ÜBERSICHT ÜBER DEN KONSENSMECHANISMUS

August 2021

Ein dezentralisiertes System impliziert, dass kein einzelner Teilnehmer die Kontrolle über die Regeln, Ein- und Ausgänge des Systems hat. Sicherheit wird daher zur größten Herausforderung für jedes dezentrale System. Dies gilt insbesondere dann, wenn sich die Teilnehmer nicht vertrauen und das System eine Aufzeichnung von Transaktionen bereitstellt, die einen Wert zuschreiben (wie bei einer öffentlichen Blockchain).

Wie können Teilnehmer ohne Überprüfung durch Dritte Transaktionen validieren und böswillige Akteure daran hindern, gefälschte und betrügerische Informationen zu verbreiten?

Satoshi Nakamoto lieferte eine Lösung für diese Frage, indem er verschiedene Ideen kombinierte, um ein verteiltes, unveränderliches und kryptografisches Transaktionsbuch zu erstellen[1] Im Zentrum steht der Proof-of-Work-Konsensmechanismus – eine Möglichkeit, Transaktionen zu verifizieren, indem anderen nachgewiesen wird, dass ein erheblicher Rechenaufwand für das Anhängen der Informationen an das Ledger aufgewendet wurde.

Seit der Geburt von Bitcoin wurden viele andere Konsensmechanismen geschaffen. Jeder von ihnen hat seine eigenen Eigenschaften, die die Attribute des zugehörigen Netzwerks bestimmen. In diesem Artikel überprüfen wir mehrere bestehende Konsensmechanismen und geben einen Überblick darüber, wie sie sich unterscheiden.

WAS IST EIN KONSENSMECHANISMUS?

Ein Konsensmechanismus ist ein Algorithmus zur Genehmigung von Transaktionen oder Aufzeichnungen in einem dezentralen Hauptbuch, sodass gefälschte oder betrügerische Aufzeichnungen abgelehnt werden.

Der Algorithmus wird ausgeführt, wenn neue Blöcke an die vorhandene Blockkette angehängt werden, wodurch die Blockchain als Nur-Anhänge-Ledger aktualisiert wird.

Die Idee ist, dass böswilligen Akteuren ein bestimmter Aufwand (oder ein einzugehendes Risiko) auferlegt wird und sie somit von einer Manipulation des Hauptbuches abgehalten werden, da sie den Aufwand (oder den Verlust) für unrentabel halten. Der allererste Zweck der Erfindung von Proof of Work bestand darin, E-Mail-Spam zu filtern.

[1] https://queue.acm.org/detail.cfm?id=3136559

Hashcash, ein von Adam Back im Jahr 1997 vorgeschlagenes Proof-of-Work-System, erfordert, dass E-Mail-Absender Stempel erstellen und an E-Mail-Header anhängen, um den Empfängern zu beweisen, dass sie CPU-Leistung zum Generieren von E-Mails aufgewendet haben. Bei diesen Stempeln handelt es sich um Einweg-Verschlüsselungsalgorithmen, die vom Empfänger leicht zu verifizieren sind, aber vom Absender (rechentechnisch gesehen) schwer zu generieren sind. Bei diesem Modell würden Spammer zögern, große Mengen an E-Mails zu versenden, da es unrentabel wird, viel CPU-Leistung zum Erstellen von Stempeln zu verwenden. Der Preis für das Versenden einer einzelnen E-Mail ist jedoch für normale Benutzer immer noch erschwinglich.

Da Konsensmechanismen in der Blockchain-Welt allgemein als Aktivitäten des „Mining" und „Staking" bezeichnet werden, werden sie häufig als Methoden zur Ausgabe neuer Coins angesehen. Ihr Hauptzweck besteht jedoch darin, das dezentrale Netzwerk zu sichern, während Belohnungen in Form von Münzen ein zusätzlicher wirtschaftlicher Anreiz für die Arbeiter sind, das Netzwerk aufrechtzuerhalten. Sie sind ein notwendiger Bestandteil jedes dezentralen Netzwerks, da sie das Netzwerk sichern und die Nachhaltigkeit und Skalierbarkeit des Netzwerks bestimmen.

