Virtuelle Losbude

2019, AK Uni im Kontext
UnderDocs 012: Virtuelle Losbude

Transcript

Prolog:
[0:00] Es ist ein Internet der Kopien gewesen. Ein Internet der Information und ein Internet der Kopien. Es gibt dort keine Originale. Die Blockchain schafft die Möglichkeit des Internets der Originale und damit das Internet der Werte.
Es ist nach unserer bisherigen Einschätzung eine großartige Technologie, die dabei ist, sich zu einer das Säulen für das Gelingen der digitalen Transformation zu entwickeln.

Intromusik

Sebastian:
[0:28] Ich habe das auch am Anfang nicht verstanden und irgendwann dann, wenn man das einmal aufgeschrieben hat und alles von vorne nochmal durchdacht hat, dann kam so langsam raus, was das eigentlich genau tut.

Begrüßung

Fabian:
[0:46] Herzlich willkommen zur zwölften Ausgabe der Underdocs. Ich freue mich, dass ihr wieder eingeschaltet habt.
Mein Name ist Fabian Link und wir machen heute quasi ein kleines Jubiläum und das Dutzend voll mit einem Jahr auf Sendung.
Und aus diesem Anlass bewegen wir uns mal in den Bereich der Informatik, den wir bisher noch nicht so richtig abgedeckt haben.
Vielleicht habt ihr das so in den Medien verfolgt,
in der letzten Zeit war Blockchain ein ziemliches Hypethema.
Jeder hat darüber geredet, aber man hatte auch so ein bisschen den Eindruck, keiner hatte so richtig verstanden, was er da eigentlich erzählt.
Wer es so richtig verstanden hat, ist mein heutiger Gast, Sebastian.
Der hat nämlich im Rahmen seiner Masterarbeit sogar eine eigene Abwandlung der Blockchain Technologie entwickelt, um sie auf bestimmte Bedürfnisse anzupassen. Was Blockchain eigentlich ist,
wie das so funktioniert und warum er die Methode anpassen musste, erzählt er uns heute. Hallo, Sebastian.

Was Ist Blockchain?

[1:41] Ich würde sagen, bei diesem verwirrenden und sehr konfusen Thema müssen wir wirklich bei den absoluten Basics einsteigen.
Und darum würde ich dich vielleicht bitten, dass du mir einfach mal erst einmal erklärst: Was ist denn eigentlich eine Blockchain?

Sebastian:
[1:54] Ja, das ist auch das, was ich immer gerne am Anfang erkläre, gerade wie du schon gesagt hast, da das in den Medien viel verwendet wurde, wurden da auch Begriffe zusammengewürfelt.
Man hat dann irgendwann angefangen ganze Systeme, die auf so einer Blockchain basieren und die Blockchain an sich synonym zu verwenden, ein schönes Buzzword dafür ist Bitcoin. Und darum
ist es wichtig, sich einmal klarzumachen, welches Prinzip eigentlich zugrunde liegt und das zugrundeliegende Prinzip ist die Blockchain.
Die Blockchain an sich ist nur eine Datenstruktur. Das heißt, man gibt ein Format an, in dem man bestimmte Daten speichern kann.

[2:45] In dem Fall ist es die Blockchain. So eine Datenstruktur hat immer bestimmte Eigenschaften.
Man kennt das, man kann sich das so ähnlich vorstellen, wie wenn man in Word Text-Dokument schreibt.
Man sagt, ich habe jetzt einen Text und ich mache den rechts bündig, dann hat dieser Text eine Eigenschaft: der erste Buchstabe steht rechts immer untereinander.
Und genauso hat eine Blockchain auch Eigenschaften und die ist, dass man Daten, die man in dieser Blockchain gespeichert hat, nicht manipulieren und auch nicht löschen kann.
Und genau dieses Prinzip möchte man ausnutzen. Lange Zeit wusste man noch nicht genau wofür.
Bis dann jemand kam und eine tolle Anwendung dafür gefunden hat.
Das war dann Bitcoin und damit wurde das Prinzip auch bekannt.
Dann ist das auch in den Medien aufgetaucht. Als man über Bitcoin gesprochen hat, hat man dann zwangsweise auch über die Blockchain sprechen müssen.
Ich kann auch noch einmal beschreiben, wie genau man sich das vorstellen kann, wie diese Blockchain so aussieht.

[3:57] Es ist tatsächlich einfach nur eine Kette von Blöcken und die Blöcke sind eine Sammlung von Daten.
Man hat ganz viele Daten ... Die fasst man einfach zu einer Gruppe zusammen und die Gruppe nennt man dann Block.
Jetzt kann man mit einer sogenannten 'Hash-Funktion',
einen Hashwert von dieser Gruppe von Daten, von diesem Block berechnen, und dieser Hashwert hat auch wieder tolle Eigenschaften, wie eigentlich alles in der Informatik irgendwelche Eigenschaften hat, die man ausnutzt ...

[4:29] Und zwar hat die 'Hash-Funktion' die Eigenschaft, dass wenn man so einen Block hat und den Hashwert daraus berechnet hat.
Das ist im Prinzip einfach nur eine relativ große Zahl ... dann ist es sehr schwer einen anderen Block zu finden, der den gleichen Hashwert hat.

Man hat zwei verschiedene Blöcke, wendet die gleiche Hash-Funktion darauf an.
Und es kommen zwei unterschiedliche Werte raus und es ist sehr schwer, dass man es schafft, zwei Blöcke zu finden, bei denen der gleiche Wert rauskommt.

Fabian:
[5:06] Es ist im Prinzip so ein bisschen eine Zahl, die sich aus den Daten in dem Block errechnen kann, die am Ende wie so ein Kennzeichen mir meinen Block individuell charakterisiert und auch eindeutig benennt.

Sebastian:
[5:20] Genau. Man kann, wenn man nur diese Zahl kennt, eindeutig sagen, ob der Block verändert wurde oder nicht.

Fabian:
[5:28] Und hinten raus kann das jeder nachrechnen. Also es ist eine mathematische Funktion.

Sebastian:
[5:32] Genau. Es ist tatsächlich eine korrekte mathematische Funktion.
Man kann Daten beliebiger Größe auf Daten fester Größe, also auf eine Zahl mit einer bestimmten Anzahl Stellen,
so kann man sich das vorstellen, abbilden. Und diese Zahl benutzt man um aus den Blöcken eine Block-Kette zu machen.
Man tut den Hashwert eines Blocks einfach in einen anderen Block rein
und damit kann man, wenn man einen Block in der Hand hat, dann hat man auch den Hashwert des Vorgänger-Blocks in der Hand, und kann dann mit Hilfe dieses Vorgänger Hashwertes den Block überprüfen,
den Vorgänger-Block überprüfen, ob der manipuliert wurde. Und in diesem Vorgänger-Block steht wieder ein Hashwert drin, von dessen Vorgänger und so weiter.
Und so kann man eine ganze Kette von Blöcken mit nur einem einzigen Hashwert auf Manipulations-Freiheit.

Fabian:
[6:37] Das Ziel der Blockchain ist also im Prinzip zu garantieren, dass der Datensatz, den ich jetzt vorliegen habe, dass der im Prinzip unverändert ist. Warum ist das wichtig?

Sebastian:
[6:49] Im Prinzip ist das erstmal nur die Eigenschaft von der Blockchain an sich,
dass man im Vergleich zu allen Daten nur einen sehr kleinen Wert braucht um die Gültigkeit aller Daten zu überprüfen.
Die Blockchain an sich als Datenstruktur, die gibt es schon relativ lange und man kannte diese Eigenschaften, nur es hatte niemand eine Verwendung dafür.
Also es ist eher andersherum, man hat nicht gesagt: "Ich habe hier eine Anwendung und brauche eine Datenstruktur mit genau dieser Eigenschaft.", sondern ... also ich weiß es nicht genau, ich stelle mir das so vor ...
Irgendwann hat mal einer rumgesucht in alten Informatikbüchern und hat dann die Blockchain gesehen und dachte sich: "Das ist doch eine coole Eigenschaft. Was kann man denn damit machen?" Und gleichzeitig

[7:34] kommt eine andere Idee der Informatik hinzu,
das ist das Dezentralisieren. Das geht immer mal, es gibt so Schübe in der Informatik, mal wird alles dezentralisiert, also jeder soll ein bisschen was selber machen.
Und mal wird alles zentralisiert, da wird alles in einen großen Server gestopft und das schwankt so je nachdem, wo man sich gerade befindet, ist mal das eine toller oder das andere toller.
Und das war dann gerade auch in der Zeit, wo das dezentralisieren gehypt wurde und da hat man sich gedacht:
"Oh toll. Ich möchte jetzt gerne was dezentralisieren.", und gleichzeitig habe ich so eine schöne Datenstruktur, die es mir erlaubt, Daten unveränderlich abzuspeichern.
Und dann kam jemand auf die Idee: "Mensch, da lässt sich doch wunderbar eine Kryptowährung draus machen."
Also ein Geldsystem, was dezentral arbeitet, nicht wie die üblichen Banken, die einen zentralen Server haben, auf dem alle Daten und alle Kontodaten gespeichert sind, sondern ein dezentrales System, in dem jeder Teilnehmer
ein bisschen mit dafür verantwortlich ist, dass die Daten sicher abgelegt sind und auch nicht verändert werden können.

Fabian:
[8:54] Das hat natürlich dann den Vorteil, dass ich im Prinzip keine zentrale Instanz mehr brauche, wie eine Bank, der ich vertrauen muss.
Wo wir heutzutage wissen, dass große zentrale Institutionen eben nicht immer vertrauenswürdig sind.
Und selbst wenn sie vertrauenswürdig sind, können sich natürlich schnell irgendwelche Akteure dazwischen schalten und eventuell die Verbindung übernehmen oder Daten manipulieren.

Sebastian:
[9:20] Genau. Genau das ist dann auch die Idee von dem Dezentralisieren. Ich möchte lieber ein bisschen mehr mir selbst Vertrauen, als irgendeiner großen Institution. Oder im Falle von
den Kryptowährungen ist es so, dass man sagt, man vertraut dem System an sich, also der Gesamtheit aller Teilnehmer,
dass das System dafür sorgt, dass niemand manipulieren kann.

Fabian:
[9:44] Okay, wenn ich das richtig verstanden habe, funktioniert die Blockchain einfach so: Ich habe Daten. Die schnüre ich in ein Paket. Dieses Paket nenne ich einen Block. Und dann bilde ich über eine mathematische Funktion, im simpelsten Fall eine Quersumme oder ähnliches, quasi einen Prüfwert, den jeder nachvollziehen kann,
egal wo auf der Welt, wenn er Teil des Blockchain Netzwerkes ist, kann er das nachvollziehen mathematisch, wie ich auf den nächsten Wert gekommen bin.
Und dann ist das quasi der erste Eintrag im nächsten Block.

Sebastian:
[10:20] Ja, genau. Wo man den Eintrag hinpackt, ist weniger wichtig, Hauptsache er steht drin.
Und insbesondere muss er auch in die Hashwert-Berechnung des Blockes mit einfließen. Also es wäre ja Quatsch, wenn man den Hashwert irgendwo so am Rand von dem Block hinschreibt und alles andere benutzt, um die Prüfsumme zu berechnen.

