

Risikohinweise zum Handel mit Kryptowerten

Wozu dienen diese Risikohinweise?

Diese Risikohinweise zum Handel mit Kryptowerten dienen der Information des Kunden und stellen keine Empfehlung der Baader Bank Aktiengesellschaft, Weihestephaner Straße 4, 85716 Unterschleißheim („Bank“) zum Kauf oder Verkauf von Kryptowerten im Allgemeinen oder von bestimmten Kryptowährungen im Besonderen dar. Diese Risikohinweise stellen keine Anlageberatung dar. Die Bank ist nicht dazu verpflichtet, zu prüfen, ob ein Geschäft über den Kauf oder Verkauf von Kryptowerten für den Kunden angemessen oder geeignet ist. Der Kunde muss daher die Risiken, die mit einem Geschäft zum Kauf oder Verkauf von Kryptowerten verbunden sind, selbst beurteilen und trägt dabei das Risiko einer Fehleinschätzung einschließlich möglicher nachteiliger finanzieller Auswirkungen.

Die Bank stellt dem Kunden diese Risikohinweise zur Verfügung, um dem Kunden eine selbständige Anlageentscheidung zu ermöglichen. Die bereitgestellten Informationen wurden von der Bank sorgfältig zusammengestellt und stammen aus Quellen, die die Bank für zuverlässig hält. Gleichwohl übernimmt die Bank für die Vollständigkeit und Richtigkeit der bereitgestellten Informationen keine Haftung. Zudem können sich im Zusammenhang mit dem Handel von Kryptowerten weitere, nicht von diesen Risikohinweisen erfasste individuelle Risiken ergeben. Die nachstehenden Informationen erheben daher keinen Anspruch auf Vollständigkeit, sondern skizzieren lediglich einige wesentliche Risiken, die mit dem Handel von Kryptowerten verbunden sind.

Diese Risikohinweise ersetzen zudem keine Steuer- oder Rechtsberatung des Kunden mit seinem eigenen Berater.

Was sind Kryptowährungen und wie funktionieren sie?

Kryptowerte sind im Vergleich zu Aktien oder Schuldverschreibungen ein relativ neues Finanzinstrument mit einem speziellen Rendite-Risiko-Profil. Sie sind gesetzlich definiert als „digitale Darstellung eines Werts oder eines Rechts, der bzw. das unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden kann“ (Art. 3 Abs. 1 Nr. 5 der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 – „MiCAR“). Kryptowerte können unterschiedliche Gestalt annehmen und unterschiedliche Rechte gewähren. Bei den von der Bank zum Handel angebotenen Kryptowerten handelt es sich ausschließlich um Kryptowährungen, die nach der MiCAR unter den weiten Tatbestand der „anderen Kryptowerte“ fallen. Bei den Kryptowährungen handelt es sich weder um nach der MiCAR regulierte E-Geld-Token, noch um vermögensreferenzierte Token oder Utility-Token.

Kryptowährungen sind nicht-staatliche Werteinheiten. Sie basieren grundsätzlich auf der Idee eines nichtstaatlichen Ersatzgeldes in begrenzter Menge. Die Schaffung neuer Werteinheiten („Kryptotoken“ auch Coins genannt) erfolgt nicht durch Notenbanken und Geschäftsbanken, wie dies bei Zentralbankgeld oder Kredit- und Buchgeld der Fall ist. Stattdessen werden Kryptotoken in der Regel in einem rechenintensiven Prozess erzeugt, in dem kryptografisch verschlüsselte Transaktionsdatensätze zu einer öffentlich einsehbaren, dezentralen Datenbank („Blockchain“) hinzugefügt werden. Bei der Blockchain handelt es sich in der Regel um eine kontinuierlich erweiterbare Aneinanderreihung von Datensätzen in einzelnen Blöcken, die nach einem Konsensverfahren erstellt und mittels eines kryptografischen Verfahrens fortentwickelt wird. Ein Kryptotoken ist dabei ein Datensatz auf dieser Blockchain und damit ein fester Bestandteil dieser Blockchain, der vom Markt ein bestimmter Wert beigemessen wird. Zu den geläufigsten und – gemessen an der Marktkapitalisierung – bedeutendsten Kryptowährungen zählen derzeit Bitcoin (BTC) und Ether (ETH).

