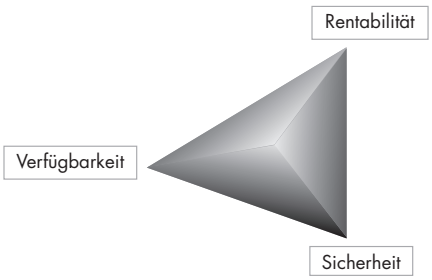
Basis- und Risikoinformationen über Kryptowerte

Max Heinr. Sutor oHG | Hermannstraße 46 | 20095 Hamburg

justTRADE
Ein Service der Sutor Bank

Kriterien der Anlageentscheidung

Zielalternativen jeder Art von Geld- und Vermögensanlage bilden die drei Kriterien des **„magischen Dreiecks"** der Geldanlage: **Rentabilität** (Ertrag der Anlage), **Sicherheit** der Anlage und **Verfügbarkeit** (Möglichkeit, die Anlage in Bargeld zurückzuwandeln). Keine Anlageform erfüllt alle drei Kriterien in gleichem Maße.
Zum einen besteht ein Spannungsverhältnis zwischen der Rentabilität und der Sicherheit einer Vermögensanlage. Zur Erreichung eines möglichst hohen Grades an Sicherheit muss regelmäßig eine niedrigere Rendite in Kauf genommen werden. Andersherum bieten spekulative Anlagen zwar höhere Ertragschancen, bergen gleichzeitig aber auch höhere Verlustrisiken. Mit steigender Sicherheit sinkt tendenziell die Rendite.
Zum anderen gibt es einen Zielkonflikt zwischen der Verfügbarkeit und der Rentabilität einer Vermögensanlage, da kurzfristig verfügbare Anlagen oftmals niedrigere Renditen erzielen als langfristige Investitionen.
Die Bestimmung, wie sich die drei Kriterien zueinander verhalten sollen, bildet die Grundlage für die persönliche Entscheidung jedes Anlegers über die Form seiner Geldanlage und dementsprechend auch über die Art des bevorzugten Investmenttyps.



Rahmenbedingungen

Kryptowerte zählen zu einem verhältnismäßig neuen Finanzinstrument mit einem speziellen Rendite-Risiko-Profil. Wer sich zum Erwerb von Kryptowerten entschließt, sollte sich umfassend mit der Funktionsweise sowie den Risiken, die sich aus dem Handel und der Verwahrung von Kryptowerten ergeben, auseinandersetzen. Aufgrund des Risikos des Totalverlustes eignet sich dieses spekulative Handelsinstrument insbesondere für sehr gut informierte und risikobereite Anleger.

Diese Informationen dienen der Unterstützung der Anleger, geben jedoch lediglich einen Überblick und stellen keine Anlageberatung dar. Darüber hinaus ist es sinnvoll, neben den hier zur Verfügung gestellten Informationen auch weitere Informationsquellen zu nutzen.

Kryptowerte sind gesetzlich definiert als „**digitale Darstellungen eines Wertes**, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Weg übertragen, gespeichert und gehandelt werden kann" (§ 1 Abs. 11 Sätze 4, 5 KWG). Sie können unter anderem die Gestalt von Kryptowährungen (auch virtuelle Währungen, digitale Währungen) annehmen und werden derzeit als fungible (= austauschbare) Vermögenswerte global an verschiedenen Finanzmärkten gehandelt. Beispiele der geläufigsten Kryptowährungen sind Bitcoin (BTC), Litecoin (LTC), Ether (ETH) und Ripple (XRP).

Im Gegensatz zu herkömmlichen Währungen basieren Kryptowährungen auf der Idee eines **nichtstaatlichen Ersatzgeldes in begrenzter Menge**. Anders als bei der Schöpfung von Zentralbankgeld durch die Notenbanken und bei Kredit- und Buchgeld, welches Geschäftsbanken erzeugen, erfolgt die Schaffung neuer Werteinheiten **(„Kryptotoken")** bei Kryptowährungen wie Bitcoin grundsätzlich in einem rechenintensiven Prozess über das Hinzufügen von kryptografisch verschlüsselten Transaktionsdatensätzen zu einer öffentlich einsehbaren, dezentralen Datenbank. Diese Datenbank hat in der Regel die Form einer Kette von aneinandergehängten, unveränderbaren Blöcken und wird deshalb meist **„Blockchain"** genannt.
Das vorbestimmte mathematische Verfahren innerhalb eines Computernetzwerks wird als **„Mining"** (Block-Schürfung) bezeichnet.