Dann könnte ja einfach jemand den Vorgänger Hashwert ändern. Es ist insbesondere wichtig, dass der Hashwert des Vorgänger-Blockes mit in den Hashwert des aktuellen Blocks mit einfließt.

Fabian:
[10:55] So haben wir so eine Art fortlaufende Zertifizierung von Blöcken.

Sebastian:
[10:59] Ja, so kann man sich das vorstellen.

Fabian:
[11:01] Du hattest da mal im Vorgespräch so eine schöne Analogie mit einer Farbpalette gebracht. Vielleicht kannst du die noch einmal wiederholen.

Sebastian:
[11:07] Ja. Das Mischen von Farben stellt diese kryptographische Hash-Funktion sehr gut dar.
Das hat die gleichen Eigenschaften wie diese kryptographische Hash-Funktion.
Und zwar, wenn man viele Farben mischt, dann erhält man eine Farbe und man kann, wenn man die ursprünglichen Farben alle kennt, auch diese Farbe wieder reproduzieren.
Man kann aber nicht nur anhand der Farbe, sich die ursprünglichen Farben berechnen.
Und genau so funktioniert die kryptographische Hash-Funktion auch.
Also kann man sich jetzt so einen Block vorstellen als Farbpalette, auf der viele Farben drauf sind und man möchte sichergehen, dass genau diese Farben auf dieser Palette bleiben und sie niemand verändert. Dann bildet man von dieser Palette einfach die Mischfarbe,
und diese Mischfarbe wird auf einer weiteren Palette eine der Farben, die auf der Palette drauf ist und so weiter und so fort.
Also die Palette ist ein Block und die Farbe ist der Hashwert.
Und jetzt könnte man, wenn man eine Palette in der Hand hat, sich die Mischfarbe raussuchen und den Block oder die Palette, die da vorkommen soll, sich angucken, die Mischfarbe aller Farben bilden und sie mit der
Mischfarbe auf der Palette, die man zuerst in der Hand hatte,
vergleichen und sieht, ob das Gleiche ist oder nicht.

Fabian:
[12:30] Und kann dann damit das bestätigen, dass die Mischfarbe mit großer Wahrscheinlichkeit aus einer Palette gekommen ist, die genauso aussieht, wie die, die ich gerade überprüft habe.
Jetzt hattest du gesagt, diese Hashwerte sind definiert lang.
Das bedeutet im Prinzip ja, dass ich eine endliche Anzahl von möglichen Hashwerten habe.
Ich habe aber eigentlich ja fast eine unendlich große Anzahl von möglichen Blöcken. Das heißt doch aber im Prinzip, dass mehrere potenziell denkbare Blöcke auf demselben Hashwert zeigen müssen, oder?

Sebastian:
[13:06] Ja, theoretisch ist das genau so. Darum benutzt man Hashwerte, die sehr lang sind,

für Bitcoin zum Beispiel, und das ist auch in der Informationssicherheit so üblich, dass man diese Art von Hashwert verwendet, mit dieser Länge ... benutzt man so genannte 'SHA 256 Hashwerte'. Die 256 steht da für die Anzahl der Bits in dieser Prüfsumme.
Das heißt, man hat zwei hoch 256, also sehr viele mögliche Hashwerte.
Und jetzt sagt man, "Okay, das sind so viele, das wird schon nicht passieren, dass zwei Blöcke mal wirklich den gleichen Hashwert haben".
Aber theoretisch kann man das nicht ausschließen.
Man könnte sogar ausrechnen, also der 'zwei hoch 256 plus eine Block',
der müsste dann einen Hashwert haben, den es vorher schon mal gegeben hat.

Fabian:
[14:05] Den könnte man dann quasi nicht unterscheiden vom wahren Block?

Sebastian:
[14:09] Ja. Die Blöcke kann man dann nicht unterscheiden. Also, wenn man sagt, ich hänge wirklich einen gültigen Block, den so-so vielten Block hinten an und der hat tatsächlich den identischen Hashwert,
dann wäre es nicht unterscheidbar, welchen Block man hat.
Es gibt natürlich noch, wie ich eben gesagt habe, es muss ein gültiger Block sein ... Also viele
Hashwerte haben mehrere Blöcke, davon sind aber nur wenige überhaupt gültige Blöcke, die irgendwie der Struktur eines Blocks an sich überhaupt folgen.

Fabian:
[14:45] Also ich kann mir im Prinzip erst neben dem Hash auch noch angucken, ist das überhaupt ein ordnungsgemäß aufgebauter Block, so wie ich das mal vor definiert habe und am Ende sind das dann zwei Kriterien, die erfüllt werden müssen.
Einerseits brauche ich einen regelhaft ausgerichteten Block und auf der anderen Seite muss dann der Hashwert.

Sebastian:
[15:04] Und die Hoffnung ist einfach, dass man das praktisch nicht hinbekommt einen Block zu finden, der sowohl gültig ist, als auch den gleichen Wert hat. Würde man es schaffen einen solchen Block zu finden,
dann könnte man den Block einfach mit dem anderen in der Blockchain austauschen und niemand könnte das überprüfen.

Fabian:
[15:22] Aber im Prinzip ist ja die Bedingung, damit so eine Blockchain funktioniert, nur damit ich das richtig verstanden habe, dass alle Daten irgendwie öffentlich einsehbar sind.
Also ich muss ja die alten Blöcke betrachten können, um am Ende nachvollziehen zu können, stimmt der folgende Hashwert.

Sebastian:
[15:40] Ja und das vom Ende der Blockchain aus gesehen. Also dort wo man neue Blöcke immer anhängen kann,
von dem Ende aus muss man alle Blöcke kennen, bis zu dem Block aus dem man die Daten haben möchte, um das nachvollziehen zu können, ob die Daten stimmen.

Fabian:
[15:57] Ok. Ich hab in meinem Laienwissen Blockchain auch immer mit irgendwie so einem großen, kollaborativen Netzwerk assoziiert.
Jetzt klingt das für mich erstmal wie ein relativ banales Datenformat, was man jetzt auch für lokale Speicherung von Daten verwenden könnte.
Inwiefern eignet sich das denn so besonders für das große zusammenarbeiten?
Denn im Prinzip kann ich ja auch in einem Word-Dokument kollaborativ arbeiten und das ist keine Blockchain.

Sebastian:
[16:28] Also die Blockchain an sich als Datenstruktur ist wie alle anderen Datenstrukturen auch weder dezentral, noch zentral. Also eine Datenstruktur an sich hat diese Eigenschaft einfach nicht,
wie ein Word-Dokument an sich. Also nur ein Text ist ja auch nicht zentral oder dezentral.
Erst das Programm, was man benutzt, um dieses Word-Dokument zu bearbeiten, das macht daraus eine dezentrale oder eine zentrale Anwendung.
Und genau das gleiche kann man auch mit einer Blockchain tun.
Man baut ein System rund herum, sodass mehrere Leute an einer Blockchain arbeiten können.
Da ich ja schon gesagt hab, dass man eine Blockchain nicht manipulieren kann und auch keine Blöcke löschen kann, bleibt eigentlich nur noch über, dass man Blöcke anfügen kann.
Und genau das tun diese Systeme. Sie sorgen dafür, dass viele Leute sich einig werden, wie und welche Blöcke jetzt an die Blockchain angefügt werden.

Blockchain In Der Praxis: Bitcoins

Fabian:
[17:24] Die Hauptanwendung für sowas sind ja, wie du es schon gesagt hast, die Kryptowährungen, von denen die prominenteste wahrscheinlich die Bitcoin-Währung ist.
Es gibt, glaube ich, ganz viele. Da gibt es einen Wikipedia-Artikel mit 300 Einträgen von verschiedenen Kryptowährungen, von denen wahrscheinlich noch nie einer gehört hat, mit zum Teil absurd geringen Werten.
Wieso ist denn die Blockchain jetzt für Kryptowährungen so geeignet?
Wie funktioniert das eigentlich so eine Kryptowährung?

Sebastian:
[17:55] Also eignen tut es sich deswegen, weil man bei Währungen im Prinzip nur eine Möglichkeit hat,
was man mit dieser Währung tun kann, es ist, etwas davon jemand anderem zu geben.
Und es ist immer schön, wenn man ein Beispiel hat, in dem man nicht viele Möglichkeiten hat. Das macht es einfacher sowas zu bauen.
Es ist die einzige Option, das Überweisen quasi von Bitcoin zum Beispiel, auch sehr einfach. Also man braucht einen Absender, man braucht einen Empfänger und man braucht einen Betrag.
Das ist nicht viel. Und da kann man dann die eigentliche Überweisung ganz schnell

bauen und muss sich dann nur noch darum kümmern,
wie kommen jetzt diese Überweisungsdaten in die Blöcke rein. Und darum eignet sich eine Kryptowährung sehr gut, um überhaupt erst einmal so ein grundsätzliches System zu bauen, mit dem man das Ganze testen möchte.
Und das andere ist,
das es ja in die Dezentralisierung ging, also man wollte viele Systeme dezentralisieren.
Und ein Beispiel für ein besonders zentralisierte System sind die Banken.
Es gibt einen großen Server der da irgendwo in der Bank steht und der kennt alle Überweisungen.
Und wenn man jetzt anfangen möchte, Sachen zu dezentralisieren, und man will richtig auf die Kacke hauen, dann fängt man natürlich bei dem zentralisiertesten System an, was man so kennt. Und das waren dann einfach Banken und Währungen, womit man dann gesagt hat: "Ja.

[19:23] Damit bauen wir jetzt was." und dann kam Bitcoin bei rum.

Fabian:
[19:28] Also ist Bitcoin im Prinzip so eine Art Bilanzbuchhaltung im Blockchain-Format.

Sebastian:
[19:33] Genau. Also es ist wie ein Überweisungsverzeichnis, in dem alle getätigten Überweisungen drin stehen.

Fabian:
[19:41] Bisschen habe ich es soweit ganz gut mitgeschnitten.
Jetzt stellt sich mir aber natürlich die Frage ... schon beim Word-Dokument
ist es ein ziemlich großes Problem, wenn zwei, drei, vier, fünf Leute daran arbeiten und gleichzeitig am selben Wort herumbasteln,
dass dann die Software eigentlich im Prinzip zusammenbricht, weil sie nicht weiß, was ist jetzt hier der richtige Wert.
Ich hab jetzt also meine Blockchain, die dazu dient im Prinzip, Überweisungen zu verzeichnen.
Wie kommen denn jetzt die Überweisungen in den Block und wer entscheidet welche Überweisung in den Block darf? Weil, wenn ich versuche ein weltweites Währungsnetzwerk aufzubauen, dann kommen ja permanent irgendwelche Überweisungen rein
und ich weiß ja gar nicht, wie das sortiert wird.