In der Blockchain wird u.a. die Legitimität einzelner Ereignisse überprüft, bevor diese irreversibel in der Blockchain als neue Ereignisse gespeichert werden. Diese Verifizierung wird bei Kryptowährungen mittels verschiedener Prüfmechanismen durchgeführt. Besonders oft wird das sog. „Proof of Work“-Verfahren genutzt, welches aktuell u.a. bei Bitcoin, Bitcoin Cash und Litecoin zum Einsatz kommt. Bei diesem mathematischen Verfahren, an dessen Ende die Erweiterung der Blockchain um einen weiteren Block steht, arbeiten all diejenigen Teilnehmer der Blockchain, die neue Coins „schürfen“ (die sog. „Miner“) zusammen daran, die abzuspeichernden Infor-

mationen durch Lösung eines kryptografischen Rätsels zu prüfen und zu dokumentieren. Dies erfordert signifikante IT-Rechenleistung der Miner. Die Teilnehmer, die das Rätsel als Erste lösen, dürfen den jeweils neuen Block zur Blockchain hinzufügen und werden dafür durch neue Einheiten der Kryptowährung (sog. *Block Rewards*) belohnt. Bei der Kryptowährung Bitcoin ist hierbei die Gesamtmenge der möglichen existierenden Bitcoins begrenzt (allerdings ist diese noch nicht erreicht). Dagegen sehen andere Kryptowährungen eine derartige Begrenzung (jedenfalls noch) nicht vor (z.B. Litecoin). Alternative Prüfmechanismen, etwa *Proof of Stake* oder *Delegated Proof of Stake*, erfordern deutlich weniger IT-Rechenleistung der Teilnehmer, da sie den Konsens darüber, welcher Teilnehmer den nächsten Block hinzufügen darf, mittels einer gewichteten Zufallsauswahl erreichen, bei der insbesondere die Teilnahmedauer sowie der gehaltene Anteil an Kryptotoken und nicht die Rechenleistung (wie beim Proof of Work) entscheidend ist.

Kryptowerten sind im Netzwerk identifizierbare Adressen zugeordnet. Eine Adresse besteht aus einer zufällig generierten Zeichenfolge, dem öffentlichen Schlüssel (*Public Key*). Der jeweilige Inhaber, dem eine Adresse zugeordnet ist, verwaltet diese mit dem zugehörigen, geheim gehaltenen privaten Schlüssel (*Private Key*), um Transaktionen (wie z.B. Übertragungen) zu signieren. Um Kryptowerte zu übertragen, müssen in der Regel die jeweiligen Zieladressen ausgetauscht werden.

Welche Risiken sind mit dem Kauf und Verkauf von Kryptowerten verbunden?

Kryptowerte sind hochriskante, hochspekulative und hochvolatile Finanzinstrumente. Zu den üblichen Risiken von Finanzanlagen, wie zum Beispiel dem Kursrisiko, treten spezifische Risiken hinzu, die sich aufgrund der besonderen Eigenschaften von Kryptowerten und der zugrundeliegenden Blockchain-Technologie ergeben. Der Handel mit Kryptowerten ist nur für gut informierte und erfahrene Anleger geeignet, die eine hohe Risikobereitschaft mitbringen und finanziell in der Lage sind, Verluste (bis hin zum Totalverlust) zu tragen.

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 und die rechtlichen und steuerlichen Implikationen einer Anlage in Kryptowerte zu verschaffen. Im Folgenden werden einige zentrale Risiken im Zusammenhang mit dem Handel mit Kryptowerten skizziert:

1. Markt-, Wert- und Kursrisiken

Kryptowerte unterliegen einem besonders hohen Kursrisiko. Bei einer Anlage in Kryptowerten kann in kurzer Zeit ein erheblicher Kursverfall bis zum Totalverlust drohen. Vergangene Kursentwicklungen können nicht als Anhaltspunkt für die künftige Kursentwicklung der Kryptowerte dienen.

Anders als bei staatlichen Währungen, hinter denen die Wirtschaftskraft eines Staates steht, und Aktien, hinter denen die Wirtschaftskraft eines Unternehmens steht, bestimmt sich der Kurs von Kryptowerten in der Regel nicht aufgrund objektiver Bewertungsfaktoren. Kryptowerte haben weder einen intrinsischen Wert (z. B. Materialwert) noch einen durch jahrzehntelange Akzeptanz der Marktteilnehmer etablierten Marktwert. Der Kurswert von Kryptowerten wird durch Angebot und Nachfrage sowie die ggf. limitierte Verfügbarkeit und die Erwartungen der Investoren hinsichtlich der künftigen Kursentwicklung bestimmt. Dabei muss es keinen nachvollziehbaren Zusammenhang zwischen der Entwicklung von Wirtschafts- oder Marktdaten und der Kursentwicklung von Kryptowerten geben, so dass die Kursentwicklungen an den Finanzmärkten und diejenigen von Kryptowerten sich auch gegenläufig entwickeln können. Meinungen und Gerüchte sowie aufkommende politische Bestrebungen für eine weitergehende Regulierung von Kryptowährungen können deren Kursentwicklung stark beeinflussen (psychologisches Marktrisiko). Es kann daher zu erheblichen Kursverlusten kommen, ohne dass ein Grund für Kursentwicklungen erkennbar wäre. Zudem wird ein möglicher Kursverfall nicht durch einen intrinsischen Wert der Kryptowerte begrenzt

