Grundwissen

Konsens in der Blockchain: Proof-of-Work vs. Proof-of-Stake

Leonie Frink

Open Peer Review

Dieser Beitrag wurde lektoriert von: Daniel Dischinger und Larissa Pilch

Leonie hat Rechts- und Wirtschaftswissenschaften studiert und absolviert gerade ihr Rechtsreferendariat in Köln. Sie interessiert sich besonders für die Potenziale der Blockchain-Technologie.

Für eine sinnvolle Interaktion in einem Netzwerk müssen sich alle Teilnehmer auf einen einheitlichen Datenbestand einigen. In einem Blockchain-Netzwerk kommunizieren die Teilnehmer direkt miteinander (*peer-to-peer*). Eine Verifikation der ausgetauschten Informationen durch einen vertrauenswürdigen Dritten wie etwa eine Bank, einen Notar oder Treuhänder soll nach dem Wesen der Blockchain grundsätzlich nicht stattfinden. Daher muss die Integrität der Daten auf andere Weise sichergestellt werden. Konsensverfahren sorgen für eine einheitliche Synchronisierung der Daten, indem sie bestimmte Bedingungen an die Aufnahme neuer Informationen knüpfen.

Konsensverfahren legitimieren die Aufnahme neuer Informationen in die Blockchain und schließen Manipulationen weitestgehend aus. In Blockchain-Protokollen finden sich ganz unterschiedliche Konsensverfahren, mit denen versucht wird, je nach den Anforderungen der Anwendung die ideale Balance zwischen Dezentralisierung, Sicherheit und Skalierbarkeit zu schaffen. Am häufigsten werden „*Proof-of-Work*“ und „*Proof-of-Stake*“ verwendet. Die beiden Konsensverfahren unterscheiden sich durch die Art und Weise der Auswahl des Teilnehmers, der den Konsens im Netzwerk herstellt und die hierfür ausgesetzte Belohnung erhält.