Während der Block-Schürfung werden die jüngsten Transaktionsdaten durch sogenannte **Miner** verifiziert, in einem Block zusammengefasst und an den vorherigen Block angehängt. Die Blöcke sind kryptografisch so miteinander verbunden, dass Transaktionen in einem angehängten Block nicht mehr verändert werden können. Die so entstehende Blockchain wird dezentral auf allen Netzwerkknoten gespeichert, sodass jeder Netzwerkknoten über alle Transaktionen informiert ist. Die Verifizierung und die dezentrale Verteilung der Informationen stellt sicher, dass gültige Transaktionen nur vom jeweiligen Eigentümer vorgenommen und Kryptotoken nicht mehrfach ausgegeben werden können.

Bei der Schaffung neuer Blöcke werden neue Token der Kryptowährung als Vergütung (sogenannter **„Block Reward"**) für das zur Verfügung stellen der Rechenleistung geschöpft. Bei Kryptowährungen wie Bitcoin können Miner neue Werteinheiten schöpfen, bis eine maximale Gesamtmenge erreicht ist; bei einer Kryptowährung wie Ether ist derzeit keine maximale Gesamtmenge definiert, wobei sich dies in Zukunft auch ändern kann.

Die einzelnen Blockchain-Netzwerke funktionieren nach dem **„Peer-to-Peer"-Prinzip**. In diesem Prinzip stehen sich alle Nutzer („Peers") grundsätzlich gleichberechtigt gegenüber; es gibt keine zentralen Parteien wie z. B. Notenbanken, Behörden oder sonstige Organisationen, die zwischengeschaltet sind und sich um Regulierung, Kontrolle, Steuerung oder Transaktionen bzw. Guthaben kümmern. Wenn die Mehrheit der Nutzer eine Transaktion nach den Regeln des jeweiligen Netzwerks als korrekt einstuft, wird die Transaktion in der Blockchain niedergeschrieben und in dem Netzwerk als gültig anerkannt. Anerkannte Transaktionen sind grundsätzlich irreversibel – sie können von niemandem, weder von den Urhebern noch von Minern oder Regierungsbehörden rückgängig gemacht werden.

Kryptotoken sind im Netzwerk identifizierbaren Adressen zugeordnet, wobei sich eine Adresse aus einer zufällig generierten Zeichenfolge, dem öffentlichen Schlüssel **(„Public Key")**, ableitet. Der jeweilige Inhaber einer Adresse verwaltet diese mit dem zugehörigen, geheim gehaltenen, privaten Schlüssel **(„Private Key")**, um Transaktionen zu signieren. Alle Nutzer können ihre Kryptotoken untereinander innerhalb des Netzwerks übertragen. Die jeweiligen Zieladressen müssen außerhalb des Netzwerks ausgetauscht werden.

Die Schlüsselpaare können von den Nutzern in einer als **„Wallet"** bezeichneten Software (ähnlich einer persönlichen digitalen Brieftasche) auf ihren Computern verwaltet und aufbewahrt werden. Wallets ähneln in ihrer Funktion normalen Geldbörsen und Bankkonten. Es handelt sich jedoch um rein digitale Geldbörsen. In den Wallets werden nicht die Kryptotoken selbst, sondern die für ihre Nutzung notwendigen Schlüssel verwahrt. Die Schlüssel können auch auf eigenen Hardware-Geräten **(„cold storages")** oder Papier **(„paper wallets")** verwahrt werden.

Die Menge an Kryptotoken, die einer Adresse zugeordnet werden, sowie alle bisherigen Transaktionen auf der Blockchain sind öffentlich einsehbar, jedoch keiner realen Person direkt zuzuordnen. Daher nennt man blockchainbasierte Kryptowährungen auch **„pseudonym"**: Transaktionen und Kryptotoken-Zuordnungen sind vollständig transparent, die natürlichen oder juristischen Personen (wirtschaftlich Berechtigten), die diese Transaktionen durchführen und Kryptotoken halten, sind jedoch unbekannt, sofern sie ihre Identität nicht außerhalb des Netzwerks zu erkennen geben.