Sebastian:
[20:29] Ja, im Prinzip geht man jetzt im grundlegenden Konzept erst einmal davon aus, dass niemand Geld überweist, das man nicht hat, und
auch der Empfänger und der Absender immer existieren. Das macht das alles viel einfacher
in dieser theoretischen Betrachtung. Also alle Überweisungen, die irgendwie in diesem System landen, sind auch gültig.
Also in dem Word-Dokument wäre es so, wenn man jetzt deutschen Text tippt, dann sind da nicht auf einmal chinesische Schriftzeichen dabei.
Das macht die ganze Überlegung schon erstmal einfacher, weil man nichts vorher filtern muss. Jetzt habe ich eine ganze Menge von Überweisungen, die in dem System herumfliegen,

und die werden jetzt von bestimmten Servern, also von bestimmten Teilnehmern im Netz, eingesammelt
und die halten die sich in so einer Art Warteschlange.

[21:19] Und jetzt versuchen die aus einem Teil der Überweisungen, die sie in der Warteschlange haben, den nehmen sie sich da raus und versuchen die in einen Block zu packen und diesen Block an die Blockchain anzuhängen.
Jetzt würde das natürlich dazu führen, dass ganz viele Blöcke erzeugt werden gleichzeitig. Darum braucht man ein System, das entscheidet, unter welcher Bedingung darf denn ein Teilnehmer überhaupt einen Block an die Blockchain anhängen.
Im Falle von Bitcoin, und das waren die Ersten, die das gemacht haben und
das ist auch die eigentliche Neuerung, was Bitcoin auszeichnet, ist das Verfahren, das die Bedingungen festlegt, mit der ein Teilnehmer so einen Block anhängen darf.
Man hat davon vielleicht schon gehört, das nennt sich Mining und bezeichnet das Finden eines bestimmten Wertes, der einen Block gültig macht.
Und nur, wenn man den bestimmten Wert gefunden hat, der diesen Block gültig macht, dann darf man diesen Block an die Blockchain, an die globale Blockchain anhängen.

Fabian:
[22:27] Also dieser bestimmte Wert, der ist eben jener genannte Hashwert. Es handelt sich quasi um ein Wettrechnen, sage ich mal.

Sebastian:
[22:34] Genau. Jetzt kommt ein zweiter Wert ins Spiel. Also aus dem Block wird weiterhin ein Hashwert berechnet,
aber dieser Hashwert muss eine bestimmte Bedingungen erfüllen. Und damit dieser Hashwert eine bestimmte Bedingungen überhaupt erfüllen kann, weil
man kann ihn ja nicht verändern, wenn man den genau gleichen Block hat,
gibt man jetzt einen zweiten Wert in diesen Block hinein, den man verändern kann. Und zwar muss man für diesen Wert,
den muss man so setzen, dass der Hashwert die Bedingung erfüllt.
Nun ist es so, dass eine kleine Änderung von den Ursprungsdaten den Hashwert nicht nur ganz klein verändert, sondern beliebig verändern kann.
Also eine kleine Änderung im Block, kann zu einer großen Änderung in dem Hashwert führen.
Das heißt, man sucht im Prinzip in dem Block eine bestimmte Zahl, die dazu führt, dass der Hashwert einem bestimmten Wert unterschreitet.
Und da der Hashwert ja so doll springt, kann man jetzt nicht einfach irgendwie die Zahl hochziehen und sieht, "Aha. Der Hashwert, der wird immer kleiner,
also muss ich einfach nur noch ein bisschen schneller hochziehen", sondern man ist wirklich darauf angewiesen, dass man durch Zufall den richtigen Wert findet, der diesen Hashwert kleiner als eine bestimmte Zahl macht.

Fabian:
[23:55] Also mein Block besteht dann am Ende quasi aus dem Hashwert des alten Blocks, den Überweisungen, die ich eingesammelt habe von einer Warteliste und aus einer Variable, die mir keiner vorgibt, sondern die ich frei durchprobieren kann.
Und jetzt errechne ich immer wieder einen Hashwert aus diesem Block und stelle fest, mit dieser Variable ist mein Hashwert noch zu hoch,
also passt einfach noch nicht an die Bedingung. Und währenddessen ist es quasi ein

Wettbewerb.
200 000 andere Leute versuchen in Konkurrenz zu mir ebenfalls die richtige Variable zu finden, die im Prinzip den Hashwert unter den Grenzwert legt.
Aber die haben nicht alle die selben Überweisungen von der Warteliste genommen, oder doch?

Sebastian:
[24:43] Genau. Theoretisch könnten die das tun.
Es ist aber sehr unwahrscheinlich, dass alle genau die gleichen Überweisungen nehmen. Die werden natürlich sehr ähnlich sein. Aber zusätzlich zu dem Hashwert des alten Blockes dieser variablen Zahl
und den Überweisungen, gibt es noch eine zusätzliche Überweisung in den Block und das ist eine Überweisung aus dem Nichts, an denjenigen der den Block erzeugt hat.
Also an denjenigen, der eine Zahl gefunden hat, die die Bedingung erfüllt.
Und zwar ist das die Motivation dafür, überhaupt diesen Rechenaufwand zu betreiben.
Wenn man den Rechenaufwand betrieben hat und
man hatte Glück und man erzeugt einen gültigen Block,
dann darf man sich als Belohnung selbst Währung aus dem Nichts überweisen.

Fabian:
[25:31] Also in der Blockchain-Grundstruktur ist quasi ein Blankoscheck vorgesehen, wo man dann einfach nur noch sich selbst als Empfänger eintragen darf.
Und das ist dann die Belohnung dafür, dass man sich die Mühe gemacht hat und mit anderen konkurriert hat um den nächsten Block.

Sebastian:
[25:47] Und genau so funktioniert das bei Bitcoin und genau so entstehen neue Bitcoin, indem ein neuer Block erzeugt wird.

Fabian:
[25:55] Das heißt, im Prinzip mit dem ersten Block sind auch die ersten Bitcoin entstanden. Jetzt hattest du gesagt, der Hashwert darf nicht über einen bestimmten Wert rüber gehen.
Ist das ein fixer Wert oder woraus ergibt sich das?

Sebastian:
[26:12] Ja,
dieser Wert wird so festgelegt, dass alle zehn Minuten ungefähr ein Block erzeugt wird.
Darum ändert sich der Wert. Also man guckt sich die, sagen wir mal, die letzten zehn erzeugten Blöcke an,
rechnet aus, wie lange die im Durchschnitt gebraucht haben.
Und wenn die jetzt nur acht Minuten gebraucht haben, dann macht man die Zahl, die der Hashwert unterschreiten muss, ein bisschen kleiner.
Man schränkt den Zahlenbereich, den man treffen muss, ein bisschen ein, um es schwieriger zu machen.
Dadurch erhofft man sich, dass es einfach ein bisschen länger dauert.
Und wenn die letzten zehn Blöcke im Schnitt zwölf Minuten gedauert haben, dann erhöht man den Wert ein bisschen, also erlaubt mehr Spielraum in dem Hashwert, um die Generierung von einem Block ein bisschen schneller zu machen.
Und so pendelt sich das dann auf zehn Minuten ein.

Und diese zehn Minuten, die sind willkürlich festgelegt. Da hat der, der Bitcoin programmiert hat, gesagt: "Ja, zehn Minuten sind eine gute Zeit."

Fabian:
[27:16] Das hat jetzt also keinen tieferen Grund oder Sinn? Das hätte man auch auf eine Minute setzen können?

Sebastian:
[27:22] Ja, allzu niedrig darf man das nicht setzen, da
hinter einem Block eine gewisse Rechenleistung stehen soll. Das ist die Idee dahinter, um das System sicher zu machen, dass man sagen kann: "Okay, ich musste doch schon Rechenaufwand für diesen Block aufwenden."
Man könnte es aber theoretisch höher machen.
Also, ob das nun zehn Minuten sind, zwanzig oder acht. Das macht kaum Unterschied.

Fabian:
[27:49] Und die Schwierigkeit der Berechnung ist quasi definiert über die Höhe der obersten, akzeptierten Hashwerte.
Je niedriger dieser obere Grenzwert ist, desto schwieriger ist es, durch einfaches Ausprobieren der Variable, einen Hashwert zu finden, der darunter liegt.

Sebastian:
[28:10] Genau. Also die Hashwerte starten bei null. Es gibt keine Hashwerte, die kleiner als Null sind.
Und wenn ich eine obere Grenze für den Hashwert setze und ich verniedrige die, dann habe ich weniger Zahlen überhaupt zur Auswahl und wenn ich die Grenze lockere, also eine höhere Zahl erlaube, dann habe ich mehr.

Fabian:
[28:29] Okay. Stellen wir uns mal vor, ich hab jetzt hier meinen Laptop angeworfen und dem gesagt: "Rechne doch mal lustig Blockchain-Blöcke aus, mach mal ein paar Überweisungen rein.",
dann sagt mein Laptop: "Ja. Ich hab jetzt hier einen Block gerechnet.", und irgendwo anders auf der Welt sagt jemand: "Ich habe aber auch einen Block ausgerechnet." ... Wer entscheidet denn dann, welcher Block jetzt der Richtige ist? Oder werden beide akzeptiert?

Sebastian:
[28:52] Genau das ist das Problem bei allen dezentralen Anwendungen: Was ist, wenn etwas gleichzeitig passiert?
Das ist in etwa so wie in dem Word-Dokument Beispiel, wenn jetzt beide das gleiche Wort ändern, aber jeweils zu einem anderen.
Dann müsste man sich entscheiden, welches Wort gilt denn jetzt. Und da hat man sich in Bitcoin gedacht:
Naja. Wir entscheiden das nicht direkt, wenn zwei konkurrierende Blöcke entstanden sind, sondern wir warten einfach ab und nehmen dann die Verzweigung, die schneller gewachsen ist.
Es kommt zu einer Verzweigung und das ist jetzt erstmal okay.

[29:33] Und die Teilnehmer, die einen Block anfügen möchten, die müssen sich jetzt entscheiden, an welches Ende sie einen Block anfügen möchten. Jetzt entscheiden die sich und
dadurch kommt es dazu, dass eine eine Verzweigung schneller wächst, als die andere. Und ab einem bestimmten Vorsprung sagt man einfach, die Verzweigung oder der Ast, der den Vorsprung hat, der ist jetzt der gültige. Und der Kleinere, also der nicht so schnell gewachsen ist, der wird verworfen.
Was natürlich dazu führt, dass die gesamte Rechenleistung, die man in den nicht so schnell wachsenden Ast gesteckt hat, verloren geht.
Genauso wie alle Rechenleistung verloren geht, die man in das Finden eines gültigen Blocks gesetzt hat,
wenn jemand anderes einfach schneller war. Also über das gesamte System gesehen, geht da ganz schön viel Rechenleistung drauf ... für erst mal nix.
Aber um die Ecke gedacht, erhöht das natürlich die Sicherheit von dem ganzen System. Je mehr mitrechnen und je mehr Rechenleistung auch verschwendet wird, im ersten Hinblick, umso mehr Sicherheit hat man im System an sich.

Fabian:
[30:45] Das heißt ja Prinzip, dass von der Rechenleistung sogar der Löwenanteil eigentlich verworfen wird, oder?

