

DIGITALISIERUNG

# Blöde Blöcke

Joël Adami

**Blockchain klingt nach Hightech und Fortschritt, ist aber alles andere als zukunftssträftig. Dennoch setzt Luxemburg starke Hoffnungen auf die diese Technologie.**

Blockchain, Kryptowährungen, Metaverse, NFTs – alles Begriffe, die in den letzten Jahren für viel Aufsehen in der digitalen Welt gesorgt haben und mittlerweile unter dem Schlagwort „Web3“ zusammengefasst werden (Begriffserklärungen im Kasten auf Seite 6). Da wäre zum Beispiel der kometenhafte Aufstieg so mancher Kryptowährung wie Bitcoin, der für einen Investitionsboom gesorgt hat. Oder NFTs, die digitalen Zertifikate, die als Zukunft der digitalen Kunst in den Himmel gelobt wurden. Die Blockchain, das Fundament dieser Entwicklungen, wird stets als Zukunftstechnologie gehandelt. Auch der Luxemburger Staat will mithilfe dieser Technologie die Digitalisierung vorantreiben – das ist aber wenig sinnvoll, wie Expert\*innen betonen.

Wie sehr die Luxemburger Regierung dem Blockchain-Hype verfallen ist, zeigt die Ansprache von Premierminister Xavier Bettel (DP) auf der Luxembourg Blockchain Week, die er im Rahmen des „Infrachain Summit“ hielt. „Was wir zu dieser Zeit mehr als alles andere brauchen, sind Lösungen für unsere Probleme. Diese Lösungen können nicht nur technologiebasiert sein, aber Technologie wird ein wichtiger Teil davon sein“, so der Premier. Er betonte die Erfolge von Infrachain, einem Verein, der an einer staatlich nutzbaren Blockchain-Infrastruktur arbeitet. Neben privaten Akteuren wie den Finanzplatzakteuren KPMG, PWC und Allen and Overy sind auch (para)staatliche Organisationen wie das Centre des technologies de l'information de l'État (CTIE), das Luxembourg Institute of Science and Technology (List), die Post und die Spuerkeess in dem Verein vertreten.

Mit „Erfolgen“ meint Bettel nicht etwa abgeschlossene, funktionierende Projekte, sondern erhaltene EU-Fördergelder. „Wenn du keine guten Projekte hast, kriegst du keine Fördergelder“, sagt der Premierminister dazu. Er freue sich, dass Infrachain nun vier Mitarbeiter\*innen habe und bereits

seit fünf Jahren bestehe. „Das bedeutet, dass Luxemburg die Blockchain-Technologie beherrscht, und das ist ein wesentlicher Teil unseres übergeordneten Ziels einer technologiegestützten Nation.“ Luxemburg habe die Zeichen der Zeit erkannt und gesehen, dass „etwas Großes“ passieren werde. Mittlerweile wisse sogar seine Mutter, was Blockchain und Kryptowährungen seien.

## Großer Hype, großes Schweigen

In der Tat sind rund um Blockchain und Kryptowährungen in den letzten Jahren „große Dinge“ passiert, die vor allem in großen Enttäuschungen endeten. 2018 gab es einen ersten Boom, der durch den Höhenflug des Bitcoin-Kurses gespeist wurde. Die Kryptowährungsbörse Bitflyer kündigte an, ihren Europasitz in Luxemburg zu beziehen, was den damaligen Finanzminister Pierre Gramagna zu einer jubelnden Pressemitteilung verleitete (siehe woxx 1460). Viele große Firmen – etwa der Fotogigant Kodak – und tausende Start-ups kündigten eigene Kryptowährungen an. Auch am Luxemburger Finanzplatz war das Interesse groß: Nicht nur an den Höhenflügen der digitalen Währungen, sondern auch an der dahinterliegenden Blockchain-Technologie (siehe woxx 1462). Die habe das Potenzial, die Fondsindustrie beinahe vollständig zu automatisieren und somit zu revolutionieren. Die Luxemburger Börse arbeitet seit 2016 an einer Blockchain-Lösung für Fonds namens „FundsDLT“, seit 2021 ist diese online.