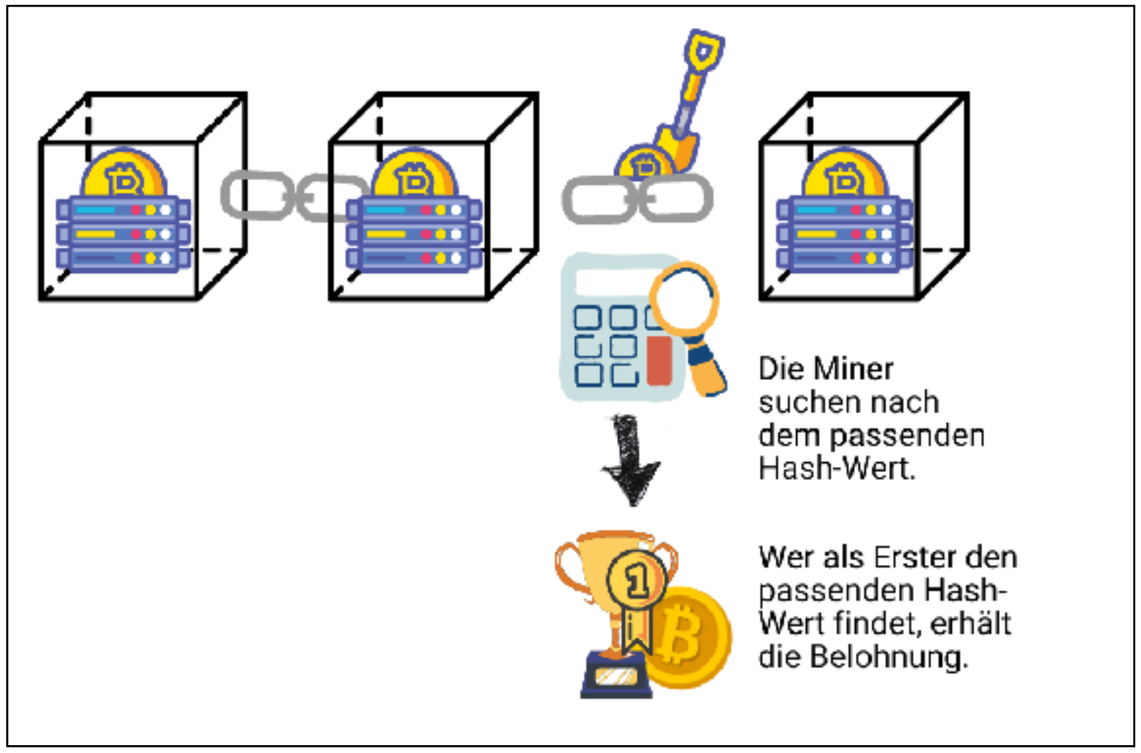
A. Proof-of-Work

Die wohl bekannteste Implementierung eines Proof-of-Work-Protokolls findet sich bei der Kryptowährung *Bitcoin*. Diese Methode wurde bereits 1993 von *Cynthia Dwork* und *Moni Naor* entwickelt, um den Versand von Spam-Mails einzudämmen. Die Idee war, dass vor Gewährung des Zugangs zu einem Dienst zunächst eine gewisse Arbeit verrichtet werden muss. Diese Arbeit sollte als Hindernis die übermäßige oder missbräuchliche Verwendung des Dienstes verhindern. Die erste moderne Anwendung, die Proof-of-Work umsetzte, wurde von *Adam Back* 1996 vorgestellt und nannte sich *Hashcash*.

Obwohl *Satoshi Nakamoto* – der anonyme Entwickler von *Bitcoin* – die Methode nicht erfunden hat, wurde durch ihn mit der Implementierung des Proof-of-Work-Algorithmus *SHA-256* in die Bitcoin-Blockchain die Art und Weise der Ausführung von Transaktionen revolutioniert. Viele große Kryptowährungen verwenden heute Proof-of-Work, beispielsweise *Litecoin* mit *Scrypt* und bisher auch *Ethereum* mit *Etash*.

Bei Proof-of-Work versuchen viele Teilnehmer eines Netzwerkes gleichzeitig Informationen, die zur Blockchain hinzugefügt werden sollen, zu validieren. Dazu werden diese Informationen zunächst zu Blöcken gebündelt. Die Miner überprüfen diese Blöcke durch eine komplexe mathematische Berechnung. Bei dieser erhält der neue Block einen Hash-Wert, der ihn mit dem vorigen Block verkettet. Der jeweiligen Blockchain liegt eine Hash-Funktion zugrunde, deren wesentliche Eigenschaft fehlende Invertierbarkeit ist. Das bedeutet, dass der Hash-Wert für die Anknüpfung des neuen Blocks nicht aus der Hash-Funktion berechnet werden kann. Der Miner muss daher verschiedene Werte ausprobieren, bis er zufällig den korrekten Wert findet. Derjenige, der diesen Wert als Erster findet, erhält hierfür eine zuvor durch den Algorithmus ausgesetzte Belohnung. Der Hash-Wert verkettet den neuen Block mit der bisherigen Blockchain.

Da die Teilnehmer die Hash-Funktion der Blockchain kennen, können sie nun ihren Datenbestand einheitlich synchronisieren. Infolgedessen erkennen die Teilnehmer die so verlängerte Blockchain einheitlich als legitimen Datenbestand an.



Verkettung eines Blocks mit Proof-of-Work

Bei der Bitcoin-Blockchain handelt es sich inhaltlich um ein Transaktionsbuch, das dokumentiert, wer wem wann wie viele Bitcoins gesendet hat. Die von den Teilnehmern des Netzwerkes getätigten Transaktionen werden nach dem vorher festgelegten Rhythmus alle 10 Minuten in Blöcken gebündelt und dann von Minern überprüft. Nachdem der neue Block validiert wurde, können die übrigen Teilnehmer des Netzwerkes ihre lokalen Kontoinformationen aktualisieren. Die Miner erhalten als Belohnung eine bestimmte Anzahl von Bitcoins.

