Was ist Hashgraph ?

Dieser Text ist größtenteils des englischen Whitepapers von Swirld.com übernommen

Die Hashgraph-Datenstruktur und der **Swirlds-Konsensus-Algorithmus** bieten eine neue Plattform für verteilten/dezentralen Konsens.

Im Folgenden sollen einige seiner Eigenschaften im Vergleich zur Bitcoin Blockchain beschrieben werden. Der Begriff "Blockchain" bezieht sich dabei im Allgemeinen auf das „Proof-of-work“-System, wie es beim Minen von Bitcoin verwendet wird, anstatt auf die große Anzahl von Varianten, die es mittlerweile gibt.

Das Ziel eines verteilten Konsensusalgorithmus ist es, einer Gemeinschaft von sich unbekannten Benutzern zu ermöglichen, zu einem Konsens / einer Vereinbarung zu kommen über die Echtheit und Reihenfolge, in der einige von ihnen Transaktionen generiert haben, obwohl kein einziges Mitglied einem einzelnen anderen vertraut.

Es soll ein mathematisch sicheres System zur Erzeugung von Vertrauen bei Einzelpersonen geschaffen werden. Das Swirlds Hashgraph System erreicht dies zusammen mit Fairness, Schnelligkeit, Beweisbarkeit, Byzantinismus, ACID-Konformität, Effizeinz, Kostengünstigkeit, Zeitstempelung, DoS-Resistenz und Freiheit. Hier ist, was diese Begriffe bedeuten:

Der Hashgraph ist **fair**, weil niemand die Reihenfolge der Transaktionen manipulieren kann.

In der Blockchain könnte ein Miner über die Reihenfolge im Block entscheiden oder darüber, welche Transaktionen er bevorzugt verarbeitet (z.B. Nach Preiskategorien).

Im Hashgraph gibt es keine Möglichkeit, dass ein Individuum die Konsensusreihenfolge von Transaktionen beeinflusst.

Der Hashgraph ist auch auf andere Weise fair, weil niemand eine Transaktion stoppen oder verzögern kann. In der Blockchain hängt dies von der Akzeptanz durch die Miner ab.

Aber im Hashgraph können Angreifer nicht verhindern, dass ein Mitglied eine Transaktion auf irgendeine Weise aufzeichnet. Die einzige Restriktion ist die Bandbreite der Internetverbindung für das Herunterladen von Transaktionen auf den jeweils beteiligten Rechner.

Zum Herunterladen von 4.000 Transaktionen pro Sekunde würden wahrscheinlich nur ein paar Megabit pro Sekunde erforderlich, was ein typisches privates Hausnetz leisten kann. Es wäre schnell genug, um alle Transaktionen des gesamten Visa Karten Netzwerks, weltweit durchzuführen. Das Bitcoin-Limit von 7 Transaktionen pro Sekunde kann da momentan nicht mithalten. Obwohl es einige Möglichkeiten der Optimierung gäbe.

Der Hashgraph ist **nachweisbar**. Sobald ein Ereignis / eine Transaktion eintritt, weiss innerhalb von ein paar Minuten die gesamte Gemeinschaft darüber Bescheid, was und wann es passiert ist. Alle einzelnen Teilnehmer am Netzwerk wissen dies sofort, und sie wissen, dass es alle wissen. Sie tauschen sich aus wie bei einem instantanen Klatsch und Tratsch (gossip).

Somit kann ein Konsensus in der gesamten Gemeinschaft darüber entstehen, was wann, also in welcher Reihenfolge transferiert wurde.

Der Hashgraph ist anders als Blockchain **byzantinisch**. Dies ist ein technischer Begriff, der bedeutet, dass kein einzelnes Mitglied (oder eine kleine Gruppe von Mitgliedern) verhindern kann, dass die Gemeinschaft einen Konsens erreicht. Auch kann niemand den

einmal entstandenen Konsensus ändern. Jedes Netzwerkmitglied weiss dies.

Der Hashgraph ist **ACID**-konform. Dies ist ein Datenbankbegriff und gilt für den Hashgraphen. Er wird als dezentrale Datenbank verwendet. Eine Community von Mitgliedern nutzt diese, um zu einem Konsens über die Reihenfolge zu gelangen, in der Transaktionen aufgetreten sind. Nach dem Erreichen eines Konsens speichert jedes Mitglied diese Transaktionen in seiner eigenen lokalen Kopie der Datenbank. Wenn die lokale Datenbank alle Standardeigenschaften einer Datenbank hat (ACID: Atomicity (Wertigkeit), Konsistenz, Isolation, Dauerhaftigkeit), dann kann gesagt werden, dass die Gemeinschaft als Ganzes eine einzige, verteilte Datenbank mit denselben Eigenschaften besitzt.

Der Hashgraph ist im Gegensatz zur Blockchain **100% effizient.** Beim Mining in der Blockchain werden manchmal Blöcke erarbeitet und verschwendet, weil sie später von der Community verworfen werden. Im Hashgraph wird das Äquivalent eines "Blocks" niemals verworfen.

Der Hashgraph ist **kostengünstig** im Sinne der Vermeidung von Miningkosten. Beim Minen von Bitcoin entstehen langwierige Wartezeiten und hohen Kosten für Hardware, Gebäude und Elektrizität. Diese Kosten haben zudem keinen Nutzen. Beim Hashgraph fallen solche Kosten nicht an.

(Hinweis: Es gibt Blockchain-Varianten, die auch keinen Arbeitsnachweis verwenden; aber Bitcoin erfordert einen Arbeitsnachweis = „Proof-of-work“).