Die Coronapandemie hat den Hype um Kryptowährungen als Investitionsmodell noch einmal verstärkt. Das Versprechen, schnell reich zu werden, lockte viele Menschen, die ihre Arbeit wegen der sanitären Krise kurzfristig oder für immer niederlegen mussten. Das nächste Phänomen waren die Non-Fungible Token (NFTs), die angeblich den Kunstmarkt revolutionieren sollten (siehe woxx 1631). Der Versuch, Besitztum für mehr oder weniger hässliche digitale Zeichnungen als Geldanlage zu verkaufen, dürfte in den meisten Fällen jedoch gescheitert sein. Obwohl mehrere Museen versuchten, NFT-Prägungen als besonders innovative Kunstprojekte zu verkau-

fen, ist die Relevanz eher gering. Vor allem sind die Preise und damit das Interesse stark gefallen. Die durch die Inflation ebenfalls gestiegenen Zinsen haben Kryptowährungen und NFTs als Anlageobjekte für viele uninteressant gemacht. Viele Projekte – wie etwa der „Kodakcoin“ – wurden nie realisiert oder sind sang- und klanglos untergegangen.

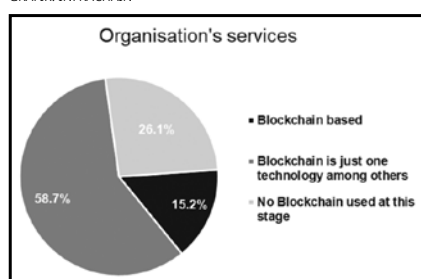
Bei dem ganzen Hype und dem Versprechen des schnellen Reichtums ging es vor allem darum, dass viele Menschen Geld in das Kryptowährungs-Ökosystem einspeisen. Wer hypothetisch Millionen in Bitcoin – oder in Form eines NFTs – besitzt, kann sich mit diesem Geld nur dann etwas kaufen, oder wenn sich genügend Käufer\*innen für die digitalen Güter finden. Es muss genügend Echtgeld im System sein, um Bitcoin in Euro umzutauschen zu können.

## Es läuft alles wunderpräftig

Der Wechsel der zweitwichtigsten Kryptowährung Ether und der damit zusammenhängenden Blockchain Ethereum vom energiefressenden „Proof of Work“ zu „Proof of Stake“ hat einige ökologische Bedenken beseitigt. Das neue System bedeutet jedoch, dass nur wenige die Blockchain, auf der sämtliche Transaktionen gespeichert werden, kontrollieren können. Das sind jene, die bereits viel Ether besitzen oder es sich leisten können, große Mengen der Kryptowährung zu kaufen. Das Versprechen einer dezentral regulierten Währung ist damit dahin.

Auf ihrem Blog „Web3 is going just great“ dokumentiert die Softwareentwicklerin Molly White die unzähligen Betrügereien, Anklagen, Insolvenzen und andere Hinweise darauf, dass im sogenannten Web3 alles „großartig“ läuft. Ein Zähler am rechten Bildschirmrand zeigt die Summe an, um die Menschen im Web3 betrogen wurden. Je tiefer man ins Archiv scrollt, umso höher wird die Summe: 11,128 Milliarden Dollar sind es laut Whites Schätzungen insgesamt. Eine theoretische Zahl, da die virtuellen Währungen und Objekte erst in echtes Geld umgewandelt werden müssten, was zunehmend schwieriger wird.

GRAFIK: INFRACHAIN



Auch unter den Akteur\*innen des Luxemburger „Blockchain Ökosystems“ ist die Blockchain für viele nur eine Technologie unter vielen.



FOTO: MICHAŁ PARZUCHOWSKI/UNSPASH

Ist die Blockchain wirklich eine innovative Kette aus Blöcken – oder doch eher ein Jenga-Turm, der demnächst zusammenfallen wird?

