Per Anhalter durch die Blockchain

Marcel Waldvogel • DNIP • 2022-04-11

Blockchain, Kryptowährungen, Smart Contracts, Web3 und NFTs sind zur Zeit in aller Munde. Fast jeder hat dazu eine Meinung, aber kaum jemand versteht die Hintergründe und Zusammenhänge. Diese Artikelserie bietet eine strukturierten Einordnung von Versprechen, Technik und Realität; allgemeinverständlich erklärt an praktischen Beispielen wie weltraumfahrenden, anarchistischen Notaren. Hier ist der druckfrische Teil 1 einer Trilogie in fünf Bänden: Die eigentliche Blockchain, Kryptowährungen, Smart Contracts, Web3 und NFTs.

Lösungen auf Blockchain-Basis werden schon seit Jahren als Antwort auf jedes Problem gehandelt, was nur halbwegs mit IT, Digitalisierung, Demokratie und Gesellschaft zu tun hat. Wie immer, wenn es um Neues geht, tauchen Denker, Goldgräber, Trittbrettfahrer, Scharlatane und Endzeitpropheten auf und erschweren den Durchblick. Das Ziel dieser Serie ist es, sowohl Neulingen als auch Kennern einen verständlichen, fundierten Einblick zu geben. Insbesondere, soll–so gut es bei diesem sehr komplexen Themengebiet möglich ist–Eigenschaften und Zusammenhänge transparent, fundiert und strukturiert vermittelt werden. Einleuchtende und eingängige Metaphern dürfen dabei natürlich nicht zu kurz kommen.

Dazu wird das Themengebiet in die folgenden fünf Schichten aufgeteilt:

1. Die eigentliche **Blockchain**, in der die Daten transparent und unveränderlich gespeichert werden (hier in diesem Artikel),
2. den darauf aufsetzenden **Kryptowährungen** wie Bitcoin und deren Verwandten, welche das Finanzsystem revolutionieren sollen (in einem Folgeartikel),
3. **Smart Contracts**, «intelligente Verträge», die als Verallgemeinerungen von Kryptowährungs-Transaktionen auch komplexe Verträge abbilden sollen (in einem Folgeartikel).

Auf diesen Smart Contracts wiederum bauen auf:

4. Non Fungible Tokens (**NFTs**), in etwa «nicht-austauschbares digitales Objekt», digitale Kunstwerke, welche den Kunsthandel und das Urheberrecht revolutionieren wollen (in einem Folgeartikel); und
5. das Versprechen eines demokratisierten Internets, des Web 3.0 oder auch **Web3**, das unter anderem Dezentrale Autonome Organisationen (DAO) ermöglichen soll (in einem Folgeartikel).

Jede dieser fünf Schichten wird zuerst in vier Kapiteln möglichst verständlich und objektiv analysiert, gefolgt von einer persönlichen Bewertung und einer Liste von Fragen zum Mitnehmen. Aufgrund der Komplexität der Materie ist diese strikte Trennung nicht immer aufrechtzuerhalten, aber ich versuche es zumindest.

1. Welche **Hoffnungen und Versprechungen** hinter der entsprechende Technologie stehen und welche Problem sie lösen sollen.
2. Einen allgemeinverständlichen Überblick über die Funktionsweise der **zugrundeliegenden Technik** und über ihre Möglichkeiten und Grenzen.
3. Ist die Blockchain-basierte Lösung die einzige Möglichkeit, dieses Problem anzugehen? Wenn nein, welche **Alternativen** gibt es?
4. Wie sieht eigentlich die **Realität** hinter den Versprechungen aus?
5. Eine subjektive **Bewertung** der Technologie auf Basis der obigen vier Punkte.
6. Eine Liste von **Fragen**, die sich jeder stellen sollte, bevor er (mehr) in die jeweilige Schicht investiert, sowohl technologisch als auch finanziell.

Also, strecken wir alle gemeinsam unsere elektronischen Daumen hoch, stecken die Babelfische in die Ohren und ab geht die Post! Erster Halt: Die grundlegende Schicht, die Blockchain selbst.

Ich habe versucht, den ganzen Text neutral zu schreiben. Doch im Laufe meiner Recherchen habe ich zwei Dinge gelernt:

- Von den Blockchain-Verfechtern wird kritisiert, dass das aktuelle Wirtschaftssystem von Gier, Ineffizienz, Intransparenz und übermässiger Komplexität geprägt sei. Aber das Ziel, auf das die Verfechter hinarbeiten, ist ein neues, nun digitales Wirtschaftssystem, welches von Gier, Ineffizienz, Intransparenz und übermässiger Komplexität geprägt wird.
- Wann immer ich nach dem konkreten Vorteil von Blockchain-basierten Technologien gegenüber einem Ansatz ohne Blockchain gefragt habe, wurden die Antworten ausweichend oder widersprüchlich.

Trotzdem denke ich, dass dieses Umfeld eine sachliche Betrachtung verdient hat, weil durch das Blockchain-Umfeld etliche wichtige Fragen aufgeworfen werden, die für unseren Zukunft als Gesellschaft und unseren Umgang mit Technik relevant sind. Schon alleine, dass der Begriff «Blockchain» sich eine Dekade lang in den Buzzword-Charts halten konnte, erfordert eine vertiefte sachliche Betrachtung mit dem Phänomen.

Teil 1: Die Blockchain

TL;DR (oder das Summary für alle, die keine Manager sind)

- «Hinreichend fortschrittliche Technologie ist nicht von Magie zu unterscheiden», aber wenn eine Technologie als Magie verkauft wird, sollte man unbedingt fragen, ob sie auch nur dazu taugt. (Oder anders gesagt: Wenn etwas zu gut scheint, um wahr zu sein, ist es das häufig auch.)
- «Wenn Sie einen Scheissprozess mit einer Blockchain versehen, haben Sie einen Scheiss-Blockchain-Prozess». (Oder anders gesagt: Gute Lösungen entstehen nicht quasi automatisch durch Einkauf von Beratern oder Technologie, schon gar nicht, wenn diese neue Komplexität und Ineffizienzen mit sich bringen.)
- Eine gute Idee alleine ist nicht automatisch Teil einer guten Lösung. (Oder anders gesagt: Auch ein Hammer sollte mal andere Freunde kennenlernen als nur Nägel.)
- Vertrauen erhöht die Effizienz und reduziert Komplexität. Blockchainlösungen wollen auf jegliche Form von Vertrauen verzichten. Sie erkaufen sich dies mit Ineffizienz und Komplexität. (Oder anders gesagt: Komplexität ist der Feind von Sicherheit, Transparenz, Effizienz und Vertrauen.)

Dies ist kein «Management Summary» sondern ein «Summary für Nicht-Manager» (bzw. Nicht-Entscheidungsträger), weil ich der Meinung bin, dass ganz besonders Entscheidungsträger so viel von einer als revolutionär gehandelten Technologie verstehen sollten, dass sie auch die richtigen Fragen stellen können, um Blendwerk von echtem Nutzen zu unterscheiden.

Die Blockchain wurde als Lösung für ein ganz spezifisches, besonders komplexes Problem geschaffen. Für dieses Problem mag es–direkt angewandt–eine gute Lösung sein. Für die meisten anderen Prozesse ist es massives Over-Engineering, da bereits kleine Änderungen an den Vorbedingungen zu deutlich effizienteren Lösungen führen. Um diese Faktoren zu kennen und zu begreifen ist aber ein tiefer gehendes Verständnis nötig. Und genau dies ist das Ziel dieses Textes.

Der Text ist im Laufe seines Entstehens grösser geworden als geplant. Er hat aber dadurch auch an Lesbarkeit und Verständlichkeit gewonnen. Anders gesagt, er wurde *gerade* mit dem Zielpublikum Führungskräfte und Entscheidungsträgerinnen (und Grossväter und Enkelinnen) geschrieben: Viele einprägsame Analogien und erklärende Vergleiche mit der realen Welt, auch geeignet, um ein Geschäfts- oder Familienessen aufzulockern.

Ich finde, der Text verdient Chance: Der Vorteil von Text ist, dass man jederzeit einzelne Passagen überfliegen kann und ihn später reumütig doch noch lesen, ohne dass er das einem übel nimmt. Die oft überspitzten, farbig hervorgehobenen Einleitungssätze eines Kapitels helfen hoffentlich bei diesen Leseentscheidungen.

Die Blockchain und mit ihr der Bitcoin entstanden zum Höhepunkt der Finanzkrise 2008. Sie sind als Gegenbewegung zur Rolle der Banken in dieser Krise zu sehen, die mit intransparenten Finanzprodukten auf schlechten Hypothekarrisiken zuerst Gewinne und nachher, bedingt durch ihre Systemrelevanz («too big to fail»), Rettungsgelder erwirtschafteten. Entsprechend zieht sich auch der Wunsch zur Transparenz und nach Unabhängigkeit von zentralen Organisationen (Banken, Staaten) als Leitmotiv durch alle Ebenen des Blockchain-Ökosystems.

Diese Entwicklung trägt die Handschrift der Kryptoanarchie und des Anarchokapitalismus, also von Bewegungen, welche Vertrauen in Organisationen und Strukturen vermeiden wollen und insbesondere dem Staat misstrauen. Vertrauen verdienten nur Programme («Code is Law,» (Programm-)Code ist Gesetz) oder freie, d.h. unregulierte, Märkte. Diese Handschrift zieht sich durch alle Ebenen, auch wenn sie bei den Kryptowährungen und Smart Contracts am stärksten sichtbar sind.

Versprechungen

Das einzige Kapitel, das Ihnen Blockchain-Enthusiasten empfehlen würden.

Da Blockchain und Bitcoin gleichzeitig entstanden sind, wird der Begriff **Blockchain** umgangssprachlich (*pars pro toto*) für darauf aufsetzende **Anwendungen** (Kryptowährung, Smart Contracts etc.) sowie das jeweilige **Ökosystem** verwendet. Im Rahmen dieser Serie versuche ich, die Begriffe klar zu trennen.

Die vier bis sechs Eigenschaften (Tabelle 1), die eine Blockchain hat bzw. haben soll, sind nicht einheitlich definiert:Sehen wir uns exemplarisch die vier Kategorien aus Christian Cachins Präsentation an:

- Eine **verteilte Buchführung** (engl. «distributed ledger») als Transaktionsliste mit unveränderlicher Vergangenheit.

Wikipedia	Christian Cachin/IBM	MoreThanDigital
Verkettung	Verteilte Buchführung	Datenintegrität
Dezentrale Speicherung	Kryptographie	Zuverlässigkeit
Konsens	Verteilter Konsens	Schnelle Speicherung
Manipulationssicherheit	Geschäftsprozesse	Analyse, Transparenz
Transparenz, Vertraulichkeit	—	—
Nichtabstreitbarkeit	—	—

Tabelle 1: Eigenschaften der Blockchain

- **Kryptographie** zur Gewährleistung der Integrität der Buchführung und Authentizität der Transaktionen.
- Verteilter, ausfalltoleranter **Konsens** über den Inhalt der Buchhaltung und die Validität der Transaktionen: Alle Blockchain-Teilnehmer sollen sich auf eine einheitliche Weltsicht (z.B. Kontostände) einigen können, auch wenn nicht immer alle Teilnehmer verfügbar sind.
- **Geschäftsprozesse** («business logic»), welche die Validität der Transaktionen gewährleisten und diese umsetzen sollen (Kontoführung, Smart Contracts, …). Diesen Bereich verschieben wir auf die nächsten beiden Artikel.

Das ist sehr abstrakt, insbesondere, wenn unklar ist, was damit eigentlich erreicht werden soll. Da sich dieser Artikel vorgenommen hat, die komplexe Materie klar zu strukturieren: Wozu möchte man aber diese Eigenschaften nutzen? Schauen wir uns also eine typische «10 Anwendungen für Blockchain»-Liste an und extrahieren bzw. strukturieren dann die dort aufgezählten Nutzen:

- **Internationale Finanztransaktionen:** Datenkonsistenz, Manipulationssicherheit, keine Intermediäre → geringere Transaktionskosten und höhere Transaktionsgeschwindigkeit.
- **Gesundheitswesen:** Ablage in verteiltem Netz erlaubt Speicherung sensibler Daten: Patientenakte, medizinische Befunde und Krankheitsverläufe. Zugriff nur vom Eigentümer freigeschaltete Nutzer.
- **Identitätsmanagement:** Ausweisdokumente digital sicher umsetzbar, keine Datenverluste; sicherer und schneller.
- **Vermeidung von Geldwäsche:** Transparenz, Aufzeichnungen und Zuordnung.
- **Versicherungen:** Smart Contracts zur Abwicklung von Schadensfällen, Erkennung von Versicherungsbetrug.
- **Supply Chain Management:** Einfachere Verträge, kontinuierliches Tracking der Güter, transparente Dokumentation der Lieferketten vom Ursprung in den Laden. Schnellere/einfachere/günstigere Nachforschungen.
- **Mobilität:** Zugriffsrechte, Dokumentation von Eigentum, automatische Fahrzeugmiete+Abrechnung, sichere Abrechnung auch bei Elektrifizierung.
- **Energiemarkt:** Umgang mit Wandel, Nachvollziehbarkeit von Transaktionen (private Energieeinspeisung), Abrechnung/Bezahlung an E-Tankstellen.
- **Digitale Wahlen:** Keine Angst vor Manipulation, Nachverfolgung jeder Stimme.
- **Zertifikate (Abschlusszeugnisse):** Nicht fälschbare Abschlüsse/Zertifikate ausstellen, international anerkannt.

