SCHNIGGE
Wertpapierhandelsbank SE

Deckblatt: # Basisinformationen zu Kryptowährungen (virtuelles Geld)

Basisinformationen, technische und wirtschaftliche Zusammenhänge, Chancen und Risiken sowie Anwendungsmöglichkeiten

SCHNIGGE
Wertpapierhandelsbank SE

Stand: 01. Dezember 2017


Querstraße 8-10 ; 60322 Frankfurt am Main **www.schnigge.de**



Der Inhalt wurde mit größtmöglicher Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität des Inhalts übernimmt die SCHNIGGE Wertpapierhandelsbank SE keine Haftung.

Sehr geehrte Damen und Herren,

herzlichen Dank für Ihr Interesse an Wertpapierdienstleistungen der **SCHNIGGE Wertpapierhandelsbank SE**.

Vor der Erbringung von Dienstleistungen im Zusammenhang mit Kryptowährungen für Sie sind wir gesetzlich verpflichtet, Ihnen eine **Aufklärung über Risiken** zukommen zu lassen. Aber auch über unsere gesetzliche Verpflichtung hinaus sind wir als Ihr Vertragspartner daran interessiert, dass Sie jederzeit einen vollständigen Überblick über Wertpapiere, deren Chancen aber auch Risiken haben. Denn nur, wenn Sie verstehen, in was und wie Sie Ihr Geld investieren, ist zu erwarten, dass Sie langfristig erfolgreich bei Ihrer Geldanlage sind. Da wir ein Interesse daran haben, mit Ihnen eine möglichst langfristige und erfolgreiche Geschäftsbeziehung einzugehen, liegt uns Ihre möglichst umfassende Aufklärung am Herzen.

In den letzten Jahren ist die Beratung durch Banken gegenüber Anlegern aus den verschiedensten Gründen zurückgegangen. Sie als Anleger sind daher vermehrt bei der Auswahl und der Durchführung ihrer Geschäfte mit Finanzinstrumenten auf eigene Kenntnisse angewiesen und dabei überwiegend auf sich alleine gestellt. Eine besondere Kenntnis insbesondere neuer Finanzinstrumente, wie es **Kryptowährungen** sind, ist daher für Sie von großer Bedeutung. Gleichzeitig nimmt die Anzahl der Kryptowährungen und die Komplexität der damit verbundenen Blockchain-Technik und Währungsinhalte kontinuierlich zu. Für Sie als Investor wird es daher immer komplexer und schwieriger, eine Entscheidung über den Erwerb von Finanzinstrumenten wie Kryptowährungen zu treffen, der Ihrer persönlichen Lebenssituation, Ihren wirtschaftlichen Verhältnissen und Ihrem Chance/Risiko-Profil entspricht.

Auch wenn wir mit einer Standardbroschüre natürlich nicht auf Ihre individuellen Bedürfnisse oder Erwartungen eingehen können, so wollen wir mit dieser Aufklärung dafür Sorge tragen, Ihnen einen möglichst **umfassenden Überblick** über Kryptowährungen und die damit verbundene Blockchain-Technologie zu vermitteln.

Darüber hinaus enthält diese Basisinformation wichtige Angaben über die mit diesen Geschäftsformen standardisiert und regelmäßig zusammenhängenden **Risiken**. Da die Finanzbranche kreativ ist und sich immer neue Finanzinnovationen, Finanzprodukte oder gar neue Märkte einfallen lässt, ist der Informationsbedarf wichtig, zumal neue Produkte oftmals eine Kombination bestehender Produkte oder Produktmerkmale ist. Daher weisen viele dieser neuen Produkte eine übergreifende Risikostruktur über mehrere bestehende Anlageprodukte auf. Somit verfügen diese Kombiangebote sowohl über eigene Produkteigenschaften als auch Risikostrukturen der einzelnen Produktbestandteile.