	Invented Year	Nouns	Pros	Cons	Blockchain
Proof-of-Work	1997	mining I miners	• secure • long history	• energy intensive • susceptible to be more centralized	Bitcoin, Litecoin, Ethereum before 2.0
Proof-of-Stake	2011	minting I validators	• energy efficient • less centralized • better designed for attack recovery	• shorter track record • nothing-at-stake problem • long-range attacks	Ethereum
Delegated Proof-of-Stake	2014	minting I witness, delegates	• same as PoS • but more democratic • faster	• partially centralized	Bitshares, Steemit, Ark, Lisk

Quelle: Zhanga, Shijie und Lee, Jong-Hyouk. Analysis of the main consensus protocols of blockchain. Science Direct Vol. 6, Issue 2. Juni 2020

PROOF-OF-WORK (POW)

Proof-of-Work ist der älteste und beliebteste Konsensmechanismus. Er macht mehr als 75 % der Marktkapitalisierung von Blockchain-Protokollen aus. Er wird von Bitcoin, Ethereum (bis Serenity) und Litecoin usw. verwendet.[2]

In PoW rennen die Miner darum, einen Datenblock zu generieren, der drei Dinge enthält: neue Transaktionen, die auf die Überprüfung warten, eine Aufzeichnung des vorherigen Blocks und eine neue Transaktion (die so genannte „Coinbase"), die sich selbst eine Belohnung auszahlt (und dabei das Währungsangebot erhöht).

Dieser Block muss eine bestimmte mathematische Anforderung erfüllen, wenn der Datenblock kryptographisch „gehasht" wird. Miner können alle Transaktionen, die sie überprüfen möchten, aus einem Pool von nicht überprüften Transaktionen (d. h. nicht in einem bereits in der Blockchain befindlichen Block) wählen, die vom Netzwerk verwaltet werden. Bevor der Miner eine Transaktion zu seinem Block hinzufügt, überprüft er die digitale Signatur des Absenders bei jeder Transaktion und ob die Partei, die Coins sendet, zuvor genügend Coins in einer vorherigen Transaktion erhalten hat, die in einem Block in der Blockchain aufgezeichnet wurde.

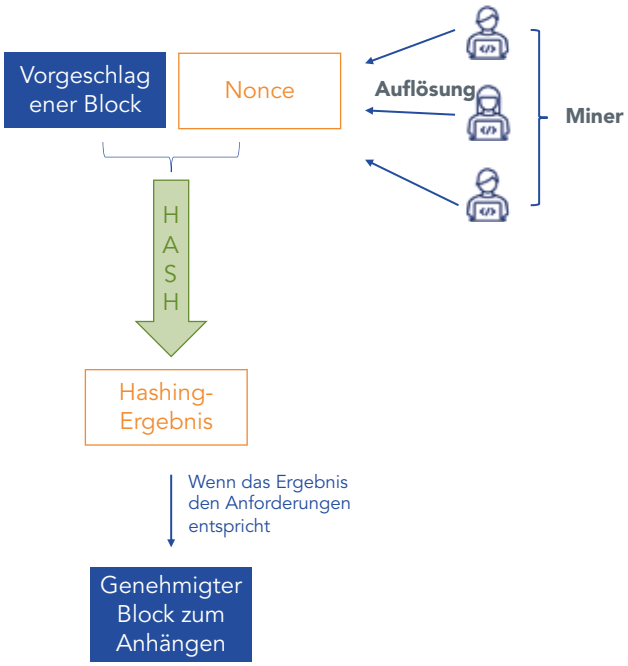
2 Ab dem 23.07.2021. Mithilfe von CoinMarketCap-Daten berechnet.

Eine Hash-Funktion nimmt eine beliebige Menge von Eingabedaten und berechnet eine numerische Ausgabe fester Länge, die mehrere wichtige Eigenschaften hat: für dieselben Eingabedaten erhält jeder, der dieselbe Hash-Funktion verwendet, dieselbe Hash-Ausgabe; die Ausgabe ist unvorhersehbar und kann nicht erraten werden; und es gibt keine Möglichkeit, von der Hash-Ausgabe zurück zu den Eingaben zu gelangen. Blockchains können unterschiedliche Hash-Funktionen verwenden (Bitcoin verwendet beispielsweise die SHA256-Funktion), aber was auch immer sie wählen, hat typischerweise diese Eigenschaften.