Obwohl Blockchain-Anwendungen wie Kryptowährungen und NFTs in den letzten Jahren vor allem für Enttäuschungen sorgten, während sich einige wenige bereicherten, ist der Hype alles andere als vorbei. Bei der Blockchain Week waren die Themen neben NFTs und „dezentralisierten Identitäten“ auch Nachhaltigkeit und Gesundheit. Die Akteur\*innen drängen also darauf, ihre Technologie in immer mehr Bereichen einzusetzen. Der Nachweis, dass sich Blockchain für irgendetwas anderes als das Management einer Kryptowährung tatsächlich anbietet, wurde nämlich noch nicht erbracht. Viele Anwendungen könnten mit einer simplen, altbekannten Datenbank schneller, effizienter und ressourcenschonender umgesetzt werden, lautet seit Jahren die Kritik von Beobachter\*innen wie White.

### Erfolg ist, wenn man aufgekauft wird

„Manchen Blockchain-Start-ups ist es egal, dass sie eine schlechte Lösung anbieten. Für sie bedeutet Erfolg, dass jemand sie finanziert oder am Ende aufgekauft – ob das Produkt so funktioniert wie es soll, ist zweitrangig“, sagt Rainer Rehak im Gespräch mit der woxx. Der Informatiker und Philosoph ist davon überzeugt, dass die Blockchain-Technologie keine Lösungen für gesellschaftliche Probleme bietet. Er promoviert aktuell zum Thema systemische IT-Sicherheit und gesellschaftlicher Datenschutz am Weizenbaum-Institut. Auf mehreren Konferenzen hielt er Vorträge zum Thema Blockchain, wie etwa im September auf der „Bits und Bäume“ zur Nicht-Nachhaltigkeit von Blockchain und Web3.

Den Eindruck, dass der tatsächliche Nutzen einer Blockchain-Anwendung eigentlich egal ist, kann man auch gewinnen, wenn man sich die Redner\*innen des Infrachain Summits ansieht. Da sprach zum Beispiel Michael Jackson von Concordium über „ein Ausweis-Ökosystem für eine Milliarde Menschen“. Das Start-up bietet Entwickler\*innen Blockchains für verschiedenste Zwecke an. Ein Blick in die bisher umgesetzten Projekte zeigt, dass es sich vor allem um NFT-Pro-

jekte handelt, bei denen mit dem Verkauf digitaler Besitztifikate schnelles Geld gemacht werden soll.

Während ein Start-up vor allem seinen Investor\*innen und Kund\*innen verpflichtet ist, ist das beim Staat anders: Steuergeld sollte möglichst nicht in unsinnige Technologien gesteckt werden. Gerade wenn administrative Prozesse digitalisiert werden, sollten sie einfacher und nicht aufwändiger werden. In Luxemburg existiert bisher ein staatliches Blockchain-Projekt: der Studienkredit.

Zwar kündigte Digitalisierungsminister Marc Hansen (DP) bereits 2019 die Schaffung einer staatlichen Blockchain an, eine Anwendung dafür gab es jedoch nicht. Seit 2021 kann man das Darlehen, das man vom Dokumentations- und Informationszentrum für die Hochschulbildung (Cedies) gewährt bekommt, vollständig digital anfragen. Davor war es nur möglich, den Antrag über die staatliche Plattform guichet.lu digital anzufordern. Die Studienbeihilfe wurde automatisch ausbezahlt, der Kredit muss jedoch bei einer Bank angefragt werden. Den Bescheiden des Cedies ist seit September 2021 ein QR-Code beigelegt, der mittels App eingescannt und so automatisch an die Bank weitergeleitet wird. Realisiert wurde das mittels Blockchain.

### Die unnötige Cedies-Blockchain

Im Studienjahr 2021-2022 haben 4.305 Studierende insgesamt 6.749 Semester-Kredite mittels QR-Code aufgenommen, teilte Tom Wenandy vom Hochschulministerium der woxx per E-Mail mit. Insgesamt gab es in dem Studienjahr laut dem Dashboard des Hochschulministeriums 62.173 Anträge auf Studienbeihilfe, davon knapp 36.763 von Studierenden mit Wohnsitz in Luxemburg. Bisher also eher ein

mäßiger Erfolg. Noch sind auch noch nicht alle Banken am Projekt beteiligt, wie Wenandy betonte: „Bis jetzt sind zwei von sechs Banken, die beim Projekt mitmachen, auf der Blockchain. Bis zum 1. August 2023 sind alle Banken auf der Blockchain und jedes Darlehen läuft darüber.“