Diese Themen decken ein breites Spektrum ab, von der eigentlichen Blockchain über Kryptowährungen bis zu Smart Contracts. Es wäre grossartig, wenn damit so viele offenen Probleme der modernen Zivilisation gelöst werden könnten. Da dies in den letzten 14 Jahren aber nicht passiert ist, scheint es doch nicht ganz so einfach zu sein.

Schauen wir uns im folgenden (grossen) Technikkapitel die Eigenschaften und Techniken an, mit denen diese Herausforderungen gelöst werden sollen, bevor wir uns an den Realitätscheck machen. Da wir uns hier auf die eigentliche Blockchain fokussieren, werden wir am Ende dieses Kapitels die Bereiche Datenkonsistenz/Manipulationssicherheit, Vermeidung von Datenverlusten, Transparenz/Aufzeichnungen und (teilweise) Zuordnung/Nachvollziehbarkeit/Fälschungssicherheit aufgreifen. Den Rest der Punkte schauen wir in den nachfolgenden Kapiteln genauer an, nachdem die dafür notwendigen Grundsteine gelegt wurden.

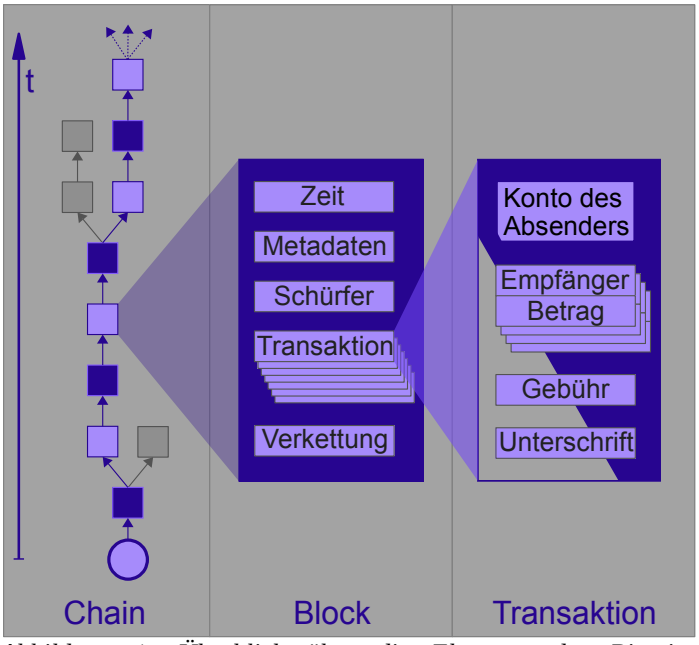

Abbildung 1: Überblick über die Elemente der Bitcoin-Blockchain. Links, die eigentliche Chain, eine Verkettung von Blöcken. Jeder Block (Mitte) beinhaltet insbesondere eine Liste von Transaktionen (Rechts).

Technik

Das Kapitel, in dem der schier undurchdringliche Dschungel erkundet und kartiert wird.

Schon alleine die Technik der untersten Ebene ist ziemlich komplex. Bevor wir in die Tiefe gehen, hier ein Überblick, basierend auf Bitcoin.

Die Bitcoin-Blockchain besteht aus einer Kette aus Blöcken («Chain» im rechten Bild), die im Verlaufe der Zeit wächst. (In Ausnahmefällen kann sie sich auch verzweigen, wie wir weiter unten noch sehen werden.)

Aktuell ist die Bitcoin-Blockchain rund 725 000 Blöcke lang und etwa alle 10 Minuten kommt ein neuer hinzu. Jeder dieser Blöcke beinhaltet eine Sammlung von Transaktionen. Verwaltet wird das ganze gemeinsam (im Konsens) von den Rechnern (Knoten), die das System aufbauen und wo eigentlich jeder mitmachen kann (es braucht keine spezielle Berechtigung).

Um das Zusammenspiel zu verstehen, sehen wir uns das in mehreren Teilschritten an, die zusammen ein Inhaltsverzeichnis dieses Technikkapitels ergeben:

1. Die Struktur und Funktion der Blockchain.
2. Wie ein Block hinzugefügt wird, obwohl kein Dienstplan existiert (der Konsens).
3. Wie die Knoten miteinander kommunizieren (das Peer-to-Peer-Netzwerk).
4. Wieso sich das jemand antut (der Anreiz).
5. Wie ein gültiger Block erzeugt wird (das Mining und «Proof of Work»).
6. Wie man das sonst noch regeln könnte («Proof of Stake» und Freunde).

Danach folgt eine kurze Zusammenfassung, damit man nach lauter Bäumen den Wald wieder sieht.

Bevor wir eine digitale Blockchain analysieren, bauen wir uns eine Analogie mit Papier und Büros und schauen zu, anarchische Buchhalter oder Notare eine fälschungssichere Loseblattsammlung führen würden. Wer will (und die Hitchhiker's-Guide-Hintergründe kennt), darf sich diese gerne als Mitglieder der golgafrinchanischen «B»-Arche vorstellen.

Analogie: Notariat

Das Unterkapitel, in dem wir uns eine unveränderliche Loseblattsammlung bauen.

Beginnen wir unsere Annäherung an die Blockchain-Technik mit einer Analogie aus der analogen Welt: Einer anarchischen Mischung zwischen Buchhaltung und Notariat. (Als Jungnotare dürfen sie vorerst nur mit kleinen Finanzwerten jonglieren. In späteren Kapiteln dürfen sie dann auch Verträge und Transfers von Sachwerten beglaubigen. Deshalb nennen wir sie auch jetzt schon «Notare», auch wenn sie vorerst eher Buchhaltung betreiben.)

```
Transaktionsliste #1
vom 2022-02-22:

1. Hans → Regula: 500 CHF
2. Karin → Peter: 800 CHF

Die Richtigkeit bestätigt
Notarin Nora
```

Abbildung 2: Erstes gestempeltes Loseblatt

Aus Effizienzgründen teilen sich mehrere Notare die Arbeit. Weil sie es alle mit dem Rücken haben, wurde das grosse, schwere Notariatsbuch mit den gesammelten Bestätigungen der letzten Jahrhunderte abgeschafft. Stattdessen wird eine (bei Juristen sowieso viel beliebtere) Lo-

Abbildung 3: Zweites Loseblatt mit Kopie des ersten

seblattsammlung verwendet. Am ersten Tag (Abbildung 2) füllt also die zuständige Notarin die Liste der Transaktionen aus und bestätigt ihre Richtigkeit mit ihrem amtlichen Stempel.

Am nächsten Tag (Abbildung 3) wiederholt der diensthabende Notar dasselbe Prozedere. Damit aber keiner der Notare später das Blatt vom Vortag durch ein anderes ersetzen kann, beinhaltet seine heutige Liste eine verkleinerte Kopie der gelben Liste vom Vortag. Diese Zusammenstellung stempelt er am Abend wie gewohnt zur Bestätigung der Richtigkeit.

Am dritten Tag (Abbildung 4) wiederholt sich der Vorgang mit einem dritten Notar. Auch dieser stempelt am Abend seine Liste zusammen mit einer verkleinerten Kopie der Liste vom Vortag, auf der wiederum eine verkleinerte Kopie des vorletzten Tages zu erkennen ist und so weiter.

So erzeugen die Notare koordiniert eine gemeinsame Kette von Dokumenten. In dieser Kette kann kein vorheriges Dokument ausgetauscht werden, ohne dass gleichzeitig alle nachfolgenden Dokumente ebenfalls angepasst werden müssten. Und das würde definitiv auffallen.

Koordination bedingt aber auch Vertrauen und Anerkennung von Autorität. Weiter unten werden wir sehen, wie wir die Papier-Blockchain auch ohne diese vorherige Absprache (und damit Vertrauen in irgend jemanden) lösen können, denn das ist auch die kryptoanarchische Grundlage für die digitale Blockchain.

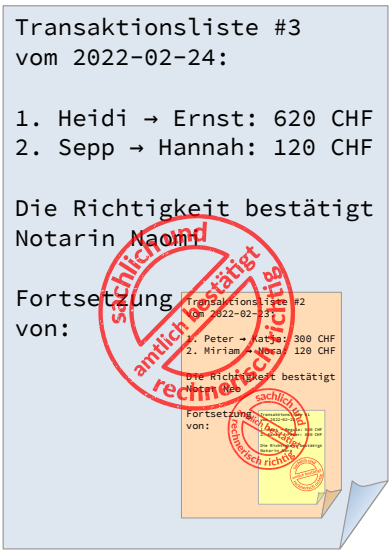

Abbildung 4: Drittes Loseblatt mit Kopie des zweiten, auf dem auch das erste sichtbar ist

Der Einfachheit halber haben unsere Junior-Notare vorerst einen festen Arbeitsplan und lieben ihre Freizeit, also gibt es keine Konflikte, wer für welchen Tag zuständig ist. Dies wird

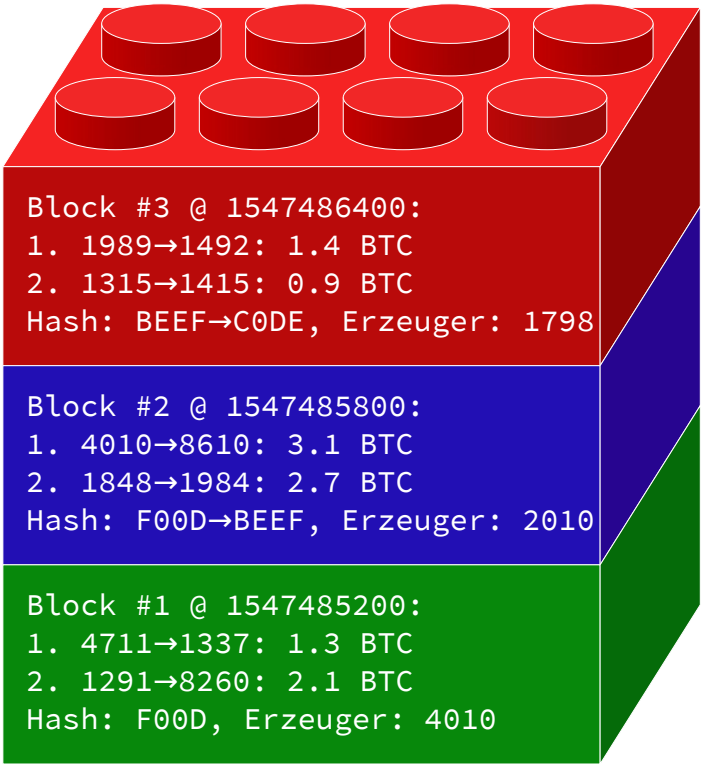

Abbildung 5: Die Blockchain als gestapelte Lego-Blöcke

sich noch ändern, wenn wir uns der realen Blockchain nähern.

Die digitale Blockchain

Das Unterkapitel, in dem wir die Loseblattsammlung mit Legosteinen digitalisieren.

Wechseln wir zur digitalen Blockchain, so wie sie beispielsweise von Bitcoin verwendet wird. Sie funktioniert sehr ähnlich wie die obige Loseblattsammlung: Jeder Block besteht aus einer Liste von Transaktionen und jemand bestätigt die Liste. Dieser Jemand ist hier allgemein der «Erzeuger»; bei Kryptowährungen wird er meist «Miner» genannt.

Über jeden Block kann man eine kryptografische Prüfsumme, einen sogenannten Hash, berechnen und die Prüfsumme des Vorgängerblocks wird–analog zur verkleinerten Kopie des Vortags im Notariatsbeispiel–im aktuellen Block abgespeichert. Damit ist der neue Block unabänderlich an seinen Vorgängerblock und indirekt damit auch an alle dessen Vorfahren gebunden.

Zum genaueren Verständnis passen wir unsere stapelbaren Blöcke etwas an: Statt des immer gleichen, regelmässigen Legomusters, bei dem jeder Stein auf jeden anderen passt, hat nun jeder Block ein eindeutiges Punktemuster oben, entsprechend seinem einmaligen Hash (Abbildung 6). Der nachfolgende Block muss nun—wie Schlüssel und Schloss—genau das dazu passende Lochmuster haben,

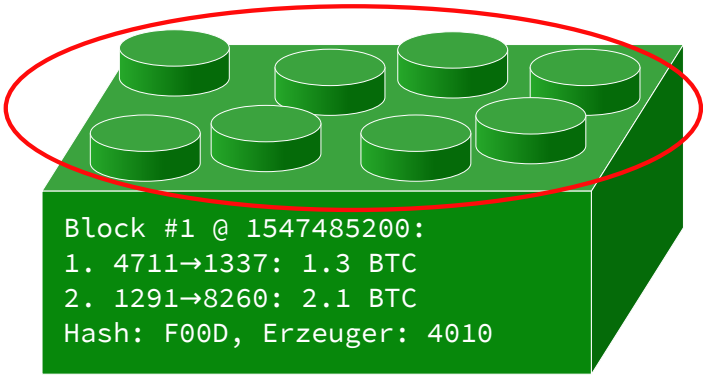

Abbildung 6: Jeder Block ist einmalig (besonders sein Abschluss)

damit die beiden Blöcke gestapelt werden können (Abbildung 7).

Die Eigenschaften der verwendeten Hashes sind so, dass auch wenn alle Computer dieser Welt über Jahrmilliarden nichts anderes tun würden, sie keinen zweiten Block finden könnten, der denselben Hashwert besitzt. Im Endeffekt haben wir damit eine perfekte Verkleinerung des Vorgängerblocks im aktuellen Block gespeichert: Anstelle der 1-2 Megabyte, die ein typischer Vorgängerblock belegt, werden nur 32 Byte oder rund 50 000x weiger verwendet.