Bei der Erstellung der Unterlagen haben wir versucht, die Formulierung trotz Fachbegriffen möglichst leicht verständlich und anschaulich zu wählen, um Ihnen auch als Nicht-Fachmann die Möglichkeit zu geben, sich selbständig Wissen anzueignen. Sollten Sie einzelne Punkte nicht verstanden haben, so können Sie sich jederzeit an die SCHNIGGE Wertpapierhandelsbank SE wenden. Wir werden dann versuchen, Ihnen Sachverhalte zu erklären und darzulegen.

Generell bitten wir Sie, sich als mündigen Anleger zu fühlen und sich daher auch zu trauen, Fragen zu stellen. Bei jedem Kauf eines Autos werden kritischere Fragen gestellt als wenn es um Ihr Geld geht.

**Nachfragen** hilft und **schützt** Sie und Ihr **Vermögen!** Es entspricht unserem Selbstverständnis, Ihnen hierbei durch **Aufklärung** zu helfen. Scheuen Sie sich daher also nicht, sich bei bestehenden Fragen an uns zu wenden! Es ist wesentlich einfacher, vor der Umsetzung einer Anlageentscheidung zu sprechen, als im Nachhinein Probleme zu bereinigen! Wir betrachten uns als Ihr Partner und würden uns daher freuen, wenn Sie diese Standardinformationen dazu nutzen würden, sich aktiv mit Ihren Vermögensanlagen zu beschäftigen.

Gerade weil wir uns als Ihr Partner verstehen, haben Sie bitte auch Verständnis dafür, dass wir von Ihnen eine Reihe von Fragen zum Beispiel über Ihre bisherigen **Kenntnisse und Erfahrungen** mit Vermögensanlagen stellen werden.

Dabei erfüllen wir einerseits die **gesetzlichen Verpflichtungen**, andererseits ist es aber auch für uns wichtig zu verstehen, wie **risikofreudig** oder **risikoscheu** Sie sind. Nur das bewahrt Sie und uns davor, dass Sie im Zweifel in Produkte investieren, die nicht zu Ihnen passen und zu hohe Risiken verursachen. Dies hilft, Verluste zu vermeiden. Zu den notwendigen Daten, die wir von Ihnen erfragen gehören auch Angaben zu Ihren **finanziellen Verhältnissen** sowie den von Ihnen mit einer Anlage in Wertpapieren und weiteren Kapitalanlagen verfolgten **Anlagezielen**.

Wir wünschen Ihnen mit den hier enthaltenen Angaben jederzeit ein gutes Händchen bei Ihrer Investition in Kryptowährungen und viel Erfolg!

# Inhalt

# Hilfen zur Nutzung dieses Dokuments

Sehr geehrte Anlegerin, sehr geehrter Anleger,

unser Auftrag und unser Anspruch ist es, Sie als interessierten Anleger über die verschiedenen Möglichkeiten der Anlage sowie des Handels in Kryptowährungen und über die damit üblicherweise verbundenen Risiken zu informieren. Dabei soll auch dieser Inhalt möglichst verständlich und selbsterklärend sein, dabei keine wichtigen Gesichtspunkte außer Acht lassen und dennoch möglichst vollständig sein.

Das Inhaltsverzeichnis soll es Ihnen zunächst erleichtern, die einzelnen Bestandteile so zu sortieren, dass Sie sich über die für Sie relevanten Bereiche informieren können. Wir weisen aber ausdrücklich darauf hin, dass es nicht nur sinnvoll ist, sich alle Bereiche anzusehen, sondern teilweise auch notwendig, da es Querverweise zwischen einzelnen Bereichen gibt und auch gegenseitige Abhängigkeiten bestehen.

Lesen Sie sich daher alle Bestandteile möglichst sorgfältig durch! Wenn Sie nicht alles verstanden haben, fragen Sie nach oder verzichten Sie zur Sicherheit lieber auf Investitionen!

