Wie könnte man das machen? Es gäbe die Möglichkeit, dass eine Partei das Protokoll auf den neuesten Stand bringt, der anderen Partei zur Bestätigung übersendet und die letzte Fassung dann immer abgespeichert. Vielleicht speichert man diese Version dann bei einer externen Plattform mit digitalem Speicher ab und macht die Datei für künftige Änderungen beiden Parteien zugänglich. So weit, so gut. So etwas erfordert aber Arbeit und einen Dritten, die Plattform mit Arbeitsspeicher. Außerdem funktioniert dieser Vorgang zwischen zwei Parteien noch recht gut, kompliziert wird es aber, wenn tausende Teilnehmer involviert sind und ihre Zahlungen untereinander protokolliert haben wollen. Spätestens dann ist der klassische Weg über Aktualisierung und Bestätigung ineffizient und langwierig. Gesucht wird ein Mechanismus, der ohne mentale Anstrengung der Teilnehmer die erfolgten Transaktionen zuverlässig, sicher und manipulationsfrei dokumentiert. Dafür muss insbesondere eine einfache Regel getroffen werden, unter welchen Umständen eine Protokollaktualisierung vom System akzeptiert wird. Diese Regel muss sich automatisch vollziehen und sie muss so ausformuliert sein, dass Manipulationen nahezu unmöglich sind. Blockchainanwendungen können die zentrale Antwort auf diese Frage liefern und eine solche Infrastruktur liefern. Wie das genau geht, wird anhand des nachfolgenden, einfachen und lebensnahen Beispiels deutlich klarer.

2.5 Was ist die Blockchain (II): Polonäse Blankenese

***Blockchain & Schlagerparties: Die ungleichen Zwillinge *** Goldgräberstimmung und Freigetränke

2.5.1 Blockchain & Schlagerparties: Die ungleichen Zwillinge

Beim Wörtchen Blockchain handelt es sich um einen Begriff, der einem mittlerweile täglich in der Zeitung begegnet, der aber nicht zwingend etwas mit Kryptowährungen zu tun hat. Denn nicht jede Kryptowährung basiert auf einer Blockchain (übrigens ist auch der Bitcoin nur eine von vielen virtuellen Währungen) und nur wenige Anwendungsmöglichkeiten der Blockchain hängen direkt mit Kryptowährungen zusammen. Aber was ist die Blockchain eigentlich? Sie finden im Internet hunderte Erklärungen, die meisten davon sind eher technischer Natur. Diese erfordern meist die Fähigkeit, sich in einem Dickicht aus Fremdwörtern und Fachbegriffen zurechtzufinden, also ein enormes Vorverständnis. Ich meine, man kann das Blockchainprinzip auch anders erklären. Und dafür brauchen Sie nur ein klein wenig Fantasie.

Es ist ein sommerlicher Samstag im September, 19:32 Uhr. Bei Michael trudeln die ersten Gäste ein. Gabi, Gerd, Heike, Horst, Thorsten, Tim, Simon, Udo, Uwe und Volker. Das halbe Lehrerkollegium. Es wird gefeiert und gelacht. Simon macht demnächst Wanderurlaub, Heikes Kind ist erkältet und Tims Hemd hat nach dem Gang zum Buffet etwas Kartoffelsalat abbekommen. Naja, so oder so ähnlich. Irgendwann dröhnt das Lied „Polonäse Blankenese“ aus den Lautsprechern und die ganze feierwütige Meute tanzt in der Reihe aus der Reihe. Mit diesem inneren Bild vor Augen möchte ich Ihnen die Funktionsweise der Blockchain erklären. Passen Sie bitte gut auf!