Sebastian:
[30:54] Ja. Also man könnte sich jetzt ein Extrembeispiel vorstellen, dass man sagt, es ist ja wirklich zufällig, ob man die richtige Variable in so einem Block rein setzt oder nicht und damit einen gültigen Block erzeugt.
Also du könntest jetzt einfach auf deinem Laptop Glück haben und direkt der erste Block mit der ersten Variable, der funktioniert.
Und nebenbei läuft irgendwo so eine riesige Bitcoin Mining-Farm, die in der Zeit schon ein paar Milliarden durch getestet hat. Und
das ist alles hinfällig, was dann dieser riesige Server da ausgerechnet hat, nur weil dein Laptop jetzt gerade Glück hatte und das direkt mit dem ersten Versuch geschafft hat.

Fabian:
[31:32] Also es ist so ein bisschen eine Mischung aus Wettrechnen und Lotto.

Sebastian:
[31:37] Ja, also Wettlotto quasi.

Fabian:
[31:41] Was mir noch nicht so ganz klar geworden ist ... Ich möchte ja mit meinen Bitcoins irgendetwas bezahlen.
Und wer garantiert mir denn jetzt, dass meine Überweisung überhaupt mal in so einen Block kommt? Also so wie ich das verstanden habe, suchen sich die Miner einfach die Überweisungen raus, die ihnen irgendwie gerade in den Kram passen.
Wer garantiert, dass meine Überweisung irgendwann mal dran kommt? Oder kann ich auch einen leeren Block abgeben?

Sebastian:
[32:08] Ja, man kann leere Blöcke abgeben, das funktioniert. Gerade in der Anfangszeit von Bitcoin ist das sehr häufig passiert, dass einfach, es gab keine Überweisung. Also

gerade überhaupt
der zweite Block, wohin soll der Erste seine,
ich weiß nicht, wie viel es damals waren, ich glaube, 10 Bitcoin hat man noch bekommen, wohin soll der die Überweisung direkt im nächsten Block?
Das hat er einfach nicht getan und darum gab es sehr viele leere Blöcke.
Mittlerweile sieht das sehr viel voller aus. Es gibt auch eine Obergrenze für die Anzahl der Überweisungen in diesen Blöcken.
Darum ist es auch wichtig, dass man eine Warteschlange hat. Wenn mehr Überweisungen ankommen, als in den nächsten Block passen, dann muss man die auch so aufstauen können. Und dadurch kann es halt auch passieren, dass man einige Blöcke warten muss, bis seine Überweisung überhaupt in einem Block angekommen ist.
Aber garantieren, dass eine Überweisung überhaupt in einen Block kommt, kann man eigentlich gar nicht, weil sich die Teilnehmer, die die Blöcke generieren, das ja aussuchen können.
Wenn man das wirklich garantieren möchte, dann müsste man selbst mitrechnen und würde dann natürlich seine eigene Überweisung, wenn man einen gültigen Block erzeugt, da mit rein tun. Warum sollte man die auch draußen lassen?
Aber es kann einem auch niemand garantieren, dass man überhaupt mal einen gültigen Block erzeugt.
Und darum ist es praktisch nicht garantiert, dass eine Überweisung überhaupt ankommt.

[33:34] Aber jetzt geht man davon aus, da draußen wird es hinreichend viele Mining-Teilnehmer geben, also Teilnehmer, die auch mit an den Blöcken rechnen,
die so halbwegs fair die Überweisungen in ihre eigenen Blöcke aufnehmen, sodass meine Überweisung dann schon in einer angemessenen Zeit drin landet.
Und das ist auch das Vertrauen von dem ich ganz am Anfang gesprochen hatte, dass man sagt: "Ich vertraue erstmal dem System an sich, dass es sicher ist.", und das System baut darauf,
dass man der Gesamtheit vertrauen kann.
Also, dass ich sage: "Es gibt einfach genügend Teilnehmer, die sich schon nach den Regeln verhalten."

Fabian:
[34:18] Weißt du, wie viele Überweisungen in so einen Block hineinpassen?

Sebastian:
[34:21] Bei Bitcoin sind es 1024. Das kann man natürlich ändern. Das ist auch eine einfach so festgelegte Zahl.
Das sorgt einmal dafür, dass die Hashwert-Berechnung nicht zu lange dauert, weil je größer die Daten werden, die ich in diese Hash-Funktion rein tue, desto länger dauert das.
Zum anderen ist es eventuell auch ein Anreiz für die Teilnehmer, jetzt nicht für eine Überweisung einen Block zu generieren.
Aber wenn natürlich nur eine Überweisung daliegt, kann man auch für eine Überweisung einen Block generieren. Aber man hat das nach oben begrenzt.
Also, sodass auch die Berechnung der Blöcke, also die Dauer, die es braucht, um einen Hashwert zu berechnen, irgendwie ein bisschen vorhersehbar bleibt.

Fabian:
[35:05] Im Prinzip habe ich ja als Miner aber erst nicht so den großartigen Anreiz mich darum zu kümmern, ob andere Überweisungen machen können, denn meine 'Null-Überweisungen', mein Blankoscheck, den bekomme ich ja trotzdem, oder?

Sebastian:
[35:18] Ja, das ist richtig. Das ist wirklich das Vertrauen dann, dass es da draußen genügend Teilnehmer gibt, die auch meine Überweisungen mit aufnehmen würden.

Fabian:
[35:27] 1024 Überweisungen in zehn Minuten kommt mir jetzt erst mal nicht so wahnsinnig viel vor. Ich kann es nicht so richtig einschätzen, wie viel weltweit in einer Minute überwiesen wird.
Aber das limitiert die praktische, alltägliche Anwendbarkeit von Bitcoin schon. Also wenn man quasi, wie jede Kartenzahlung ist ja eigentlich eine Finanztransaktionen, wenn ich das jetzt auf Bitcoin basieren lassen möchte, dann wird es ganz schön eng in den Blöcken oder.

Sebastian:
[35:53] Ja, es reicht nicht aus. Paypal hat zum Beispiel viel mehr Überweisungen.
Das könnte man mit der Bitcoin-Blockchain überhaupt nicht tun.
Das geht nicht. Darum gibt es andere Blockchain-Ansätze, die das so ähnlich machen.
Und an den Parametern, aber so rum geschraubt haben, dass sie mehr Blöcke erzeugen können. Dadurch kann man schon mal mehr überweisen.
Und zum anderen auch die Größe ein bisschen größer gemacht haben. Aber hauptsächlich geht es darum, dass man einfach mehr Blöcke in der gleichen Zeit erzeugt, um mehr Überweisungen machen zu können.
Aber das ist eine große Schwachstelle von diesen Kryptowährungen, dass die Anzahl der Überweisungen pro Minute begrenzt ist.

Fabian:
[36:33] Und gleichzeitig ist auch der Punkt sicherlich einer Limitierung, dass mir niemand garantieren kann, ob und in jedem Fall niemand garantieren kann, wann eine Überweisung denn tatsächlich ankommt.

Nachteile Von Bitcoin

[36:44] Also der Supermarkt möchte ja schon gerne wissen, dass ich ihn jetzt auch tatsächlich bezahlt habe, oder?

Sebastian:
[36:49] Genau, das große Problem ist das 'Wann'. Das ist die Praxis-Untauglichkeit für Bitcoin, daran scheitert dieses System im Alltag. Wenn man sich jetzt ein Haus kaufen würde mit Bitcoin,
da kann man auch mal zwei Wochen warten, das ist kein Problem. Oder wenn man sich ein Auto kauft, das müssen die nochmal flott vorher aussaugen und dann wird da noch etwas anderes dran rumgeschraubt, das holt man sich erst ein paar Tage später ab,
da funktioniert das. Aber wenn man sich mal schnell Kaffee kaufen möchte und

Bitcoin alle zehn Minuten einen Block generiert und man hat gerade Pech, dann muss man wenigstens zehn Minuten warten, dann hat man noch ein bisschen mehr Pech, und im nächsten Block ist eine eigene Überweisung gar nicht drin. Keiner steht 20 Minuten an der Caféteria-Theke und wartet bis er seinen Cappuccino nun endlich trinken darf.
Das ist natürlich völlig Praxis untauglich. Da kann man sich Lösungen für überlegen, die sind alle jetzt nicht so prickelnd.
Die eine wäre, man guckt sich nur an, welche Überweisungen in dem System sind, und wenn da die Überweisung drin ist, dann akzeptiert man die schon.

[37:53] Also der Verkäufer sagt: "Ich gucke mal schnell nach, ob die Überweisung jetzt schon im Netzwerk ist, ob die schon von den Teilnehmern, die Blöcke berechnen, bearbeitet wird und akzeptiere die dann.
Es kann natürlich immer passieren, dass sie gar nicht drin vorkommt. Oder der andere Fall,
man kann in Bitcoin das gleiche Geld mehrmals ausgeben.
Also könnte es sein, dass man in eine Kaffeebar geht, sich da einen Capuccino kauft, schnell über die Straße rennt, sich noch einen kauft und dann von dem gleichen Geld noch einen kauft,
und dann wird nur einer von beiden bezahlt, weil die andere Überweisung damit ungültig wird.

Fabian:
[38:31] Okay, das ist natürlich ein großes Problem. Gibt es dafür irgendwie eine Lösung?

Sebastian:
[38:36] Die einzige Lösung, um das zu verhindern, ist, dass man halt wartet. Man könnte sich jetzt in beiden Cafés einen Kaffee kaufen und beide können erst dann sicher sein, dass die Überweisung überhaupt in einem Block ist,
wenn Sie das auch selber sehen. Sie müssten wirklich warten bis die Überweisung in einem Block drin ist. Und dann kann es ja immer noch sein, dass dieser Block zu so einem kleineren Ast gehört, der später abgeschnitten wird.
Das heißt, man wartet nicht nur bis die Überweisung überhaupt in einem Block ist, sondern bis die Überweisung hinter einer bestimmten Anzahl von Blöcken steht.
Und da kommt es jetzt wieder ins Spiel, dass eine gewisse Menge Rechenleistung für einen Block aufgewendet werden muss.
Man guckt sich an, wie viel Rechenleistung ist mir jetzt dieser Kaffee wert.
Ich sage zum Beispiel: "Der Kaffee ist mir die Rechenleistung von zwei Blöcken wert."

[39:29] Das heißt, ich sehe die Überweisung ist in einem Block und warte noch zwei weitere Blöcke ab, bis ich die Überweisung als akzeptiert ansehe. Dann ist die Überlegung, ich sage:
"Gut, diese zwei Blöcke sind so viel Rechenleistung wert, wie mir dieser Kaffee wert ist."
Also hätte jetzt dieser eine Kunde, der gerade vor mir steht, so viel Rechenleistung aufgewendet und hätte diese beiden Blöcke selber erzeugt, um mich auszutricksen, dann hätte er so viel Strom verbraucht, dass er sich einen zweiten Kaffee auch noch hätte kaufen können und damit kein Plus gemacht hat. Das ist die Überlegung dahinter.

Fabian:
[40:07] Also um das nochmal in andere Worte zu fassen, wenn sich so eine Aufsplittung ergibt, du hattest gesagt, das nennt man Fork.