Neben einzelnen **Erklärungen** führen wir hier zusätzlich weitere Tipps an, die Ihnen über die Sachaufklärung hinaus wertvolle Hinweise und Erläuterungen geben sollen.

Solche Stellen sind als

„**TIPP**:“

gekennzeichnet.

Fachbegriffe sind, sofern nicht auf sie verzichtet werden konnte, grundsätzlich im Text selbst erklärt. Einzelne weitere Ausdrücke, die einer weiteren Erläuterung bedürfen, sind zusätzlich unter Fachworterklärungen **(Kapitel G)** aufgeführt.

Darüber hinaus finden Sie eine nicht abschließende und unvollständige Liste mit exemplarischen Schäden **(Kapitel F)**, die Nutzern und Handelsplattformbetreibern entstanden sind. Dies soll Ihnen einen realistischen Eindruck von den Risiken dieser Kryptowährungen geben.

Viel Spaß und Nutzen mit diesen Informationen wünscht Ihnen

Ihre SCHNIGGE Wertpapierhandelsbank SE

# A Einführung

Kryptowährungen sind seit den starken Kursanstiegen der Kryptowährung „**Bitcoin**“ in den Fokus der Anleger gerückt. Neben den allgemeinen Risiken von Finanzinstrumenten, zu denen auch die Kryptowährungen zu zählen sind, haben Kryptowährungen jedoch eine Reihe von spezifischen Problemen und Risiken, die wir Ihnen mit diesen Informationen nahebringen und aufführen wollen.

**Generell gilt: Bitcoin und andere Kryptowährungen haben nur Wert, solange die Nutzer einen Wert darin sehen und eine Nachfrage nach Kryptowährungen besteht. Die teilweise rasanten Kursanstiege einzelner Kryptowährungen sind keine Garantie für eine analoge Kursentwicklung in der Zukunft!**

Sie als Anleger dürfen sich daher nicht durch die massiven Kursanstiege der als Leitwährung der Kryptowährungen bezeichneten Bitcoins verleiten lassen. Stattdessen bitten wir darum, sich unbedingt mit dem Thema Herkunft und Zweck der Kryptowährungen auseinander zu setzen, um ein grundsätzliches Verständnis dieser Finanzinstrumente zu erhalten. Ein **unkritisches Verhalten**, bei dem die Risikobetrachtung aufgrund hoher Kursgewinne außer Acht bleibt, **ist mit sehr hohen Verlustgefahren verbunden**.

Im weiteren Verlauf wird nicht besonders auf die fortgesetzte Generierung neuer Kryptowährungseinheiten eingegangen. Zwar ist das so genannte **Mining** ein wichtiger Vorgang, mit dem bis zum Erreichen einer möglichen Maximalgrenze von ausgegebenen Kryptowährungen neue Währungseinheiten „geschürft“ werden. Dieser Vorgang ist jedoch keine Finanzdienstleistung und wird hier daher nicht weiter beleuchtet sondern nur in einem Exkurs erklärt.

## 1 Historie der Kryptowährungen

Kryptowährungen sind eine relativ junge Erscheinung im Kapitalmarkt. Das Konzept hinter den digitalen Währungen stammt aus dem Jahr 1998. Wei Dai formulierte den Grundgedanken und machte sie über die Cyberpunk Mailingliste publik. Bis die Idee umgesetzt wurde, vergingen zehn Jahre.