Neben dem Transfer von Kryptotoken innerhalb des Netzwerks ist es ebenfalls möglich, Kryptotoken durch die Weitergabe der Schlüssel an neue Eigentümer zu übertragen.

Ähnlich wie bei der Anlage in Wertpapieren sind mit der Anlage in Kryptowerten generell sowie in Kryptowährungen im Besonderen Risiken verbunden:

Mit der Anlage in Kryptowerten generell verbundene Risiken

Unter **Kursrisiko** versteht man die möglichen Wertschwankungen einzelner Vermögensanlagen. Üblicherweise orientiert sich der Kurs z. B. einer Aktie an der wirtschaftlichen Entwicklung des Unternehmens sowie an den allgemeinen wirtschaftlichen und politischen Rahmenbedingungen. Der Wert von Kryptowährungen wird durch Angebot und Nachfrage an speziellen Börsen gebildet. Er kann sehr stark schwanken. Vergangene Kursentwicklungen können nicht als Anhaltspunkt für künftige Preise der Kryptowerte dienen.

Neben handfesten Faktoren bestimmen auch Meinungen und Gerüchte die Kursentwicklung an der Börse. Obwohl sich objektive Bewertungsfaktoren nicht verändert haben, können solche Stimmungslagen den Kurs eines Vermögenswertes und somit den Ertrag der Vermögensanlage stark beeinflussen **(Psychologisches Marktrisiko)**. Für Kryptowährungen, die keinen eigenen inneren Wert besitzen, gilt dies in hohem Maße.

Das Maß für die Schwankungsbreite eines Kurses innerhalb eines bestimmten Zeitraums wird auch als **Volatilität** bezeichnet. Je höher die Volatilität ist, umso stärker schlägt der Kurs nach oben und unten aus und desto riskanter aber auch chancenreicher ist eine Investition in diese Kapitalanlage. Kryptowährungen sind durch eine besonders hohe Volatilität gekennzeichnet.

Die Möglichkeit, einen Vermögenswert jederzeit zu marktgerechten Preisen verkaufen zu können, wird Handelbarkeit (= Liquidität) genannt. Ein liquider Markt zeichnet sich dadurch aus, dass ein Anleger seine Vermögenswerte verkaufen kann, ohne dass schon ein durchschnittlich großer Verkaufsauftrag (gemessen am marktüblichen Umsatzvolumen) zu spürbaren Kursschwankungen führt und nicht oder nur auf einem deutlich niedrigeren Kursniveau abgewickelt werden kann **(Liquiditätsrisiko)**. Keine oder nur eine geringe Liquidität kann dazu führen, dass der Anleger die von ihm gehaltenen Kryptowerte nicht oder nicht innerhalb des beabsichtigten Zeitraums zu marktgerechten Preisen veräußern oder erwerben kann. Liquiditätsrisiken existieren bei Kryptowährungen in besonderem Maße, insbesondere bei Kryptowährungen, deren Marktkapitalisierung niedriger ist als bei der führenden Kryptowährung Bitcoin.

Der **Kauf von Vermögenswerten auf Kredit** stellt durch den Hebeleffekt ein erhöhtes Risiko dar, da der aufgenommene Kredit unabhängig vom Erfolg

des Investments zurückgeführt werden muss und die Kreditkosten darüber hinaus den Ertrag schmälern. Der Kauf von Kryptowährungen ist aufgrund ihrer Volatilität besonders risikoreich.Ein **Konjunkturrisiko** entsteht dann, wenn die Konjunkturentwicklung bei der Anlageentscheidung unzureichend berücksichtigt wird. Kryptowährungen reagieren auf Konjunkturentwicklungen anders als wertpapierbasierte Vermögensanlagen, was das Risiko für weniger informierte Anleger steigert.

Steuerliche Risiken können sowohl auf den Kapitalmärkten durch Änderungen des Steuerrechts der jeweiligen Länder als auch durch die steuerliche Situation beim Anleger entstehen (insbesondere Kapitalerträge und Erträge aus privaten Veräußerungsgeschäften).