Damit ein Block gültig ist, muss die Hash-Ausgabe eine 256 Bit lange Zahl sein, die mit einer bestimmten Anzahl führender Nullen beginnt (bekannt als Schwierigkeit). In binärer Notation hat diese Zahl 256 Einsen oder Nullen. Eine so große Zahl kann alle Atome im Universum eindeutig beschreiben. Daher ist eine gültige Hash-Ausgabe normalerweise eine sehr kleine Zahl im Verhältnis zu allen möglichen Zahlen mit 256 Bit.

Da die kryptografische Hash-Funktion diese Ausgabe auf unvorhersehbare Weise generiert, kann der Miner nicht wissen, was das Ergebnis sein wird, und es besteht die Möglichkeit, dass die Hash-Ausgabe nicht mit genügend Nullen beginnt. Der Miner ändert und hasht den Block wiederholt, indem er eine als Nonce bekannte Zahl inkrementiert und die Nonce zu den Daten des Blocks hinzufügt – wodurch jedes Mal eine andere Hash-Ausgabe garantiert wird.

Wenn der Miner eine Nonce und eine Reihe von Transaktionen findet, die, wenn sie gehasht werden, die Schwierigkeitsanforderung erfüllen, sendet er diesen Block an andere Miner, damit sie diesen Block überprüfen und akzeptieren können. Sobald andere Miner die Gültigkeit eines Blocks überprüfen, fügen sie diesen Block zu ihrer Kopie der Blockchain hinzu und beginnen mit dem Mining eines neuen Blocks, einschließlich eines Hashs des vorherigen Blocks in ihrem neuen Block. Es besteht kein Anreiz, weiterhin Transaktionen zu überprüfen, die in einem neuen Block enthalten sind, da andere Miner nur zur längsten Kette von Blöcken hinzufügen.



Der Vorteil dieses Mechanismus ist seine Sicherheit und lange Geschichte, aber der Nachteil ist, dass er energieintensiv ist, da jeder Miner Rechenleistung verwendet, um Billionen Mal pro Sekunde Blöcke zu hashen. Es neigt auch dazu, zentralisierter zu sein, da der Mechanismus fortschrittliche Maschinen erfordert, um den Vorgang auszuführen. Miner mit aggregierten fortgeschrittenen Maschinen haben einen Vorteil in der Anzahl der Hashes, die sie ausführen können, und haben eine größere Chance, einen gültigen Block zu produzieren.

PROOF-OF-STAKE (POS)

Der Proof-of-Stake ist der zweitbeliebteste Konsensmechanismus.

Ethereum geht derzeit von Proof-of-Work zu Proof-of-Stake über, um effizienter, skalierbarer und nachhaltiger zu sein.

Im Gegensatz zu PoW erfordert PoS nicht, dass die Teilnehmer Rechenleistung verwenden, um Blöcke zu hashen und eine mathematische Anforderung zu lösen, sondern sie müssen Ether einsetzen. Die Teilnehmer werden im Gegensatz zu Minern als Validatoren bezeichnet, und die Aktion des Anhängens wird als Minting statt Mining bezeichnet.

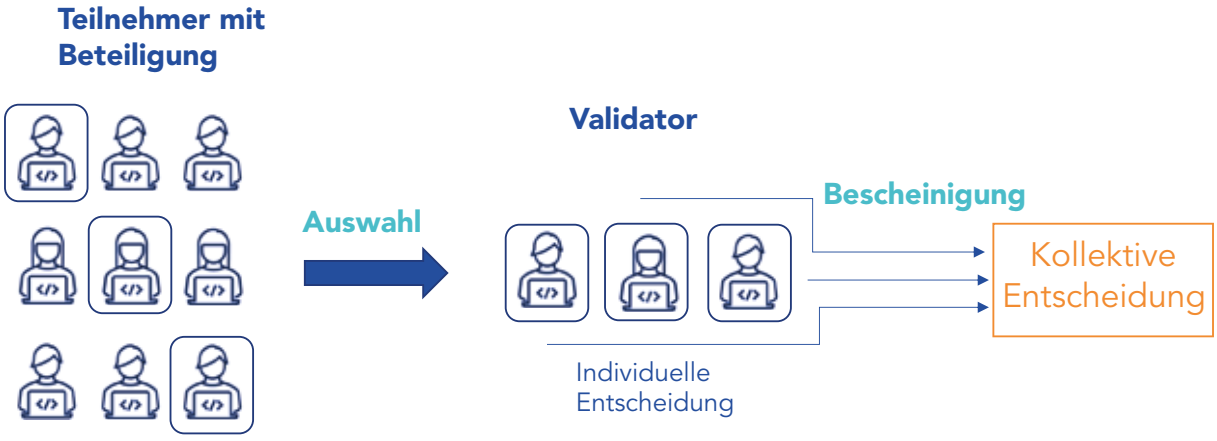
Der Proof-of-Stake kann auch in zwei Prozessen beschrieben werden: Auswahl und Attestierung.

