



Der Weltcomputer

Einführung in Ethereum (ETH)

April 2021

Ether ist nach der Marktkapitalisierung die zweitgrößte Kryptowährung nach Bitcoin. Seine Marktkapitalisierung beträgt derzeit 290,69 Milliarden USD, was einem Anteil von ca. 14 Prozent am gesamten Kryptowährungsmarkt entspricht¹.

Das Blockchain-Netzwerk Ethereum wurde 2013 erfunden und 2015 eingeführt. Seitdem hat es an Innovation und Nutzen gewonnen. Im Gegensatz zu Bitcoin, dessen Hauptfunktion in einem elektronischen Peer-to-Peer-Zahlungssystem besteht, erfindet Ethereum eine neue Welt der Peer-to-Peer-Anwendungen.

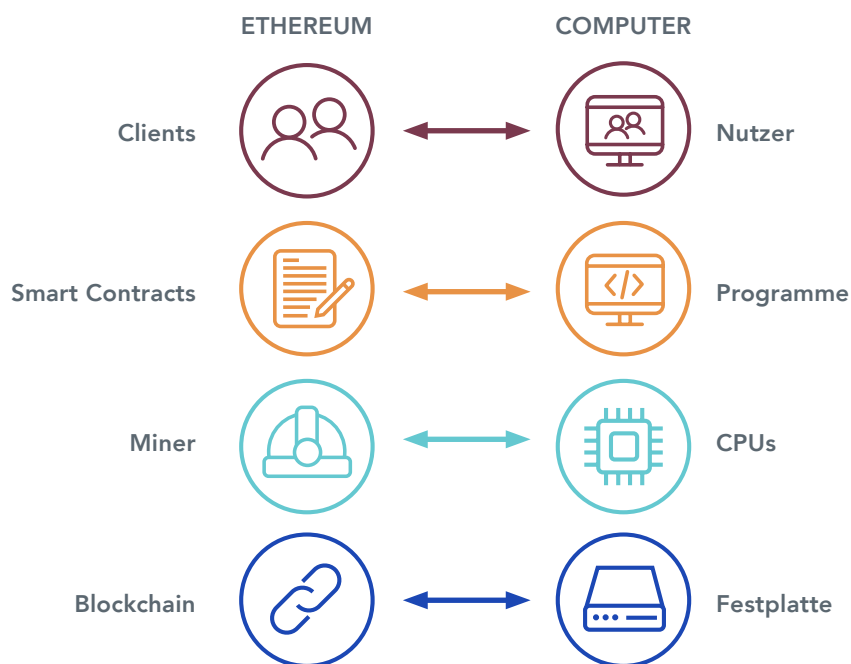
Doch bevor wir ins Detail gehen, ist es wichtig, zwischen Ether (ETH) und Ethereum zu unterscheiden. **Ether** bezieht sich auf die Kryptowährung, die auf der Ethereum-Blockchain verwendet wird. **Ethereum** bezieht sich auf das Blockchain-Netzwerk.

Was ist Ethereum?

Die Plattform baut auf der öffentlichen, dezentralisierten und kryptografischen Open-Source-Blockchain-Technologie auf. Sie ermöglicht dezentralisierte Anwendungen (**dApps**), die von einem Transaktionsprotokoll unterstützt werden, das als **Smart Contract** bezeichnet wird.

Mithilfe ihrer kollektiven Rechenleistung auf dem verteilten Netzwerk (**der Ethereum Virtual Machine**) führt sie Peer-to-Peer-Transaktionen aus und ermöglicht dadurch einen automatischen, bedingten Vermögens- und Informationstransfer, u. a. von Geld, Wahlrechten und Eigentum.

Ethereum lässt sich mit einem „Weltcomputer“ auf einer Blockchain vergleichen, bei dem die zugrunde liegende Blockchain-Technologie die Festplatte des virtuellen Rechners ist, Smart Contracts Programme sind, die Miner CPUs sind und die Nutzer mit ETH für die Nutzung dieses „Computers“ bezahlen.



¹ Am 15. April 2021.

² <https://ethereum.org/en/what-is-ethereum>

Problemlösung

Die Erfindung von Ethereum wurde durch Bitcoin inspiriert.