Der Hashgraph ist **zeitgestempelt**. Jeder Transaktion wird eine Konsensuszeit zugewiesen, also die Median-Zeit, zu der jedes Mitglied die Transaktion erhielt. Dieser Zeitstempel ist wichtiger Teil des Konsenses und wird z.B. für Transaktionen wie Smart Contracts

benötigt, denn es wird Konsens darüber geben, ob ein Ereignis zu einem bestimmten Zeitpunkt stattgefunden hat, weil der Zeitstempel manipulationssicher ist.

In der Blockchain enthält jeder Block einen Zeitstempel, der aber vom Computer des Miners stammt, der diesen Block generierte.

Der Hashgraph ist **DoS resistent**. Sowohl Bitcoin-Blockchain als auch Hashgraph sind so verteilt, dass sie „Denial of Service“ (DoS) – Angriffen widerstehen. Ein Angreifer kann ein einzelnes Element im Hashgraphen oder einen Miner mit einem Flooding überfluten, um sie vorübergehend vom Internet zu trennen. Aber der Gemeinschaft als Ganzes wird ein solcher Angriff nicht schaden und sie wird normal weiterarbeiten. Ein Angriff auf das System als Ganzes würde eine Überschwemmung erfordern, die praktisch unmöglich ist.

Blockchainalternativen zur Proof-of-work , wie Proof-of-stake, haben den Nachteil, dass sie anfällig für DoS-Angriffe sind. Ein Angreifer kann dort die Macht übernehmen und das ganze System lahmlegen. Dazu reicht es, nur einen oder wenige Computer anzugreifen.

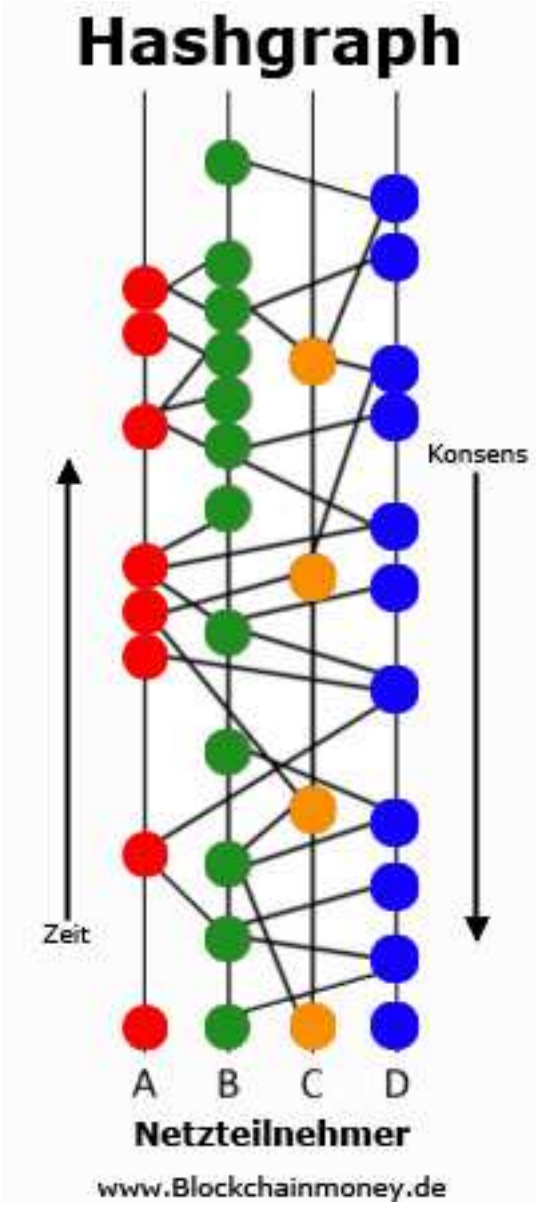
Hashgraph vermeidet dieses Problem, weil es keinen Arbeitsnachweis benötigt.

Die Hashgraph-Technologie ist also sowohl sicher, schnell, skalierbar, kostengünstig, byzantinisch als auch fair.

<u>Und so funktioniert sie im Groben:</u>

Die Teilnehmer im Netzwerk generieren **Events** (Aktionen). Das kann das Versenden von Geld-Transaktionen sein, das Versenden von Smart-Contracts, das Abstimmen über eine Wahl, eine Spielaktion, eine Wette oder alles mögliche andere.

Jede Transaktion / jedes Event spricht sich via **Gossip-Protokoll** (gossip = Klatsch; Tratsch) sofort herum und wird mit **Zeitstempel**



und einem **Hash** des Empfängers und des Senders versehen. So lassen sich alle Events zurückverfolgen und zeitlich einordnen (strukturieren).

Über ein **Voting-Protokoll** werden nun alle zurück liegenden Events im System befragt und abgeglichen (wer weiss was). Da alle Events dieselben Informationen besitzen, können Sie zu bestimmten Fragestellungen mit ja oder nein antworten. So wird ein Konsensus über die Echtheit und die zeitliche Struktur hergestellt.

Mit dieser superschnellen (Tests ergaben mind. 250.000 mögliche Transaktionen pro Sekunde) Technologie können unlimitierte Zahlungssyteme, Wahlsysteme, IOT-Systeme (internet of things), Verwaltungssyteme oder jedes beliebige andere System von Internettransaktionen geschaffen, gesichert und vertrauensvoll angewendet werden.

<< geschrieben von Blockchainmoney.de>>