Spezifische, mit der Anlage in Kryptowerten verbundene, Risiken

Marktakzeptanzrisiko
Der Wert der Kryptowährungen hängt maßgeblich von der Akzeptanz als Zahlungsmittel unter den Marktteilnehmern ab. Die Anbieter von Waren / Dienstleistungen sowie sonstige Marktakteure sind gesetzlich nicht verpflichtet, Kryptowährungen als Zahlungsmittel anzunehmen. Es besteht daher das Risiko, dass die Kryptowährungen zukünftig in einem geringeren Umfang als bisher als Zahlungsmittel akzeptiert werden.

Wertrisiko
Kryptowährungen besitzen keinen eigenen oder inneren Wert, wie dies beispielsweise bei Silbermünzen in Form eines Materialwertes der Fall sein kann. Der Wert von Kryptowährungen folgt dem Grundsatz der Preisbildung an der Börse, Angebot und Nachfrage auszugleichen. Er wird daher durch den Marktpreis (siehe „Kursrisiko" sowie „Psychologisches Marktrisiko") bestimmt. Es besteht das Risiko eines Verfalls des Marktpreises, ohne dass dieser Verlust durch einen inneren Wert begrenzt würde.

Einstellung bzw. Reduktion der Mining-Tätigkeit
Die Nutzungsmöglichkeiten von Kryptowährungen basieren auf den ihnen zugrundeliegenden Blockchains. Ihr Funktionieren hängt maßgeblich von der Fähigkeit und Bereitschaft der Miner ab, ihre Rechenleistung für die Bildung neuer Blöcke zur Verfügung zu stellen. Diese „Technologie-Betreiber" können ihre Tätigkeit aus verschiedenen Gründen aufgeben oder so stark reduzieren, dass die Funktionsfähigkeit der Blockchain nicht mehr ausreichend gewährleistet ist. Beispiele hierfür sind mangelnde Finanzierung, fehlendes öffentliches Interesse an den jeweiligen Kryptowährungen oder unzureichende Erträge.

Gabelungsrisiko / Hard Fork-Risiko / Nichtteilnahme an Zuflussereignissen
Eine sogenannte „Hard Fork" ist eine Aufteilung der Blockchain in zwei unterschiedliche Werte. Diese Änderung im Protokoll einer Blockchain, welche nicht mit früheren Versionen kompatibel ist, hat zur Folge, dass alle Nutzer der neuen Software von denen der veralteten Software getrennt werden. Damit die neuen Blöcke auch erkannt werden, ist es für alle Marktakteure der betreffenden Blockchain erforderlich, nur noch die aktuelle Version der Software zu benutzen. Die zwei Blockchains trennen sich in zwei neue Pfade. Es besteht das Risiko, dass der Anleger die Kryptowerte des abgespaltenen Netzwerks nicht erhält, da die für den Zufluss der neuen Kryptowerte erforderlichen Voraussetzungen nicht vorliegen und dass es aufgrund der Teilung der Blockchain zu erheblichen Preisschwankungen kommen kann. Das Risiko der Nichtteilnahme an Zuflussereignissen besteht z.B. auch bei Airdrops, der zusätzlichen Ausschüttung von Einheiten an die Halter der Kryptowährung.

Transfergebührrisiko
Bei vielen Blockchains ist eine Kryptowährungstransaktion an eine andere Adresse mit einer Transfergebühr verbunden. Sollte diese Gebühr auf ein unangemessen hohes Niveau steigen, kann der Kryptotoken insbesondere als Zahlungsmittel nicht mehr rentabel erscheinen und dieses zu einem Verfall des Marktpreises führen.

Regulatorisches Risiko
Sofern Regierungen / Regierungsbehörden bestehende Vorschriften ändern, anders anwenden oder neue Vorschriften einführen, ist mit Wertveränderungen der Kryptowährung zu rechnen. Starke Einschränkungen durch staatliche Regulation bzw. Änderungen der regulatorischen Einstufung innerhalb der einzelnen Länder können zu Veränderungen der Akzeptanz von Kryptowährungen führen. Bereits die Ankündigung von Regulierungsmaßnahmen kann zu Kursturbulenzen führen.Eine Untersagung des Handels mit bestimmten Kryptowerten oder des Besitzes von bestimmten Kryptowerten durch staatliche Stellen kann dazu führen, dass bestimmte Marktplätze den Handel mit Kryptowerten einstellen müssen und die Anleger ihre Kryptowerte nicht mehr verkaufen können.