Bitcoin schuf die Grundlage für die dezentralisierte Blockchain-Technologie. Seine Funktion beschränkt sich jedoch auf elektronische Peer-to-Peer-Überweisungen. Ethereum erweitert die Funktion von Bitcoin um programmierbare Apps. Im Prinzip zielt es auf die Schaffung eines dezentralisierten Computernetzwerks ab, das verschiedene Anwendungen ausführt. Der Gründer Vitalik Buterin verwendet folgende Metapher: Bitcoin ist wie ein Taschenrechner, doch Ethereum möchte zu einem Smartphone werden, das zahlreiche Anwendungen ausführt³.



Dieses dezentralisierte Netzwerk würde Entscheidungen und Transaktionen automatisieren und damit den Bedarf nach einer vertrauenswürdigen zentralen Instanz senken. Es kann den Bedarf nach Intermediären senken, die Kosten für Schiedsverfahren reduzieren, Betrug verhindern und versehentliche Ereignisse minimieren.

Wie funktioniert Ethereum?

SMART CONTRACTS

Smart Contracts stehen bei Ethereum im Mittelpunkt.

Es handelt sich dabei um eine der zwei Arten von Ethereum-Konten, in die festgelegte Anweisungen einprogrammiert sind. Nick Szabo, der Entwickler des Konzepts, verglich dies häufig mit den Codes an Verkaufsautomaten.

Ein Smart Contract wird ausgeführt, wenn er durch eine Transaktion ausgelöst wird. Im Beispiel mit dem Verkaufsautomaten entspricht die Transaktion dem Einwerfen einer Münze. Sobald ein Smart Contract ausgelöst wurde, werden auf der Grundlage der Wenn-Dann-Bedingungen, die im Code des Smart Contract verankert sind, Aktionen ausgeführt.

Beispielsweise wird durch Drücken einer Tastenkombination an einem Verkaufsautomaten eine Flasche Wasser ausgegeben. Der Artikel, der durch den Automaten ausgegeben wird, ist das Ergebnis des Smart Contracts. Auf dem Ethereum-Netzwerk könnte es sich dabei entweder um einen Vermögenstransfer in ETH an ein anderes Konto handeln oder um eine Transaktion, die einen weiteren Smart Contract auslöst.

³ Vitalik Buterin erwähnte diese Metapher am 10. Oktober 2016 in einer Rede mit dem Titel „Ethereum in 25 Minuten“.

Ein Smart Contract unterliegt vorab festgelegten Regeln, durch die er auf einer beliebigen Ethereum-Node des Netzwerks Code automatisch auf dieselbe Weise ausführen kann. Dadurch fällt der Bedarf nach einem Dritten weg, der die Ausführung des Codes im Namen des Nutzers übernimmt, und das System wird somit zu einem dezentralisierten System. Durch die Kombination verschiedener Smart Contracts ermöglicht dies Programmierern die Entwicklung vielfältiger Anwendungen.

Ein konkretes Beispiel dazu liefert Etherisc, eine dezentralisierte Versicherungsanwendung auf dem Ethereum-Netzwerk. Die Mitglieder können Versicherungen direkt in der Anwendung mit ihrem nativen Token kaufen. Daraufhin wird ein Pool gebildet, in dem die Versicherungsbeiträge aller Mitglieder zusammengefasst werden. Bei Eintreten eines Versicherungsfalls erfolgen Auszahlungen an die betroffenen Mitglieder, ohne dass dazu ein schwerfälliger Rückerstattungsvorgang wie in der herkömmlichen Versicherungsbranche notwendig wäre. Zum Beispiel könnte eine Ernteversicherung automatisch ausgezahlt werden, wenn staatliche Agenturen Dürren oder Überschwemmungen in einem Gebiet melden.

GAS

Gebühren sind den Minern gegenüber in ETH fällig, um Transaktionen zu ermöglichen und Smart Contracts auszuführen. Die fällige Gebühr wird als **Gas** bezeichnet. Beim Preis für Gas handelt es sich häufig um einen kleinen Bruchteil von ETH, der in der Einheit Gwei (10^9 Gwei = 1 ETH) angegeben wird.

Gas ist zur Aufrechterhaltung des Ethereum-Netzwerks wesentlich. Es motiviert die Miner zur Bearbeitung und Prüfung von Transaktionen gegen eine Entlohnung. Die Menge an Gas, die für eine Transaktion notwendig ist, entspricht ungefähr dem Wert an benötigter Energie zuzüglich einer geringen Transaktionsgebühr. Der **Gaspreis** schwankt mit dem Angebot von und der Nachfrage nach Rechenleistung, da die Miner sich bei niedrigen Gaspreisen gegen die Bearbeitung einer Transaktion entscheiden können.