Das Problem von Proof-of-Work ist vor allem die für den Mining-Prozess erforderliche Rechenleistung. Allein Bitcoin-Transaktionen im Jahr 2020 sollen so viel Strom wie Dänemark verbraucht haben. Aber nicht nur der hohe Energieverbrauch wird kritisiert: Je mehr Teilnehmer sich am Netzwerk beteiligen, desto mehr Konkurrenz herrscht um die Belohnungen, die zur Validierung der Blöcke ausgesetzt werden.

Unter dem Anreiz der ausgesetzten Belohnung setzen Miner immer leistungsfähigere Computer ein, um als erste den passenden Hash-Wert zu finden. Somit wird faktisch der Großteil der Teilnehmer, die keine Hochleistungsrechner besitzen, von einer Beteiligung an dem Verifizierungsprozess ausgeschlossen. Das entspricht nicht der ursprünglichen Idee der Blockchain, wonach der Verifizierungsprozess allen Teilnehmern offen stehen sollte. Zu einer verstärkten Zentralisierung führen auch die sogenannten *Mining-Pools*, in denen Teilnehmer ihre Rechenleistung bündeln. Damit erhöht sich die Wahrscheinlichkeit, dass ein Mitglied des Mining-Pools den richtigen Hash-Wert findet. Ist dies der Fall, erhält jedes Mitglied einen Anteil der Belohnung, der häufig vom Umfang der bereitgestellten Rechenleistung abhängt. *Mining-Pools* können jedoch so groß werden, dass sie die Kontrolle über die Blockchain vollständig übernehmen.

„Die ideale Balance zwischen Dezentralisierung, Sicherheit und Skalierbarkeit lässt sich nicht per se bestimmen."