Im Jahre 2008 wurde mit dem Bitcoin die erste Kryptowährung konzeptionell geschaffen. Als Erfinder gilt Satoshi Nakamoto, dessen Identität bis heute nicht geklärt ist. Ob sich hinter dem Pseudonym eine Person oder eine Gruppe verbirgt, ist ebenfalls unbekannt. Die Kryptowährung wurde als Antwort auf die weltweite Finanzkrise, ausgelöst durch die Pleite des Bankhauses Lehman Brothers, geschaffen. Die Zusammenhänge des Finanzsystems mit gegenseitigen Abhängigkeiten von Wirtschaften und Ländern, mit staatlichen Eingriffen von mehr oder weniger unabhängigen Zentralbanken, haben fast zu einer weltweiten wirtschaftlichen Katastrophe geführt. Nur das massive Eingreifen von Zentralbanken sowie Regierungen zur Stützung von Währungen und wirtschaftlichen Gefügen hat einen Bankrott der bestehenden Währungssysteme verhindert. Die zur Liquiditätsstützung der Systeme eingesetzte Niedrigzinspolitik begleitet nicht nur die europäische Wirtschaft bis heute sondern sorgt bei gleichzeitiger Inflation für eine schleichende Enteignung von Sparvermögen.

## 1.1 Unabhängigkeit von staatlichem Einfluss

Die Philosophie der neuen Kryptowährung ist explizit darauf ausgelegt, eine Unabhängigkeit von diesen staatlichen Kontrollen und Einflussnahmen zu erzielen. Der gezielte Einsatz geldpolitischer Maßnahmen durch Politik und Zentralbanken hat seit Jahrzehnten zu Verschiebungen von Einfluss und wirtschaftlicher Kraft von Ländern und Regionen geführt. Die Abschaffung des Goldstandards und der gezielte Einsatz von Währungskursen zur Steuerung der Absatzfähigkeit einer Wirtschaft zu Lasten einer anderen Volkswirtschaft ist hier ein Synonym für den staatlichen Einfluss auf ein Währungssystem. Ebenso im Fokus der Beeinflussung steht immer wieder die Zinspolitik, bei der durch niedrige Zinsen eine Investitionsbereitschaft gefördert werden soll, wogegen hohe Zinsen Anleger und Investoren bewegen sollen, ihr Geld aus dem Wirtschaftskreislauf zu nehmen und es auf Konten zu deponieren. Darüber hinaus lebt eine Währung vor allem vom Vertrauen der Menschen, die die Währung benutzen. Ist kein Vertrauen in eine Währung vorhanden, so wird bezweifelt, dass man sich für diese Währung noch etwas kaufen kann – Inflation entsteht, so wie zunächst in den Jahren 1720, ausgelöst durch John Law in Paris, der für Papiergeld nicht mehr nur auf eine reine Münzdeckung sondern auch Immobilienbesitz heranzog. Später musste in den 1920er Jahren weltweit eine Hyperinflation hingenommen werden, die letztlich in eine Weltwirtschaftskrise durch kreditfinanzierte Spekulation mündete.

Als Ergebnis daraus wurde formuliert:
„Benötigt wird ein elektronisches Zahlungssystems, das auf einem kryptografischen Beweis anstelle von Vertrauen basiert, und es zwei Parteien erlaubt, direkt und ohne einen Mittelsmann, dem sie vertrauen, miteinander zu handeln“, schrieb Nakamoto damals in einem so genannten White Paper, einer allgemein zugänglichen Information und Leitgedanken eines Kryptowährung. Aus diesem Grund installierte er einen wichtigen Grundgedanken der Kryptowährungen: Transparenz für alle Nutzer! Dies erreichte er u.a. durch die technische Nutzung einer „open source“, übersetzt „frei zugängliche Quelle“. Er hat damit die Software für alle Interessierten geöffnet, frei zugänglich und nutzbar gemacht – damit sollte Vertrauen und Verständnis in die Technik als Allgemeingut gefördert werden. Im Gegensatz dazu stehen die Bestrebungen kommerzieller Softwareanbieter, die Inhalte ihrer Software als Geschäftsgeheimnis vertraulich zu halten.