Um ein Validator zu werden, müssen die Teilnehmer einen bestimmten Betrag der Kryptowährung beiseite legen, und je nach Blockchain werden die Validatoren unterschiedlich ausgewählt. Eine der beliebtesten Auswahlmethoden ist die randomisierte Blockauswahl, die von Ethereum verwendet wird. Der Mechanismus wählt nach dem Zufallsprinzip eine Gruppe von Validatoren basierend auf der Menge der eingesetzten Kryptowährung aus. Je mehr Vermögen man einsetzt, desto wahrscheinlicher werden sie ausgewählt.

Nach der Auswahl beginnt der Bestätigungsprozess.

Validatoren müssen einen Betrag an Kryptowährung einsetzen, der die Transaktionsgebühr und ihre potenzielle Belohnung abdeckt, bis der Block erfolgreich angehängt wird. Validatoren bestätigen den Block einzeln und senden ihre Entscheidung an das Netzwerk. Wenn eine bestimmte Anzahl von Validatoren dies genehmigt, wird der Block angehängt und den Validatoren wird eine anteilige Belohnung gewährt. Wenn der Block von der Gruppe der Validatoren abgelehnt wird, wird der Block nicht angehängt.

Betrug wird durch ein vorcodiertes Regelwerk erkannt, das durch inkonsistentes, fehlendes und anormales Verhalten ausgelöst wird. Unehrliche Teilnehmer könnten ihren Einsatz verlieren und aus dem Netzwerk ausgeschlossen werden.



PoS reduziert die Mining-Energie, da nur das Abstecken erforderlich ist. Es erfordert auch keine Validatoren, die über fortschrittliche Maschinen verfügen, was die Eintrittsbarriere senkt und weniger konzentriert als PoW macht[3]. PoS sieht sich jedoch mehreren potenziellen Exploits durch das „Nothing-at-Stake"-Problem[4] und Angriffen über große Entfernungen ausgesetzt, die Abschwächungen aus anderen Bereichen erfordern.

[3] https://vitalik.ca/general/2020/11/06/pos2020.html.

[4] https://medium.com/@abhisharm/understanding-proof-of-stake-through-its-flaws-pt-1-6728020994a1

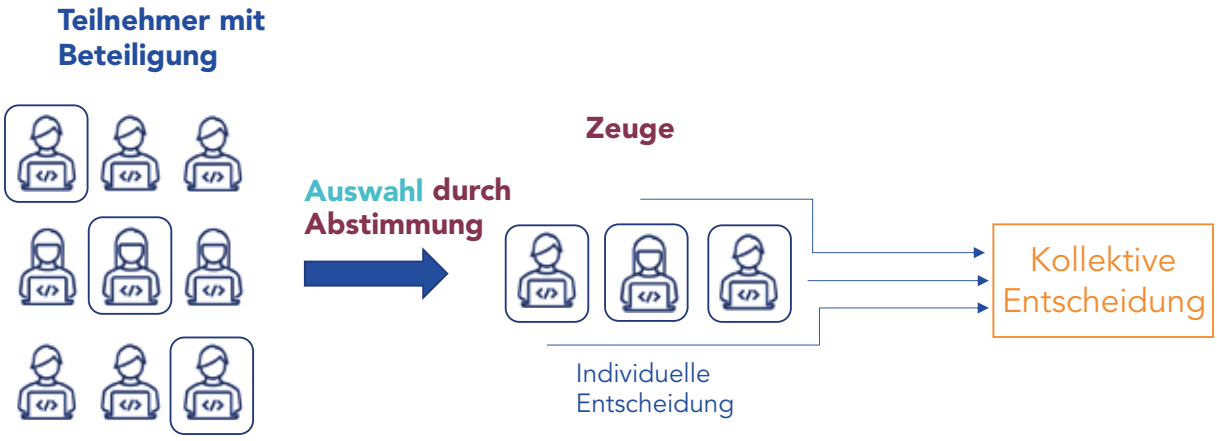
Nur für professionelle Kunden

DELEGATED PROOF-OF-STAKE (DPOS)

Der delegierte Proof-of-Stake ist eine Variante des Proof-of-Stake. Es ändert den Auswahlprozess in PoS von randomisierten Algorithmen zu einem demokratischeren Ansatz.