Volatilität

Kryptowerte sind in der Regel sehr volatil. Ihr Kurs bestimmt sich im Wesentlichen nach Angebot und Nachfrage am Markt, die sich kurzfristig stark ändern können. Zudem ist für die Kursentwicklung die Akzeptanz der Marktteilnehmer mit Bezug auf die jeweilige Kryptowährung entscheidend. Besonders stark ist die Volatilität bei Kryptowerten mit geringer Liquidität, da hier bereits kleinere Transaktionen erhebliche Kursbewegungen auslösen können. Daher kann es bei Kryptowerten erhebliche Kursausschläge innerhalb eines Handelstags oder sogar innerhalb einer Handelsstunde geben. Der Kunde kann dadurch in einem kurzen Zeitraum einen erheblichen Verlust erleiden.

Da Kryptowerte weltweit rund um die Uhr und ohne Unterbrechung gehandelt werden, findet die Kursentwicklung und Preisbildung für Kryptowerte ganztätig und unabhängig von den Handelszeiten der Bank statt. Der Kunde sollte bei seiner Anlageentscheidung daher berücksichtigen, dass eine Kryptowährung über Nacht oder an Sonn- und Feiertagen eine erhebliche Wertveränderung erfahren und sich zum Nachteil entwickeln kann, so dass der Kunde auch außerhalb von Handelszeiten signifikante Verluste erleiden kann.

Liquiditätsrisiko

Liquiditätsrisiken existieren bei Kryptowerten in besonderem Maße. Dies gilt insbesondere für Kryptowerte, deren Marktkapitalisierung niedriger ist als bei der führenden Kryptowährung Bitcoin. Die Liquidität eines Kryptowerts kann sich auch über die Zeit stark verändern. Keine oder nur eine geringe Liquidität kann dazu führen, dass der Anleger die von ihm gehaltenen Kryptowerte nicht oder nicht innerhalb des beabsichtigten Zeitraums veräußern oder erwerben kann oder dass dies nur mit deutlichen Preisabschlägen möglich ist. Dies kann zu erheblichen Verlusten beim Kunden führen.

Marktentwicklungs- und Marktakzeptanzrisiko

Die langfristige Kursentwicklung von Kryptowerten hängt maßgeblich davon ab, dass andere Marktteilnehmer diese freiwillig als Zahlungsmittel, Wertspeicher oder Investmentobjekte akzeptieren und die allgemeine Akzeptanz von Kryptowerten steigt.

Kryptowährungen sind in Deutschland und vielen anderen Staaten derzeit nicht gesetzlich als Währung anerkannt. Die Anbieter von Waren- und Dienstleistungen sowie sonstige Marktakteure sind daher nicht verpflichtet, Kryptowerte als Zahlungsmittel anzunehmen. Wenn Kryptowerte zukünftig in einem geringeren Umfang als bisher oder überhaupt nicht mehr als Zahlungsmittel akzeptiert werden, könnte es zu einem Kursverfall von Kryptowerten kommen.

Darüber hinaus ist es noch unklar, ob Kryptowerte sich generell langfristig als Zahlungsmittel, Wertspeicher oder Investmentobjekte durchsetzen, u.a. deshalb weil sie mit gesetzlichen Zahlungsmitteln und anderen Finanzanlagen konkurrieren. Zudem kann es sein, dass sich nur bestimmte Kryptowährungen durchsetzen, während andere an Akzeptanz verlieren. Auch innerhalb von Kryptowerten besteht Wettbewerb und kann es sein, dass andere Kryptowerte oder Vermögenswerte innovativer sind und dadurch bestimmte Kryptowerte an Akzeptanz verlieren. Wenn der Anleger in einen Kryptowert investiert ist, der keine dauerhafte Marktakzeptanz erlangt, kann er erhebliche Verluste erleiden.

2. Rechtliche Risiken

Die von dem Europäischen Parlament beschlossene MiCAR und die entsprechenden nationalen Begleitgesetze (in Deutschland insbesondere das Kryptomärkteaufsetzungsgesetz) wird Ende 2024 vollständig in Kraft treten und dient der Regulierung von Kryptowerten (bzw. den damit verbundenen Handelsaktivitäten), um den Anlegerschutz zu erhöhen und gleichzeitig die Funktionsfähigkeit der Märkte zu gewährleisten. Die Verordnung soll Rechtssicherheit für Innovationen im Bereich der Distributed-Ledger-Technologie (DLT) schaffen und so das Potenzial von Kryptowerten unter Berücksichtigung der Finanzstabilität fördern. Die MiCAR regelt Transparenz- und Offenlegungspflichten bei der Emission von und dem Handel mit Kryptowerten, die Zulassungspflicht und Aufsicht über die Anbieter von Kryptowerte-Dienstleistungen (Crypto Asset Service Provider) sowie Emittenten von Kryptowerten. Darüber hinaus werden Investoren- und Verbraucherschutzvorschriften gestärkt und Maßnahmen zur Bekämpfung von Marktmissbrauch auf Kryptohandelsplätzen eingeführt. Die Regulierung von Kryptowerten befindet sich jedoch nach wie vor in der Entwicklung und bestehen daher nach wie vor rechtliche Unsicherheiten und im Vergleich zu

traditionellen Finanzinstrumenten eine geringere Regelungsichte. Anleger sollten sich daher auch nach dem Inkrafttreten von MiCAR sich der hohen und spezifischen Risiken im Zusammenhang mit Kryptowerten bewusst sein.