Die Vermeidung unbeabsichtigter Energieverschwendung ist eine weitere wichtige Funktion von Gas. Da die Programmiersprache für Ethereum Turing-vollständig ist, besteht die Möglichkeit, dass ein Programm unendlich lang ausgeführt wird und eine Transaktion dadurch sehr viel Energie verbraucht. Ein **Gaslimit** entspricht dem maximalen Preis, zu dessen Zahlung die Nutzer bereit sind, um Transaktionen zu ermöglichen. Wenn das Gas ausgeht, wird das Programm beendet und es wird keine zusätzliche Energie aufgewendet.

ANWENDUNGEN

Die Anwendungen von Ethereum nutzen die dezentralisierte und unveränderliche Eigenschaft der Blockchain-Technologie. Jeder kann sie entwickeln und zu ihnen beitragen, ohne die Sicherheit des Systems zu beeinträchtigen. Ihre Funktionalitäten sind weitreichend. Hier einige wichtige Beispiele:

- + Decentralized Finance (DeFi): DeFi hat den Aufbau eines offenen und weltweiten Finanzsystems zum Ziel, das jedem zugänglich ist, der über einen Internetzugang verfügt. Im Gegensatz zur vertrauensbasierten Finanzbranche oder FinTech strebt DeFi eine Vertrauensminimierung an. Damit ist gemeint, dass der Betrieb des Systems nicht von einer einzelnen Instanz abhängig ist, sondern sich im Besitz aller Nutzer befindet. Durch diesen Aufbau ist es je nach Bedarf zugänglich, transparent und potenziell schneller und günstiger. Es verbindet Angebot und Nachfrage direkt miteinander, ohne dass dazu Intermediäre notwendig sind.

Die Funktionalitäten von DeFi haben sich seit seiner Einführung zu einem Finanz-Ökosystem entwickelt. Die Nutzer können nun auch wie im herkömmlichen Finanzsystem Darlehen aufnehmen, Kredite vergeben, investieren, handeln, Zinsen einnehmen, Versicherungen kaufen und Geldüberweisungen vornehmen.

- + Decentralized Autonomous Organization (DAO): Eine DAO ist eine Organisation ohne Dritte, die mit einem gemeinsamen Ziel gegründet wird. Diese Organisation arbeitet und kooperiert über ein gemeinsames, definiertes und automatisiertes Protokoll. So wird sichergestellt, dass die Meinungen aller Gruppenmitglieder gehört werden und der Entscheidungsfindungsprozess transparent ist. Jede DAO verfügt über eine eingebettete Kasse, in der die Finanzmittel gespeichert werden. Die Ausgabe der Finanzmittel erfolgt anhand von Entscheidungen, über die die Mitglieder abstimmen.

Ein Beispiel für eine DAO ist ein dezentralisierter Venture-Capital-Fonds mit dem Namen „The DAO“, die 2016 gegründet wurde. Die Mitglieder können DAO-Tokens kaufen, um sich Stimmrechte für Anlagevorschläge zu sichern. Sollte das in einer Abstimmung gewählte Projekt profitabel werden, erhalten die Mitglieder entsprechend ihrer Einlage eine Rendite. Obwohl es sich bei The DAO um eine innovative Idee handelte, scheiterte sie aufgrund eines Programmfehlers im Code ihres Smart Contracts. Ein Teil der Finanzmittel der Organisation fiel dem Diebstahl durch Hacker zum Opfer. Dieses Ereignis führte zu der Entscheidung über die Durchführung einer Hard Fork im Ethereum-Netzwerk. Dadurch entstand eine Verzweigung, die Ethereum Classic genannt wird. Andere Beispiele für eine DAO werden weiterhin erfolgreich betrieben. MakerDAO ermöglicht die fortlaufende Erzeugung von Dai, einer dezentralisierten Stablecoin.

- + Non-fungible Tokens (NFT): NFTs sind Datensätze auf der Blockchain, die die zugrunde liegenden Assets unveränderlich und differenziert machen. Es kann sich dabei um digitale Assets wie Fotos, Audioaufnahmen, Videos, Aktien und Zertifikate oder auch um physische Assets wie Immobilien oder Gemälde handeln.