Keine Regulierung von Handelsplätzen
Viele Handelsplätze für Kryptowerte im Ausland unterliegen entweder keiner staatlichen Aufsicht oder nur einer eingeschränkten staatlichen Aufsicht, die nicht mit der staatlichen Aufsicht für Börsen vergleichbar ist. Dies kann dazu führen, dass die Handelsplätze anfälliger sind für Kursmanipulationen der am Handelsplatz gehandelten Kryptowerte oder für kriminelle Handlungen.

Softwarefehler
Kryptowährungen sind wie alle softwarebasierten Systeme nicht vor Softwarefehlern sicher. Sollten solche Störfälle nicht durch Softwarekorrekturen oder kooperatives Verhalten der Beteiligten behoben werden können, drohen Verluste, weil der Blockchain als Software-Basis der Kryptowährung nicht mehr getraut wird, oder Totalverluste, weil die Blockchain insgesamt nicht mehr funktionsfähig ist.

Fehler im Programmcode
Fehler im Programmcode der Blockchains oder in der zugrundeliegenden Verschlüsselungstechnologie können Dritten unbefugten Zugriff auf Kryptotoken geben oder die gesamte Blockchain wertlos machen.

Irreversibilität von Transaktionen
Sofern die jeweilige Blockchain über keine integrierte Adressvalidierung verfügt, führen fehlerhafte Adresseingaben beim Transfer von Kryptotoken aufgrund der Nicht-Umkehrbarkeit zum Verlust der transferierten Kryptotoken.

Wallet-Fehler
Bei Auszahlung der Kryptotoken auf eigene Wallets besteht das Risiko, dass eingegebene Wallet-Adressen fehlerhaft sind, nicht zum eigenen Wallet gehören oder durch einen Hacker-Angriff bzw. Computervirus eine fehlerhafte Wallet-Adresse übermittelt wird.

Datenverlust
Die Verfügungsgewalt über ein Guthaben in Kryptowährungen entsteht durch den Besitz des geheimen privaten Schlüssels, der ausschließlich dem Besitzer zugänglich ist. Beim Verlust dieses Schlüssels sind die damit verbundenen Werteinheiten sowohl für den Besitzer als auch das gesamte Netzwerk verloren.

Ausspähen von Daten
Die für die Verfügung über ein Kryptowährungs-Guthaben erforderlichen Schlüssel sind vom Speicherbedarf her vergleichsweise klein und ein leichtes Ziel für Computerkriminelle. Sie lassen sich ähnlich wie Passwörter mit Schadprogrammen ausspähen. Durch das Ausspähen von privaten Schlüsseln erhält ein Angreifer ebenso Zugang zu den Kryptotoken des Anlegers. Es ist möglich, dass solche als gestohlen bezeichnete Kryptotoken in späteren Transaktionen zwar zugeordnet werden können, aufgrund der Fungibilität (ähnlich zu Geld) jedoch eine Identifizierung der „Diebe" ähnlich wie beim Bargeld nur in Ausnahmefällen möglich ist.

Sicherheitsrisiko / Technologierisiko
Zum Schutz vor Datenverlust oder Angriffen bieten Firmen die sichere Verwahrung von Kryptowährungs-Guthaben als Dienstleistung an. Die Anbieter solcher Wallets verwahren die Kryptotoken nach sehr hohen Sicherheitsstandards und implementieren dementsprechende Sicherheitskonzepte. Diese garantieren jedoch ebenfalls keine 100%-ige Sicherheit. Es besteht das Risiko, dass auch die verwendeten Technologien Ziele von Cyberangriffen oder physischen Angriffen werden.

Manipulationsrisiko
Jede einem Kryptowert zugrundeliegende Blockchain beruht auf einem bestimmten kryptografischen Verfahren zum Schutz vor Manipulationen. Diese Verfahren oder die Implementierung dieser Verfahren erweisen sich zukünftig möglicherweise als nicht ausreichend sicher, sodass das Risiko einer Beeinträchtigung oder kompletten Aufhebung der Funktionsfähigkeit der Blockchain beispielsweise durch Cyberangriffe besteht.