So ist unter anderem die zivilrechtliche Behandlung von Kryptowerten in Teilen ungeklärt. Da Kryptowährungen weder als Sache noch als Recht qualifiziert werden können, können sie weder Eigentum noch Besitz vermitteln und fallen daher aus dem Schutzbereich absoluter Rechte heraus. Dies hat unter anderem zur Folge, dass kein Gutgläuberschutz im Hinblick auf die faktische Kontrolle an einem Kryptowerte besteht und jegliche Art von Schutz und Berechtigung lediglich vertraglich gewährt werden kann. Des Weiteren bleibt Klärungsbedarf hinsichtlich der Fragen, welches Recht bei der Übertragung von Kryptowerten anzuwenden ist, ob und wie an Kryptowerten Sicherheitenrechte wie bspw. Pfandrechte bestellt werden können und unter welchen Voraussetzungen Kryptowerte wieder erlöschen.

Änderungen des regulatorischen Umfelds

Staaten schauen auch nach der Verabschiedung von MiCAR teilweise nach wie vor kritisch auf Kryptowerte, weil diese in Konkurrenz zu staatlichen Währungen treten. Es kann daher nicht ausgeschlossen werden, dass ein Staat, eine Staatengemeinschaft oder eine Aufsichtsbehörde Kryptowerte weitergehend reguliert oder auch verbietet und es in der Folge zu einem Kursverfall kommt. Zudem könnten staatliche Stellen den Handel mit Kryptowerten ganz oder teilweise untersagen oder in sonstiger Weise beschränken. Dies hätte zur Folge, dass der Handel in einem Kryptowert an dem jeweiligen Handelsplatz eingestellt oder beschränkt würde. Der Anleger könnte den Kryptowert wenn überhaupt – möglicherweise nur außerhalb von Handelsplätzen veräußern. Eine solche Veräußerung wird regelmäßig nur zu erheblichen Preisabschlägen möglich sein. Auch eine zunehmende Regulierung von Kryptowerten könnte dazu führen, dass deren Attraktivität für Anleger sinkt und die Kurse fallen und der Anleger entsprechende Verluste (bis hin zum Totalverlust) erleidet. Die Bank ist nicht verpflichtet, dem Kunden den Schaden zu ersetzen, der aus staatlichen Maßnahmen gegen Kryptowerte resultiert.

Regulierung von Handelsplätzen im Ausland

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 oder in der EU regulierten Handelsplätzen vergleichbar ist. Dies kann dazu führen, dass die Handelsplätze für Kryptowerte anfälliger sind für Kursmanipulationen oder sonstige kriminelle Handlungen. Zudem könnten aufsichtsrechtliche Vorgaben des Staats, in dem der Handelsplatz seinen Sitz hat und dessen Regulierung er unterliegt, im Widerspruch zu europarechtlichen sowie deutschen aufsichtsrechtlichen und zivilrechtlichen Vorgaben stehen, was zu einer eingeschränkten Handelbarkeit von Kryptowerten führen könnte. Auch ist die Markttiefe und -liquidität sowie die Entwicklung und der Reifegrad von Handelsplätzen für Kryptowerte sehr unterschiedlich. Aufgrund des frühen Entwicklungsstadiums der Märkte und Handelsplätze für Kryptowerte und der global bestehenden unterschiedlichen Regulierungsansätze unterscheiden sich die Handelsplätze in Bezug auf den Status ihrer (technische) Entwicklung, Reifegrad, Professionalität und Größe erheblich. Auch der Zugang zu Markt- und Handelsplätzen ist sowohl aus technischen als auch aus rechtlichen Gründen fragmentiert. Dies kann zu einer Marktkonzentration führen, die Schwankungen in der Markttiefe und -liquidität in den verschiedenen Rechtsordnungen und auf den einzelnen Marktplätzen und Handelsplätzen zur Folge hat.