Da sich digitale Dateien einfach replizieren lassen, sind Non-fungible Tokens wichtig, um das Eigentum an digitalen Dateien nachzuweisen. Beim Kauf eines NFTs erhält der Eigentümer einen unveränderbaren Eigentumseintrag. Die Attraktivität von NFTs für digitale Assets liegt in der Seltenheit, die erzeugt wird und die somit den Sammlerwert des Assets verbessert. Den Künstlern, die die Assets verkaufen, ermöglichen NFTs eine direkte Distribution ihrer Arbeiten ohne Drittplattform, wodurch ihre Urheberrechte besser geschützt und ihre Erträge erhöht werden könnten.

Im Fall von NFTs, hinter denen echte physische Vermögenswerte stehen, weist die Tokenisierung das digitale Eigentum an einer Sache nach und bewahrt die Einzigartigkeit dieser Sache. Obwohl der NFT-Markt für physische Vermögenswerte nicht so entwickelt ist wie der Markt für digitale Assets, bestehen zahlreiche Möglichkeiten zur Nutzung von tokenisierten Vermögenswerten. Dies könnte den Kauf und Verkauf von NFTs und ihre Nutzung als Sicherheit bei der Darlehensaufnahme fördern.

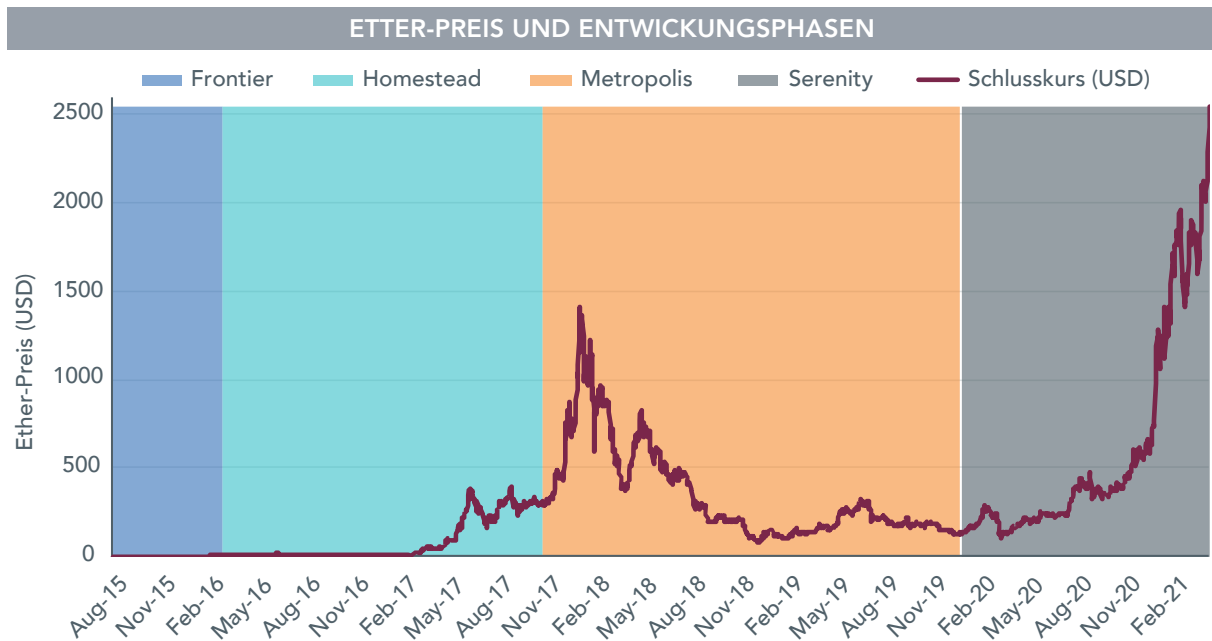


Nyan Cat GIF von Chris Torres wurde am 19. Feb. 2021 für 300 ETH (~600.000 USD) verkauft.

Wie geht es mit Ethereum weiter?

Die Idee von Ethereum wurde 2013 vorgeschlagen. Am 30. Juli 2015 wurde die erste Version von Ethereum mit dem Namen „Frontier“ veröffentlicht. Die Entwicklung von Ethereum lässt sich in vier Hauptstufen einteilen:

- + Frontier (Juli 2015–März 2016)
- + Homestead (März 2016–Oktober 2017)
- + Metropolis (Oktober 2017–Dezember 2019)
- + Serenity (Dezember 2019–2022)



Daten vom 09.08.2015 bis zum 15.04.2021. **Die historische Performance ist kein Anhaltspunkt für die künftige Performance und jedes Investment kann im Wert sinken.**

Derzeit befinden wir uns noch in der sich entwickelnden Serenity-Phase, die auch Ethereum 2.0 genannt wird. Diese Version soll zwei Hauptprobleme lösen, denen sich Ethereum gegenüber sieht: ein von Engpässen geplagtes Netzwerk, das nur eine begrenzte Anzahl von Transaktionen pro Sekunde verarbeiten kann, und der hohe Energieverbrauch, der durch den Proof-of-Work-Mechanismus verursacht wird⁴.