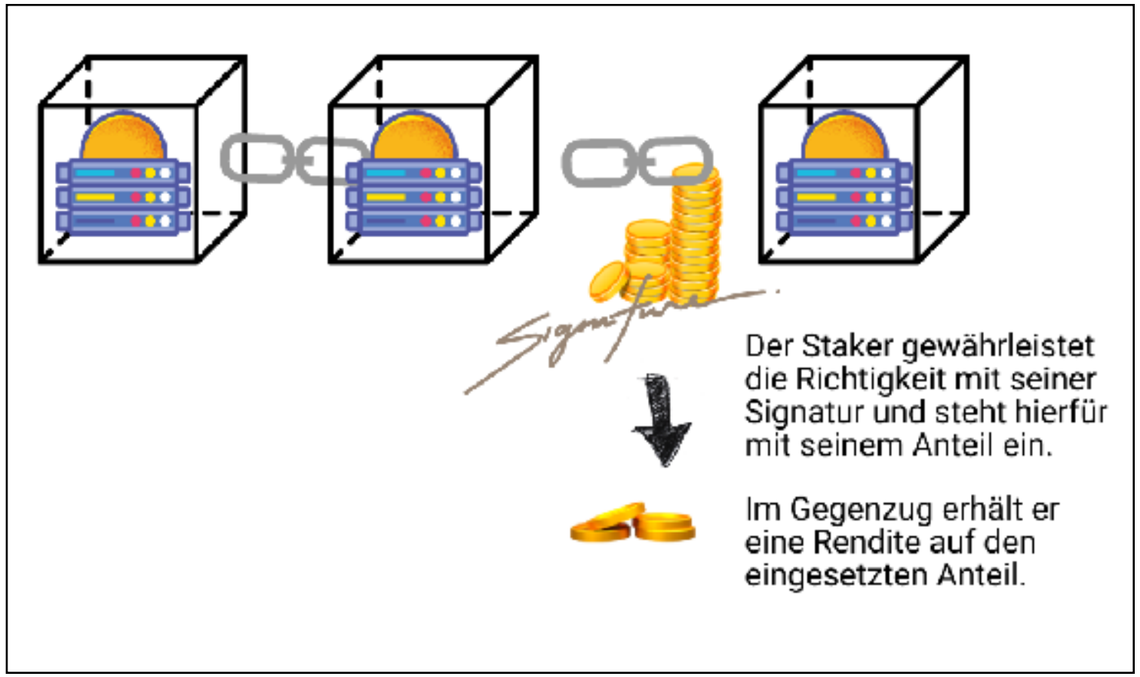
B. Proof-of-Stake

Proof-of-Stake sollte in erster Linie das Problem des hohen Energieverbrauchs lösen, das bei der Verwendung von Proof-of-Work-Protokollen entsteht. Das Konsensverfahren wurde von *Sunny King* und *Scott Nadal* entwickelt und erstmals 2012 vorgestellt. 2013 schuf *Sunny King* dann *Peercoin*. Dies war die erste Kryptowährung, die Proof-of-Stake implementierte. Seither verbreitet sich Proof-of-Stake als Alternative zu Proof-of-Work immer mehr. Auch der Schöpfer der *Ethereum*-Blockchain, *Vitalik Buterin*, wird dieses Jahr mit *Ethereum 2.0* seinen Mechanismus von Proof-of-Work auf Proof-of-Stake umstellen.

Während bei Proof-of-Work jeder am Validierungsprozess teilnehmen kann, wird bei Proof-of-Stake die Entscheidung über den validierenden Teilnehmer vor dem Validierungsprozess getroffen. Bei Proof-of-Stake wird zur Bestimmung desjenigen, der einen Block validieren darf, eine gewichtete Zufallsauswahl eingesetzt.

Die genauen Kriterien, die dabei gewichtet werden, sind in der Struktur des Algorithmus festgelegt und können je nach Anwendungsbereich der Blockchain variieren. Auswahlkriterien sind meist die Höhe eines bestimmten Anteils und die damit verbundene Reputation des sogenannten Stakers.

Bei Kryptowährungen ist oftmals die Anzahl und Haltedauer von Coins, die ein Staker besitzt, maßgeblich dafür, ob er für die Validierung eines neuen Blocks ausgewählt wird. Validieren darf dann derjenige, der die meisten Coins am längsten hält. Der ausgewählte Staker signiert die neuen Transaktionen und gewährleistet ihre Richtigkeit mit seinem Einsatz. Im Gegenzug erhält er eine Rendite auf den von ihm eingesetzten Anteil, die sich zwischen 2 % und 10 % im Jahr bewegen kann. Hierdurch wächst der Anteil, den der Staker hält. Durch den wachsenden Anteil erhöht sich gleichzeitig die Wahrscheinlichkeit, auch in Zukunft für die Signierung von Blöcken



Verkettung eines Blocks mit Proof-of-Stake

ausgewählt zu werden. Diese Aussicht schafft für den Staker den Anreiz, sauber zu arbeiten. Validiert ein Staker einen nicht legitimen Block, wird er für weitere Validierungen gesperrt und vom Netzwerk ausgeschlossen.

Dass Staker umso größere Chancen haben, einen Block zu validieren und die Belohnung dafür zu erhalten, je mehr Anteile sie am Gesamtvolumen sammeln („*staking*"), setzt positive Arbeitsanreize und gewährleistet die Sicherheit des Systems. Gleichzeitig werden aber erhebliche Zinseszinseffekte ausgelöst, die den Eintritt in das Geschäft für neue Investoren schwierig machen und nach einiger Zeit sogar nahezu ausschließen können. Dies führt zu einer Zentralisierung der ‚Staking-Power' auf wenige Staker; vergleichbar mit dem Mining-Pool-Problem bei Proof-of-Work.

Ein weiteres Problem von Proof-of-Stake ist das sogenannte *nothing-at-Stake*-Problem. Es kann vorkommen, dass in einem Netzwerk mehrere Blöcke mit verschiedenen Informationen parallel verkettet werden, da sie bei dem Verkettungs-Prozess nicht miteinander kommunizieren. Dann entstehen mehrere Zweige und es herrscht keine Einigkeit über einen einheitlichen Datenbestand. Für die einheitliche Synchronisierung der Daten muss Konsens über den legitimen Zweig hergestellt werden. Staker erhalten allerdings den Anreiz, missbräuchlich alle Zweige der Blockchain fortzuführen, da sie hierfür keinen erheblichen Arbeitsaufwand betreiben müssen und eine mehrfache Belohnung erhalten.