Sebastian:
[40:15] Ja oder Verzweigung, das schöne deutsche Wort dafür.

Fabian:
[40:19] Dann hab ich ja im Prinzip jetzt die doppelte Anzahl an Konten und habe spontan mein Geld verdoppelt, weil das setzt zwei Blöcke gibt, in denen ich jetzt Überweisungen tätigen kann.

Sebastian:
[40:31] Man muss das schon mit Absicht getan haben, dass man bewusst zwei verschiedenen Teilnehmern, die so Blöcke erzeugen, zweimal
die Transaktion des gleichen Geldes an einen anderen Empfänger gegeben hat und hofft jetzt darauf, dass die beide gleichzeitig einen gültigen Block erzeugen, in den nun zweimal die Überweisung des gleichen Geldes drinsteht.
Das ist genau das, was du gerade gesagt hattest, aber das das passiert nicht aus Versehen, sondern man muss das wirklich beabsichtigen.

Fabian:
[41:05] Was ja aber aus Versehen passieren könnte, wenn ich es richtig verstanden habe, dass wenn jetzt spontan ohne meine eigene Beteiligung so ein Aufzweigung
entsteht und der eine Miner hat meine Überweisung mit hinein genommen und der andere nicht, dann hab ich quasi in der einen Realität
die Überweisung getan.
Der Händler guckt nach, sagt: "Steht im Block drin, alles gut."
Und in dem anderen Block ist die Überweisung aber gar nicht drin und ich hab das Geld noch nicht bezahlt.
Und wenn sich dieser dann als der richtige Strang entwickelt, könnte ich ja zum Beispiel nachträglich die Überweisung dann vielleicht wieder raus killen und hätte meinen Kaffee umsonst bekommen, oder?

Sebastian:
[41:44] Das kann durchaus passieren.

Fabian:
[41:46] Und da hilft dann aber im Prinzip wieder nur, auf das Schneckenrennen abzuwarten. um zu gucken, welcher Strang ist der, der sich am Ende durchsetzt und steht dann die Überweisung da auch wirklich drin.

Sebastian:
[41:59] Genau. Also die universale Lösung ist warten.

Fabian:
[42:08] Also um es ein bisschen plump zu sagen, Bitcoin ist etwas für Leute, die Zeit haben.

Sebastian:
[42:11] Ja, man muss sich Zeit lassen beim Kaffee trinken. Das ist vielleicht auch ganz gut für die Gesellschaft.

Fabian:
[42:15] Entschleunigung als Trend.

Sebastian:
[42:18] Das war vielleicht das eigentliche Ziel von Bitcoin überhaupt, das hat nur noch niemand herausgefunden.

Fabian:
[42:24] Aber das ist doch im Prinzip schon ganz schön enttäuschend, dass so viel Rechenleistung, was ja im Prinzip auch Strom ist, einfach nur verpufft, oder?

Proof Of Work Vs. Proof Of Stake

Sebastian:
[42:33] Genau das haben sich auch andere Leute gedacht, es ist ja ziemlich offensichtlich, dass das irgendwie doof ist, wenn so viel Rechenleistung verpufft.
Und dann hat man sich andere Methoden überlegt, wie man denn die Zusammenarbeit der Teilnehmer anders regeln könnte.
Ein anderer Ansatz, der nennt sich 'Proof of Stake'.
Ich weiß gar nicht, ob ich den Namen des Bitcoin-Ansatzes gesagt hatte, der nennt sich 'Proof of Work'. Das 'Work' ist jetzt mittlerweile ziemlich selbsterklärend, denke ich.

[43:02] Und Proof of Stake hat die gleiche Idee, dass man nach einer gewissen Anzahl oder nach einer gewissen Leistung entscheidet, wer dran sein darf.
In dem Fall bei Proof of Stake ist es so, dass man nach dem Anteil der Token, also dem Anteil, das man selbst an der Währung hat.
Also es gibt zum Beispiel zehn Bitcoin, davon gehören mir zwei,
also habe ich einen Anteil von zwei Zehntel. Und wenn man jetzt jeden Teilnehmer betrachtet und in so einen Graphen eintragen würde, dann würde man so eine Art Kurve bekommen.
Jeder Teilnehmer hat ein Gewissen Anteil und das betrachtet man jetzt als Wahrscheinlichkeitsverteilung.
Je mehr Anteile ein Teilnehmer hat, desto wahrscheinlicher ist es, dass er den nächsten Block erzeugen darf.
Jetzt braucht man trotzdem für die Entscheidung, welcher Teilnehmer jetzt konkret dran ist, noch einen Zufallsgenerator.
Also im Prinzip bräuchte man jetzt noch jemanden, der würfelt und da sitzt und die ganze Zeit Zufallszahlen erzeugt.
Das Problem bei Zufallszahlen im Computer ist es, dass ein Computer keinen echten Zufall erzeugen kann.

[44:24] Ein Computer kann aus einer Zahl durch eine mathematische Funktion eine neue Zahl erzeugen
und die kann man so gestalten, dass ein bestimmter Zahlenbereich gut abgedeckt ist und

das sieht, wenn man es von außen betrachtet, auch zufällig aus.
Also die nächste Zahl ist nicht immer 1, 2, 3 und 4 und so weiter, sondern das ist 1,110, 12, 43. Es springt wild durch die Gegend, aber deckt den Bereich, den man gerne haben möchte relativ gut ab.
Dieser mathematischen Funktion muss man natürlich einmal eine Startwert geben.
Und wenn man diesen Startwert kennt, kann man den Pfad, den die mathematische Funktion durch die Zahlen nimmt, auch exakt vorberechnen.
Das wäre natürlich doof für so ein 'Proof of Stake'-Prinzip, wenn man quasi vorher schon weiß, welcher Teilnehmer wann dran ist mit 'Block generieren'.
Darum müsste man dieser Zufalls-Funktion auch einen tatsächlichen Zufall füttern, also zum Beispiel die Lottozahlen,

[45:31] die sind zufällig. Man geht davon aus, dass sie nicht manipulierbar sind, für jeden überprüfbar.
Und dann kann man, davon ausgehend, eine gewisse Strecke Zufallszahlen erzeugen lassen.
Man müsste dann aber wieder neue Lottozahlen reinwerfen, um den echten Zufall in diesem System zu erhalten.
Und dann würde das,
nein, würde nicht nur, das hat auch schon jemand gebaut. Das funktioniert dann auch, also dass die Teilnehmer dann in einer gewissen Reihenfolge dran sind
und über den großen Zeitraum betrachtet auch die Teilnehmer nach dem Anteil ihrer Token, die sie besitzen an der Gesamtanzahl der Token, auch so oft die Blöcke generieren durften.

Fabian:
[46:17] Also ist es am Ende wie bei der Losbude. Bloß dass der, der schon sehr viele Token hat, einfach sehr viele Lose ziehen darf und der, der wenig Token hat, der darf halt nur ein Los ziehen.

Sebastian:
[46:29] Genau. Also ich finde diese Lotto-Analogie so toll.
Also bei Proof of Work war es ja quasi so, man darf Lottoscheine ausfüllen und man hat entweder Glück oder nicht und der, der schneller Lottoscheine ausfüllen kann, der hat halt öfter Glück.
Und hier ist es, wie du gerade gesagt hast, jeder bekommt eine unterschiedliche Anzahl an Lottoscheinen, darf die alle ausfüllen und es gewinnt aber auch nicht immer automatisch der, der die meisten Lottoscheine bekommen hat, sondern das ist dann zufällig verteilt.

Fabian:
[46:59] Es ist nur sehr wahrscheinlich, dass jemand mit vielen Lottoscheinen gewinnt, gegenüber jemandem, der nur einen hat.

Sebastian:
[47:03] Genau und gerade auf einen größeren Zeitraum gesehen hat natürlich der, der den größten Anteil hat, auch die meisten Blöcke erzeugt.
Das nennt sich in der Mathematik das Gesetz der großen Zahlen. Also würde man unendlich Blöcke erzeugen, dann würde die Verteilung der erzeugten Blöcke genau der Verteilung der Lottoscheine entsprechen.

Fabian:
[47:28] Aber ist das nicht eigentlich für eine Währung völlig ungeeignet, weil ich dann ja im Prinzip dafür sorge, dass die Leute, die ohnehin schon viele Token haben, kostenlos neue bekommen.

Sebastian:
[47:40] Genau. Das ist ein Problem. Es gibt noch ein grundlegenderes Problem: Womit fängt man an? Man hat am Anfang, hat niemand Token.
Und wenn niemand einen Lottoschein bekommt, dann ist auch nie jemand dran. Das wäre ein ziemlich langweiliges System.
Und darum benutzt man dann so hybride Verfahren. Man macht so ein bisschen Proof of Work am Anfang, damit das anläuft und wenn man genug Token hat, dann macht man Proof of Stake und hofft einfach, dass sich das nicht bei Einem akkumuliert.
Ja sonst ist das System natürlich übern Haufen.

Fabian:
[48:12] Und ist dieses Proof of Stake schon tatsächlich auch umgesetzt worden? Setzen Kryptowährungen darauf? Oder hat sich Proof of Work da als Kompromiss oder als beste Lösung durchgesetzt?

Sebastian:
[48:24] Ja, also Proof of Work hat natürlich einmal den Vorteil, dass man es aus dem Nichts starten kann,
im Gegensatz zum Proof of Stake. Und das funktioniert die ganze Zeit. Also egal wie viele Teilnehmer im Netz sind, das funktioniert immer.
Und man muss auch nicht aufwendig echten Zufall erzeugen und man muss auch nicht aufwendig vorher die Anteile der Teilnehmer rausfinden.
Und das macht es sehr einfach im Bau und darum gibt es sehr viele Kryptowährungen, die genau darauf setzen.
Für Proof of Stake gibt es aber auch Implementierungen, die kennt nur keiner, außer wahrscheinlich der, der das gebaut hat.
Es gibt auch noch Abwandlungen davon, wo man den eigenen Anteil jemand anderem so verleihen kann, damit der, man kann seine Lottoscheine jemand anderem geben.
Das ist auch umgesetzt, aber das benutzt einfach niemand. Das ist nicht so groß geworden wie Bitcoin.

Asynchrone Verschlüsselung Und Sicherheit

Fabian:
[49:19] Ich wollte eine andere Sache noch einmal ansprechen, die mir aufgefallen ist: Wenn wir jetzt davon reden, dass wir im Prinzip ja gerne das Bankenwesen ersetzen möchten mit Bitcoin
und wir müssen garantieren, dass alle Blöcke öffentlich einsehbar sind, denn nur so können wir ja die Integrität der Daten garantieren, dann heißt das ja, dass jeder meinen Kontostand nachvollziehen kann.