Coin-Inhaber mit einer Beteiligung an einem DPoS-Netzwerk wählen ständig Blockvalidatoren durch Abstimmung aus. Die Stimmmacht wächst mit dem Vermögen. Alle Münzinhaber haben das Potenzial, gewählt zu werden, indem sie andere Teilnehmer davon überzeugen, für sie zu stimmen. Einige der Überlegungen, die bei der Abstimmungsentscheidung eine Rolle spielen, umfassen die Robustheit der Hardware, dedizierte Teams usw.

Gewählte Validatoren werden Delegierte oder Zeugen genannt und sind für das Unterschreiben und Verifizieren neuer Blöcke verantwortlich. Um Manipulationen vorzubeugen, wird eine Gruppe von Zeugen (normalerweise 21-100) für einen bestimmten Zeitraum ausgewählt.[5] Während dieser Zeit (die als Epoche bezeichnet wird) überprüfen und signieren Zeugen abwechselnd neue Blöcke mit ihren privaten Schlüsseln. Diese signierten Blöcke bleiben dann unbestätigt, bis die Mehrheit der Zeugengruppe zustimmt.



Genehmigte Blöcke belohnen Zeugen, und diese Belohnungen werden normalerweise mit den Wählern geteilt. Fehlgeschlagene Blöcke hinterlassen keine Belohnung. Böswillige Schauspieler würden nach ihrer Entdeckung schnell abgewählt.

DPoS führt ein kollektives menschliches Urteilsvermögen ein, um einen Wettbewerb um reine Rechenleistung zu ersetzen. Es kann viel mehr Transaktionen verarbeiten, selbst im Vergleich zu PoS. Es reduziert auch die Sperrzeit für Sicherheiten, die abgesteckt werden. Dadurch, dass die Teilnehmer abstimmen können, wird das Netzwerk demokratischer als PoW und PoS.

Der Abstimmungsprozess kann jedoch auch das Netzwerk zentralisieren, da Münzinhaber mit einem kleinen Anteil ihre Stimmen aufgrund ihrer Bedeutungslosigkeit verlieren würden.

ANDERE KONSENSMECHANISMEN

Neben PoW, PoS und DPoS gibt es viele Proof-of-X-Mechanismen, die versuchen, ein dezentrales und sicheres Netzwerk aufzubauen. Dazu gehören Leistungsnachweis, Nachweis der verstrichenen Zeit, Nachweis der Bedeutung usw.

---

5 https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-stake/delegated-proof-of-stake-dpos

6 Is a term that describes a situation where all participants in a system need to agree on a strategy in order to avoid catastrophic failure of the system, however, some participants are unreliable or malicious.

Eine weitere wichtige Familie von Konsensmechanismen ist die byzantinische Fehlertoleranz; Dies ist das Merkmal eines verteilten Netzwerks, um einen Konsens (Einigung über denselben Wert) zu erzielen, selbst wenn einige der Knoten im Netzwerk nicht oder mit falschen Informationen antworten. Es gibt mehrere Variationen wie die praktische Byzantinische Fehlertoleranz (pBFT), die derzeit von Hyperledger Fabric verwendet wird, und ihre verbesserte Version wird von der People's Bank of China (PBoC) verwendet, um ihre Central Bank Digital Currency (CBDC) zu entwickeln. Eine andere Variante heißt delegierte byzantinische Fehlertoleranz (dBFT), die von Neo verwendet wird. Das Konsensmodell des Stellar-Netzwerks nutzt ein Modell des föderierten byzantinischen Abkommens (FBA) und versucht, auf diesen Modellen aufzubauen, um ein offenes Netzwerk zum Speichern und Bewegen von Geld aufzubauen.