Mehrheitsangriff / 51%-Angriff
Sofern Miner sich zusammenschließen und insgesamt mehr als die Hälfte der Rechenleistung bündeln, besteht bei Kryptowährungen wie dem Bitcoin die Möglichkeit eines Mehrheitsangriffes (auch 51%-Angriff / Mehrheitsbeschluss per Rechenleistung). Hierbei kann die Mehrheit der Mining-Kapazität übernommen werden und der Angreifer bestimmen, welche Transaktionen vom Netzwerk zugelassen und anerkannt werden und welche nicht. Bei dieser gezielten Marktmanipulation durch große Marktteilnehmer kann die Funktionsfähigkeit der Blockchain beeinträchtigt oder ganz aufgehoben werden. Dies kann zu einem Verfall des Marktpreises führen.

Handelsaussetzungsrisiko
Die Einschränkung oder Aussetzung der Handelbarkeit von Kryptowährungen an verschiedenen Finanzmärkten (z.B. aus technischen Gründen oder Fehlern) kann zu (temporären) Marktverwerfungen führen.

Risiko einer Einstellung des Handels
Falls eine staatliche Behörde den Handel mit einem oder mehreren Kryptowerten untersagt oder Kryptowerte aus anderen Gründen nicht mehr gehandelt werden können oder dürfen, wird der Handel in diesem Kryptowert an dem jeweiligen Handelsplatz für Kryptowerte eingestellt
Dies kann dazu führen, dass der Anleger den Kryptowert wenn überhaupt nur außerhalb von Handelsplätzen veräußern kann. Eine solche Veräußerung wird regelmäßig nur zu wesentlich geringeren Preisen möglich sein, als zu denen der Kryptowert zuletzt auf den Handelsplätzen gehandelt worden ist.

Indexbezogene Risiken
Ein Portfolio verschiedener Kryptowerte kann dazu genutzt werden, Indizes für Kryptowerte physisch nachzubilden. Hierbei ist nicht auszuschließen, dass die Wertentwicklung des jeweiligen Markts nicht vollständig oder korrekt abgebildet wird. Bei der Berechnung, der Anpassung sowie der Veröffentlichung der Zusammensetzung der Indizes kann es zu Fehlern kommen. Darüber hinaus werden für die Berechnung und Anpassung der Indizes öffentlich zugängliche Daten verwendet Es kann nicht ausgeschlossen werden, dass die mit großer Sorgfalt ausgewählten und überprüften Daten für die Indexberechnung nicht fehlerhaft, unvollständig oder manipuliert wurden und somit die tatsächlichen Marktgegebenheiten nicht korrekt wiedergeben.

Steuerliche Behandlung
Der Erwerb von Kryptowährungen ist im Gegensatz zu Wertpapieren abgeltungsteuerfrei, d. h. Kursgewinne aus dem Verkauf von Kryptotoken sind nach einem Jahr Haltedauer steuerfrei zu vereinnahmen. Bei einer kürzeren Haltedauer anfallende Steuern sind an das zuständige Finanzamt abzuführen. Bei Fragen sollte sich der Kunde an die für ihn zuständige Steuerbehörde bzw. seinen steuerlichen Berater wenden.

Allgemeine Hinweise

Es ist zu beachten, dass diese Risiko- und Basisinformationen keine Empfehlung in Bezug auf den Kauf oder Verkauf von Kryptowerten im Allgemeinen oder Kryptowährungen im Besonderen enthält, insbesondere keine Anlageberatung darstellt.

Aufgrund der mit Kryptowährungen einhergehenden Risiken ist deren Handel nur für risikobereite Anleger geeignet. Da mit dem Kauf von Krypotwerten auch das Risiko eines Totalverlustes des eingesetzten Kapitals einhergeht, sollten Kryptowährungen nur dann erworben werden, wenn der Anleger finanziell in der Lage ist, einen solchen auch zu verkraften.

In diesem Zusammenhang ist es ratsam, sich selbst oder gemeinsam mit einem geeigneten Berater, beispielsweise einem Anlage-, Steuer- und/oder Rechtsberater, ein Bild über die eigene Risikotragfähigkeit, die Anlageziele sowie den Anlagehorizont zu verschaffen.

Diese Basis- und Risikoinformationen über Kryptowerte ersetzen keine Steuer- oder Rechtsberatung.

Stand: 22.05.2020