3. Handelspartnerrisiko / Mistrade-Risiko

Die Bank hat zu jeder Zeit mindestens einen Handelsplatz für Kryptowerte angebunden und beabsichtigt, weitere Handelspartner anzubinden. Die Bank kann jedoch nicht ausschließen, dass ein angebundener Handelsplatz den Handel mit Kryptowerten – beispielsweise bei erhöhter Volatilität im Markt – aussetzt. Daneben könnte es zu Einschränkungen oder einer Aussetzung der Handelbarkeit von Kryptowerten aus technischen Gründen kommen. Kunden könnten ihre Kryptowerte während der Handelsaussetzung nicht verkaufen und dadurch Verluste erleiden. Sollte nur ein Handelsplatz angebunden sein, besteht während eines Ausfalls der Handelsmöglichkeit über diesen Handelsplatz keine Möglichkeit zum Handel der Kryptowerte über die Bank. Der Kunde könnte daher nicht auf Kursentwicklungen eines Kryptowerts durch das Tätigen von Kauf- und Verkaufsaufträgen reagieren und würde ggf. entsprechende Verluste erleiden.

Handelsplätze stehen zudem typischerweise besondere vertragliche Rechte für den Fall der Bildung nicht marktgerechter Preise („**Mistrade**“) zu, die sich negativ auf den Kunden auswirken können. Kommt es zu einem Mistrade, steht dem Handelsplatz gegenüber der Bank ein vertragliches Aufhebungsrecht nach näherer Maßgabe des zwischen der Bank und dem Handelsplatz abgeschlossenen Handelsvertrags das sich in der zwischen dem Kunden und der Bank vereinbarten Gesonderten Vereinbarung zum Depotvertrag: Handel mit Kryptowerten („**Vertragsbedingungen**“) widerspiegelt. In diesem Fall kommt es zu einer Rückabwicklung des getätigten Geschäfts. Übt der Handelsplatz sein Aufhebungsrecht aus, wirkt diese Aufhebung des Ausführungsgeschäfts zwischen dem Handelsplatz und der Bank auch gegenüber dem Kunden, dem in diesem Fall keine Ansprüche auf Herausgabe des aus dem Ausführungsgeschäft Erlangten (insbesondere der Kryptowerte) zustehen. Hierdurch kann dem Kunden ein erheblicher Schaden entstehen. Hat die Bank das aus dem Ausführungsgeschäft Erlangte (insbesondere die Kryptowerte) bereits an den Kunden herausgegeben, ist das Erlangte (insbesondere die Kryptowerte) an die Bank zurück zu erstatten. Zudem ist dem Kunden alles, was er zur Durchführung des Ausführungsgeschäfts bereitgestellt hat (insbesondere den für die Anschaffung der Kryptowerte aufgewendeten Kaufpreis), von der Bank zurück zu erstatten.

Zwar ist der Kunde ggf. ebenfalls berechtigt, unter bestimmten Voraussetzungen bei der Bank die Stornierung eines Ausführungsgeschäfts wegen eines Mistrades zu verlangen. Allerdings ist nach Maßgabe der Vertragsbedingungen eine Stornierung wegen eines Mistrades nur dann möglich, wenn der von dem Handelsplatz gestellte Preis erheblich vom zum Zeitpunkt des Zustandekommens des Geschäfts marktgerechten Preis abweicht. Ferner ist zu beachten, dass Mistrades bei Kryptowerten unter Umständen schwer nachzuvollziehen sind. Aufgrund der hohen Volatilität und der Nicht-Existenz von zentralen und regulierten Handelsplätzen können daher Schwierigkeiten bei der für den Nachweis eines Mistrades erforderlichen Ermittlung eines Referenzpreises bestehen.

4. Risiken aufgrund der Verwahrung der Kryptowerte Verlust von Kryptowerten

Die Verfügungsgewalt über ein Guthaben in Kryptowerten entsteht durch die Kenntnis des geheimen privaten Schlüssels (Private Key). Beim Verlust dieses Schlüssels sind die damit verbundenen Kryptotoken sowohl für den Inhaber des Kryptotokens als auch für das gesamte Netzwerk verloren. Anders als zum Beispiel bei einer Bank-PIN gibt es keine Möglichkeit, den Schlüssel zurückzusetzen oder wiederherzustellen.

Die Bank selbst verwaltet und verwahrt keine Kryptowerte für Kunden. Die Verwahrung der von den Kunden über die Bank erworbenen oder veräußerten Kryptowerte erfolgt selbstständig durch den in den Vertragsbedingungen genannten Kryptoverwahrer nach Maßgabe dessen Verwahrbedingungen, die der Kunde mit dem Kryptoverwahrer vereinbart hat.

Für die Verwahrung der Kryptowerte des Kunden durch den Kryptoverwahrer und die sich daraus ergebenden Risiken gelten ausschließlich die zwischen dem Kunden und dem Kryptoverwahrer vereinbarten Verwahrbedingungen. Die Bank kann nicht ausschließen, dass es zu physischen oder sonstigen Angriffen (z. B. Hackerangriffe) auf den Kryptoverwahrer oder dessen Verwahrstruktur kommt und solche Angriffe negative Auswirkungen auf die Kundenbestände haben, bspw. indem Daten – inkl. des privaten Schlüssels – gelöscht oder unzugänglich gemacht werden. Es ist auch denkbar, dass die privaten Schlüssel beim Kryptoverwahrer von einem Dritten ausgespäht werden und sodann der Dritte die Kryptowerte unberechtigt transferiert und damit „stiehlt“.