Diese Mechanismen werden häufiger in zugelassenen Protokollen verwendet, für die vorherige Berechtigungen für den Beitritt erforderlich sind. Sie sind frühe Lösungen des Byzantinischen Fehlers[6], der dasselbe Problem ist, das Bitcoin zu lösen versucht.

Zu den Vorteilen dieser Mechanismen gehören Energieeffizienz, Transaktionsendgültigkeit, die weniger Validierungen von Knoten erfordert, um eine Transaktion zu bestätigen, und verbesserte Fähigkeit zur Koordination in einem geschlossenen System. Sie haben jedoch eine geringere Toleranz für böswillige Knoten im Netzwerk und sind möglicherweise schwer zu skalieren, sodass sie kein idealer Kandidat für öffentliche Blockchains sind.

Property	PoW	PoS	DPoS	PBFT	Ripple
Type	Probabilistic-finalist	Probabilistic-finalist	Probabilistic-finalist	Absolute-finalist	Absolute-finalist
Fault Tolerance	50%	50%	50%	33%	20%
Power consumption	Large	Less	Less	Negligible	Negligible
Scalability	Good	Good	Good	Bad	Good
Application	Public	Public	Public	Permissioned	Permissioned

Quelle: Zhanga, Shijie und Lee, Jong-Hyouk. Analysis of the main consensus protocols of blockchain. Science Direct Vol. 6, Issue 2. Juni 2020. Die Grafik stellt die Unterschiede der diskutierten Konsensmechanismen im Überblick dar. „Finality type" (Finalitätstyp) bezieht sich auf das Modell für die Bestätigung und Unveränderbarkeit vergebener Blöcke. „Probabilistic finality" (probabilistische Finalität) bedeutet, dass es mit zunehmender Blockchain-Länge immer schwieriger wird, Blöcke wieder herauszulösen. „Absolute finality" (absolute Finalität) bedeutet, dass Blöcke bereits finalisiert werden, wenn sie an die Blockchain angefügt werden. „Fault tolerance" (Fehlertoleranz) beschreibt die Toleranz eines Systems gegenüber nicht funktionsfähigen oder böswillig eingeschleusten Komponenten, die den Systembetrieb beeinträchtigen würden. „Power consumption" (Energieverbrauch) bezieht sich auf den möglichen Verbrauch großer Energiemengen durch das System. „Scalability" (Skalierbarkeit) beschreibt, wie einfach das System vergrößer- und erweiterbar ist. „Application" (Anwendung) bezieht sich auf den idealen Blockchain-Typ, in dem der Konsensmechanismus angewendet werden soll. Das Attribut „public" (öffentlich) beschreibt Blockchains, auf die beliebige Personen frei zugreifen können. Das Attribut „private" (privat) beschreibt Blockchains, bei denen der Zugriff eine gesonderte Berechtigung erfordert.

6 Ist ein Begriff, der eine Situation beschreibt, in der sich alle Teilnehmer eines Systems auf eine Strategie einigen müssen, um einen katastrophalen Ausfall des Systems zu vermeiden, einige Teilnehmer jedoch unzuverlässig oder böswillig sind.

FAZIT:

Der Konsensmechanismus ist eine Schlüsselkomponente für ein dezentralisiertes Netzwerk. Es sichert nicht nur das System, sondern beeinflusst auch dessen Effizienz und Skalierbarkeit.

Bei der Untersuchung eines Konsensmechanismus ist es wichtig, seine Funktionalität anhand von drei Aspekten zu betrachten: Dezentralisierungsgrad, Sicherheit und Skalierbarkeit. Die meisten Konsensmechanismen können nur auf zwei der drei Faktoren optimieren – Sicherheit geht auf Kosten der Skalierbarkeit und des Risikos der Zentralisierung, und skalierbare Netzwerke könnten anfälliger für Angriffe sein.

Daher müssen unterschiedliche Konsensmechanismen basierend auf den Bedürfnissen des jeweiligen Netzwerks analysiert werden.

WICHTIGE INFORMATIONEN

Im Europäischen Wirtschaftsraum („EWR") herausgegebene Mitteilungen: Dieses Dokument wurde von WisdomTree Ireland Limited, einer von der Central Bank of Ireland zugelassenen und regulierten Gesellschaft, herausgegeben und genehmigt.