Sebastian:
[49:44] Ja, das ist tatsächlich so. Das ist auch gewollt. Der einzige Unterschied zu dem normalen Bankkonto ist, dass der Name, mit dem man dieses Bankkonto eröffnet, nicht der eigentliche Name von einem selbst ist,
sondern so eine Art Nummer bekommt. So kann man sich das erst einmal vorstellen. Jeder Teilnehmer denkt sich eine Nummer aus, die es noch nicht gibt und sagt: "Hier, hallo, das bin ich."
Und wenn ich jetzt jemandem etwas überweise, dann muss ich auch seine Nummer kennen und schreibe in die Überweisung rein:
Die Nummer, die ich bin, überweist so und so viel an die andere Nummer.
Und ein Dritter, der drauf guckt, der sieht nur den Betrag und die Nummern von den beiden Leuten, an die das gegangen ist und die Anonymität, die dahinter steht, ist einfach nur, dass man nicht zu der Nummer auch die Person kennt.

Fabian:
[50:34] Also ein bisschen wie ein Schweizer Nummernkonto. Okay,
na dann suche ich mir doch jetzt einfach aus der Blockchain die Kontonummer mit dem höchsten Betrag raus und geh damit fröhlich einkaufen. Weil das kann ja niemand überprüfen, dass ich das bin.

Sebastian:
[50:47] Genau, das möchte man natürlich auch verhindern. Und darum ist es nicht einfach nur eine banale Nummer, sondern man benutzt asynchrone Verschlüsselungen.
Asynchrone Verschlüsselung hat immer zwei Schlüssel.
Es gibt einen privaten Schlüssel und es gibt einen öffentlichen Schlüssel. Den privaten Schlüssel, wie der Name schon sagt, den hält man geheim,
den kennt man nur selbst. Und den öffentlichen Schlüssel, den kann man allen anderen auch geben, die können dann auch untereinander noch weiter verteilen,
den darf ruhig jeder haben. Und es ist so, dass wenn man mit dem öffentlichen Schlüssel etwas verschlüsselt, dann kann man das nur mit dem privaten Schlüssel entschlüsseln.
Und umgekehrt funktioniert das auch, wenn man mit dem privaten Schlüssel etwas verschlüsselt, dann kann man das nur mit dem dazugehörigen öffentlichen Schlüssel wieder entschlüsseln. Und seine eigene Identität
weist man mit seinem eigenen privaten Schlüssel nach.
Man geht hin in das Netzwerk und sagt: "Hallo, ich bin die Nummer 3."
Dann sagt der andere: "Das glaub ich dir nicht. Beweis das mal."
Und dann nehme ich einen Wert, den ich mir ausdenke, zum Beispiel ABC und sage dem, der mir gesagt hat, er wäre Nummer 3, dem sag ich: "Hier verschlüssel mal ABC mit dem privaten Schlüssel von Nummer 3."
Dann tut er das. Dann bekomme ich das Verschlüsselte wieder.
Ich kenne den öffentlichen Schlüssel von Nummer 3. Und wenn ich

[52:17] das Verschlüsselte, was ich bekommen habe, mit dem öffentlichen Schlüssel wieder entschlüssele und ich erhalte ABC, dann weiß ich, aha, mein Gegenüber, was behauptet, es wäre Nummer 3, hat auch dem privaten Schlüssel von Nummer 3, dem glaub ich das jetzt.
Und wenn ich irgendwas anderes als ABC entschlüssele, dann weiß ich, er hat den privaten Schlüssel von Nummer 3 nicht und ich glaube ihm nicht, dass er Nummer 3 ist.

Fabian:
[52:42] Würde das auch anders funktionieren, dass ich mir ABC ausdenke, das mit dem öffentlichen Schlüssel verschlüssele und dann frage: "Was steht da?"

Sebastian:
[52:50] Das würde auch funktionieren, aber das könnte ein dritter umleiten.
Also man würde ja im Klartext zurück übertragen, was da steht. Also wenn ich ABC verschlüssele,
dann würde ich das dir hingeben, du würdest ABC sehen und müsstest das jetzt mit meinem öffentlichen Schlüssel verschlüsseln, damit nur ich das wieder entschlüsseln kann.
Das ist ein bisschen viel hin und her, darum tut man das nicht so.

Fabian:
[53:19] OK. Ich habe es richtig verstanden. Es wäre technisch denkbar, es ist nur unpraktisch. Und der öffentliche Schlüssel ist dann einfach meine Kontonummer, oder?

Sebastian:
[53:22] Genau. Ja genau.

Fabian:
[53:28] Oder ist das anhänglich an die Kontonummer?

Sebastian:
[53:30] Ja, man kann sich den öffentlichen Schlüssel wie eine Kontonummer vorstellen.
Der öffentliche Schlüssel ist quasi nicht direkt eine Kontonummer,
aber man kann es so betrachten.

Fabian:
[53:41] Also so ein universelles Identifikationensmerkmal, das ich überprüfen kann.

Sebastian:
[53:44] Ja, es ist quasi das Authentifizierungsmerkmal.
Damit identifiziert man niemanden, sondern derjenige, der dazu gehört, authentifiziert sich damit.
Also ich weiß, es gibt jemanden mit der Nummer 3 und ich weiß, das ist der öffentliche Schlüssel dazu.
Und wenn jemand kommt und sagt: "Ich bin Nummer drei" und ich kenne den öffentlichen Schlüssel dazu, dann kann ich das überprüfen.
Unpraktisch ist es, wenn ich nur den öffentlichen Schlüssel auch als Identifikationsmerkmal nehme, weil ich dann immer alle, die ich habe, durchprobieren müsste und das wäre auch ein bisschen unpraktisch.

Fabian:
[54:22] Also ist es im Prinzip so, dass bei den Kryptowährungen gibt es einmal sozusagen die Teilnehmer-Nummer und dem zugeordnet, separat nochmal einen öffentlichen Schlüssel, den ich mir dann raussuchen kann, wenn ich etwas überprüfen möchte.
Und eine Überweisung funktioniert dann quasi durch paralleles Bearbeiten von mehreren Geschichten.
Also ich kündige mich dir an, ich sage: "Ich möchte dir einen Bitcoin überweisen."

Dann ist der eine Prozess, dass ich diese Überweisung in eine Warteliste schreibe und ganz fest die Daumen drücke und hoffe, dass irgendein Miner das in seine Rechenoperationen mit aufnimmt.
Und der zweite Schritt ist, dass du überprüfst, ob ich wirklich Konto 3 bin.

Sebastian:
[55:02] Genau. Also man kann ungefragt Leuten Bitcoin geben.
Das ist sehr praktisch. Man kann einfach Leute mit Geld bewerfen. Eine Überweisung gestaltet man so: Man schreibt seinen eigenen Absender rein,
man schreibt den Empfänger rein und schreibt den Betrag rein. Man baut davon wieder so einen Hashwert, wie vorhin auch, und
verschlüsselt diesen Hashwert mit seinem privaten Schlüssel.
Und das nennt sich dann Signatur. Es ist vergleichbar mit einer Papier-Signatur, also einer Unterschrift.
Und jetzt kommt das in so einen Block rein. Und der andere, der das Geld haben möchte, der geht jetzt hin, guckt sich die Überweisung an, sagt: "Okay, ist alles schick."
Und jetzt berechnet der daraus den Hashwert und nimmt die Signatur, die da drin steht, entschlüsselt das mit dem öffentlichen Schlüssel.
Und wenn da auch dieser Hashwert bei rauskommt, dann weiß man, okay, die Überweisung ist genau so, wie der Absender das haben wollte und es hat niemand zwischendurch was dran rummanipuliert, zum Beispiel
den Absender geändert. Das wäre ja fatal.

Fabian:
[56:11] Also der Miner überprüft nichts. Der nimmt das einfach auf und du überprüfst hinterher anhand des verschlüsselten Eintrags im Block dann, ...

Sebastian:
[56:13] Dem ist das völlig egal.

Fabian:
[56:22] ob die Überweisung so eingetragen wurde, wie ich dir das mal angekündigt hatte.

Sebastian:
[56:28] Genau.

Fabian:
[56:29] Also auch hier wieder das Problem: Ich kann es eigentlich erst dann überprüfen, sobald alles akzeptiert ist.

[56:39] Okay, dann hab ich, glaube ich, verstanden, wie man bei Bitcoin etwas überweist.

Sebastian:
[56:42] Ja, da gibt es dieses eine Bild dazu, das zeigt das, ... der private Schlüssel steht da immer in so einer Box und
dann geht da so ein Pfeil zu Hashwert. Und genau das ist das.
Also man nimmt die Prüfsumme für die Überweisung und wenn man die mit seinem privaten Schlüssel verschlüsselt, dann hat man es signiert und jeder andere kann überprüfen, ob das noch genauso in dem Zustand ist, wie als ich das signiert habe.

Fabian:
[57:08] Weil alle Leute den öffentlichen Schlüssel kennen und die können dann einfach das zurück rechnen und sagen: "OK.
Da wurde nichts dran rummanipuliert." Und wäre es manipuliert, dann würde es am Ende nicht mehr aufgehen, weil man ja den privaten Schlüssel nicht kennt und das nicht so nachrekonstruieren kann,
dass es so aussieht, als käme es von mir.

Sebastian:
[57:28] Genau man müsste zwei Hürden überwinden. Einmal hat man auch wieder das gleiche Problem mit den Hashwerten.
Es gibt wieder zwei Überweisungen, die den gleichen Hashwert haben.
Die sind theoretisch da, nur muss man aber auch erst einmal finden und das wäre eine Hürde die man überwinden könnte. Und die andere wäre,
man schafft es den privaten Schlüssel zu erraten. Und damit man das noch schwerer macht, macht man diesen privaten Schlüssel noch viel länger als diese Hash-Funktion, die 256 Bit lang sind.
So ein privater Schlüssel ist irgendwas standardmäßig zwischen 4 096, kann aber bis zu 12 000 lang sein und 'zwei hoch zwölftausend' ist schon eine verdammt große Zahl. Da muss man schon ganz schön lange rumprobieren.

Proof Of Participation

Fabian:
[58:14] Du warst aber weder mit Proof of Work noch mit Proof of Stake so richtig glücklich für deine Anwendung.

Sebastian:
[58:21] Ja, also ich weiß nicht, ob ich damit so unglücklich war. Auf jeden Fall die Leute, die das haben wollten, waren damit nicht glücklich.
Die hatten das Problem, sie haben sehr wenig Teilnehmer.
Das ist doof für sowas wie Proof of Stake, weil die Verteilung einfach nicht so schön aussieht. Und sie wollen auch möglichst wenig Rechenleistung dafür investieren.
Da ist wieder Proof of Work nicht so günstig. Gleichzeitig möchten die sehr hohe Sicherheit haben. Da ist beides ungeeignet, wegen der statistischen Ungenauigkeiten, die man in diesen Systemen hat.

[58:59] Da sagt man, dass es sobald bei Proof of Work ein Teilnehmer zwischen 20 und 30 Prozent der Gesamtrechenleistung hat, wird das gesamte System instabil.
Wenn man aber nur 10 Teilnehmer hat, dann ist es schon recht wahrscheinlich, dass einer dieser Teilnehmer so viel Rechenleistung aufbringt.
Bei Proof of Stake ist es das gleiche Problem. Sobald einer mehr als 50 Prozent
der Token hat, also wenn einer die Hälfte aller Lottoscheine bekommt, dann ist er ja jedes zweite Mal mit Block erzeugen dran.
Das heißt, er könnte, wenn er alleine an einer Verzweigung rechnet, an einem Ast dieser Verzweigung rechnet, könnte er die
mit allen anderen Teilnehmern parallel aufbauen und man könnte nie entscheiden, welche Verzweigung nun die richtige ist. Und das möchte man natürlich nicht haben.