Benötigt man für die Generierung eines QR-Codes eine Blockchain? Die Impffertifikate, die uns im Jahr 2021 begleiteten, wurden ohne Blockchain erstellt. Im Hochschulministerium sieht man dennoch Vorteile: „Die Vorteile gegenüber einer traditionellen Datenbank sind jene, die Blockchain generell gegenüber Datenbanken hat: Dezentralisierung, Rückverfolgbarkeit und Robustheit. Die Nachteile sind die Geschwindigkeit, die Komplexität und der wenig effiziente Datenspeicher.“

Die Nachteile alleine sollten eigentlich ein Ausschlusskriterium sein. Warum sollten wir im Jahr 2022 noch eine wenig effiziente Lösung nehmen, die dazu auch noch langsam ist? Was für einen Vorteil eine wie auch immer geartete Dezentralisierung bieten soll, ist ebenfalls unklar. Immerhin handelt es sich sowohl bei einer Bank als auch beim Staat um Institutionen, denen man ein Minimum an Vertrauen schenken sollte, wenn man einen Studienkredit aufnimmt. Bei näherer Betrachtung stellt sich zudem heraus, dass die Cedies-Blockchain überhaupt nicht dezentral ist.

Auf die Frage, wie denn der Energieverbrauch sei, antwortet das Hochschulministerium nämlich Folgendes: „Die Blockchain der Studienkredite basiert nicht auf dem ‚Proof-Of-Work‘-Algorithmus, sondern auf dem ‚Proof-Of-Authority‘-Algorithmus. Dadurch sind die Energiekosten für die Public Sector-Blockchain vernachlässigbar, weil das ‚Mining‘ neuer Blöcke bei uns nicht von irgendwelchen aufwändigen Rechenoperationen abhängt.“

Im Klartext heißt das: An der Blockchain-Lösung ist nichts dezentral. Das zeigt laut Rehak, wie absurd die Idee ist, staatliche Prozesse mittels Blockchain umsetzen zu wollen: „Der Sinn einer Blockchain ist es, Vertrauen für Akteure herzustellen, die sich eigentlich nicht gegenseitig vertrauen. Daher soll die Technologie dafür sorgen, dass sich alle gegenseitig kontrollieren. Eine Blockchain dafür zu benutzen, staatliche Dokumente wie etwa einen Grundbuchauszug, einen Führerschein oder ein Zeugnis zu verifizieren, ist widersinnig. Das sind Dokumente, die ohnehin von einer zentralen Stelle ausgegeben werden, die müssen nicht in eine Blockchain geschrieben werden.“

### Eine Blockchain schafft kein Vertrauen

Im Hochschulministerium sieht man dennoch Vorteile in der Blockchain-Lösung: „Die Banken sehen genau wie das Hochschulministerium in Echtzeit, welchen Status ein Darlehen hat, das der Student mittels QR-Code abschließen will: gewährt, abgeschlossen oder aufgekündigt. Die Bank kann das Darlehen nur dann ausbezahlen, wenn der Status auf „gewährt“ steht. So besteht maximale Sicherheit, dass ein Darlehen nicht zweimal ausbezahlt werden kann.“ Warum diese „maximale Sicherheit“ nicht auch anders hergestellt werden kann, ist unklar.

Infrachain, der parastaatlische Blockchain-Verein, arbeitet an anderen Projekten, unter anderem an „Ebsilux“. Damit sollen Zeugnisse in eine Blockchain gesetzt werden, was laut der Projektbeschreibung eine bessere und einfachere Anerkennung im Ausland bedeuten würde. Dafür sollte eigentlich eine digitale Signatur reichen, die als QR-Code aufgedruckt

## THEMA

wird. Da es kein Misstrauen in die ausstellende Institution – der Staat oder eine Hochschule – gibt, ist ein zentraler Server vollkommen ausreichend.