In Ländern außerhalb des EWR herausgegebene Mitteilungen: Dieses Dokument wurde von WisdomTree UK Limited, einer von der United Kingdom Financial Conduct Authority zugelassenen und regulierten Gesellschaft, herausgegeben und genehmigt.

WisdomTree Ireland Limited und WisdomTree UK Limited werden jeweils als „WisdomTree" bezeichnet. Unsere Richtlinie über Interessenkonflikte und unser Verzeichnis sind auf Anfrage erhältlich.

Nur für professionelle Kunden. Die in diesem Dokument enthaltenen Informationen dienen ausschließlich Ihrer Information und stellen weder ein Angebot zum Verkauf bzw. eine Aufforderung oder ein Angebot zum Kauf von Wertpapieren oder Anteilen dar. Dieses Dokument sollte nicht als Basis für eine Anlageentscheidung verwendet werden. Anlagen können an Wert zunehmen oder verlieren und Sie können einen Teil oder den gesamten Betrag der Anlage verlieren. Die Wertentwicklung in der Vergangenheit ist nicht notwendigerweise ein Hinweis auf zukünftige Ergebnisse. Anlageentscheidungen sollten auf den Angaben im entsprechenden Prospekt sowie auf unabhängiger Anlage-, Steuer- und Rechtsberatung basieren.

Bei diesem Dokument handelt es sich nicht um Werbung bzw. eine Maßnahme zum öffentlichen Angebot von Anteilen oder Wertpapieren in den USA oder einer zugehörigen Provinz bzw. einem zugehörigen Territorium der USA, und es darf unter keinen Umständen als solche verstanden werden. Weder dieses Dokument noch etwaige Kopien dieses Dokuments sollten in die USA mitgenommen, (direkt oder indirekt) übermittelt oder verteilt werden.

Dieses Dokument kann unabhängige Marktkommentare enthalten, die von WisdomTree auf der Grundlage öffentlich zugänglicher Informationen erstellt wurden. Obwohl WisdomTree bestrebt ist, die Richtigkeit des Inhalts dieses Dokuments sicherzustellen, übernimmt WisdomTree keine Gewährleistung oder Garantie für seine Richtigkeit oder Genauigkeit. Die Drittanbieter, deren Dienste in Anspruch genommen werden, um die in diesem Dokument enthaltenen Informationen zu beziehen, übernehmen keine Gewährleistung oder Garantie jeglicher Art bezüglich dieser Daten. Dort, wo WisdomTree seine eigenen Ansichten in Bezug auf Produkte oder Marktaktivitäten äußert, können sich diese Auffassungen ändern. Weder WisdomTree, noch eines seiner verbundenen Unternehmen oder einer seiner jeweiligen leitenden Angestellten, Verwaltungsratsmitglieder, Partner oder Mitarbeiter übernimmt irgendeine Haftung für direkte Schäden oder Folgeschäden, die durch die Verwendung dieses Dokuments oder seines Inhalts entstehen.

Dieses Dokument kann zukunftsorientierte Aussagen enthalten, einschließlich Aussagen hinsichtlich unserer aktuellen Erwartungen oder Einschätzungen im Hinblick auf die Wertentwicklung bestimmter Anlageklassen und/oder Sektoren. Zukunftsorientierte Aussagen unterliegen gewissen Risiken, Unsicherheiten und Annahmen. Es gibt keine Sicherheit, dass diese Aussagen zutreffen, und die tatsächlichen Ergebnisse können von den erwarteten Ergebnissen abweichen. WisdomTree empfiehlt Ihnen deutlich, sich nicht in unangemessener Weise auf diese zukunftsgerichteten Aussagen zu verlassen.

Jegliche in diesem Dokument enthaltene historische Wertentwicklung kann u. U. auf Backtesting beruhen. Backtesting ist der Prozess, bei dem eine Anlagestrategie evaluiert wird, indem sie auf historische Daten angewandt wird, um zu simulieren, was die Wertentwicklung solch einer Strategie in der Vergangenheit gewesen wäre. Durch Backtesting erzielte Wertsteigerungen sind jedoch rein hypothetisch und werden in diesem Dokument einzig und allein zu Informationszwecken aufgeführt. Daten, die durch Backtesting gesammelt wurden, stellen keine tatsächlichen Wertsteigerungen dar und dürfen nicht als Indikator für tatsächliche oder zukünftige Wertsteigerungen angesehen werden.