(Im Gegensatz zur Papieranalogie, wo man aus der etwas verkleinerten Kopie immer man noch alle Details direkt herauslesen kann, ist es jedoch unmöglich, nur aus dem Hash irgendwelchen Inhalt des Vorgängerblocks herauszulesen. Der eigentliche Zweck sowohl von Papierkopie als auch Hash–die *eindeutige Identifikation* des Vorgängerblocks–ist in beiden Fällen vollständig erfüllt.)

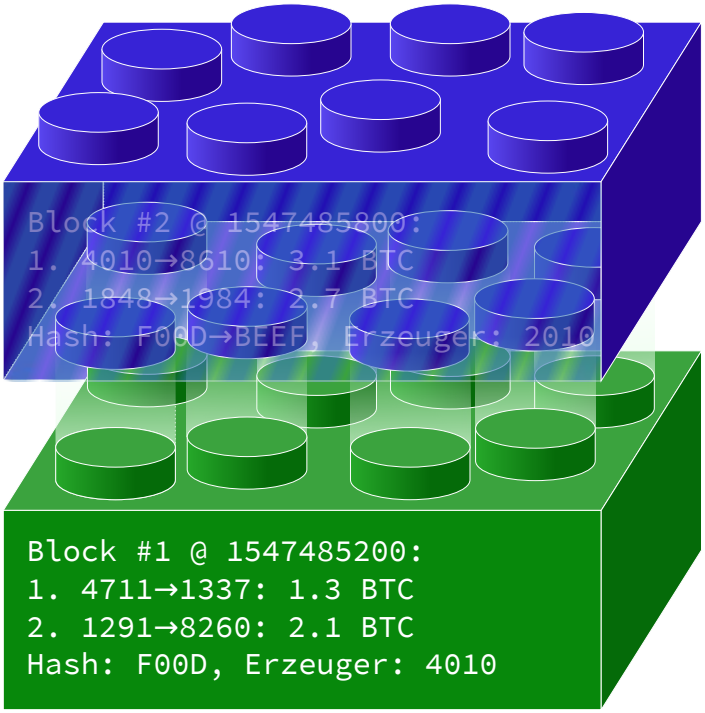

Abbildung 7: Der nächste Block muss die passenden Löcher aufweisen, sonst ist nichts mit Stapeln

Abbildung 8: Wohl die bekanntesten Beispiele solcher Selbstorganisation liefern Fisch- und Vogelschwärme. Vielleicht erinnern sich einige von Ihnen an die überspitzte (und damit besonders eingängige) Darstellung der Mondfische in «Findet Nemo». (Bild: adiprayogo liemena bei Pexels)

Gesucht: Notare ohne Dienstplan

Das Unterkapitel, in dem wir die Notare befreien und sie endlich selbstbestimmt leben und arbeiten dürfen.

Unsere Notarinnen und Notare hatten bisher einen klaren Dienstplan: An jedem Tag war genau eine einzige Person für das Führen der Liste zuständig. Dafür haben sie sich einvernehmlich abgesprochen oder ihre Chefin hat sie so eingeteilt. Bitcoin ist ein Kind sowohl der Krypto-Anarchie als auch der Empörung über das Verhalten der zentrale Machtstrukturen in der Finanzkrise; entsprechend *darf* da auf keinen Fall eine irgendwie geartete Vorgesetztenrolle existieren! Egal wie nützlich sie ist, wenn es um Steigerung der Effizienz von Koordination und Schaffung von Regeln geht: Irgendwann einmal *könnte* ein Chef seine Macht missbrauchen und es gäbe innerhalb des Systems keinen Mechanismus, dies zu verhindern.

In der realen Welt gibt es Mechanismen zur Absetzung einer solcher missbräuchlichen oder korrupten Vorgesetzten, aber diese Korrekturen können mitunter langwierig und mühsam sein. Damit in der realen Welt solche Entwicklungen möglichst häufig früh erkannt werden können und rechtzeitig Gegensteuer gegeben werden kann, hat der Mensch in seiner Entwicklungsgeschichte Mechanismen wie Ehrlichkeit, Empathie und Vertrauen geschaffen. Diese benötigen aber regelmässige Interaktion und skalieren deshalb nicht auf 8 Milliarden Menschen. Und passen sowieso nicht in das kryptoanarchische Weltbild, nachdem man sich von niemandem abhängig machen will.

Damit bleibt nur noch die Absprache zwischen den Notaren als Ansatz, der oben schon angesprochene Konsens. Wir haben aber nicht nur keine Chefin, die einen Dienst-

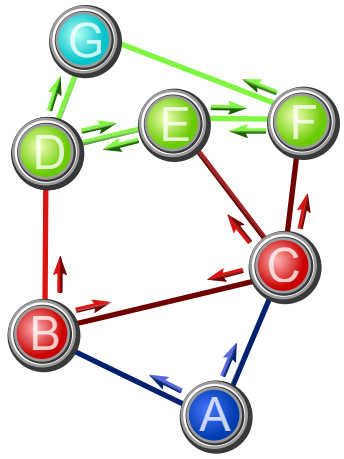

Abbildung 9: Ein Netzwerk, um sie alle zu (ver-)binden

plan macht, wir haben auch keine Chefin, die Notare einstellt oder sie zurückpfeift, wenn einer der Notare halt mal gerade keine Lust haben sollte, zur Arbeit zu erscheinen. Das heisst, wir brauchen ein System, das mit einer ständig wechselnden Menge an Notaren zurechtkommen muss, die alle auch vorher keinen Eignungstest ablegen wollen und ihre An- und Abwesenheiten auch vorher nicht ankündigen möchten. Das reinste Chaos. Oder, etwas netter, ein selbstorganisierendes (oder, gebildeter) autopoietisches System.

Menschlichen Gruppen sind deutlich weniger homogen als Fischschwärme; entsprechend gibt es kaum selbstorganisierende Gruppen mit mehr als einem Dutzend Menschen. Spätestens für grössere Gruppen bilden sich deshalb Strukturen für die Arbeitsteilung heraus. Diese reduzieren bei standardisierten Arbeitsabläufen den Koordinationsaufwand und erhöhen damit die Effizienz. Aber genau diese Strukturen und die damit einhergehenden Machtpositionen und Abhängigkeiten will man bei Kryptowährungen vermeiden. Dies geht auf Kosten der Effizienz, wie im Folgenden erläutert.

Struktur des Notariats

Das Unterkapitel, in dem die Notariate aus ihren Home-Offices miteinander zu kommunizieren lernen.

Damit unser papierbasierten Notare zusammen ein Notariat bilden können, brauchen wir dazu sowohl

1. eine organisatorische Struktur (in diesem Unterkapitel) und
2. ein Anreiz- bzw. Strafsystem (Zuckerbrot und Peitsche), also einen Ersatz für Chefinnen und Löhne, welches wir uns im Folgekapitel ansehen.

Zuerst zur Struktur: Alle, die sich als Notare versuchen wollen, werden zum Zwecke des Informationsaustausch Teil eines Netzwerks von gleichberechtigten Partnern, im Englischen auch als «Peer» bezeichnet. In diesem so aufgebauten Peer-to-Peer-Netzwerk werden (1) Transaktionen, welche in die Blockchain aufgenommen werden sollen, allen mitgeteilt und (2) die neu geschaffenen fertigen Blöcke (oder in der Analogie die gestempelten Papierzettel) gemeinsam gespeichert.

Dieses Peer-to-Peer-System ist eine Ansammlung von Rechnern («Knoten», in der Abbildung 9 die Kreise mit den Buchstaben) und einer Anzahl Verbindungen (Kanäle oder «Kanten») zwischen ihnen, über die Nachrichten ausgetauscht werden können. Hat jetzt der blaue Knoten A eine neue Nachricht, schickt er sie, gekennzeichnet durch die blaue Pfeile, an alle seine Nachbarn; in diesem Falle B und C. Wenn die Information für diese beiden neu ist und gültig aussieht, senden sie die Information wiederum weiter an alle ihre anderen Nachbarn: So sendet B die Nachricht an C und D (rote Pfeile); A wird ausgespart, da B die Nachricht ja von dort empfangen hat und damit weiss, dass A diese Informationen schon kennt.

C wiederum sendet die Nachricht an seine Nachbarn B, E und F. Auf der Verbindung zwischen B und C ist die Nachricht in beide Richtungen einmal unterwegs, da zum Zeitpunkt des Versands B und C noch nicht wissen, dass das jeweilige Gegenüber die Nachricht bereits kennt.

Dieses sogenannte «Flooding» sorgt für eine (winzige) Flutwelle, die von A nach G durch das ganze System an Kanälen schwappt. Viele der Teilnehmer erhalten die Nachricht mehrfach, im schlimmsten Fall je einmal von jedem Nachbarn. Nicht sehr effizient, aber so ist das nun einmal, wenn man niemandem trauen kann oder will.

Schlussendlich bedeutet das nun für unsere Notare, dass sie ihre Freizeit in den Kamin schreiben können: Dies ist zwar nicht besonders motivationsförderlich, dafür aber robust gegen den Ausfall (oder gar Böswilligkeit) von einzelnen Teilnehmern. Mangels zentraler Autorität fehlen Möglichkeiten für Sanktionen, also muss jeder zuerst für sich selbst schauen und sich möglichst wenig auf Andere verlassen. Aus dem kryptoanarchischen Blickwinkel ist diese Verschwendung besser als Vertrauen; ein Muster, das uns im gesamten Ökosystem immer wieder begleitet.

Zuckerbrot und Peitsche

Das Unterkapitel, in dem wir die freien Mitarbeiter motivieren.

Das obige Fluten der Nachrichten durch das Notariatsnetzwerk ist jedoch nur ein winziger Teil der Arbeit: Unsere Notare müssen nicht nur dauernd alle Nachrichten weiterleiten, es muss auch jeder dauernd die Transaktionsliste nachführen, denn man will ja seinen Kollegen nicht trauen. Das bedeutet im Gegenzug aber auch, dass man von nun an keine Freizeit mehr hat, weil man rund um die Uhr damit beschäftigt ist, zu Arbeiten und die Arbeit der Kollegen zu kontrollieren. Und das erst noch auf sehr ineffiziente Art und Weise.

Doch zuerst zum realweltlichen Arbeitsalltag: Eine Möglichkeit, ein Team «auf Kurs» zu halten, ist die Schaffung eines Anreizsystems mit definierten Kriterien und Belohnungen. Bei menschlichen Teams ist die Überprüfung der Erreichung von Kriterien sehr schwierig, auch wenn es beispielsweise bei Akkordarbeit versucht wurde; dies reduziert die Motivation auf eine rein extrinsische, meist monetäre (der sogenannte Overjustification Effect). Diese ist kaum nachhaltig, da Quantität auf Kosten der Qualität geht oder die Teammitglieder versuchen, die eigene Leistung besser darzustellen oder die Leistung der Kollegen herabzusetzen: Intrigen, Verheimlichung, Lügen, Manipulationen bis zur Sabotage. Derartige Elemente garantieren in Filmen und Romanen den Spannungsbogen, in der Realität sind sie der Produktivität und gemeinsamen Zielerreichung allerdings höchst abträglich.

In unserem exotischen Notariat sind die Prozesse einfach, repetitiv und standardisiert, weshalb die meisten Blockchains von einer objektiven Messbarkeit der Arbeitsleistung ausgehen. So wurde für Bitcoin ein Anreizsystem geschaffen, welches auf Basis konkreter, überprüfbarer Regeln für das Erstellen eines Blocks eine Belohnung vergibt, wenn dieser Block allgemein anerkannt wird. Deshalb nennt man dieses Verfahren «Proof of Work», abgekürzt PoW; Deutsch etwa «Beweis geleisteter Arbeit».

So weit, so einfach. Wie kann man aber jemanden bestrafen, wenn er seine Arbeit nicht gewissenhaft genug erledigt hat? Man macht die Arbeit so anstrengend und mühsam, dass sie sich niemand freiwillig antut, wenn er sich dafür nicht eine grosszügige Entlöhnung erhoffen kann.

Damit basiert der Anreiz auf einem der stärksten Motivatoren, die Menschen haben: Gier. Gier nach Geld und Macht. Und dieser Anreiz funktioniert auch perfekt, zumindest vordergründig. Aber genau wegen ihrer mittlerweile korrumpierenden Stärke führt die Gier dazu, dass die unerschöpfliche menschliche Erfindungskraft in ihren Dienst gestellt wird und Schlupflöcher gesucht und gefunden werden. Mehr dazu nach den Fakten in den «Realität»-Kapiteln in diesem und im nächsten Beitrag.

Arbeit und Lohn

Das Unterkapitel, in dem ehrliche Mitarbeit endlich entlöhnt wird.

Wer einen neuen Block in die Bitcoin-Blockchain einfügen will, erhält für das Erzeugen («mining») des neuen Blocks eine Belohnung («reward») von aktuell 6¼ Bitcoin (₿), was knapp einer Viertelmillion Franken entspricht. Nicht schlecht für 10 Minuten Arbeit! Und kein Wunder, dass Gier zur treibenden Kraft geworden ist. (Mehr zu Finanzen und deren Rolle im Ökosystem im nächsten Artikel.)

Abbildung 10: Dieser sogenannte 100er-Würfel hat «nur» 100 Flächen. Im Durchschnitt jedes hundertste Mal zeigt er eine Eins.

Wenn ich diese Viertelmillion will, was muss ich dafür tun?

1. Einkommende gültige Transaktionen werden gesammelt (mehr dazu dann im nächsten Artikel zu Kryptowährungen und Transaktionen).
2. Es werden möglichst viele pendente Transaktionen in den neu zu schaffenden Block aufgenommen.
3. Der Block wird jetzt so lange bearbeitet, bis «genügend Arbeit» geleistet wurde.
4. Der Erzeuger («Miner») diese Blocks erhält dann die 6¼ ₿ Belohnung (den «Reward») sowie die Transaktionsgebühren aller in diesem Block eingeschlossenen Transaktionen (diese Transaktionsgebühren sind heutzutage in der Summe etwa um den Faktor 100 kleiner als der Mining Reward).