Keine Einlagensicherung – Insolvenz des Kryptoverwahrers

Für die beim Kryptoverwahrer verwahrten Kryptowerte gibt es keine Einlagensicherung. Die Bank kann nicht bewerten, ob, wie und in welchem Umfang der Kryptoverwahrer die Bestände von Kunden abgesichert hat. Zudem könnte der Kryptoverwahrer in wirtschaftliche Schwierigkeiten oder gar in Insolvenz geraten. Der Kryptoverwahrer Tangany ist gemäß § 26b Abs.1 Kreditwesengesetz („**KWG**“) verpflichtet, im Rahmen der gemeinschaftlichen Verwahrung von Kryptowerten (in sog. omnibus wallets) die Kryptowerte der Kunden getrennt von den eigenen Kryptowerten zu verwahren. Die bei dem Kryptoverwahrer verwahrten Kryptowerte des Kunden werden gemäß § 46i Abs. 1 und 2 KWG haftungsrechtlich dem Vermögen des Kunden zugeordnet, es sei denn, der Kunde hat die Einwilligung zur Verfügung über den Kryptowert für Rechnung des Kryptoverwahrers oder Dritten erteilt. Im Insolvenzverfahren über das Vermögen des Kryptoverwahrers stünde dem Kunden aufgrund dieser haftungsrechtlichen Zuordnung der Kryptowerte zum Vermögen des Kunden insoweit ein Aussonderungsrecht gemäß § 47 Insolvenzordnung („**InsO**“) gegenüber dem Insolvenzverwalter des Kryptoverwahrers zu, sofern das Insolvenzverfahren in Deutschland eröffnet

wurde. Dem Kunden stehen bei einer Insolvenz des Kryptoverwahrers und einem daraus folgenden Verlust seiner Kryptowerte keine Ersatzansprüche gegen die Bank zu.

5. Risiken im Zusammenhang mit der zugrundeliegenden Blockchain-Technologie

Die Nutzungsmöglichkeiten von Kryptowerten basieren auf der ihnen in der Regel zugrundeliegenden Blockchain-Technologie. Kommt es zu Störungen der Funktionalität der Blockchain, kann dies zu einem Kursverfall des Kryptowerts führen und kann der der Kunde diese während der Störung nicht veräußern bzw. übertragen. Dies kann zu erheblichen Verlusten bis hin zum Totalverlust der Anlage führen.

Softwarerisiken

Kryptowerte sind software- und protokollbasiert und sind daher anfällig für Softwarefehler oder Angriffe durch Schadsoftware. Solche Störfälle oder Angriffe könnten das Vertrauen in die Blockchain beschädigen und zu einem Kursverfall des darauf basierenden Kryptowerts führen. Zudem könnte sogar ein Totalverlust drohen, wenn die Blockchain insgesamt nicht mehr funktionsfähig ist.

Es könnten zudem Fehler im Programmcode der Blockchains oder in der zugrundeliegenden Verschlüsselungstechnologie auftreten, die Dritten unbefugten Zugriff auf Kryptowerte geben oder die gesamte Blockchain wertlos machen.

Kryptowerte sind zudem abhängig von der Weiterentwicklung des ihnen bzw. der für sie genutzten Blockchain zugrundeliegende Protokolls. Die Entwicklung der Protokolle kann verhindert oder verzögert werden, wenn es zu Unstimmigkeiten zwischen Teilnehmern, Entwicklern und Mitgliedern des jeweiligen Netzes kommt oder es, z.B. aufgrund fehlender Vergütung für die Entwickler an einem Anreiz für die Weiterentwicklung fehlt. Dies kann sich negativ auf den Wert der Kryptowerte auswirken.

Manipulationsrisiko

Die den Kryptowerten in der Regel zugrundeliegende Blockchain-Technologie beruht auf bestimmten kryptografischen Verfahren zum Schutz vor Manipulationen. Diese Verfahren oder die Implementierung dieser Verfahren könnten sich (jetzt oder durch technische Weiterentwicklungen in der Zukunft, wie z.B. der Entwicklung von Quantencomputern, die durch eine sehr hohe Rechenleistung möglicherweise aktuell sichere Verschlüsselungen entschlüsseln kann) als nicht ausreichend sicher erweisen, so dass das Risiko einer Beeinträchtigung oder kompletten Aufhebung der Funktionsfähigkeit der Blockchain beispielsweise durch Cyberangriffe besteht.