[59:51] Darum hat man sich gesagt: "Wir möchten das zusammenmischen." Und dann hab ich gesagt: "Na, dann mache ich das doch.", und hab mir die Vorteile von jedem System herausgepickt und hab das in ein neues System gegossen.
Das habe ich dann Proof of Participation genannt.
Also der Name kommt von diesem 'Proof of'-Verfahren und
das 'Participation' kommt davon, dass die Teilnehmer Punkte dafür bekommen, wenn sie sich irgendwie an diesem Netzwerk, an diesem System beteiligen.
Also zum Beispiel haben die Teilnehmer die Möglichkeit, einen erstellten Block zu signieren, also zu bestätigen, dass da drin alles okay ist. Und dafür bekommen sie einen Punkt.
Man könnte sich auch vorstellen, dass wenn ein außenstehender Teilnehmer, der nicht an der Berechnung der Blöcke beteiligt ist und sich auch nicht leisten kann, alle Blöcke zu speichern und
trotzdem eine Informationen aus dieser Blockkette haben möchte, könnte er in das Netzwerk fragen und sagen: "Kann mir mal bitte jemand diese Information raussuchen?"
Und alle, die das getan haben, bekommen auch einen Punkt.

[1:01:00] Man beteiligt sich am Netz, sorgt dafür, dass das gut funktioniert, dass es sicher bleibt und wird dafür belohnt.
Und jetzt häufen die Teilnehmer nicht einfach sinnlos Punkte an.
Sondern der, mit den meisten Punkten, der darf den nächsten Block erzeugen. Das löst mehrere Probleme.
Einmal wächst die Anzahl der Punkte nicht ins Unendliche.
Zum anderen ist es immer definiert, wer den nächsten Block erzeugen darf.
Das heißt, man schließt Verzweigungen, die aus Versehen passieren, schon vorne herein aus, indem man genau einen Teilnehmer hat, der einen Block erzeugen darf.

Fabian:
[1:01:43] Die Punkte sind aber nicht dasselbe wie Token?

Sebastian:
[1:01:48] Man kann sie sich wie Token vorstellen, aber sie werden hier nicht wie Bitcoin als Währung benutzt.
Also man kann diese Punkte nicht jemand anderem geben, das funktioniert nicht. Und sie sind auch nicht explizit in der Blockchain gespeichert,
sondern man kann sie sich aus den Aktionen der Teilnehmer, die in der Blockchain hinterlegt sind, errechnen.

Fabian:
[1:02:10] Und was passiert, wenn zwei Leute dieselbe Anzahl von Punkten haben?

Sebastian:
[1:02:14] Genau, das ist ein schönes Problem. Entweder gibt es einfach eine Rangfolge und da ist Gut. Das ist natürlich auch doof,
weil das ist wieder vorhersehbar. Und für den Fall gibt es, das nennt sich Münzwurf-Verfahren.
Da können beide Teilnehmer so eine virtuelle Münze werfen und aus ihren Münzwürfen wird ermittelt, wer dran ist.
Und das funktioniert so, dass beide Teilnehmer das Ergebnis zwar beeinflussen durch

ihre Würfe, aber nicht bestimmen können.

Fabian:
[1:02:48] Das habe ich nicht ganz verstanden.

Sebastian:
[1:02:51] Ein schönes schönes Beispiel dafür ist, wie bringst du zwei Kinder dazu, gerecht ein Stück Kuchen zu teilen.

Fabian:
[1:02:58] Na ja. In dem Eines den Kuchen aufteilt und das andere darf sich aussuchen welches Stück.

Sebastian:
[1:03:03] Und genau nach dem Verfahren funktionieren diese Münzwurf-Verfahren. Die werfen beide eine Münze und können das Ergebnis zwar beeinflussen, aber nicht bestimmen und dadurch wird zufällig fair ausgehandelt, wer dran ist.

Fabian:
[1:03:18] Okay. Also ich habe einen Einfluss darauf welche Münze Ich werfe. In einem gewissen Rahmen. Ich kann es aber nicht endgültig festlegen. Ich kann bestimmen, es ist wahrscheinlicher, dass ich Kopf bekomme.

Sebastian:
[1:03:33] Du könntest deine eigenen Münzwürfe quasi fälschen, also vorherbestimmt. Aber das ändert das Ergebnis nicht. Das ist das gleiche, als würdest du jetzt ein ganz kleines Stückchen von dem Kuchen abschneiden.
Dann nimmt sich der andere natürlich das große. Und so kannst du zwar deine Münzwurfwürfe fälschen und damit auch das Ergebnis beeinflussen,
aber wenn du es übertreibst, gehst du leer aus.

[1:04:00] Und um das Ganze noch zu toppen, ist in diesem System nicht nur Proof of Work und Proof of Stake drin.
Also Proof of Work ist die Arbeit, die man reinsteckt, um Punkte zu bekommen und Proof of Staake ist, dass man Punkte ansammelt. Nein, gleichzeitig ist noch ein komplett anderes Verfahren enthalten, was aber mathematisch sicher ist und das funktioniert über eine Zweidrittelmehrheit.
Man verteilt einen Block und wenn zwei Drittel aller anderen Teilnehmer gesagt haben: "Der ist ok.", dann wird er erst angehängt.

[1:04:32] So lange will ich bei meinem Proof of Partizipation nicht warten,
also wird der nach den Punkten, nachdem der die meisten Punkte hat angehängt. Und wie ich schon gesagt hatte, bekommen Teilnehmer dafür Punkte, dass sie Blöcke bestätigen.
Jetzt bestätigen die den Block, der zwar schon in der Blockchain drin ist, aber wo noch nicht zwei Drittel aller Teilnehmer gesagt haben: "Der ist ok."
Und da die aber Punkte haben wollen, weil sie ja auch mal einen Block erzeugen wollen, bestätigen die natürlich die anderen Blöcke.
Und sobald zwei Drittel der Teilnehmer einen Block bestätigt haben und dafür auch einen Punkt erhalten haben, dann habe ich in diesem Block eine Zweidrittelmehrheit.

Und das gibt mir eine mathematische Sicherheit, dass dieser Block vom Netzwerk angenommen wurde.
Das ist das Gleiche, wie bei einer Zweidrittelmehrheit in Abstimmungen.
Das ist mathematisch korrekt nachvollziehbar und beweisbar, dass man mit dieser Zweidrittelmehrheit auch gegen das System verhaltende Teilnehmer kompensieren.

Fabian:
[1:05:37] Also mit deinen Punkten hältst du dir quasi die ganzen Teilnehmerinnen und Teilnehmer als Bilanzbuchhalter, sagst quasi: "Ihr überprüft immer schön alle Einträge, ob die auch stimmen, und dann gebe ich euch dafür auch schön euren Punkt."
Und so sorgst du einfach dafür, dass sich das System quasi selbst erhält, weil immer Leute einen Anreiz dafür haben, zu überprüfen, ob alles, was aufgeschrieben wurde, tatsächlich stimmt.

Sebastian:
[1:06:01] Genau. So virtuelle Punkte zu kriegen, ist jetzt natürlich nicht das Allerbeste. Aber ich gehe davon aus, dass sind wenig Teilnehmer und die haben alle ein Interesse daran, das Netz sicher zu halten, weil sie auch ihre eigenen Daten in diesem Netz speichern wollen.
Und darum haben sie dadurch einen Anreiz, immer mal wieder einen Block zu generieren, um für Sicherheit zu sorgen und deswegen auch einen Anreiz haben, möglichst viele Punkte bei sich zu sammeln.

Fabian:
[1:06:26] Dein System funktioniert nur in einer Situation, wie beispielsweise bei einer Firma, wo man einfach die Grundannahme,
alle haben Interesse das System aufrecht zu erhalten, einfach akzeptieren kann.

Sebastian:
[1:06:40] Oder innerhalb einer großen Organisation,. Wenn sie Server an mehreren Standorten haben, könnte man diese Server,
selbst wenn das nur zehn sind, zu einem solchen Blockchain-Netzwerk zusammenschließen, meinen Mechanismus dann benutzen.
Und natürlich hat die Firma in sich selbst ein Interesse daran, dass das sicher bleibt und man kann durch diese Dezentralisierung aber Ausfälle von einzelnen Servern oder sogar Kompromittierung von einzelnen Surfern ausgleichen.

Fabian:
[1:07:13] Also wenn ich sehr sensible Daten speichern möchte, dann ist an mehreren Orten zu speichern, ja sowieso eine gute Idee.
Und damit ich quasi sicher sein kann, dass an allen Orten auch wirklich dasselbe gespeichert ist, benutze ich das Blockchain-Format und lass die Server sich gegenseitig alle immer überprüfen.

Sebastian:
[1:07:31] Ja, man will aber eher erreichen, dass sich Fehler nicht verbreiten.
Man sorgt so schon dafür, dass überall das gleiche gespeichert ist. Man möchte jetzt aber nicht, dass wenn ein Angreifer einen Server übernehmen kann und darin eine Änderung macht,
ist bei gängigen Speicher-Lösungen, wird diese Änderung

zu allen anderen übertragen und die machen die Änderung auch, ungesehen, ungefragt. Und mit so einer Blockchain könnte man das verhindern, dann würden die anderen Teilnehmer sagen: "Ja, Moment mal. Hier haben wir einen, der will einfach eine Änderung machen."
Das könnten wir im besten Fall in der Blockchain vermerken, dass der diese Änderung machen wollte.
Aber er kann dann nicht einfach irgendwelche Daten in der Blockchain verändern.

Fabian:
[1:08:20] Du hattest gesagt, dein System ist optimal für eine kleinere Anzahl von Teilnehmerinnen und Teilnehmern.

Sebastian:
[1:08:27] Ja, ich hätte jetzt eher gesagt, es ist darauf ausgelegt, aber ...

Fabian:
[1:08:35] Und du hast gesagt, die Punkte-Werte werden nicht spezifisch aufgeschrieben, sondern ergeben sich immer aus dem Verlauf der Aktivitäten.
Also ich sehe ja, wenn jemand einen Eintrag signiert hat und dann kann ich immer zurück gucken, wie viele Punkte hat er bisher angesammelt.
Wenn ich das so korrekt interpretiere, bedeutet das, ich muss mir immer die gesamte Blockchain angucken, bevor ich entscheiden kann, wer den nächsten Block generieren darf.

Sebastian:
[1:08:59] Ja und das macht meine Test-Implementierung tatsächlich so.
Und genau deswegen schmiert die nach einer gewissen Anzahl Blöcken einfach ab, weil die Berechnung der Punkte länger dauert, als die Zeit haben, den nächsten Block zu erzeugen.
Und dann werden die sich alle total uneinig, wer jetzt eigentlich dran ist und irgendwann sagt jeder zu jedem anderen: "Du bist jetzt gar nicht dran.", und niemand erzeugt mehr Blöcke. Und das ganze Ding steht still.
Das ist natürlich praktisch nicht gewollt. Das kann man aber ganz einfach umgehen. Man müsste sich die aktuelle Punktzahl merken, würde sich den nächsten Block angucken und dann nur noch die Veränderungen auf den gemerkten Punktsatz drauf rechnen.