Der Begriff Polonäse kommt vom französischen polonaise (danse), dem polnischen Tanz. Der Duden spricht vom „festlichen Schreittanz im $\frac{3}{4}$ -Takt, wobei die Ausführung der geometrischen Figuren dem anführenden Paar überlassen bleibt“.²

Blankenese ist ein vornehmer Stadtteil in Hamburg, von dem böse Zungen behaupten, dass kleine Kinder aus diesem Ort teilweise schon mit Segelschuhen an den Füßen geboren werden. Ob das stimmt oder nicht, kann an dieser Stelle aber offenbleiben. Jedenfalls bilden bei der Polonäse die teilnehmenden Personen eine Kette, jeder legt der vor ihm oder ihr stehenden Person beide Hände auf die Schultern und so wabert der Tanztross dann in Reih und Glied und untrennbar über die Schultern miteinander verbunden von A

2 <https://www.duden.de/rechtschreibung/Polonaise>

nach B. Alle Personen auf der Feier bilden nun eine solche Kette. Sie müssen sich nun Folgendes vorstellen: Michaels Gäste stehen in alphabetischer Reihe hintereinander (Gabi-Gerd-Heike-Horst-Thorsten etc...). Jede Person trägt ferner einen transparenten Brustbeutel um den Hals, in dem ein nach außen sichtbarer, mit einem Wort beschriebener Zettel steckt. Dieses Dokument ist von außen lesbar. Auf Gerds linker Schulter stehen auf einem großen Aufkleber die Namen der vor ihm tanzenden Gabi und Gerd, auf Heikes Aufkleber auf der linken Schulter stehen Gabi, Gerd, Heike usw. Das bedeutet: Gerd darf nur zwischen Gabi und Heike stehen, Heike nur zwischen Gerd und Horst usw. Auf der rechten Schulter steht statt der Namen und an deren Stelle eine Abkürzung für den Inhalt des Dokuments im Brustbeutel der jeweiligen Person. Auf dem Zettel in Heikes Brustbeutel findet sich das Wort „Feierbiene“, auf Gabis Papier steht „Partymaus“. Auf den rechten Schultern der nachfolgenden Personen befindet sich als Abkürzung dafür an der Position neben Heike „FB“ und bei Gabi „PM“. Alles wird gefilmt und im Internet für jedermann einsehbar übertragen, die Filmdatei wird auf einigen Rechnern automatisch abgespeichert und jedes Mal durch eine neue Datei ersetzt, wenn sich eine weitere Person einreihet. Sie haben jetzt ein ziemlich sonderbares, vielleicht verwirrendes und vermutlich auch ein wenig belustigendes Bild vor Augen. Doch das Beste daran: Sie haben das Block-chainprinzip verstanden.

Jedenfalls sind Sie kurz davor. Stellen Sie sich vor, Sie wollen sich einreihen. Das geht, wenn Sie auf Ihrer linken Schulter alle vorherigen Namen in richtiger Reihenfolge aufgeschrieben haben und sich Abkürzungen für die Worte in den Touristengeldbeuteln in korrekter Reihenfolge auf Ihren rechten Schultern befinden. Jemand möchte Sie dazu motivieren, dass Sie mitmachen und sich ebenfalls an die Kette ran hängen. Sie stimmen im Grundsatz zu, möchten dafür aber zumindest ein Getränk ausgegeben bekommen. So viel Bewegung ist schließlich anstrengend. Sie bekommen ein Glas Wasser und reihen sich ein. Ganz ähnlich funktionieren blockchainbasierte Kryptowährungen.

Wieso, weshalb, warum? Wir haben vorhin davon gesprochen, dass traditionelle Währungen unter folgenden Mängeln leiden: Sie können gefälscht werden, für den bargeldlosen Transfer braucht man Banken und die Geldmengenvergrößerung verursacht eine schleichende, aber auf Dauer spürbare Geldentwertung. Kryptowährungen sind anders. Generell bewegen diese sich in einer sogenannten DLT-Umgebung. DLT steht für Distributed Ledger Technologies. „Ledger“ bedeutet so viel wie Protokoll oder Kontobuch. Dieses wird nicht zentral geführt, sondern dezentral, der Inhalt wird verteilt auf die Teilnehmer am System (engl.: distribute = verteilen). Die Idee hinter Kryptowährungen ist, dass Zahlungen von A nach B nicht zwischen zwei