«Genügend Arbeit» ist dann geleistet, wenn ein kryptografisches Puzzle gelöst wurde, welches wiederholtes, beschwerliches Ausprobieren erfordert. Beispielsweise

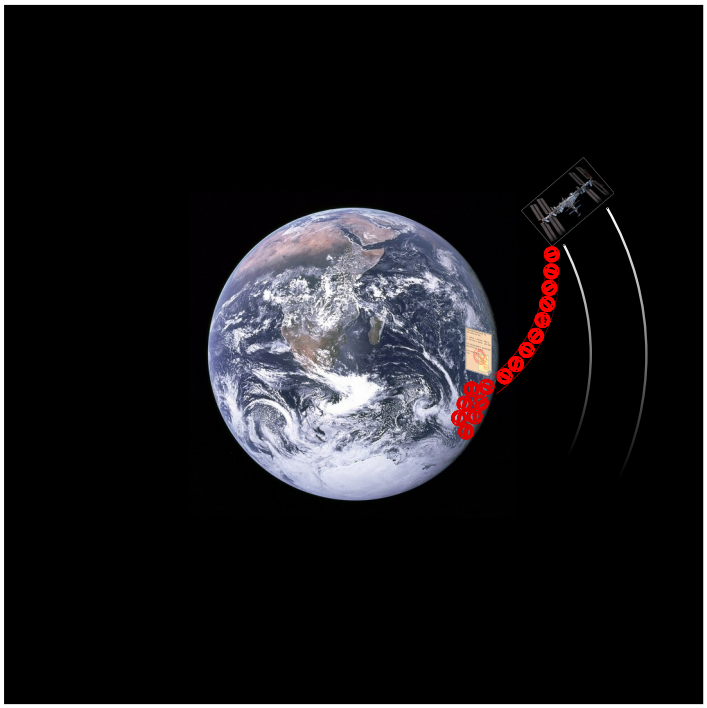

Abbildung 11: Unsere Notare werfen 120 Trilliarden Stempel aus der ISS ab

könnte jeder Mining-Rechner im Bitcoin-Netzwerk unermüdlich so lange einen 120-Trilliarden-seitigen Würfel (1 Trilliarde ist eine 1 mit 21 Nullen!) werfen, bis er eine Eins erzielt. Dieses erfolgreiche Würfelergebnis erhält man im Durchschnitt nach 120 Trilliarden Versuchen. Mit diesem Ergebnis, dem «Proof of Work», kann der Miner den Block für sich beanspruchen und die Belohnung einstreichen.

Unsere Notare würfeln natürlich nicht. Aber sie lieben Versteckspiele, sind sehr vergesslich und gleichzeitig auch passionierte Weltraumtouristen. Deshalb verstecken sie nach getaner Arbeit ihre Transaktionsliste irgendwo auf den 510 Millionen Quadratkilometern der Erdoberfläche, vergessen sofort wieder, wo sie es hingelegt haben und machen sich auf in den Weltraum. Von dort werfen sie so schnell sie können ihre Stempel auf die Erdoberfläche, bis einer das 6x7 cm grosse Stempelfeld ihrer Transaktionsliste trifft (Abbildung 11).

(510 Millionen km² / 120 Trilliarden ≈ 42 cm². 42. Ehrlich! Hoffentlich kommt niemand ernsthaft auf die Idee, die Erde als riesigen Spielball zu benutzen…)

Computer würfeln nicht und werfen auch keine Stempel, da Mauscheln bei beiden Techniken zu einfach wäre. Deshalb wird beim Versuch, einen neuen Block zu «minen», in diesem neuen Kandidatenblock ein extra dafür vorgesehenes Feld so lange mit einem zufälligen Inhalt befüllt, bis der Wert der Prüfsumme («Hash») über den Block genügend klein ist; so klein, wie er nur alle 120 Trilliarden Male wird. Dieser nach unzähligen Versuchen genügend kleine Hash ist damit der Beweis unserer Arbeit. (Der Hash des Blocks ist übrigens nicht vorhersehbar, ohne ihn auch wirklich zu berechnen, d.h. es gibt keine Abkürzung.)

Je mehr Rechenleistung vorhanden ist, desto schneller ist dieses Puzzle gelöst. Eine Designentscheidung des Bitcoin-Protokolls sagt aber aus, dass im Durchschnitt alle 10 Minuten ein neuer Block hinzugefügt werden solle. Damit dies auch bei steigender bzw. schwankender Rechenleistung bestehen bleibt, muss die Definition von «genügend Arbeit» regelmässig an die im Netz vorhandene Rechenleistung angepasst werden. Bei Bitcoin passiert diese Anpassung der Schwierigkeit («difficulty») alle zwei Wochen.

In der Würfelanalogie würde das bedeuten, dass wenn mehr oder schnellere Teilnehmer im Netz sind, auch mit einem entsprechend grösseren Würfel gewürfelt wird und damit häufiger gewürfelt werden muss, bis eine Eins erscheint. (Bei unseren Weltraumnotaren würde die Grösse des Stempelfeldes verkleinert.)

Daraus ergibt sich Folgendes:

1. Es hängt extrem vom **Zufall** ab, wer den Block «minet» und die Viertelmillion «gewinnt». Um gleichmässigere, kalkulierbarere Auszahlungen zu erreichen, sammeln sich Miner in Pools, welche dann den Erlös untereinander aufteilen.

2. Es kann vorkommen, dass mehrere Knoten beinahe **gleichzeitig** Glück haben und eine der unzähligen (rund 1 Nonillion, eine 1 mit 54 Nullen) möglichen Lösungen des kryptographischen Puzzles finden. Damit existieren gleichzeitig mehrere gültige neue Blöcke. Im Allgemeinen unterscheiden sich diese Blöcke durch die Liste der in sie aufgenommenen Transaktionen, sind also nicht austauschbar. Entsprechend muss das System eine Auswahl treffen, mit welchem Block weitergearbeitet wird. Details dazu weiter unten.
   Alle anderen, die erfolglos «mitgewürfelt» haben, haben (wie beim Lotto) beim nächsten Block wieder eine Chance. Irgendwann muss der grosse Gewinn ja kommen…

3. Während das Zuckerbrot die Chance auf einen Gewinn ist (wie ein gespielter Lottoschein), könnte man die **Peitsche** als das mutwillige Zerreissen des Lottoscheins sehen: Falls man den immensen Aufwand getrieben hat, einen gültigen Block zu minen («eine Eins gewürfelt»), aber die anderen Knoten im Bitcoin-Netzwerk diesen Block nicht übernehmen, weil man einen Fehler begangen hat (z.B. ungültige Transaktion aufgenommen), dann verwirkt man seine Gewinnchance und bleibt garantiert auf den aufgelaufenen Kosten (Stromkosten für Rechner und Kühlung, Miete, Amortisation, …), ohne auch nur den Hauch einer Gewinnchance.

4. Solange jemand glaubt, dass seine aufgelaufenen Kosten niedriger sind als der erwartete Anteil am Erlös eines Blocks, wird er oder sie versuchen, zusätzliche **Miningkapazität** einzurichten. D.h. die Rechenleistung folgt dem Kurs des Bitcoin, solange keine Verbote die Regeln ändern.)

5. Vorteil hat, wer möglichst günstig an den Strom kommt (oder günstig kühlen kann). Das führt dazu, dass Mining tendenziell an Standorten mit niedrigen **Stromkosten** betrieben wird, was häufig auch Kohlestrom ist. (Ausser man «bekommt» den Strom gratis.)

Der Cambridge Bitcoin Energy Consumption Index (CBECI) geht von jährlich 125 TWh Stromverbrauch für Bitcoin-Mining aus (Abbildung 12), der Digiconomist von 200 TWh. Zu den vom CBECI angenommenen, für Westeuropa unrealistisch günstigen, Strompreis von 5 US-Cent pro kWh, würde alleine für Strom 6.25 bzw. 10 Mil-

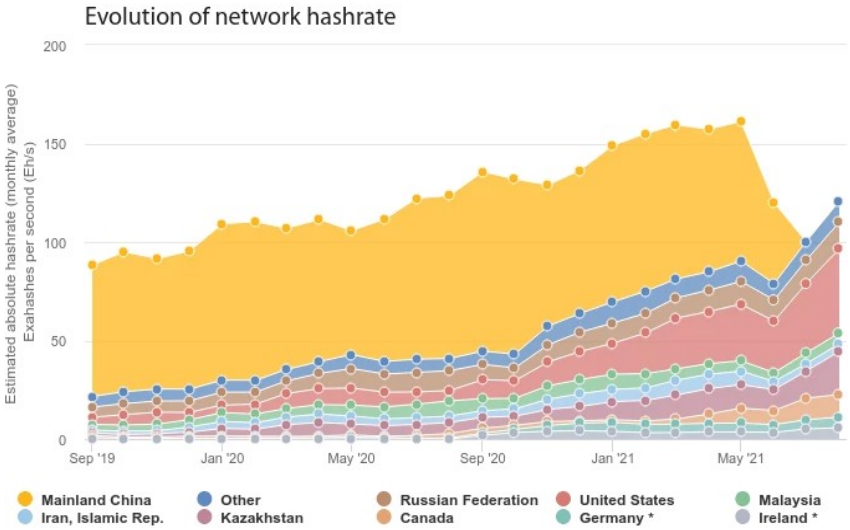

Abbildung 12: Zusammenbruch der Miningrate in China (gelb) nach dem de-facto-Verbot von Kryptowährungen (Bild: CBECI, Leerraum eliminiert)

liarden USD anfallen oder 20 bzw. 32 Millionen Dollar *pro Tag(!)*, Tendenz steigend.

Dieser hohe Energieverbrauch wird zwischendurch auch als Argument für ein Verbot von Proof-of-Work-Kryptowährungen eingebracht. So hoch dieser Aufwand auch ist, er sollte (wie alle politischen Entscheidungen, aber nicht nur diese) immer als Ergebnis einer Kosten-/Nutzenanalyse gesehen werden. Für diese vertröste ich auf den folgenden Kryptowährungsartikel.

Unveränderbarkeit in der Blockchain

Das Unterkapitel, in dem wir uns als Fälscher versuchen und glorios scheitern.

Eines der wichtigen Argumente für eine Blockchain ist ihre Unveränderbarkeit. So ist das spätere Ersetzen eines bestehenden, etablierten Blocks in der Blockchain durch einen einen anderen nicht möglich, ohne jeden einzelnen der nachfolgenden Blöcke ebenfalls aufwändig anzupassen. D.h. wir können nicht einfach einer der blauvioletten Blöcke nehmen (beispielsweise den mit «OK» beschrifteten in Abbildung 13) und «mal kurz so» durch den hellblauen Block («BAD») ersetzen, weshalb er auch rot durchgestrichen ist. Das liegt an der Sicherheit der verwendeten kryptografischen Hashfunktion.

Was müsste passieren, um den Block «einfach so» zu ersetzen?

Das Bitcoin-Netzwerk vereinigt für sein Proof of Work eine massive Rechenleistung auf sich, und verbraucht dafür 500 Mal mehr Strom als der weltweit leistungsfähigste Supercomputer. Umgerechnet entspricht das etwa dem doppelten Elektrizitätsverbrauch der gesamten(!) Schweiz.Und trotz dieser phänomenalen Rechenleistung müsst das gesamte Bitcoin-Netzwerk 20 Oktillionen Jahre lang rechnen, um einen Block so durch einen anderen zu ersetzen, dass seine Prüfsumme (Hash) dieselbe ist wie die des Ursprungsblocks, er also als gültiges Mitglied der Kette akzeptiert werden könnte. (Ob er auch wirklich akzeptiert würde, steht auf einem anderen Blatt.)

20 Oktillionen Jahre schreibt man als 2 mit 49 Nullen. Wer Vergleiche zum Alter des Universums bevorzugt: Die ganzen Rechner hätten seit dem Urknall vor über 13 Milliarden Jahren durchgehend rechnen müssen und hätten erst einen Sextilliardstel ihrer Sisyphusarbeit hinter sich gebracht. (Und selbst Deep Thought fände wahrscheinlich die Antwort auf die «Frage aller Fragen nach dem Leben, dem Universum und dem ganzen Rest» schneller als einen Ersatzblock.)

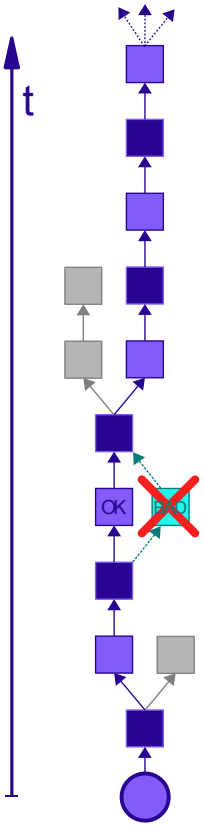

Abbildung 13: Einen passenden Ersatzblock zu finden ist «unmöglich»

Leute aus dem IT-Sicherheitsumfeld nennen das zurückhaltend «impraktikabel»; Normalsterbliche bevorzugen jedoch «unmöglich».

Alternative Regeln

Das Unterkapitel, in dem sich die Notare nach einem weniger repetitiven, einfacheren Job umschauen.