Dies führt zu Problemen bei Nutzern, die Transaktionen über die Blockchain abwickeln wollen. Verschiedene Überlegungen, wann und wie die parallele Erzeugung von Blöcken sanktioniert werden könnte, konnten bisher noch keine zufriedenstellende Lösung des Problems erreichen.

Der amerikanische Blockchain-Entwickler *Dan Larimer* hat das Proof-of-Stake-Verfahren weiterentwickelt und versucht, wieder eine größere Dezentralisierung im Validierungsprozess herzustellen. Mit seiner Kryptowährung *BitShares* hat er die *Delegated-Proof-of-Stake-Methode* erstmals implementiert.

Beim *Delegated-Proof-of-Stake* erwerben die Staker mit ihrem Anteil an den Netzwerkressourcen nicht das Recht zur Validierung eines Blocks, sondern das Recht zur Auswahl eines Zeugen. An diesen delegieren die Staker ihr Recht, die Blöcke zu signieren. Mit ihrem Einsatz bürgen sie dann lediglich noch für die vom Zeugen vorgenommene Verifizierung. Hierdurch soll der Validierungsprozess besser skalierbar werden. Das Recht zur Validierung erhält also nicht derjenige, der durch seinen Anteil ohnehin eine große Macht im Netzwerk hat. Vielmehr kann jeder, der sich vertrauenswürdig verhält, am Verifizierungsprozess teilhaben.

C. Fazit

Proof-of-Work schafft nach wie vor die höchste Dezentralität, da potenziell jeder an dem Validierungsprozess teilnehmen kann. Das Konsensverfahren ist sehr sicher, wegen der hohen benötigten Rechenleistung aber schlecht skalierbar. Proof-of-

Stake löst das Problem der Skalierbarkeit, indem es die Anzahl der am Validierungsprozess Beteiligten von vornherein begrenzt. Das geht jedoch wiederum zulasten der Dezentralität. Die ideale Balance zwischen Dezentralisierung, Sicherheit und Skalierbarkeit lässt sich nicht per se bestimmen. Es ist vielmehr eine Frage der konkreten Anwendung und ihrer Philosophie, wie viele Abstriche bei den einzelnen Anforderungen geduldet werden können. Die bestehenden Konsensverfahren weisen nach wie vor Schwächen auf. Es bleibt also spannend.

Weiterführende Hinweise:

Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin Whitepaper v. 01.11.2008, hier abrufbar (Stand: 15.12.2021).

King/*Nadal*, PPCoin: Peer-to-Peer Kryptowährung mit Proof-of-Stake, Peercoin Whitepaper v. 19.08.2012, hier abrufbar (Stand: 15.12.2021).

Buterin, What Proof-of-Stake Is And Why It Matters, Bitcoin Magazine v. 26.08.2013, hier abrufbar (Stand: 15.12.2021).

Wie funktioniert die Blockchain?: *Frink*, CTRL 1/21, 15, hier abrufbar (Stand 15.12.2021).

Anwendungspotenziale der Blockchain: *Dischinger*, CTRL 1/21, 18, hier abrufbar (Stand 15.12.2021).

Talking Legal Tech – Folge 5

Was ist die Blockchain, Florian Glatz?

Zurück zum dynamischen Inhaltsverzeichnis?

Zum dynamischen Inhaltsverzeichnis

1/22

2. Jahrgang, 1. Ausgabe
www.legaltechcologne.de/ctrl

CTRL

Cologne Technology & Law Review

Hier geht es zur ganzen Ausgabe

Dort findest Du in 19 Beiträgen alles von Datenschutz bei Connected Cars über Krypto-Auktionen bis hin zum Artificial Intelligence Act und Legal Tech.

LEGAL TECH LAB COLOGNE