MAERKI BAUMANN & CO. AG

PRIVATBANK

Staking – Passiveinkommen und Sicherheitskomponente zugleich

Proof-of-Work, Proof-of-Stake oder doch lieber Proof-of-History? Konsensmechanismen sind das Rückgrat einer jeden Blockchain und für das Erreichen von Übereinstimmung in einem dezentralen Netzwerk verantwortlich. In der Welt der digitalen Vermögenswerte kaufen Investoren im Vergleich zur traditionellen Finanzindustrie keine Anteile an einem Unternehmen, sondern Anteile an einem netzwerkbasierten Projekt. Sie profitieren somit vom Wachstum des Netzwerkes, indem dieses und damit dessen Coin bei steigender Transaktionszahl und somit grösserer Nachfrage an Wert zulegt. Was jedoch viele nicht wissen: Auch digitale Vermögenswerte können produktive Vermögenswerte sein und in Form von «Staking Rewards» Erträge auf das zur Verfügung gestellte Kapital generieren – ähnlich wie bei einer Wertpapierleihe.

Konsensmechanismen – das Rückgrat einer jeden Blockchain

Eine Blockchain stellt Vertrauen, Nachvollziehbarkeit, Transparenz und Unveränderbarkeit ohne die Involvierung einer zentralen Kontrollinstanz dar. Die Transaktionen laufen dezentral und zwischen den einzelnen Nutzenden direkt («peer-to-peer», P2P) ab. Sie müssen auf eine einheitliche Art und Weise, nach den Parametern des Codes und den Regeln der Community, validiert werden können.

Hierfür dienen bei einer Blockchain die sogenannten Konsensmechanismen. Um zu verstehen, wie Konsens in einem Netzwerk hergestellt werden kann, bedarf es zuerst einer Definition. Einfach ausgedrückt, ist der Konsensmechanismus eine vordefinierte Regel (Konsensprotokolle oder Code), welche es den jeweiligen Nutzenden in einem dezentralen Netzwerk ermöglicht, die Aktivitäten zu koordinieren und Unstimmigkeiten vorzubeugen. Dabei ist es von höchster Bedeutung, dass sich alle Akteure im Netzwerk auf eine einzige Quelle der Wahrheit einigen. Dies sollte auch dann der Fall sein, wenn einige Akteure, beispielsweise aufgrund eines Stromausfalls, zeitweise nicht mehr online sind.

Doch weshalb brauchen wir in einem dezentralen System zwingend eine solche Einstimmigkeit? In einem zentralisierten System gibt es Personen oder Instanzen, welche Entscheidungen treffen und dafür sorgen, dass diese Entscheidungen auch effektiv – über die verschiedenen Ebenen hinweg – umgesetzt werden. Da in einem dezentralen Netzwerk keine solchen Funktionen vorgesehen sind, bedarf es Wege, wie solche Entscheidungen getroffen und dementsprechend umgesetzt werden können. In einem dezentralen Netzwerk unterstützt also das Konsensprotokoll (der Code) jene Aufgaben, welche in einem zentralisierten Netzwerk vom jeweiligen Entscheidungsträger übernommen werden.

Dabei existieren drei wichtige Regeln, die für beinahe alle Konsensmechanismen gelten und dafür sorgen, dass Einigkeit zwischen den verschiedenen Akteuren erreicht werden kann:

1. Jene Teilnehmende im Netzwerk, welche der Blockchain neue Blöcke hinzufügen, werden «Validatoren» genannt. Die Validatoren müssen dabei einen Input leisten, um überhaupt an der Generierung von neuen Blöcken teilnehmen zu können. Dieser Input kann beim «Proof-of-Work»-Mechanismus in Form von Rechenleistung oder beim «Proof-of-Stake»-Mechanismus durch die Hinterlegung von Coins erfolgen. Dies stellt sicher, dass die Validatoren pflichtbewusst und im Einklang mit den Netzwerkregeln handeln.
2. Um die Validatoren sozusagen bei Laune zu halten (Incentivierung), bedarf es im Gegenzug für den Input und das wahrheitsgetreue Handeln eines attraktiven Outputs – einer Vergütung. Diese Vergütung wird in den meisten Netzwerken in der Währung der jeweiligen Blockchain in einem festgelegten Rhythmus ausbezahlt. Der Output, welchen die Validatoren erhalten, besteht dabei jeweils aus den Transaktionsgebühren, aus neu geschaffenen Coins oder aus einer Kombination von beidem.
3. Die dritte und letzte Regel ist die Schaffung von Transparenz. Fehlt diese Nachvollziehbarkeit des Handelns seitens der Validatoren, ist es nicht möglich, betrügerisches Verhalten aufzuspüren und dieses zu bestrafen.