Systembetreiberrisiko

Die Funktionalität von Kryptowerten hängt davon ab, dass bestimmte Stellen bzw. Systembetreiber (sog. „**Full-Nodes**“) das System durch Fortschreibung der Blockchain aufrechterhalten. Dies geschieht ohne zentrale Kontrolle oder Verpflichtung. Es ist nicht ausgeschlossen, dass vereinzelte oder alle dieser Full-Nodes die Tätigkeit für eine bestimmte Kryptowährung beenden und damit, wenn kein Ersatz gefunden wird, die Kryptowerte dieser Kryptowährung nicht mehr handelbar sind. Auch könnten diese Full-Nodes die Transaktionskosten für Kryptowerte deutlich erhöhen und Transaktionen damit unwirtschaftlich machen.

Zudem ist denkbar, dass diese Systembetreiber sich teilweise zusammenschließen und dadurch weniger Kontrollinstanzen für eine Kryptowährung bestehen, was diese wiederum anfälliger für Angriffe von außen machen könnte.

Einstellung bzw. Reduktion der Mining-Tätigkeit

Das Funktionieren der Blockchain 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 Kryptowerten oder unzureichende Erträge.

Mehrheitsangriff / 51 %-Angriff

Wenn Miner sich zusammenschließen und insgesamt mehr als die Hälfte der Rechenleistung bündeln, besteht bei Kryptowerten wie dem Bitcoin die Möglichkeit eines Mehrheitsangriffes (auch „**51 %-Angriff**“ oder Mehrheitsbeschluss per Rechenleistung genannt). Indem sie über die Mehrheit der Mining-Kapazität verfügen, könnten die Angreifer bestimmen, welche Transaktionen vom Netzwerk zugelassen und anerkannt werden und welche nicht. Solche gezielten Manipulationen könnten die Funktionsfähigkeit der Blockchain beeinträchtigen und das Vertrauen in die Sicherheit der Blockchain beschädigen. Dies könnte zu einem Kursverfall der betroffenen Kryptowerte führen.

Fork-Risiko / Airdrops

Eine sogenannte „Hard Fork“ ist eine Aufteilung der Blockchain in zwei unterschiedliche Stränge. Diese Änderung im Protokoll einer Blockchain, die 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. Darüber hinaus kann es aufgrund der Teilung der Blockchain zu erheblichen Kursschwankungen kommen. Ein Hard Fork könnte theoretisch dazu führen, dass eine lange zurückliegende Transaktion wieder „beseitigt“ wird.

Der Kunde hat bei einem Hard Fork gegenüber der Bank keinen Anspruch auf die Lieferung zusätzlicher Kryptowerte aus der neu entstandenen Blockchain. Zudem könnte die Bank im Falle eines Hard Fork die Handelbarkeit des betroffenen Kryptowerts einzustellen. Soweit einem Kunden im Rahmen eines Hard Fork Kryptowerte zugeteilt wurden, wird die Bank im Einzelfall nach billigem Ermessen prüfen, ob der Handel mit den zugeteilten Kryptowerten des Hard Fork weiter unterstützt wird. Dies macht die Bank u.a. davon abhängig, ob die Kryptowerte bei den von der Bank verwendeten Kooperationspartnern und Handelsplätzen sowie bei Tangany unterstützt werden. Sollte dies nicht der Fall sein, könnte es sein, dass der Kunde die ihm zugeteilten Kryptowerte nicht über das bestehende Arrangement mit der Bank erhalten oder nicht über diese verfügen kann.

Auch bei Airdrops, der zusätzlichen Ausschüttung von Einheiten, d.h. weiteren Kryptowerten, an die Halter der Kryptowährung, besteht das Risiko, dass der Kunde an dieser Zuteilung nicht teilnehmen kann, z.B. weil hierzu besondere technische Voraussetzungen bestehen müssten, die über den technischen Aufsatz der Bank bzw. des Kryptoverwahrers hinausgehen. In diesem Fall gelten die vorstehenden Risiken entsprechend.

6. Abwicklung und Gebühren Abwicklungsrisiko

Die Abwicklung von Transaktionen mit Kryptowerten kann unter Umständen erheblich länger dauern als die Abwicklung von Finanzinstrumenten wie z.B. Aktien. Zudem kann es zu Schwierigkeiten bei der Belieferung von Kryptowerten und/oder Zahlungen kommen. Dies kann dazu führen, dass die entsprechenden Transaktionen eines Kunden rückabgewickelt werden müssen. Soweit die Bank dem Kunden zugleich mit der Ausführungsanzeige über die Durchführung des Ausführungsgeschäfts den Vertragspartner des jeweiligen Geschäfts benennt, also den jeweiligen Handelsplatz, mit dem die Bank das Ausführungsgeschäft abgeschlossen hat, haftet sie nach den Vertragsbedingungen gegenüber dem Kunden nicht für die ordnungsgemäße Erfüllung des Ausführungsgeschäfts durch den Vertragspartner. Der Kunde trägt insofern das Abwicklungsrisiko aus dem Ausführungsgeschäft. Sollte es bei der Abwicklung des Ausführungsgeschäfts zu Verzögerungen oder zu einem Lieferausfall kommen, hätte der Kunde keinen Ersatzanspruch gegen die Bank.