## 1.2 Innovation mit Dezentralität

Das Bitcoin-Konzept ist eine echte Innovation und in der Geldgeschichte ohne Beispiel. Im Unterschied zu anderen Währungen gibt es bei Bitcoins keine Scheine oder Münzen. Es handelt sich vielmehr um eine abstrakte Recheneinheit, die dennoch an Börsen gehandelt und gegen andere Währungen getauscht werden kann. Ebenso neu ist, dass das Geld nicht von einer Zentralbank verwaltet und gesteuert wird, sondern dezentral über die Rechner der Bitcoin-Nutzer nach bestimmten Algorithmen. Der Grundgedanke der Dezentralität ist zentraler Punkt der Kryptowährungen!

Die Unabhängigkeit von Staaten und Notenbanken ist eine der größten Vorzüge und Schwächen des virtuellen Geldes zugleich. Anders als bei Euros, US-Dollars, Yen usw. kann es hier keine Geldmengensteuerung und -politik von zentraler Stelle geben. Diese Manipulationsfreiheit wird in einer Ära der lockeren Geldpolitik oft als Vorteil gegenüber den realen Währungen gesehen. Andererseits hat die fehlende Steuerung auch zu hoher Volatilität und Blasenbildung und permanente Kritik an einem potentiell zwielichtigen Gebrauch der Kryptowährungen zur Durchführung krimineller Transaktionen beigetragen.
Kryptowährungen sind letztlich eine vereinfachende Bezeichnung einer kryptografisch legitimierten Zuordnung von Arbeits- oder Rechenaufwand. Dabei kommt der Art der

Kommunikation und der damit zusammenhängenden Technologie eine zentrale Bedeutung zu! Kryptowährungen sind untrennbar mit einer neuen Technologie verbunden, die im Finanzwesen unabhängig von der Nutzung bei Kryptowährungen zukünftig Experten zufolge eine wesentliche Änderung der Verwaltungs- und Abwicklungslogiken verursachen wird.

## 1.3 Peer-to-Peer Kommunikation

Die **Kommunikation** innerhalb von Beteiligten einer Kryptowährung wird von einem **Zusammenschluss von Rechnern** über das Internet mithilfe einer speziellen Peer-to-Peer-Anwendung abgewickelt, so dass im Gegensatz zum heute üblichen Bankverkehr keine zentrale Abwicklungsstelle mehr benötigt wird. Unter einer Peer-to-Peer (P2P) Verbindung (aus dem Englischen „peer“ mit der Bedeutung „Gleichgestellter“, „Ebenbürtiger“) bzw. Rechner-Rechner-Verbindung versteht man synonyme Bezeichnungen für eine Kommunikation unter Gleichen, hier bezogen auf ein Rechnernetz. In einem reinen Peer-to-Peer-Netz sind **alle Computer gleichberechtigt** und können sowohl Dienste in Anspruch nehmen, als auch zur Verfügung stellen.

Die **Computer** sind also alle **untereinander** verbunden, also **vernetzt**, und kommunizieren untereinander regelmäßig und mit allen notwendigen Informationen. Diese Kommunikation steht im bewussten Gegensatz zu einer aktuell überwiegend eingesetzten Zentralkommunikation mit einem Zentralrechner eines Dienstleisters wie einer Bank.

# 2 Blockchain Technologie

Die Blockchain Technologie ist grundsätzlich das Herz einer jeden Kryptowährung. Da eine Kryptowährung eine virtuelle Währung ist, also nicht in Münzen oder Geldscheinen tauschbar ist, sprechen wir letztlich von einer Software Währung. Im Grundsatz bestehen also Kryptowährungen wie jede Software aus Nullen und Einsen (0/1).

Das Kryptowährungs-Netzwerk basiert auf einer von den Teilnehmern gemeinsam mit Hilfe einer Software verwalteten dezentralen Datenbank (der Blockchain), in der alle Transaktionen verzeichnet sind. Die einzige Bedingung für die Teilnahme ist der Betrieb eines Kryptowährungs-Clients; alternativ kann auch einer der Online-Dienste genutzt werden (z. B. für mobile Geräte). Dadurch unterliegt das Kryptowährungs-System keiner geographischen Beschränkung – ein Internetzugang genügt – und kann länderübergreifend eingesetzt werden.