Die Proof-of-Work-Regeln führen zwangsläufig zu Energieverschwendung, die meist erst noch mit der Zeit bzw. Popularität steigt. Dies behagt weder Umweltschützern noch den Betreibern der Mining-Rechner selbst: Sie würden lieber mehr Geld selbst einstreichen, als dieses für Elektrizität und Hardware auszugeben. Entsprechend wurde und wird über alternative Systeme nachgedacht, insbesondere «Proof of Stake» (PoS, «Anteilsnachweis» oder «Beweis eines Einsatzes») und «Proof of History» (PoH, «Beweis verstrichener Zeit»).

Eigentlich wollen alle diese Regeln Sicherheit, Geschwindigkeit und Dezentralisation erreichen. Leider hat es bisher niemand geschafft, alle drei gleichzeitig in einer offenen Blockchain zu erreichen. Trotz intensiver Versuche sind bisher immer Abstriche nötig gewesen, eine Erkenntnis, welche als «Blockchain-Trilemma» bezeichnet wird.

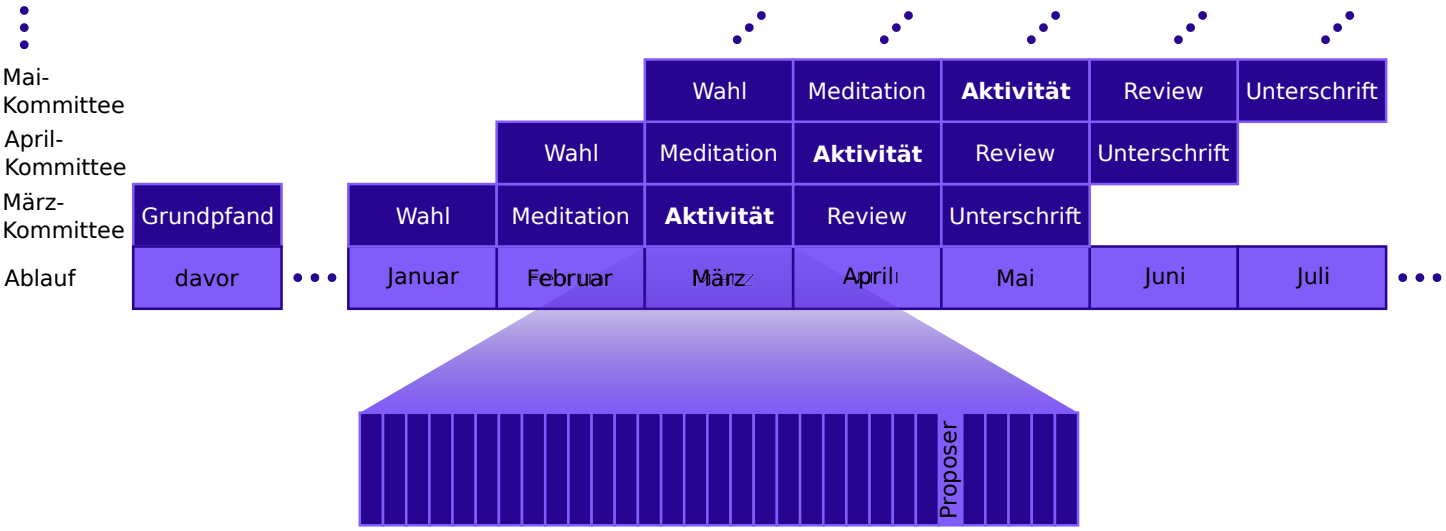

Abbildung 14: Zeitlicher Ablauf der Kommitteetätigkeit bei Proof of Stake

Proof of Stake

Keine der prominenten Blockchains verwendet bisher Proof of Stake produktiv. Ethereum, die Nummer zwei hinter Bitcoin mit Sitz in Zug, arbeitet aktuell noch auf Proof-of-Work-Basis, wofür aktuell nochmals über die Hälfte des Bitcoin-Stromverbrauchs verwendet wird. Ethereum will PoS seit Jahren produktiv einführen; nach mehreren Verschiebungen ist es aktuell für das zweite Quartal 2022 vorgesehen, parallel zum weiterhin laufenden PoW.

Was ist Proof of Stake? Die grundlegende Annahme ist, dass je mehr Anteile einer Kryptowährung man besitze, desto eher liege einem das Wohlergehen der Kryptowährung als solcher am Herzen und man würde deshalb nicht gegen die Interessen der Kryptowährung handeln. (Da dies eine extrem homogene Menschheit voraussetzen würde, trifft diese Aussage sicher nicht auf alle Menschen zu.)

Beginnen wir wieder mit einer Analogie, einem selbstorganisierenden Dorf. Die Dorfbewohner fühlen sich in Arbeit und Freizeit Tag und Nacht vom hektischen Herumgerenne der Proof-of-Work-Notare gestört. Durch ihren Schlafmangel sind die Notare auch sehr asozial geworden, keiner will mehr mit ihnen zu tun haben. Deshalb beschliesst der Ältestenrat, auf Proof of Stake umzustellen. Hier der Ablauf am Beispiel des für den März zuständigen Validatorenkommittees (Abbildung 14):

- Pro Hektar Grundbesitz kann ihre Besitzerin Mitspracherecht im neuen Dorfrat beantragen. Wer weniger besitzt, muss sich mit anderen zusammen tun und jemand vertritt diesen Pool; die interne Organisation im Pool ist den anderen Bewohnern egal.
- **Davor:** Wer das Mitspracherecht beantragen will, muss dazu sein Grundstück aufs Spiel setzen, sogenannt «staken» («… is at stake» bedeutet auch «… steht auf dem Spiel»). Dieser Willen (und die damit einhergehende Verpfändung des Grundstücks) wird in der Blockchain eingetragen und notarisiert (wie, sehen wir gleich).
- **Januar:** Aus den Hektaren mit Mitspracherechtsantrag werden jeden Monat für übernächsten Monat 128 Hektaren ausgewählt. Ihre Vertreterinnen werden als «Validator» (Validatorinnen oder Bestätigerinnen) für die übernächsten Monat (hier: März) verpflichtet.
- Diese PoS-Mitsprache ersetzt das PoW-Mining; auch dieses kommt mit Zuckerbrot und Peitsche: In ihrem Dienstmonat (und nur dann) arbeiten die Validatorinnen analog zu den PoW-Notaren. Statt ihre Ehrlichkeit durch den Willen zu nutzloser Arbeit (endloses Würfeln oder Stempelabwurf) zu bestätigen, tun sie das, indem sie wie oben gesehen einen Teil ihres Grundbesitzes als Pfand für ihre Ehrlichkeit geben.
- **Februar:** Das Kommittee bereitet sich mental auf ihren Einsatz vor.
- **März:** Für jeden Tag wurde auch eine der diensthabenden Validatorinnen als «Proposer» (Vorschlagerin) ausgewählt. Diese führt an diesem Tag die Loseblattliste. Am Ende des Tages stempelt sie die Liste, wieder mit einer kleinen Kopie des Vortagesblatts zur Verkettung.
- **April:** Alle Validatorinnen überprüfen nochmals die Loseblattsammlung ihres Dienstmonats.
- **Mai:** Unsere (März-)Validatorinnen zu den für den aktuellen Monat zuständigen (Mai-)Validatorinnen. Dort erklären sie ihre Unterstützung für die von ihren jeweiligen Tages-Proposerinenn abgelegten Arbeiten mit ihrer Unterschrift. Diese sogenannte «Attestation» (Beglaubigung) erfolgt auf dem aktuellen (Mai-)Loseblatt. Sobald ⅔ aller März-Validatorinnen unterschrieben haben, gilt der März als «justified» (gerechtfertigt

oder, einfacher, bestätigt) und die März-Validatorinnen erhalten ihre Erfolgsprämie: zusätzliche, neue Grundstücksanteile (das Zuckerbrot, der Ersatz für den «Mining Reward» bei PoW).

Die dumme, repetitive Arbeit von PoW ist weggefallen auf Kosten von deutlich komplexerer Koordination. Auf dieser Abstraktionsebene klingt es noch recht einfach und überzeugend. Die obige Beschreibung ist jedoch im Vergleich zur eigentlichen Funktion von PoS bei Ethereum massiv vereinfacht.

Zusätzliche Komplexität entsteht dadurch, dass Ethereum diese Arbeit auf 65 Blockchains aufteilt (eine Haupt- bzw. Koordinationschain, die «Beacon Chain»; und 64 Transaktionschains, die «Shard Chains»)

Am meisten Komplexität entsteht aber in jedem verteilten System immer durch das Abfangen von Fehlern und Umgang mit Spezialfällen. Es gilt die unzählige seltenen Konstellationen sinnvoll abzuwickeln und dafür zu sorgen, dass alles trotzdem weiterläuft: Proposerin oder sonstige Validatorin krank, überlastet oder sonstwie nicht verfügbar; Uneinigkeit zwischen Proposerin und sonstigen Validatorinnen; Einschlafen während der Wahl; .... Im Falle von Ethereum sind alle automatisiert mit geeigneten Strafen für die Missetäter und Belohnungen für den Rest umgesetzt. Auch unter unglücklichsten Kombinationen von Fehlern muss das System immer sinnvoll weiterarbeiten können.

Ein besonderes Augenmerk verdienen Zufallszahlen, die z.B. für die zufällige, faire Auswahl der Kommitteemitglieder oder die Aufteilung der Proposer-Tätigkeiten unter den Mitgliedern benötigt werden. In einer Blockchain-Umgebung ist Zufall jedoch alles andere als trivial und die scheinbar triviale Aufgabe wird bei Ethereum-PoS umgesetzt mit einem aufwändigen «Smart Contract» mit (1) eigenen Stakeholdern, (2) noch mehr aufs Spiel gesetzte Kryptowährung sowie (3) nochmals Zuckerbrot und Peitsche mit verteiltem bzw. eingezogenen Guthaben. Dieser Zufallszahlen-Smart Contract, «RANDAO» genannt, ist eines der vielen kleinen Rädchen im ganzen Prozess. (Der Funktionsweise von Smart Contracts wird ein eigener Artikel gewidmet.)

Wir sehen, die Blockchain selbst kann nur funktionieren, wenn dauernd unzählige Smart Contracts immer wieder korrekt ineinander greifen, wie ein fein abgestimmtes Uhrwerk. Im Gegenzug hängt aber auch das sauberen Funktionieren der Blockchain von diesen Smart Contracts ab. Solche zyklischen Abhängigkeiten versuchen Informatiker in verteilten Systemen wenn immer möglich zu vermeiden, da sie zu mehr Komplexität und zusätzlichen Single Points of Failure führen.

So richtig mitmachen bei Ethereum-PoS kann man im Übrigen erst ab 32 Ether, aktuell für rund 80 000 Franken erhältlich. Teile dieses Einsatzes oder gar der Gesamteinsatz gehen verloren, wenn ein Rechner im falschen Moment abstürzt oder seine Netzwerkverbindung gestört wird (z.B. während dem oben erwähnten «RANDAO»).

Risiken bei Proof of Stake vs. Proof of Work

Wenn ein **Proof-of-Work**-Rechner ausfällt (Absturz, Stromausfall, Netzwerkproblem, DoS-Angriff, ...), reduziert sich u.U. seine Chance auf einen Gewinn, aber das bisher erarbeitete Kapital bleibt unangetastet.

Bei **Proof of Stake** will man hingegen einen möglichst grossen Teil seines Vermögens «staken», da die Gewinne proportional zum riskierten Kapital verteilt werden. Und wenn der Rechner in einem dummen Moment ausfällt, ist das ganze gesetzte Kapital weg.

Permissioned Blockchains

Neben den öffentlichen, offenen («permissionless») Blockchains nach Bitcoin-Vorbild sind für geschlossene Benutzergruppen in Businessapplikationen sogenannte private oder «permissioned» Blockchains beliebt: Zum Beitritt in die geschlossenen Benutzergruppe werden traditionelle Verträge mit Papier und Unterschrift abgeschlossen. Die Mitglieder dürfen dann je einen Rechenknoten in dieses abgeschlossene System integrieren.

Diese Rechnerknoten sorgen dann dafür, dass neue Einträge nur dann in die Blockchain aufgenommen werden, wenn diese mindestens eine ⅔-Mehrheit an Zustimmung erhalten. Das System ist damit immun gegen byzantinische Fehler, d.h. das System funktioniert korrekt, solange weniger als ⅓ der Knoten ausfallen oder fehlerhaft/böswillig agieren.

In einer solchen kontrollierten Umgebung ist das Erkennen oder Verhindern von dominanten Akteuren viel einfacher als in einem Jekami-Modell. Im Gegensatz dazu fehlt diesem Modell auch die Universalität, welche eine öffentliche Blockchain anstrebt.

Oben wackelt es am meisten

Das Unterkapitel, in dem wir Konflikte beim Lego-Turmbau lösen und die Stabilität nochmals überprüfen.

Die Bitcoin-Blockchain ist seit 2009 auf eine Höhe von inzwischen über 730'000 «Legoblöcken» angewachsen. Wir haben gesehen, dass es «unmöglich» ist, unten einen

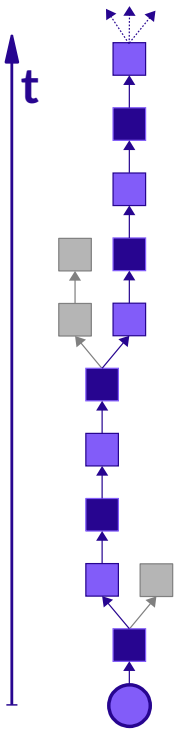

Abbildung 15: Es kann manchmal auch mehr als einen (gleichzeitigen neuen Block) geben

Block rauszuziehen und zu ersetzen. Schliesslich ist es ja auch Lego und nicht Jenga!