Die Blockchain ist also eine unnötig komplizierte Technologie, mit der Probleme gelöst werden sollen, die sich auch mit traditioneller, bereits bestehender Technologie lösen ließen – und das vermutlich kostengünstiger und schneller. In Luxemburg geht der Blockchain-Hype so weit, dass laut woxx-Informationen im April sogar Schulungen für Lehrer\*innen zu dem Thema angeboten wurden. Das Großherzogtum ist mit seiner Förderung von Blockchain-Lösungen längst nicht alleine, auch in unseren Nachbarländern werden viele solcher Projekte gefördert. „Die wenigsten politischen Entscheidungsträger\*innen haben das nötige technische Wissen, um evaluieren zu können, ob die ganzen Versprechungen mit einer Blockchain überhaupt umgesetzt werden können“, analysiert Rehak dieses Phänomen.

Da das Wort „Blockchain“ modern und technologiefreundlich wirkt, findet es Einzug in Wahlprogramme, Sonntagsreden und später auch in För-



Im September 2021 stellten Marc Hansen und Claude Meisch (beide DP) die Blockchain für den Cedies-Studienkredit vor. Der Einsatz der Technologie ist jedoch sinnlos.

derrichtlinien. Das beeinflusst auch, wie wirtschaftliche oder akademische Akteur\*innen sich verhalten, erklärt Rehak: „Der Hype um Blockchain-Technologien führte dazu, dass ‚Blockchain‘ zu einem Buzzword in Förderkatalogen wurde, so wie es auch Technologien wie KI oder Big Data sind. Wenn zum Beispiel ein Stadt-

werk Digitalisierung vorantreiben wollte, sah es sich gezwungen, eine Blockchain als Zwischenebene einzuziehen, obwohl die gar nicht benötigt worden wäre. So haben sie Fördergelder bekommen, an die sie anders nicht gekommen wären, weil ein normales Digitalisierungsprojekt zu langweilig klingt.“

Diese Tendenz, Blockchain als Technologie wie jede andere „mitlaufen“ zu lassen, spiegelt sich auch in der Luxemburger Blockchainlandschaft wider. In einer Umfrage, die Infrachain bei 46 Organisationen aus dem Luxemburger „Blockchain-Ökosystem“ durchgeführt hat, gaben rund 59 Prozent an, dass Blockchain nur eine Technologie von vielen sei. Bei knapp über einem Viertel der Befragten wurde überhaupt keine Blockchain eingesetzt.

Die technologischen Lösungen, von denen Xavier Bettel beim Infrachain Summit sprach, müssen sicher kommen – oder einfach umgesetzt werden, denn in vielen Fällen existieren ja bereits fertige Lösungen. Die Idee, dass der digitale Umbau der Gesellschaft mittels Blockchain-Lösungen passieren soll, sieht Rehak hingegen sehr kritisch: „Wer Gesellschaft und Staat mit Blockchain optimieren will, hat nicht verstanden, wie Gesellschaft funktioniert und welche Rolle Aushandlungsprozesse und Vertrauensbildung dabei spielen. Das kann nicht in einer Blockchain abgebildet werden.“

## Begriffserklärungen

### Kryptowährung

Digitale Vermögenswerte, die als Tauschmittel funktionieren können. Wer wie viele Einheiten der Währung besitzt, ist in einer dezentralen Datenbank, der sogenannten Blockchain, festgeschrieben. Der Name stammt von der Kryptografie, die benutzt wird, um die Transaktionen fälschungssicher in die Blockchain zu schreiben.

### Bitcoin

Die wichtigste Kryptowährung existiert seit 2009. Um unabhängig von Banken oder anderen zentralen Stellen zu sein, sollen alle Transaktionen in der Blockchain festgehalten werden. Ein dezentrales Netzwerk soll dafür sorgen, dass keine einzelne Person oder Institution die Kontrolle über die Transaktionen hat, sondern ein Konsens besteht. Dies wird über die „Proof of Work“-Technologie abgewickelt. Der Kurs gegenüber dem Dollar ist seit einem Boom im Jahr 2018 enorm gestiegen, seit Anfang 2022 ist er allerdings wieder stark gefallen.

### Ether(um)

Ether ist die zweitgrößte Kryptowährung, die dazugehörige Blockchain nennt sich Ethereum. Sie besteht seit 2015. Auf der Ethereum-Blockchain können sogenannte „Smart Contracts“ ausgeführt werden, also Verträge, die automatisch als Programme ausgeführt werden. Seit August 2022 ist Ethereum von Proof of Work auf den Proof of Stake-Algorithmus gewechselt. Dadurch soll sich der Energieverbrauch um 90 Prozent gesenkt haben.