Transfergebührenrisiko

Bei vielen Blockchains fällt bei Transaktionen zum Transfer von Kryptowerten an eine andere Adresse (Wallet) des Kunden eine (in der Regel an die Systembetreiber der Blockchain zu zahlende) Transfergebühr an. Sollte diese Gebühr auf ein unangemessen hohes Niveau steigen, könnte der Kryptowert als Zahlungsmittel nicht mehr rentabel erscheinen oder insgesamt für

Marktteilnehmer unattraktiv werden. Dies könnte zu einem Kursverfall und entsprechenden Verlusten führen.

7. IT-Risiken

Die Bank bindet in den Handel mit Kryptowerten verschiedene Kooperationspartner ein, mit denen sie über IT-Schnittstellen elektronisch Daten austauscht. Hierbei besteht die Möglichkeit des Missbrauchs bei der Übermittlung von elektronisch erteilten Aufträgen, z.B. Fälschung und Verfälschung durch schattenloses Kopieren, Fälschung von Unterschriften oder Veränderungen am Originalbeleg und Verzögerungen wegen möglicher technischer Probleme. Die Bank ist nicht in der Lage, elektronisch übermittelte Aufträge auf ihre Echtheit und die Übereinstimmung mit dem Original hin zu überprüfen. Die Bank ist daher nach den Vertragsbedingungen zur Belastung des Verrechnungskontos und zur Durchführung von Aufträgen auch dann berechtigt, wenn sie der übermittelte Auftrag später als gefälscht herausstellt. Eventuelle Schäden trägt nach den Vertragsbedingungen der Kunde, soweit sie nicht von der Bank verschuldet wurden. Hierdurch kann sich für den Kunden ein erhebliches finanzielles Risiko ergeben.

8. Steuerliche Risiken

Der Erwerb und die Veräußerung von Kryptowährungen, die als Zahlungsmittel eingesetzt werden können und darüber hinaus keine weiteren Funktionen bzw. Eigenschaften besitzen, unterliegen in Deutschland – im Gegensatz zu Wertpapieren – nicht der Abgeltungssteuer. Stattdessen wird der Handel mit Kryptowährungen als privates Veräußerungsgeschäft besteuert, sofern kein gewerblicher Handel erfolgt. Davon zu unterscheiden sind sogenannte Utility Token, Security Token, Debt Token oder Hybride Token. Auf Grundlage dieser Rechtsauffassung sind Kursgewinne aus der Veräußerung von Kryptowährungen grundsätzlich steuerfrei, wenn der Zeitraum zwischen Anschaffung und Veräußerung mehr als ein Jahr beträgt („Haltedauer“) oder wenn der aus den privaten Veräußerungsgeschäften erzielte Gesamtgewinn im Kalenderjahr weniger als der in § 23 Abs. 3 S. 5 EStG genannte Betrag betragen hat. Die Haltedauer von mehr als einem Jahr verlängert sich auf mehr als 10 Jahre, wenn Kryptowährungen zur Erzielung von Einkünften genutzt werden (z.B. Lending, Staking, Mining, Airdrop).

Die Bank ist nicht verpflichtet, den Kunden auf Änderungen der steuerlichen Einordnung von Kryptowährungen hinzuweisen. Der Kunde muss anfallende Steuern eigenständig in seiner Steuererklärung angeben. Die Bank führt bei Geschäften mit Kryptowährungen keine Steuer für den Kunden ab und nimmt keine steuerlich relevante Erklärungen für den Kunden vor. Die Bank erbringt keine Steuerberatung für den Kunden. Dem Kunden wird dringend empfohlen, sich bei Fragen an die für ihn zuständige Steuerbehörde bzw. seinen Steuerberater zu wenden.

9. Risiken im Zusammenhang mit dem Erwerb von Kryptowerten aus zweifelhaften Quellen

Erwirbt der Kunde Kryptowerte, die aus illegalen Quellen stammen, kann er dadurch erhebliche Schäden erleiden. Dies kann beispielsweise Kryptowerte umfassen, die aus Geldwäschegeschäften, Drogenhandel, illegalem Waffenhandel oder ähnlichen Geschäften stammen. Gleiches gilt für den Erwerb von Kryptowerten von Personen, gegen die staatliche Sanktionen verhängt wurden. Ein solcher Erwerb könnte zu staatlichen Maßnahmen gegen die betroffenen Kryptotoken führen. Zudem könnten Handelsplätze die betroffenen Kryptotoken vom Handel ausschließen. Dadurch könnten die von dem Kunden gehaltenen Kryptotoken erheblich an Wert verlieren oder sogar vollständig wertlos werden und vom Handel ausgeschlossen werden.