Doch wie sieht es oben aus? Im durch (Wurf- bzw. Würfel-)Glück geprägten Miningprozess können mehrere neue gültige, aber unterschiedliche Blöcke praktisch gleichzeitig entstehen (Abbildung 15). Bis alle Knoten über einen neuen Block informiert sind, dauert es häufig mehrere Dutzend Sekunden, manchmal auch mehr als eine Minute. Rund alle 11 Tage sind deshalb zwei potenzielle neueste Blöcke gleichzeitig im breiten Umlauf. Aber es kann nur einen geben, weil der Konsens über den Kontostand irgendwie gewährleistet sein muss.

Aus diesem Grund werden die obersten paar Blöcke als unsicher angesehen, häufig bis etwa sechs Blöcke darüber gestapelt wurden, was im Durchschnitt eine Stunde dauert, aber zwischendurch auch mal 6 Stunden in Anspruch nehmen kann (die Wartezeit hängt ja nur vom Würfelglück ab). Dann ist die Wahrscheinlichkeit hoch, dass nicht plötzlich doch noch irgendwo ein zusätzliche, längere Kette auftaucht.

Daraus ergeben sich weitere Folgerungen:

1. Falls mehrere Kandidatenblöcke im Spiel sind, wird von jedem Teilnehmer unabhängig von den Entscheidungen aller anderen Teilnehmer einer der Kandidaten als Basis für den Folgeblock ausgewählt. (Typischerweise ist das der erste gültige Block, den er gesehen hat.)
2. Kandidatenblöcke, die der Mehrheit nicht «gefallen», bleiben in irrelevanten Seitenarmen der Blockchain und werden daher ignoriert.
3. Das «Gefallen» wird durch die Regeln im Programmcode definiert und kann sich mit der Zeit verändern.
4. D.h. die Mehrheit bestimmt den Kurs, auch wenn es einzelne hartnäckige Minderheiten gibt, die dann ihren Sonderzug fahren («Hard fork», eine Art Unabhängigkeitserklärung). Dieser Mechanismus wurde auch schon zur gezielten Diskriminierung bzw. Ausschluss von Mitgliedern und Technologien genutzt.
5. Eine Transaktion, die nur in einem dieser Seitenarme auftauchen, wird von den meisten Mitgliedern nicht anerkannt. Wenn die Transaktion aber grundsätzlich gültig ist, sollte sie in einem der nächsten regulären Blöcke aufgenommen werden und damit zu Anerkennung kommen.

Technische Zusammenfassung

Das Unterkapitel, das alles nochmals schön büschelt.

Millionen von Rechnern mit einem Stromverbrauch von 500 Supercomputern oder eines Industrielandes versuchen andauernd, ein kryptografisches Puzzle zu lösen. Dieses Puzzle wird um so schwieriger, je mehr bzw. schnellere Rechner sich daran beteiligen, damit im Durchschnitt alle 10 Minuten eine neue Lösung entsteht. Mit dem Lösen dieses kryptografischen Puzzles («Proof of Work») soll bestätigt werden, dass man genügend Interesse daran hat, sich ernsthaft den Prinzipien der Blockchain zu verschreiben, also nicht zu schummeln.

Falls aber genügend Viele mit den Regeln nicht einverstanden sind (oder gemeinsam schummeln) werden *de facto* diese Regeln zum Standard («Code is Law»). So werden Veränderungen umgesetzt oder es entstehen Abspaltungen bzw. Ausschlüsse.

Der Anreiz, diese Rechenressourcen bereit zu stellen, die enormen Stromkosten von 20-30 Millionen Franken täglich zu tragen und sich an die Regeln zu halten, basiert auf den mit der Erzeugung jeden Blocks frisch gemünzte Kryptowährung (aktuell rund eine Viertelmillion Franken alle 10 Minuten), die aus dem Nichts entsteht und den Transaktionsgebühren, aktuell ein paar Tausend Franken pro Block. Im Gegenzug, wie wir später auch noch sehen werden, gibt es auch den Wunsch, die Regeln so zu gestalten, dass das Einkommen bzw. der Wert der Kryptowährung möglichst hoch wird.

Alternativen

Das Kapitel, in dem wir andere Schöpfungen begutachten.

Aus Sicht der Blockchain-Afficionados war die Welt wüst und leer, bevor Satoshi Nakamoto am ersten Tag die Welt in Hell (Blockchain und Bitcoin) und Dunkel (alles andere) trennte und sich danach zur Ruhe setzte; vielleicht, um die Kursentwicklung seiner ersten Million Bitcoins genüsslich zu beobachten.

Doch Digitalarchäologen haben in unermüdlicher Kleinarbeit herausgefunden, dass es bereits davor wichtige Ansätze gab:

Table 1. A timeline of selected discoveries in cryptography and blockchain technology.	
1970	James Ellis, public-key cryptography discovered at Government Communications Headquarters (GCHQ) in secret
1973	Clifford Cocks, RSA cryptosystem discovered at GCHQ in secret
1974	Ralph Merkle, cryptographic puzzles (paper published in 1978)
1976	Diffie and Hellman, public-key cryptography discovered at Stanford
1977	Rivest, Shamir, and Adleman, RSA cryptosystem invented at the Massachusetts Institute of Technology
1979	David Chaum, vaults and secret sharing (dissertation in 1982)
1982	Lamport, Shostak, and Pease, Byzantine Generals Problem
1992	Dwork and Naor, combating junk mail
2002	Adam Bach, Hashcash
2008	Satoshi Nakamoto, Bitcoin
2017	Wright and Savanah, nChain European patent application (issued in 2018)

Abbildung 16: Eine andere Priorisierung der Geschichte. (Bildquelle: Alan T. Sherman, Farid Javani, Haibin Zhang, and Enis Golaszewski: On the Origins and Variations of Blockchain Technologies, IEEE Security & Privacy, Jan/Feb 2019)

Ur- und Frühgeschichte

Das Unterkapitel, in dem wir eine Zeitreise vor den Bitcoin-Urknall tätigen.

David Chaum, der umtriebige Kryptograf, dem wir in dieser Artikelserie noch ein paar Mal begegnen werden, hat sich 1982 in seiner Dissertation «Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups» (in etwa «Wie gegenseitig misstrauende Gruppen gemeinsam Computersysteme aufsetzen, unterhalten und ihnen vertrauen können») bereits einem Blockchain-ähnlichen Protokoll gewidmet.

1990/91 haben Stuart Haber und W. Scott Stornetta sich dem Thema Nachvollziehbarkeit von digitalen Vorgängen mittels Zeitstempeln angenommen, digitalen Signaturen, welche die Existenz einer digitalen Datei zu einem bestimmten Zeitpunkt bestätigen. Dabei sind sie insbesondere der Frage nachgegangen, wie man das Ausstellen von verfälschten (zurückdatierten) Zeitstempeln transparent und damit als Fälschung erkennbar machen könne. Eine Variante ihres Verfahrens ist seit 1995 durchgehend als PGP Digital Timestamping Service im Einsatz.

Zeitstempel sind speziell dann hilfreich, wenn man die Existenz eines Dokumentes zu einem bestimmten Zeitpunkt nachweisen will oder aufzeigen will, dass ein Dokument seit einem bestimmten Zeitpunkt nicht mehr verändert wurde. Anwendungsgebiete sind vielfältig und reichen von der Patentierung von Erfindungen über Urheberrecht bis zum Einsatz in der Forensik.

Ross Anderson beschrieb 1997 den Eternity Service, ein anonymes, dezentrales Speichermedium, mit dem Dokumente gegen gezielte Zugangsverweigerung (Denial of Service) geschützt wurden. Seit 2000 schützt das LOCKSS-System (Lots of Copies Keep Stuff Safe) dezentral digitale Dokumenten vor Verlust oder Verfälschung. Aus der LOCKSS-Forschung heraus ergab sich 2003 auch das erste (preis-gekrönte) Proof-of-Work-System zur Konsensbildung.

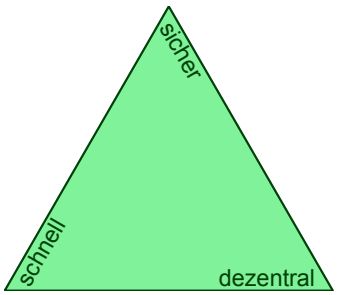

Abbildung 17: Nicht alle drei aufs Mal

Seit 2001 gibt es verteilte Systeme für die Nachvollziehbarkeit der Entwicklung von Programm-Quellcode, bei welchen der aktuelle Zustand auf den Vorgängerzustand verweist, indem er dessen Hash (die oben wiederholt erwähnte «Prüfsumme») referenziert und damit hinterrückses Austauschen von früheren Zuständen verunmöglicht. Das 2005 veröffentlichte Quellcode-Verwaltungssystem Git, welches für die verteilte Entwicklung des Linux-Kernels geschrieben wurde, ist die dominante Form der Quelltextverwaltung für Open-Source-Projekte geworden und ist auch aus der Unternehmenssoftwareentwicklung nicht mehr wegzudenken. Damit könnte man Git wohl auch als weltweit meistgenutzte Blockchain-Lösung bezeichnen. Im Gegensatz zu den vorher beschriebenen Systemen kann jeder Entwickler seine private Kette beliebig wachsen lassen. Ein Konsens erfolgt im Dialog. Mehrere Chains sind nicht wirklich ein Problem und bei der Etablierung eines neuen Konsenses geht die verteilt geleistete Arbeit nicht verloren.

Blockchain-Trilemma

Das Unterkapitel, in dem wir Hansdampfs im Schnäggeloch nicht alles bekommen, was wir wollen.

Das Blockchain-Trilemma postuliert, dass man maximal zwei der drei Umsetzungs-Attribute Sicherheit, Geschwindigkeit und Dezentralisierung gleichzeitig erreichen kann (Abbildung 17). Es gibt dafür keinen formalen Beweis, bisher ist jedes Blockchain-Projekt in irgendeiner Form gegen diese Barriere gelaufen.

Entsprechend sollte jede Behauptung des Gegenteils mit höchster Vorsicht genossen werden: «Wenn etwas zu gut scheint, um wahr zu sein, ist es das wahrscheinlich auch».

Darf es ein bisschen weniger sein?

Das Unterkapitel, in dem wir nochmals sehen, dass wir mehr bekommen, wenn wir weniger wollen.

Aus Sicht der Funktionalität ergibt sich ebenfalls ein Dreieck (Abbildung 18):

1. Das Erreichen eines **globale Konsens** (alle sehen den gleichen Zustand in ihren Büchern, dem Distributed Ledger),
2. die vollständige **Abwesenheit jeglichen Vertrauens** zwischen den Teilnehmern; sowie
3. dem Wunsch, dass **jeder seine Daten selbst eintragen** kann, wenn sie nur bestimmten Mindestanforderungen genügen; dazu muss er keinen Koordinator bemühen.

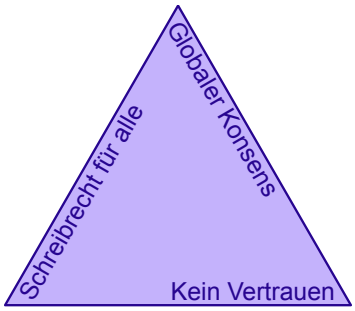

Abbildung 18: Alles wird einfacher, wenn man eines davon weglassen kann (siehe Aufzählung)

Alle drei Ziele gleichzeitig zu erreichen ist sehr aufwändig, wie wir gesehen haben. Wenn wir einen davon weglassen könnten, wäre das Problem häufig deutlich einfacher zu lösen. Sehen wir uns diese deshalb einzeln der Reihe nach an:

Brauchen wir globalen Konsens?

Unterteilen wir das Problem in drei Fälle: Private Blockchains unter Vertragspartnern, öffentliche Blockchains für die Nachvollziehbarkeit und öffentliche Blockchains mit Kryptowährungen.

Die Hauptanwendung von **privaten Blockchains** besteht darin, dass sich Geschäftspartner gewisse Dinge zusichern. Entsprechend der Natur der Dinge sind das meistens bilaterale Verträge. Dafür ist kein globaler Konsens nötig, nur die beiden Geschäftspartner müssen sich einig sein. Dies ist deutlich einfacher (Abbildung 19) und lässt sich deutlich effizienter umsetzen als ein globaler Konsens; die Komplexität der Blockchain ist dabei völlig unnötig und sogar schädlich (langsamere Reaktionszeiten, unnötige Öffentlichkeit, Kosten, …).

Bei einer **öffentlichen Blockchain,** auf der eine **Währung** oder andere Elemente aus den Folgekapiteln aufsetzen, scheint globaler Konsens auf den ersten Blick wichtig zu sein, da jeder über jeden Kontostand informiert sein sollte. Doch auch dies ist nicht zwingend, wie wir bei alternativen Bezahllösungen sehen werden; lokaler Konsens oder die einfacheren Konsistenz (=Widerspruchsfreiheit) reicht oft. Mehr dazu aber im Kapitel über Kryptowährungen.

Wenn **öffentliche Blockchains** jedoch nur als **Informationsablage** genutzt werden, wie das bei den meisten Blockchain-basierten Digitalisierungsprojekten der öffentlich Hand der Fall ist, ist globaler Konsens unnötig. Integrität, Transparenz und der Beweis der Unveränderbarkeit der Informationen ist völlig ausreichend und diese Attribute sind viel einfacher zu erreichen. Wenn ich zeigen will, dass ein Zeugnis nicht verändert wurde, reicht eine digitale Signatur einer vertrauenswürdigen Stelle. Obwohl Unveränderbarkeit regelmässig als Ziel genannt wird, ist es häufig keines. Irrtümer wie Tippfehler oder Vandalismus soll behoben werden können, auch das Recht auf Vergessen ist zu berücksichtigen. D.h. Einträge sollen korrigiert oder gelöscht werden können, aber diese Änderungen sollen nachvollziehbar sein, je nachdem nur von Aufsichtsgremien oder aber der breiten Bevölkerung.