Mit Hilfe kryptographischer Techniken, also Verschlüsselungslogiken, wird sichergestellt, dass Transaktionen mit der Kryptowährung nur vom jeweiligen Eigentümer vorgenommen und die Geldeinheiten nicht mehrfach ausgegeben werden können. Eine **Blockchain** ist eine kontinuierlich erweiterbare Liste von Datensätzen, genannt „Blöcke“, welche mittels kryptographischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptographisch sicheren **Hash** des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten. Eine Hashfunktion ist eine Funktion, die eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge mit fester Länge abbildet.

Der Begriff *Blockchain* wird synonym für ein Konzept genutzt, mit dem ein Buchführungssystem dezentral geführt werden kann und dennoch ein Konsens über den *richtigen* Zustand der Buchführung erzielt wird, auch und gerade wenn viele Teilnehmer an der Buchführung beteiligt sind. Dabei gibt es Konzepte, die das Vertrauen in eine zentrale Instanz erfordern, aber auch solche, die vollständig ohne das Vertrauen in einen Mittelsmann auskommen. Worüber in dem Buchführungssystem Buch geführt wird, ist für den Begriff der Blockchain unerheblich. Es können Werte einer Währung, Immobiliengrundbücher, Sammlungsgegenstände oder Verträge sein. Daher wird die Blockchain auch außerhalb der Kryptowährungen zukünftig bei der Verwaltung von Daten eine wesentliche Rolle spielen.

Entscheidend ist, dass spätere Transaktionen auf früheren Transaktionen aufbauen und diese als richtig bestätigen, indem sie die Kenntnis der früheren Transaktionen beweisen. Damit wird es unmöglich gemacht, Existenz oder Inhalt der früheren Transaktionen zu manipulieren oder zu tilgen, ohne gleichzeitig alle späteren Transaktionen ebenfalls zu zerstören, die die früheren bestätigt haben. Andere Teilnehmer der dezentralen Buchführung, die noch Kenntnis der späteren Transaktionen haben, würden die manipulierte Kopie der Blockchain ganz einfach daran erkennen, dass sie viel kürzer ist als die eigene oder Inkonsistenzen in den Beweisen aufweist. Daher kommt der vorgenannten **Peer-to-Peer Kommunikation** mit einer Vielzahl von Computern innerhalb eines großen Nutzernetzes eine wesentliche Bedeutung zu. Je mehr Computer innerhalb eines Netzes zusammengeschlossen sind, umso mehr Computer führen dann über die Existenz und den Inhalt von Transaktionen Buch mit.

Das Verfahren ist die technische Basis für Kryptowährungen und trägt zur **Verbesserung bzw. Vereinfachung der Transaktionssicherheit** im Vergleich zu zentralen Systemen bei.

Die Funktionsweise ähnelt dem Journal der Buchführung. Es wird daher auch als „Internet der Werte“ (Internet of value) bezeichnet. Eine Blockchain ermöglicht es also, dass in einem dezentralen Netzwerk eine Einigkeit zwischen den jeweils im Netzwerk enthaltenen Computern erzielt werden kann. Dies sorgt für eine vollkommene Unabhängigkeit von

zentralen Systemen (Zentrales Rechenzentrum, Zentraldatenbank usw.), wie sie im etablierten Finanzsystem eingesetzt werden.

Mithilfe dieser Technologie ist das Ziel des Bitcoin-Vaters Nakamoto erreicht, eine dezentrale, nicht beeinflussbare Währung zu erhalten.

**TIPP:** Vor einem Engagement in virtuellen Währungen rufen Sie sich bitte immer wieder ins Gedächtnis: Eine Kryptowährung ist eine technische, eine Software-Währung. Sie existiert nur virtuell auf Computern, lässt sich nicht ausdrucken oder in Münzen prägen oder in Geldscheinen ausdrucken. Allerdings lässt sie sich übertragen, sie hat einen wie auch immer gearteten Wert und man kann damit Transaktionen vornehmen.