Proof-of-Stake – der Konsensmechanismus der Zukunft?
In den letzten Jahren entstanden viele neuartige Konsensmechanismen. Für einen Laien kann es verständlicherweise schwierig sein, den Überblick zu behalten. Im Grundsatz verfolgen alle dasselbe Ziel, die Ansätze könnten jedoch kaum unterschiedlicher sein: Von Proof-of-Work über Proof-of-Stake bis hin zu Proof-of-Burn oder Proof-of-Authority – es gibt keinen richtigen oder falschen Ansatz. Im Folgenden wollen wir die beiden wichtigsten Ansätze erklären.

Proof-of-Work (PoW)
Der Proof-of-Work-Konsensmechanismus ist der Urvater aller Konsensmechanismen und ist jener, welcher der Krypto-Währung Bitcoin (BTC) zugrunde liegt. Bei diesem Verfahren konkurrieren Teilnehmende im Netzwerk darum, einen neuen Block zur Blockchain hinzuzufügen, indem sie eine bestimmte kryptografische Aufgabe lösen, die im Wesentlichen darin besteht, einen Hash-Wert zu finden, der den vorgegebenen Schwierigkeitsgrad erfüllt. Das Lösen dieser Aufgaben ist dafür verantwortlich, dass ein neuer Block hinzugefügt wird, und sorgt dafür, dass die Transaktionen fehlerfrei durchgeführt und validiert werden («Mining»). Für das Lösen dieser Aufgabe bedarf es eines Energieaufwandes in Form der investierten Rechenleistung. Weil etliche Teilnehmende, sogenannte «Miner», gleichzeitig versuchen, neue Blöcke zu schürfen, ist der Stromverbrauch enorm hoch.

Proof-of-Stake (PoS)
Proof-of-Stake hingegen kann allgemein als die umweltfreundlichere Alternative zum Proof-of-Work-Protokoll aufgefasst werden, da die Validatoren neuer Blöcke vordefiniert sind. Der Ansatz ist grundlegend gleich: Validatoren müssen einen Input leisten. Im Vergleich zu Proof-of-Work werden beim Proof-of-Stake jedoch keine Rechenleistung, sondern Coins als Input zur Verfügung gestellt. Während dieses Prozesses stellen die Netzwerkteilnehmenden ihre Coins zwar den jeweiligen Validatoren zur Verfügung, bleiben jedoch in deren Besitz («Staking»). Je nach Art des Stakings werden diese Coins dann für einen bestimmten Zeitraum blockiert. Proof-of-Stake baut folglich auf der Prämisse auf, dass jene Akteure im Netzwerk, welche viele Coins besitzen, grosses Interesse daran haben, das Netzwerk stabil zu halten und den Wert ihrer Coins zu sichern.
Wenn Nutzende eines Netzwerks ihre Coins zur Verfügung stellen, erhalten sie im Gegenzug Belohnungen – analog zu Erträgen aus einer Wertpapierleihe. Die Netzwerke unterscheiden sich dabei in der Höhe der ausbezahlten Erträge, in der Dauer ihrer Sperrfristen für die ausgeliehenen Coins, in den Auszahlungszyklen sowie in der Art der Erträge.

Und so funktioniert der Proof-of-Stake-Konsensmechanismus:

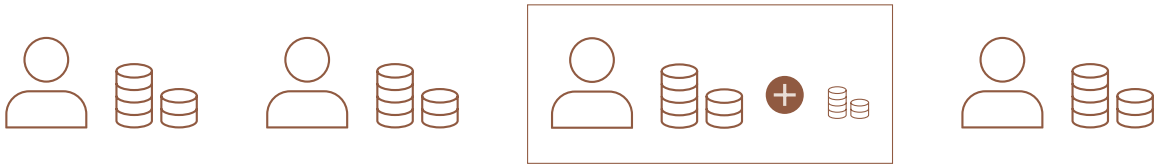
Nutzer staken ihre Vermögenswerte, um einen neuen Block zu validieren.

Falls der Block nicht legitim ist, wird der gestakte Betrag gestrichen.

Falls der Block legitim ist, wird der gestakte Betrag inklusive einer zusätzlichen Belohnung ausbezahlt.

Welcher Netzwerkteilnehmende jeweils den nächsten Block validieren darf, wird mittels gewichteter Zufallsauswahl bestimmt. Für jeden neuen Block wird ein neuer Validator ausgelost. Aufgrund der gewichteten Zufallsauswahl haben aber jene, welche eine grössere Anzahl an Coins besitzen und diese aktiv für das Generieren neuer Blöcke zur Verfügung stellen, grössere Chancen, für den nächsten Block ausgelost zu werden. Grundsätzlich verhält es sich hierbei gleich wie bei einer Lotterie: Je mehr Lose gekauft werden, desto grösser ist statistisch gesehen die Chance auf einen Gewinn.

Bestimmung durch gewichtete Zufallsauswahl



Höchste Chancen

Je mehr Coins aktiv für das Generieren neuer Blöcke zur Verfügung gestellt werden, desto grösser ist die Chance, als Staker für den nächsten Block ausgelost zu werden.