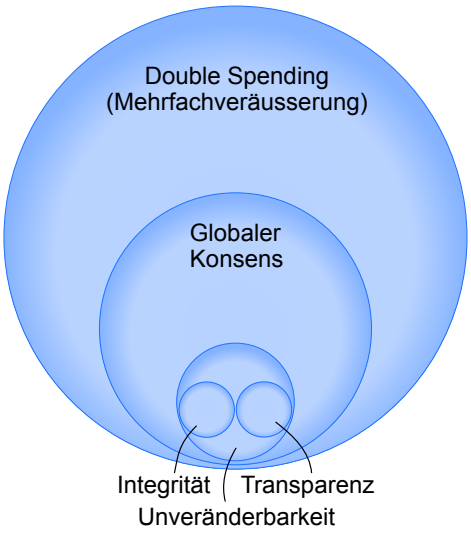

Abbildung 19: Sind die extrem teuren Zusatzoptionen wirklich nötig?

(Die technisch teuerste und komplizierteste der Zusatzoptionen ist der Schutz gegen Mehrfachveräusserung («Double Spending»). Ihn benötigen wir nur, wenn die Blockchain Buch führen soll über Dinge, die man wie Geld nur ein Mal ausgeben darf. Mehr dazu dann in nächsten Artikel zu Kryptowährungen.)

Brauchen wir Schreibrechte für alle?

In vielen Anwendungsfällen gibt es nur wenige Schreibberechtigte; im Idealfall gehören sie sogar derselben Organisation an (Handelsregister, Grundbuchamt, …). Alternativ sind sie bekanntermassen nur für einen Teil der Daten zuständig (Hierarchie, Föderalismus, …). D.h. auch wenn Konsens nötig ist, ist klar, wer was zu diesem Konsens beitragen darf. Auch hier führt das zu einfacheren Lösungen.

Darf es auch ein bisschen Vertrauen sein?

Der riesige Aufwand, der für «Proof of *Wasauchimmer*» und vollautomatischen Konsens betrieben wird, fällt weg, wenn zumindest ein Quentchen Vertrauen vorhanden ist und externe Mechanismen (Presse, Gerichte, …) eingesetzt werden können, falls dieses Vertrauen doch missbraucht wird.

Thema	Integrität	Nach-verfolg-barkeit	Unver-änder-barkeit	>2 Orga	Konsens	Double Spending	Layer 8	Idee
Finanztransaktionen	✓	✓	✓	(✓)	(✓)	✓	(✓)	✓
Gesundheitswesen	✓	✓	•	✓	•	•	✓	✗
Identitätsmanage-ment	✓	✓	•	•	•	•	✓	?
Geldwäsche	✓	✓	•	•	•	•	✓	?
Versicherungen	✓	✓	✓	(✓)	•	•	✓	?
Supply Chain	✓	✓	•	(✓)	•	•	✓	✓
Mobilität	✓	•	•	•	•	•	✓	?
Energiemarkt	✓	✓	✓	•	•	•	✓	✓
Digitale Wahlen	✓	(✗)	✓	•	•	•	•	✗
Zeugnisse	✓	•	•	(✓)	•	•	✓	?

Tabelle 2: Reality Check Marks

Realität

Das Kapitel, in dem wir die Versprechen nochmals begutachten.

Schauen wir uns nochmals die Versprechen an, für die Blockchain als Allheilmittel verkauft wird.

Gleich einmal eine Bemerkung vorab: Für die relativ allgemein gehaltenen Themen kann prinzipbedingt keine detaillierte Analyse gemacht werden. Trotzdem habe ich versucht, meine Wünsche an ein derartiges System als Anforderungen anzunehmen.

Die Themen wurden nach acht Kriterien analysiert:

- Ob sie Integrität, Nachverfolgbarkeit, Unveränderbarkeit oder Schutz gegen Double Spending benötigen
- Der «globale Konsens» wurde aufgeteilt:
  1. Brauchen wir etwas Globales bzw. Multilaterales oder reichen uns jeweils deutlich einfachere bilaterale Abkommen («Mehr als zwei Organisationen»)?
  2. Ist multilateraler/globaler Konsens nötig? (Konsens oder blosse Konsistenz zwischen zwei Organisationen ist deutlich einfacher.)
- Ob es sich überhaupt um ein technisches (oder technisch lösbares) Problem handelt, oder ob wir es hier nicht eher mit einem Layer-8-Problem zu tun haben, also z.B. dem menschlichen Wunsch, bei den Entscheidungen involviert zu sein oder seinen eigenen Weg gehen zu dürfen.
- Zu guter Letzt: Halte ich die vollständige, global einheitliche Digitalisierung des jeweiligen Prozesses überhaupt für eine gute Idee (entweder generell oder spezifisch mittels einer Blockchain).

Die reinen Finanzthemen «Finanztransaktionen» und «Geldwäsche» finden sich zwar in dieser Tabelle; sie werden trotzdem erst im nächsten Artikel behandelt.Betrachten wir exemplarisch ein paar viel diskutierte Themen:

Digitale Wahlen

Das Unterkapitel, in dem wir nochmal mehr über die Idee der Digitalisierung von Wahlen erschauern.

e-Voting war in der Schweiz vor einigen Jahren ein heiss diskutiertes Thema, deshalb hier nur einige Stichpunkte. Bei Abstimmungen ist Vertrauen essenziell:

- Vertrauen, dass meine Stimme gezählt wird (und zwar richtig);
- Vertrauen, dass niemand meine Stimme mir zuordnen kann, wenn ich das nicht will;
- Vertrauen, dass Stimmen nicht gefälscht, gekauft oder erpresst werden können (zumindest nicht skalierbar).

Deshalb wollen wir zwar Integrität und Unveränderbarkeit, aber Nachverfolgbarkeit soll maximal sehr selektiv gewährleistet sein.

Auf der anderen Seite haben wir eine strikte Organisation mit Hierarchie (Bund, Kantone, Gemeinden) und keine Horde von sich gegenseitig misstrauenden Individuen; der globale Konsens ist also einfach durch ein Weiterreichen der Resultate an die nächsthöhere Hierarchieebene gewährleistet.

Elektronische Systeme unterschiedlichster Art haben sich als unzuverlässig, manipulierbar oder fehlerhaft bzw. unsicher herausgestellt. Selbst bei Abwesenheit dieser technischen, aber z.T. auch grundsätzlichen Problemen

verbleibt das Problem der Intransparenz bzw. fehlenden Nachvollziehbarkeit: Aktuell darf in vielen Schweizer Gemeinden der papierbasierte Stimmenzählprozess beobachtet werden. Dank dieser kritischen Öffentlichkeit konnten auch einige Probleme beim e-Counting in der Stadt Bern identifiziert werden und haben zu Verbesserungen geführt.

Das heisst, eine elektronische Abstimmung mag zwar sinnvoll erscheinen, birgt aber hohe Risiken von Wahlfälschung bzw. zumindest Vertrauensverlust und bietet kaum einen Zeitvorteil (die Resultate sind meist wenige Stunden nach Urnenschliessung bekannt). Trotz der intensiven Diskussion hat bisher niemand auch nur ansatzweise gezeigt, wie eine Blockchain da (jenseits von Allgemeinplätzen) helfen könnte. Im Gegenteil, ich könnte mir gut vorstellen, dass solche Systeme der feuchte Traum von totalitären Regimes wären.

Entsprechend sehe ich keinen Grund, elektronische Blockchain-Abstimmungen für eine erstrebenswerte Idee zu halten.

Zeugnisse

Das Unterkapitel, in dem eigentlich nur ungenügende Noten verteilt werden.

In Deutschland ist soeben ein Projekt zur Blockchainisierung der Schulzeugnisse nach über einer Million € ergebnislos eingestampft worden.

Zum Einen bestehen grundsätzlichen Bedenken, dass jegliche garantiert echten Digitaldokumente den Druck zu Daten- bzw. Identitätsdiebstahl erhöhen würden. Zum Anderen ist fraglich, wie die Datenqualität gewährleistet wird, ganz nach dem Motto:

> «The blockchain can't lie to you, but you can lie to the blockchain.»
>
> *(«Die Blockchain kann dich vielleicht nicht anlügen [naja…], aber du kannst sie jederzeit belügen.» Das ist übrigens die eine Hälfte des Blockchain-Oracle-Problems.)*

Zum Dritten stellt sich auch hier die Frage, was denn Blockchains zur Zeugnisausstellung beitragen würden:

- In jeder Schule hätten naturgemäss mehrere Personen die Möglichkeit, direkt oder indirekt falsche Zeugnisse erstellen zu lassen. So in den vertrauenswürdigen Prozess eingebrachte falsche Zeugnisse wären von korrekten Zeugnissen in nichts zu unterscheiden, Blockchain hin oder her.
- Die Integrität, Nachverfolgbarkeit und Unveränderbarkeit würde in diesem Falle sowieso durch eine digitale Signatur einer offiziellen Stelle gewährleistet, also kein Grund für eine (zusätzliche) Blockchain.
- Die nachträgliche Rückdatierung von Zeugnissen könnte über unabhängige Zeitstempel verhindert werden.
- Konsens zwischen den Schulen ist nicht notwendig. Jede darf für seine Absolventinnen eigenständig Zeugnisse ausstellen.
- Sogar die Dezentralität von Blockchain wird ausgehebelt: Die Verifikation der Dokumentenechtheit funktionierte nur über den zentralen Gateway der Bundesdruckerei.
- Die Ursache liegt im Fehlen der breiten Anerkennung eines einheitlichen Verfahrens, nicht an der Komplexität seiner technischen Umsetzung.

Darüber hinaus wurden essenzielle Grundlagen des sicheren Designs von (nicht nur Web-)Anwendungen in den Wind geschlagen: Nutzung von wenigen, einfachen Werkzeugen, Vertraue keinen Nutzereingaben, …; Dinge, die man von Anfang berücksichtigen und einbauen sollte, nicht nur, wenn man eine besonders vertrauenswürdige Anwendung bauen will.

Dieses Projekt zeigt nicht nur auf, dass grundsätzliche Fragen scheinbar nie gestellt wurden. Seine Verwendung von 16 (!) Blockchains wirft grosse Fragen auf. Insbesondere, da schon vor einem Jahr ein (danach nicht in Betrieb genommener) teuren Prototyp eines Impfnachweises von verschiedener Seite verständnislos öffentlich die pompöse Verwendung von 5 Blockchains kritisiert wurde. Die neuerliche Erhöhung auf 16 Blockchains lässt eigentlich nur zwei Schlüsse zu:

1. Keiner der 16 Blockchains wird zugetraut, auch noch in Zukunft zu funktionieren und sicher zu sein, also ihre primäre Rolle spielen zu können.
2. Im Konsortium waren zu viele Partikularinteressen vertreten: Jeder wollte «seine» Blockchain pushen.

Beides spricht nicht für das Vertrauen in Blockchains und deren Proponenten.

Bei beiden abgesägten Technologien mit Blockchainnutzung (Impfnachweis als auch Zeugnis) zeigt die Verwendung mehrer Blockchains auch auf, dass der Konsens nicht notwendig ist, sondern dass es nur um den (viel einfacheren) Nachweis der Erstellung vor einem bestimmten Zeitpunkt geht, also einem Zeitstempel.

(Im Übrigen liefert dieses Projekt auch ein weiteres erschreckendes Beispiel, dass technische Umsetzungen häufig völlig an den Bedürfnissen einer wichtigen Nutzergruppe vorbei gehen. So erhoffen sich die Schülerin-

nen, sicher wichtige Nutzniesser dieser Technik, etwas ganz Anderes: Diese erwarten nämlich vor allem rechtzeitiges Feedback, wenn ihre Leistungen ungenügend seien und was sie dagegen tun könnten. Das hat rein gar nichts mit digitalen Signaturen auf Abschlusszeugnissen zu tun.)

Supply Chain 1: Provenienz/Herkunft

Das Unterkapitel, in dem wir uns nochmals wiederholen. Mit Absicht.

Wurden die Bananen auch wirklich unter menschenwürdigen Bedingungen angebaut? Sind die Medikamente auf meinem Tisch auch echt oder nicht doch potenziell gesundheitsgefährdende Fälschungen? Solche Fragen soll die Blockchaintechnologie lösen. Machen wir es kurz, die viele Überlegungen bereits bei den Zeugnissen angestellt wurden:

- Bei Ursprungs-, Bio-, etc. -Zertifikaten geht es vor allem um finanzielle Interessen; und wenn diese Prozess von skrupellosen Managern mit Lügen ausgenutzt werden, sind weder die Zertifikate noch ihre Authentizität das Papier (oder die Bits) wert, auf denen sie gedruckt sind (hier haben wir wieder das Orakel-Problem).
- Ob auf dem Lieferweg die Zertifikate oder die Produkte (oder beides) ersetzt werden, lässt sich digital nicht überprüfen.
- Auch hier werden keine technischen Eigenschaften benötigt, welche über einfache Buchführung bzw. digitale Signaturen hinausgehen.

In beiden Fällen ist nicht die Blockchain die Lösung, sondern Vertrauen (und Kontrolle). Ja, das bedingt menschlichen Kontakt und den einen oder anderen Besuch vor Ort; aber alles Andere ist nichts weiter als eine offene Einladung zum Betrug. Das nicht zu akzeptieren ist pure (Selbst-)Täuschung.

Supply Chain 2: Vertragsabschluss

Das Unterkapitel, in dem nur Standardprozesse helfen.

