Drehbuch

# Einleitung

Intro

Was ist eine Blockchain, wie funktioniert sie, wo wird sie gebraucht und wieso wird sie immer relevanter?

Doch beginnen wir erst mal mit den Grundlagen.

# Wieso wird Blockchain immer relevanter?

Da man heutzutage niemandem mehr vertrauen kann, werden immer Mittelmänner oder Thirdpartys verwendet, um sicher zu stellen, dass etwas ohne Manipulation am Zielort ankommt. In der heutigen Zeit ist dies oft eine Bank, aber diese verlangt natürlich Geld für ihre Arbeit. Hier kommt eben die Blockchain ins Spiel, denn sie wird durch mehrere Computer überprüft und benötigt kein grosses Geld für die Ausführung. Auch können mit dieser Lösung andere Daten sicher übermittelt werden, wie zum Beispiel die Herkunft eines Obstes.

# Was ist Blockchain?

Eine Blockchain oder auch eine Kette aus Blöcken sagt einem vielleicht nicht gerade viel.  
Jedoch kann es sein, dass es in Verbindung mit Kryptowährungen schon das eine oder andere Lämpchen aufleuchten lässt.

Stelle man sich vor, dass eine Party steigen soll, aber die Startzeit ist noch nicht bekannt. Nun soll diese Nachricht übermittelt werden, aber nur in 1:1 Gesprächen. Die Schwierigkeit dabei ist aber, dass auch Leute darunter sind, die bewusst eine falsche Angabe machen, damit die Party ruiniert wird. Man sieht, dass dies fast unmöglich ist, wenn man keinen WhatsApp Chat oder ähnliches hat.

Nun stellt sich aber die Frage, wie die Sicherheit bewerkstelligt werden kann.

Dabei kommt Proof-of-Work ins Spiel.

Defintion: Methode, die den übermäßigen Gebrauch eines Dienstes verhindern soll

Proof-Of-Work ist eine Überprüfung, ob die Information (Daten) korrekt übergeben wurden. Dieser wird auf verschiedenen Computer von Minern durchgeführt, denn wenn man die Nonce zum Hash als erster findet kriegt man eine Belohnung in Form von z.B. Bitcoin. Man kann es sich somit auch als Lotterie vorstellen, da nur 1 Miner die Nonce richtig herausfinden kann. Dieser Hash und der dazugehörige Nonce, zusammen mit den Daten und dem vorherigen Hash werden dann in einem so genannten Block gespeichert.

Doch was ist nun diese Nonce oder dieser Hash?

Der Hash ist ein Schlüssel, der aus den Daten, dem Zeitpunkt der Erstellung des Blocks und dem vorherigen Hash generiert wird und nicht mehr Rückgängig gemacht werden kann.

Nonce Definition: “***Nonce***” (Abkürzung für „number used once“)

Nonce ist eine Zahl, die durch denselben Generator wie der vorgegebene Hash generiert wird und dann einen Hash ergibt. Wenn dieser Hash aus der Nonce derselbe ist wie der vorgegebene Hash, hat man also den Code für den Hash gefunden.

Dies ist alles noch ein wenig kompliziert, daher etwas einfacher:

Stellen wir und ein Spiegelei vor, dass eine bestimmte Form hat. Dieses Spiegelei wurde gemacht aus dem Spiegelei des Vortags, einem bestimmten Zeitpunkt und den Genen, die darin gespeichert werden. Dieses Spiegelei ist wie der Hash, denn wenn es zerbrochen ist, kann man es nicht wieder Rückgängig machen. Nun probiert man mit verschiedenem Futter, also dem Nonce, genau dieses Spiegelei mit dieser Form zu erhalten. Dazu füttert man das Huhn und zerbricht das Ei, bis es die gewünschte Form hat. Dann hat man eben die richtige Futterkombination und diese kann dann von allen anderen Leuten genauso gemacht werden mit deinem Huhn und überprüft werden, ob dies stimmt.

# Ablauf einer Transaktion (Recheck!)

Nun setzten wir all dieses Wissen um in einer Transaktion.

Zuallererst stellst du einen Antrag für eine Transaktion in Form eines Blocks. Dieser Block erhält dann aus der Blockchain, in der du den Block veröffentlichst den vorherigen Hash und der Hash des Blockes wird mit Hilfe der Daten, dem Zeitpunkt und dem des vorherigen Hashs generiert. Danach können alle Leute, die in dieser Blockchain Minen, den Nonce des Blocks herausfinden, mit pröbeln (lotterie mässig).

Ein Block wird erst gespeichert, wenn eine gewisse Anzahl and Validator im Netz das OK geben.  
Ein Validator kann man sich als Überprüfer vorstellen, dieser kann zum Beispiel muss aber nicht zwingend ein Miner sein. Je nach Konsensus/Methode...

Block besteht aus Daten, Hash(Neu, Vorherige), Nonce

# Wo wird es gebraucht?

Der Anwendungsbereich einer Blockchain ist sehr vielfältig, da wir sehr auf Richtigkeit von Informationen angewiesen sind. Dies kann im Medizinwesen z.B. beim Haltbarkeitsdatum der Fall sein. Oder generell in der Logistik von Produkten, dass auch die gleiche Menge, welche abgeschickt wurde, auch am Zielort ankommt. Bei den Lebensmitteln kann es die Herkunft einer Frucht oder der zuständige Bauer sein, welcher klar auf der Blockchain vermerkt ist. Auch Abstimmungen können dadurch transparent und zuverlässig durchgeführt werden.

Dies werden zum Beispiel durch sogenannte Smart Contract möglich gemacht, welche eine bestimmte Abwicklung eines Vertrages automatisch durchführen und auch ausnahmelos einhalten. Somit kommt es nicht zur Korruption oder auch zu Fehlern, welcher durch Menschen entstehen.

# Schlussteil

Fassen wir nochmals kurz zusammen.  
Blockchain ist eine neue Technologie, um die Sicherheit von Transaktionen zu bewerkstelligen und so die Bank zu ersetzen. Außerdem kann sie auch benutzt werden, um andere Daten sicher zu übermitteln, was in Zukunft immer relevanter werden wird.

Dies wird durch Blockchains sichergestellt, denn bevor ein Block angehängt werden kann, muss der Prof-of-Work durchgeführt werden. Dieser ist das Auspröbeln der Nonce für den Hash, der aus den Daten und dem Hash aus dem vorherigen Block gebildet wird. Dieser Hash ist nicht umkehrbar und darum wird die Nonce gesucht. Wer diese findet wird belohnt, was es interessanter macht die Nonce zu finden, als die Blockchain zu manipulieren. Somit sind alle Blöcke zusammenhängend und man kann selbst die Nonce nochmals testen und schauen, ob man mit dem dazugehörigen Hash-Generator auf den richtigen Hash kommt.

So und mit diesem Wissen solltet ihr nun prüfungsreif sein.

Auf wiedersehen und bis zum nächsten Mal bei Systec.