Fabian:
[1:09:44] Man müsste dann quasi die Punktzahlen immer im Block dann auch irgendwie in einer Form codiert notieren.

Sebastian:
[1:09:51] Ja, man könnte sie in einen Block codieren, um zwischen allen Teilnehmern die aktuelle Zahl zu synchronisieren,
aber es würde auch reichen, wenn jeder Teilnehmer für sich selbst diese Liste sich merkt, da ja die Aktionen, mit der die Punkte manipuliert werden, schon zwischen den Teilnehmern synchronisiert werden.

Fabian:
[1:10:13] OK. Ja, spannend. Wird dein Modell konkret irgendwo angewendet? Oder ist es erstmal ein Konzept für die Schublade, was später jemand rausholen kann und dann

eine weltweit erfolgreiche Kryptowährung daraus basteln.

Sebastian:
[1:10:26] Also so konkret anwenden, kann man es natürlich nicht. Ich habe viele Annahmen gemacht. Zum Beispiel habe ich sämtliche Kryptografie aus der Blockchain rausgelassen. Also das ist offen, wie ein Scheunentor.
Und gleichzeitig habe ich, und das war auch das Ziel von der Arbeit, dass ich rausfinde, wie das funktioniert und was man eventuell noch
bauen oder was man noch erforschen muss, eh man das tatsächlich einsetzen kann.
Was ich herausgefunden habe, ist, dass das System sehr empfindlich ist gegenüber Netzwerk-Latenzen. Und zwar kann es passieren, dass wenn ein Teilnehmer gewisse Einträge zu spät bekommt,
dass er dann einen Block fälschlicherweise ablehnt und nicht seiner
eigenen Blockchain-Kopien zufügt. Und dann auch noch dem anderen sagt: "Du hast einen Fehler gemacht." Und die anderen müssen dann wieder auf diesen Fehler reagieren und zurück sagen: "Nee, das war alles ok."

[1:11:28] Und das passiert, je schneller man Blöcke erzeugt, umso häufiger passieren solche Fehler. Und was man nun braucht, ist ein
Netzwerkprotokoll, also eine Übertragungsart, die mir sagen kann, wie lange dauert so eine Übertragung im schlimmsten Fall.
Dann rechne ich die einfach mal zwei, weil ich mir denke, ich gehe ganz sicher,
und sage: "Okay das ist meine Wartezeit, die ich auf alle Aktionen anwende, damit ich mir sicher bin, dass es bei allen angekommen ist und alle Zeit hatten,
auch mit mir auf den gleichen Stand zu kommen". Damit die nicht denken, ich habe einen Fehler gemacht, den ich gar nicht gemacht habe, sondern die waren einfach noch nicht auf dem Stand, auf dem ich war.

Fabian:
[1:12:14] Aber man kann doch eigentlich die Übertragungszeit nicht vorhersagen? Weil das von so vielen lokalen Faktoren abhängig ist. Dann reißt mir kurz das WLAN ab und dann ist die Protokoll- Vorhersage schon wieder völlig für den Fuß oder?

Sebastian:
[1:12:28] Ja, damit kann man natürlich nicht rechnen. Es gibt Netzwerkprotokolle, die so ein loses Netzwerk zusammenbauen können und dann auch schon ungefähr die Zeit-Vorhersagen, die die Pakete brauchen.
Wenn man natürlich komplett die Verbindung verliert, da kann auch das dann nichts mehr helfen.
Und man würde jetzt entweder cleverer Weise direkt erkennen: "Ich habe hier die Verbindung verloren.
Ich muss die anderen mal fragen, was die in der Zwischenzeit gemacht haben."
Oder wenn ich das selber gar nicht mitgekriegt habe, dann würde ich jetzt anfangen, falsche Aktionen zu machen.
Und wie gesagt, ich sage den anderen: "sie haben Fehler gemacht", und die anderen sagen mir aber: "Nein das war kein Fehler."
Und wenn mir jetzt ganz oft Leute sagen: "Das war überhaupt kein Fehler.", dann könnte man sich selber auch denken: Naja vielleicht bin ich ja hier irgendwie asynchron.
Ich hör erstmal auf, die anderen zu nerven und frag erstmal nach, was die in der Zwischenzeit gemacht haben und bringe mich wieder auf den aktuellen Stand.

Fabian:
[1:13:30] Also quasi eine Stelle, ab der man den eigenen Fehler einsieht.

Sebastian:
[1:13:34] Genau und da hilft einem das Signierung von den Blöcken,also diese Zweidrittelmehrheit.
Der letzte Block oder der jüngste Block, der bei mir von zwei Dritteln aller Teilnehmer signiert wurden ist, so bestätigt worden ist,
der ist im gesamten Netzwerk gleich, egal was zwischendurch passiert ist.
Und wenn man den Laptop zugeklappt hat und einen WLAN-Router noch dreimal an und ausgemacht hat. Der ist immer in dem gesamten Netzwerk
kennen den alle anderen auch in genau dieser Form. Und dann kann man die Anfragen: "Hier, ich brauch mal die Änderung ab diesem Block." und so kann man sich wieder synchronisieren.

Fabian:
[1:14:11] Das heißt, die Funktionalität von solchen Blockchain-Systemen ist limitiert durch tatsächlich Netzwerk-Latenzzeiten.

Sebastian:
[1:14:21] Ja, in diesem Fall ja. Was daran liegt, dass die Teilnehmer nicht nur die Möglichkeit haben, Blöcke zu bestätigen, sondern auch die Möglichkeit haben, Fehler zu senden.
Und gerade bei diesen Fehlern ist es wichtig, die Zeit abzuwarten, die es dauert, um den Block hin zu schicken und den Fehler zurück zu erhalten.
Gerade bei Konstellationen mit mehreren Teilnehmern, wo ein Teilnehmer einen Fehler schickt, ein anderer den erhält, mit in den nächsten Block verpackt, den Block verschickt und jetzt bekommt das noch ein anderer Teilnehmer, der von dem Fehler noch gar nichts gehört hat, der sagt dann: "Ein Moment mal, in diesem Block steht irgendein Fehler drin, von dem weiß ich nichts.
Wo kommt der Fehler her? Den Block nehme ich nicht an."
Und da ist es dann wichtig, so lange zu warten, bis ich mir sicher bin, dass auch jeder diesen Fehler erhalten hat und dann erst tue ich den in einen Block rein.

Fabian:
[1:15:20] Okay, dann haben wir, glaub ich, den Bogen grob geschlossen, oder?

Sebastian:
[1:15:25] Ja. Also um Netzwerklatenzen habe ich mich nicht gekümmert, steht auch so in meiner Arbeit drin.
Also wenn das mal einer macht und ein schickes Netzwerkprotokoll baut, wo man die Teilnehmer,
also nicht nur, dass man die Latenzen herausrechnen muss, man muss dynamisch Teilnehmer hinzufügen und entfernen können aus diesem Netzwerk. Beim Entfernen ist es nicht so schlimm, da schickt man halt Pakete an jemanden, den es nicht gibt. Ist egal. Aber ich möchte natürlich auch die Pakete an die Leute schicken, die gerade frisch hinzugekommen sind.
Das Proof of Participation, das kann damit umgehen, dass Leute hinzukommen und auch wegfallen.
Das darunterliegende Netzwerk muss das dann natürlich auch können.

Fabian:
[1:16:05] Da ist dann einfach noch Entwicklungsbedarf.

Sebastian:
[1:16:08] Genau. Das darf dann irgendwie jemand machen, der nach mir eine Masterarbeit schreibt.
Der darf dann diese Blockchain nehmen, sich da reinlesen und ein Netzwerkprotokolle darunter bauen, um dann zu gucken, wie das funktioniert.
Also es gibt auch Situationen, wo sich Pakete überholen.
Also wenn man wirklich ganz extrem denkt, könnte es passieren, dass man den vorletzten Block vor dem Letzten bekommen.
Und auch das muss dieses Netzwerkprotokoll sicherstellen, dass die in der Reihenfolge auch ankommen, wie sie abgeschickt wurden, selbst wenn sie von zwei verschiedenen Leuten abgeschickt wurden.
Und das ist dann schon wieder nicht mehr so einfach.

Fabian:
[1:16:53] Da steckt wirklich noch eine Menge Musik drin, wo sich einer kluge Gedanken zu machen kann.

Take Home Message

[1:17:00] Wie du sicherlich mitbekommen hast, haben wir immer das kleine Ritual, dass die Leute eine kleine Take Home Message formulieren müssen, wenn den Zuhörerinnen und Zuhörern jetzt gerade ein bisschen die Rübe raucht,
weil sie versucht haben, nachzuvollziehen, wie eine Blockchain funktioniert.
Aber vielleicht hast du ja einen schönen Kalender-Spruch, den sie sich mit nach Hause nehmen können, der etwas leichter verdaulich ist.

Sebastian:
[1:17:25] Gerade wie der Trend in der Informatik immer zwischen Dezentralisierung und Zentralisierung schwankt. Man ist bei einem sehr zentralen System und sagt: "Das ist alles doof. Wir machen das jetzt dezentral." Dann baut man das,
und dann sagt man sich: "Oh, war
irgendwie jetzt doch nicht so prickelnd.
Dann machen wir mal alles wieder zurück." Und man schwankt die ganze Zeit zwischen diesen Extremen und keiner macht sich aber mal Gedanken: "Naja, können wir uns nicht irgendwo mal in der Mitte treffen
und mal irgendwas bauen, was das Bessere von beiden benutzt.?
Das tut irgendwie keiner.

Fabian:
[1:18:06] Weder Zentralisierung, noch Dezentralisierung sind Heilsversprechen, sondern es geht immer ein bisschen um die Umsetzung. Also ich kann beides schlecht machen.

Sebastian:
[1:18:16] Ja und gerade in dem Hype, eins besser zu machen, als das andere, wird es

meistens auch nur nix.

Fabian:
[1:18:27] Wofür ja Blockchain vielleicht an manchen Punkten ein gutes Beispiel ist.

Sebastian:
[1:18:31] Ich finde das eigentlich einen sehr schönen Schlusssatz.

Fabian:
[1:18:35] Viel heiße Luft um nix.

Sebastian:
[1:18:38] Auf aufzwang anders gemacht und doch nichts bei rumgekommen.

Fabian:
[1:18:44] Ich bedanke mich bei euch, dass ihr zugehört habt, und ich bedanke mich bei Sebastian, dass er mir hier so geduldig die Blockchain erklärt hat.

Sebastian:
[1:18:52] Schön, dass du so geduldig zugehört hast.

Fabian:
[1:18:56] Und ich freue mich darauf, wenn ich euch zur nächsten Episode Underdocs wieder begrüßen darf.

Outro