Zwei der großen Upgrades umfassen den Übergang von Proof-of-Work zu Proof-of-Stake und die Implementierung von Shard-Chains, was zu einer Verteilung der Netzwerklast führen würde⁵. Ethereum 2.0 wird als skalierbarer, sicherer und nachhaltiger betrachtet.

⁴ Proof-of-Work ist ein Konsensmechanismus, der zur Echtheitsprüfung von Blockchain-Transaktionen verwendet wird. Erreicht wird dies durch das Lösen rechenintensiver Aufgaben mithilfe der Rechenleistung der Computer der Miner.

⁵ Proof-of-Stake ist ein weiterer Konsensmechanismus, der zur Überprüfung von Blockchain-Transaktionen verwendet wird. Dabei werden jedoch die vorhandenen Coins der Miner im Rahmen des Prüfungsvorgangs als Anspruch eingesetzt, wodurch die Computer weniger Rechenleistung erbringen müssen.

Vergleich zu Bitcoin

Da das Blockchain-Rahmenwerk von Bitcoin die Inspiration für Ethereum lieferte, verfügen beide über dieselbe zugrunde liegende Blockchain-Technologie und sind somit dezentralisiert, öffentlich und unveränderlich.

Es bestehen jedoch einige Hauptunterschiede zwischen Ethereum und Bitcoin.

	Bitcoin	Ethereum
Live-Auflegung	Januar 2009	Juli 2015
Anwendungsfall	Elektronisches Peer-to-Peer-Zahlungssystem mit Schwerpunkt auf der Nutzung als Kryptowährung	Blockchain-Plattform mit Schwerpunkt auf der Entwicklung von dApps
Funktionalitäten	Buchführung	Buchführung und Code-Ausführung
Programmiersprache	Bitcoin-Skript ist weniger programmierfreundlich, nicht Turing-vollständig	Hauptsprache ist Solidity; es ist programmierfreundlich und Turing-vollständig
Hashing-Algorithmus	SHA-256	Ethash
Blockerstellungsdauer	10 Minuten	10–19 Sekunden
Gesamtobergrenze des Angebots	21 Millionen	Keine Obergrenze

Zusammenfassend lässt sich sagen, dass das Bitcoin-System stärker definiert und starr ist, da sein Schwerpunkt auf dem Anwendungsfall als Kryptowährung liegt. Das System von Ethereum ist flexibler, zugänglicher und entwickelt sich ständig weiter, da seine Entwicklung stark von Teilnahmen abhängt, sodass sich ein umfangreiches Netzwerk aus Anwendungen bildet.

Fazit

Eine dezentralisierte Anwendungsplattform – Ethereum mag sich wie eine Science-Fiction-Idee anhören. Doch es handelt sich dabei bereits um ein florierendes Ökosystem. Es gibt derzeit 148 Millionen einmalige Adressen, die Empfänger und Sender von Transaktionen sind, und 6.867 Computer-Nodes, die das Ethereum-Netzwerk verbinden. Es werden täglich durchschnittlich 1,3 Millionen Transaktionen durchgeführt und es sind mehr als 3.500 dApps verfügbar⁶.

Durch die Eliminierung von Intermediären und die Maximierung der Effizienz bietet Ethereum eine spannende Chance für eine grundlegende Veränderung herkömmlicher Branchen. Es besteht ein hohes Potenzial, dass seine Innovation und Ausführung riesige Auswirkungen auf die reale Welt haben werden.

⁶ Laut <https://etherscan.io>, www.ethernodes.org, <https://www.stateofthedapps.com/rankings/platform/ethereum>, Stand: 16. April 2021.

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.

Kryptowährungen sind eine Anlage mit hohem Risiko und möglicherweise nicht für alle Arten von Anlegern geeignet. Kryptowährungen können eine höhere Volatilität aufweisen als andere Anlageklassen.