Die Vorteile von Proof-of-Stake liegen auf der Hand: Das Proof-of-Stake-Protokoll ist bis zu 10'000 Mal umweltfreundlicher und verbraucht im Vergleich zu Proof-of-Work fast keinen Strom. Ein weiterer Vorteil kann in Zukunft die erhöhte Sicherheit bieten: Aufgrund des transparenten Aufbaus der Blockchain straft der Algorithmus Betrüger ab und sorgt dafür, dass diese ihren Input in Form der Coins verlieren («Slashing»). Die Akteure sind somit nicht nur angespornt, ihre Coins bereitzustellen, sondern auch im Sinne des Netzwerkes zu handeln.

Abschliessend kann die erhöhte Skalierbarkeit genannt werden: Die meisten Proof-of-Stake-Blockchains sind architektonisch auf eine höhere Geschwindigkeit und Anzahl Transaktionen ausgerichtet und können somit eine höhere Anzahl an Transaktionen pro Sekunde verarbeiten.

Digitale Vermögenswerte – alles aus einer Hand

Maerki Baumann hat bereits 2018 als eine der ersten Schweizer Privatbanken eine dedizierte Krypto-Strategie erarbeitet, die ab 2019 schrittweise umgesetzt wurde. Am Anfang stand das Angebot von Firmenkonten in Fiat-Währung für Unternehmen, die sich die Blockchain-Technologie oder Krypto-Anwendungen zunutze machen. Mitte 2020 folgten der Handel und die Verwahrung der gängigen Krypto-Währungen, bevor in der ersten Hälfte 2021 digitale Vermögenswerte in die Anlageberatung und Vermögensverwaltung Eingang fanden und eine erste diskretionäre Vermögensverwaltungslösung mit Krypto-Währungen lanciert wurde. Dies basierend auf unserer Überzeugung, dass digitale Vermögenswerte eine interessante Möglichkeit zur Steigerung des Rendite- und Diversifikationspotenzials eines traditionellen Portfolios darstellen können.

Fragen Sie uns danach!

Parallelen zu traditionellen Finanzmarktgeschäften

Wo Profite erwirtschaftet werden können, existieren auch Risiken. Unter anderem sehen sich Investoren mit dem Marktrisiko konfrontiert. Sowohl die hinterlegten als auch die ausbezahlten Coins unterliegen der Preisvolatilität des Marktes. Auch besteht das Risiko eines Ausfalls des Validators, was bei betrügerischen Absichten zu einem Totalverlust der Vermögenswerte führen kann. Doch auch hier gilt: Je seriöser der Validator, desto kleiner das Risiko.

Auf den ersten Blick gibt es Parallelen zum traditionellen Aktienmarkt und den jeweils ausbezahlten Leiheerträgen. Doch Staking Rewards sind mehr als nur einfache Erträge: Durch eine aktive Teilnahme am Netzwerk trägt man zu dessen Sicherheit bei und verdient dabei in einem vordefinierten Intervall Geld in Form von Coins. Das Konzept der Staking Rewards kann folglich als eine Art Leiheertrag bei Aktien verstanden werden.

Fazit

Proof-of-Stake ist inzwischen der am weitesten verbreitete Konsensmechanismus bei Krypto-Protokollen. Die Nachteile des Proof-of-Work-Ansatzes werden hiermit weitgehend beseitigt und ermöglichen es gleichzeitig vielen Teilnehmenden, ohne Investition in Infrastruktur und Rechenleistung an der Validierung von Transaktionen teilzunehmen. Die daraus resultierenden Staking-Erträge bieten einen regelmässigen Ertrag aus dem Besitz von Krypto-Währungen, die ansonsten – neben einem allfälligen Kursgewinn – kein Einkommen generieren. Die Teilnahme am Staking kann somit – sofern man sich der verschiedenen Risiken bewusst ist – einen angenehmen Nebenertrag generieren.

Informations- und Wissenstransfer

Im Rahmen der Anlageberatung und Vermögensverwaltung für digitale Vermögenswerte stehen unsere ausgewiesenen Spezialisten mit ihrer langjährigen Expertise auch persönlich für Fragen zu den Themen Blockchain und digitale Vermögenswerte zur Verfügung. Sie gewinnen so einen vertieften und gut nachvollziehbaren Einblick in die neue, aufstrebende Anlageklasse und können so Ihre Investitions- und Anlageentscheidungen mit mehr Komfort treffen.

Wann dürfen wir uns mit Ihnen austauschen?

Milko Hensel
Leiter Digitale Partnerschaften
Mitglied der Direktion
Maerki Baumann & Co. AG

Redaktionsschluss: September 2024

Maerki Baumann & Co. AG
Dreikönigstrasse 6, CH-8002 Zürich
T +41 44 286 25 25, info@maerki-baumann.ch
www.maerki-baumann.ch