Das zweite Versprechen rund um die Versorgungsketten ist der einfachere und schnellere Vertragsabschluss. Ein Vertrag ist erst dann wirklich wichtig, wenn sich die Vertragsparteien uneins sind. Dann muss er wasserdicht sein, mit klaren Regelungen, wann die Leistung als erbracht gilt und welche Schlichtungsmechanismen akzeptiert werden. Solange eitel Sonnenschein herrscht, reicht eine grobe Definition.

Abbildung 20: Falsch eingesetzte Sicherheitsmechanismen, auch Blockchain, sind ein entmutigendes Hindernis für die Guten, aber kein Schutz gegen die Bösen. (Quelle unbekannt)

Auch ein Vertrag in einer Blockchain (und erst recht, wie wir noch sehen werden, ein Smart Contract) müssen regenwettertauglich sein. Ein echter Geschwindigkeitsvorteil ergibt sich nur, wenn man sich auf die Gegenseite verlassen kann (gemeinsames Interesse, Vertrauen, kleines Risiko, ...) oder auf Standardverträge zurückgreifen kann.

Bewertung

Das Kapitel, in dem wir ernüchtert zurückschauen.

Hier eine kurze Zusammenfassung der vorangehenden Seiten:

- Blockchains werden alle mögliche Eigenschaften zugeschrieben, diese aber selten konkret begründet. Im Gegenteil, es scheint so, als ob es kaum Gründe gäbe, Schwammigkeit bei Anforderungen, Komplexität bei den Systemen oder fehlende Struktur bei den Erklärungen zu reduzieren.
- Bei jeder Umsetzung eines Prozesses sollte man im Voraus wissen, welche technischen Eigenschaften man auch wirklich benötigt. Klarheit darüber vereinfacht die Umsetzung und reduziert den Ressourcenverbrauch der sich ergebenden Lösung; oft massiv.
- Die Technik selbst ist schon fast trivial; aber durch die Annahme von komplexen verteilten Abhängigkeiten und der völligen Absenz von Vertrauen, ergeben sich komplexe und ineffiziente Lösungen.

- Einfache, klare Lösungen sind bei einem ehrlichen Wunsch nach Transparenz und Sicherheit immer zu bevorzugen. Komplexe Lösungen bieten nicht nur höheres Potenzial für Fehler oder Missbrauch; sie werden häufig auch absichtlich eingesetzt, um die wahren Abläufe zu verschleiern.
- Die Stromkosten für eine «grosse» Blockchain liegen jeweils bei mindestens rund 20 Millionen Franken pro Tag, Tendenz steigend. Eine direkte Refinanzierung ist nicht möglich und kann nur auf Hoffnung basieren (und das in einem System, welches Vertrauen als schlecht ansieht!).
- Durch den Aufbau von (z.T. exorbitanten) finanziellen Anreizen wird die menschliche Gier übermässig aktiviert und andere Tugenden geraten ins Hintertreffen.
- Alternative Ansätze (wie Proof of Stake) setzen zu sehr auf zusätzliche Komplexität, deren Nebenwirkungen kaum absehbar sind. So scheint es u.a. möglich, dass gezielte Netzwerkangriffe auf Proof-of-Stake-Teilnehmer sich für den Angreifer finanziell als sehr lukrativ erweisen können.
- Für viele Anwendungen reichen digitale Signaturen oder Zeitstempel.
- Wenn eine Anwendung sicher sein soll, muss das alle Prozesse und Teilnehmer einbeziehen, ganz besonders auch die Menschen. Komplexität und Intransparenz führen oft zu Gegenmassnahmen der Beteiligten, welche das ganze System gefährden können.
- Der unbedachte Einsatz von Sicherheitsmechanismen (nicht nur von Blockchains) führt nur dazu, dass alle ehrlichen Beteiligten in ihrer täglichen Arbeit dauernd von scheinbar sinnlosen Hindernissen demotiviert werden, während Bösewichte kaum Mehraufwand haben oder es im Gegenteil sogar noch einfacher haben. Und das sollte nie der Sinn von Digitalisierung sein.

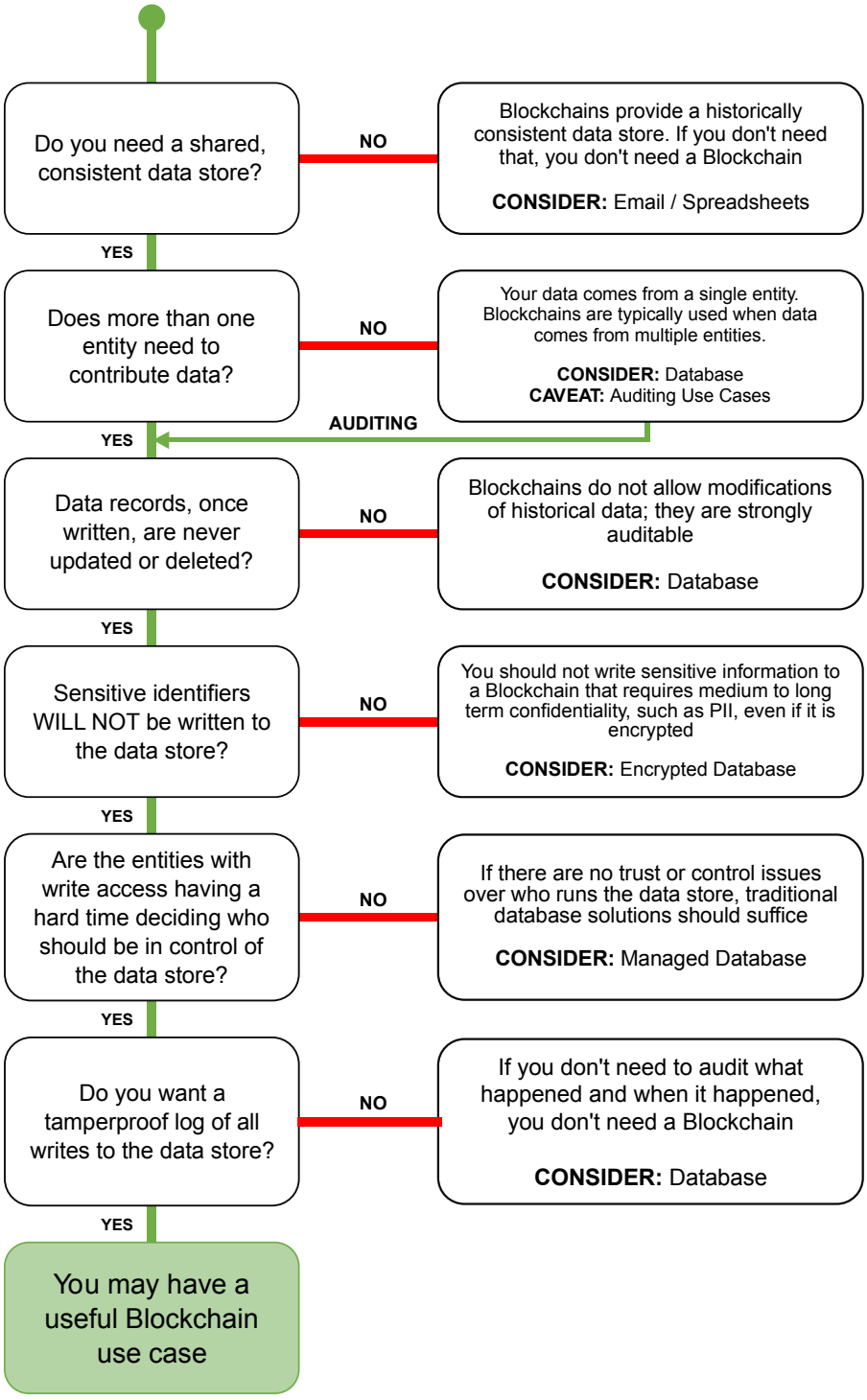

Figure 6 - DHS Science & Technology Directorate Flowchart

Abbildung 21: Mögliches Entscheidungsdiagramm für eine Blockchain nach DHS S&TD. (Bildquelle: Nach NIST IR 8202: Blockchain Technology Overview, 2018; Seite 42, PDF-Seite 53)

Daraus können wir unter anderem folgende Schlussfolgerungen ziehen:

- Kaum eine Technologie, welche als Magie verkauft wird, ist so einfach zu nutzen wie Magie. Im Gegenteil, ihre Magie kann auch grosse verborgene Gefahren bergen, wie wir aus etlichen Märchen kennen.
- Digitalisierung ist nicht einfach durch den Einsatz von Technologie (magisch oder nicht) zu lö-

sen. Die in einen Prozess involvierten Abläufe und Menschen sind mindestens so wichtig.

- Oftmals vereinfacht eine Prise Vertrauen die Lösung massiv. Dieses müssen sich aber alle Beteiligten verdienen.
- Die Blockchain wurde als Lösung für ein ganz spezifisches, besonders komplexes Problem geschaffen. Für dieses Problem mag es–direkt angewandt–eine gute Lösung sein. Für alle anderen Prozesse ist es massives Over-Engineering und bereits kleine Vereinfachungen an den Annahmen können zu deutlich effizienteren Lösungen führen. Dies verdeutlicht auch das (vereinfachende) Diagramm in Abbildung 21.

Für jeden möglichen Digitalisierungsansatz existieren Dutzende von Vorschlägen zum Einsatz von Blockchains. Trotz Millioneninvestitionen fehlen aber die breit publizierten Erfolgsrezepte, welche die spezifischen Eigenschaften der Blockchains nutzen. Etliche Aspekte und Überlegungen hinter dem Konzept Blockchain sind inspirierend und vielversprechend, diese Inspirationen konnten aber bisher nicht erfolgreich umgesetzt werden. Vielleicht liegt das daran, dass Blockchain ausserhalb des Kryptowährungs-Umfelds wirklich keinen Mehrwert bieten; vielleicht aber auch nur, weil das Verständnis der Funktionsweise fehlte. Ich hoffe, etwas zu diesem Verständnis beigetragen zu haben und würde mich über Hinweise zu erfolgreichen (aber auch erfolglosen) Digitalisierungsprojekten freuen.

Fragen

Das Kapitel zum Mitnehmen. Bitte sehr!

Hier einige Fragen, die grundsätzlich dabei helfen, die Digitalisierung eines datenzentrierten Geschäftsprozesses zu strukturieren. Wenn dieser Prozess spezifisch mittels Blockchain digitalisiert werden soll, ist Konsens über die Antworten zwischen allen Beteiligten (neudeutsch «Stakeholder») ein Muss, **bevor** man die Diskussion «Blockchain? Wenn ja, wie?» beginnen sollte. Ich hoffe, diese Fragen unterstützen möglichst viele Projekte beim klareren Umgang mit ihren Daten!

— — — — ✂ — — — — — — — — — — — —

Fragen zum Datenlebenszyklus

- **Daten:** Um welche Daten mit welchen Eigenschaften (Struktur, Abhängigkeiten, Datenschutz) geht es genau?
- **Struktur:** Wie sehen Format, Struktur und Abhängigkeiten der Daten aus?
- **Kriterien:** Sind Integrität, Nachvollziehbarkeit, Unveränderbarkeit, Vertraulichkeit oder Globaler Konsens notwendig?
- **Eingabe:** Was sind die Datenquellen? Wie kommen die Daten in das System?
- **Qualität:** Wie wird die Qualität (Korrektheit, Einheitlichkeit, Authentizität, Vollständigkeit, …) der eingehenden Daten gewährleistet?
- **Fehlerkultur:** Was kann/darf/muss geschehen, wenn sich doch einmal fehlerhafte Daten (absichtlich oder unabsichtlich) einschleichen?
- **Formatänderungen:** Wie soll mit zukünftigen Änderungen an Struktur oder Format von Daten umgegangen werden?
- **Datenschutz:** Wie soll der Anspruch auf Korrektur bzw. Löschung von persönlichen Daten umgesetzt werden?
- **Verarbeitung:** Welche Verarbeitungsschritte sollen auf diesen Daten ausgeführt werden?
- **Vertrauen:** Ist dauerhaftes Misstrauen zwischen den Akteuren zu erwarten? Kann dieses Misstrauen durch Hierarchien oder (Arbeits-)Verträge gemanagt werden?
- **Ausgabe:** Was soll mit den Daten passieren?
- **Auswirkungen:** Welche Aktionen sollen (automatisch) aufgrund dieser Resultate geschehen?
- **Ende:** Haben die Daten ein Ablaufdatum? Was soll dann geschehen?
- **Universalität:** Gelten diese Eigenschaften für alle Daten gleichwertig?

— — — — ✂ — — — — — — — — — — — —

Sobald Daten verändert oder gelöscht werden müssen, taugen diese Daten nicht für die Blockchain. Aber es gibt ja Alternativen.

Diesen Fragenkatalog zum Lebenszyklus von Daten, nicht nur für Blockchains, gibt es auch in grafisch aufbereiteter und erweiterter Form.

Weiterführende Literatur

- Thomas Schwendener: *Blockchain-Report*, Inside IT. 5-teilige Serie, erschienen zwischen dem 8. und 24. Februar 2022. Informationen zum Stand von Blockchain und -projekten in der Schweiz.
- Stephen Diehl u.a.: *Making Sense of Crypto & Web3*, Life Itself Labs, 2022. Lexikon mit Erklärungen und Podcasts zu Blockchain (Englisch).
- David S. Rosenthal: EE380 Talk, 9. Februar 2022. Transkript (und Video) seines Stanford University-Vortrags zum Blockchain-Ökosystem (Englisch).
- Petr Hudeček und Michal Pokorný: *The Deadlock Empire*, 2016–2021. Ein Spiel für angehende Informatiker, bei dem man PoS-Komplexität am eigenen Leibe erfährt und in dem man dafür sorgen muss, dass mehrere gleichzeitig ablaufende Stücke an Programmcode sich nicht gegenseitig stören.