### Blockchain

Eine kontinuierlich erweiterbare Liste von Datensätzen, die in einzelnen Blöcken gespeichert

werden. Jeder neue Block wird mit einem kryptografischen Verfahren an die bestehende Kette angehängt. Dies passiert, indem aus den bereits bestehenden Blöcken ein sogenannter Streuwert (englisch „Hash“) errechnet wird. Dadurch ist es nicht möglich, die früheren Blöcke anzuzweifeln oder zu ändern. Eine Blockchain wird also stets wachsen. Ihr können nur neue Daten hinzugefügt werden, keine alten gelöscht oder geändert werden. Typischerweise gibt es ein sogenanntes Konsensverfahren, mit dem neue Blöcke von allen Teilnehmer\*innen im Netzwerk akzeptiert werden. Beispiele hierfür sind Proof of Work oder Proof of Stake. In der Blockchain können nicht nur Transaktionen von Kryptowährungen festgeschrieben werden, sondern alle möglichen anderen Daten, zum Beispiel die Besitzverhältnisse von NFTs.

### Proof of Work

Um eine Transaktion in der Blockchain bestätigen zu können, müssen Rechner, die sich an dem Netzwerk beteiligen, eine stets schwieriger werdende Rechnung lösen, also „Arbeit“ verrichten. Im Gegenzug erhalten sie eine neu geschaffene Einheit der Kryptowährung, etwa einen Bitcoin. Diesen Prozess nennt man Mining. Die benötigte Rechenleistung wächst beim Proof of Work-Konzept stets an. Somit werden immer leistungsfähigere Rechner oder ganze Rechenzentren und immer mehr Energie benötigt.

### Proof of Stake

Ein Algorithmus, mit dem Transaktionen in einer Blockchain validiert werden können. Im Gegensatz zu Proof of Work wird nicht die Lösung schwieriger mathematischer Gleichungen verlangt, sondern der Besitz einer bestimmten Menge einer Kryptowährung. Unter allen, die dieses „Stake“ besitzen, wird zufällig ausgelost, wer den neuen Block schreiben darf. Dadurch verbrauchen die Transaktionen weniger Energie, Akteur\*innen mit

hohem Kryptowährungsvermögen gewinnen jedoch an Macht.

### Proof of Authority

Bei diesem Algorithmus, um Transaktionen in einer Blockchain zu validieren, gibt es keine oder kaum Dezentralisierung. Ein oder mehrere Rechner haben einfach die Autorität, neue Blöcke in die Blockchain zu schreiben. Das ursprüngliche Prinzip eines dezentralen Netzwerks, in dem sich die einzelnen Akteur\*innen nicht vertrauen, wird damit untergraben. Es wird vor allem bei Blockchains eingesetzt, an denen sich nur wenige Stellen, zum Beispiel der Staat und ein paar Banken, beteiligen.

### Distributed Ledger Technology (DLT)

Wörtlich übersetzt steht DLT für „verteilte Kassenbücher-Technologie“. Es handelt sich um einen generelleren Namen für die Blockchain-Technologie. Oft werden die Begriffe synonym verwendet. Besonders in der Finanzwirtschaft wird jedoch gerne von DLT gesprochen, um sich von wenig vertrauenswürdigen Kryptowährungen abzugrenzen.

### Mining

Bezeichnet den Prozess, mit dem ein neuer Block in die Blockchain geschrieben und validiert wird. Es existieren verschiedene Konzepte wie etwa Proof of Work oder Proof of Stake. Meistens werden die Rechner, die sich am Mining beteiligen, mit einer neuen Einheit der Kryptowährung belohnt.

### NFT (non-fungible token)

Eine nicht austauschbare Einheit von Daten, die in einer Blockchain gespeichert ist und verkauft und gehandelt werden kann. NFTs können mit digitalen Dateien wie Fotos, Videos und Audios verbunden sein. Sie gelten als Besitzzertifikate für diese Dateien. Anders als Kryptowährungen können NFTs nicht in kleinere Einheiten gespalten werden.