Hinweis: Nicht alle Kryptowährungen sind tatsächlich auf der Blockchain Technologie aufgebaut. Daher stehen diese Währungen auch nicht die Vorteile der Technologie zur Verfügung. Der Verzicht auf die Anwendung der Blockchain Technologie bedeutet nicht zwangsläufig einen Nachteil oder Verzicht auf Sicherheit. Es kann aber deutliche Unterschiede in der Ausgestaltung der Kryptowährungen geben. Achten Sie daher unbedingt darauf, welche Funktionsweisen die von Ihnen ausgesuchte Währung einsetzt!

## 2.1 Aufbewahrung von Kryptowährungen

Wer Geld besitzt, will dieses auch aufbewahren. US Dollar oder Euro halten Sie als Anleger auf einem Bankkonto oder aber in bar in einer Geldbörse. Kryptowährungen dagegen sind reine digitale Währungen. Der Anleger kann sie weder ausdrucken noch Münzen prägen lassen. Daher benötigt jeder Anleger eine **elektronische Geldbörse**, auch **Wallet** genannt, für die Verwaltung seiner Kryptowährungsbestände.

Bestandteil der Kommunikation innerhalb des Blockchain Netzwerkes sind unveränderbare Identitäten. Mit diesen Identitäten werden Transaktionen innerhalb der miteinander verbundenen Computer registriert und in dem zentralen Transaktionsregister festgehalten. Die zur Aufbewahrung seiner Kryptowährung geführte elektronische Geldbörse ist genau diese Identifikation, so dass bei jeder Transaktion festgehalten ist, welches Wallet eine Übertragung vorgenommen hat oder aber Kryptowährungen erhalten hat.

Im Gegensatz zum deutschen Wertpapierwesen, wo die Geldkontoführung (nach dem Kreditwesengesetz KWG), die Depotführung (nach dem Depotgesetz DepG) und der Handel von Wertpapieren (nach dem Börsengesetz BörsG) gesetzlich geregelt sind und es eine funktionale Trennung zwischen den Dienstleistungen gibt, fehlt diese gesetzliche Trennung und Regulierung im Kryptowährungsbereich. Daher können Sie als Anleger grundsätzlich überall ein Wallet anlegen lassen.

Generell tragen Sie das Risiko, dass der Anbieter von Wallet Dienstleistungen in die Insolvenz gehen kann. Im Falle einer Insolvenz greifen **keine staatlichen oder anderweitigen Schutzmechanismen** oder gar Einlagensicherungen, so dass Sie ein Totalverlustrisiko bei der Verwaltung Ihrer Kryptowährungsbestände tragen. Die Freiheit, Wallets bei verschiedenen Anbietern zu eröffnen führt dazu, dass es – aus wirtschaftlichen und sachlichen Gründen – Verknüpfungen zwischen mehreren Dienstleistungen bei einem Anbieter geben kann.

Als wichtigstes Beispiel ist hier der Handel von Kryptowährungen zu sehen. Um auf einer Plattform zu handeln, benötigt die Handelsplattform ein Wallet des Anlegers, welches in der Regel auch bei der Handelsplattform geführt wird. Damit verknüpft die Handelsplattform sowohl den Handel als auch die Wallet-Verwahrung unter einem Dach. Da der Handel in Kryptowährungen extrem volatil ist und es nicht auszuschließen ist, dass Handelsplattformbetreiber auch eigene Positionen in Kryptowährungen halten, kann ein massiver Kurssturz die Insolvenz der Handelsplattform zur Folge haben. In diesem Fall sind alle bei der Handelsplattform gehaltenen Kryptowährungen der Anleger voraussichtlich verloren. Sie tragen daher das Totalverlustrisiko.

Aufgrund der sofortigen Übertragungsfreiheit kann der Anleger aber eine Übertragung der von ihm gehaltenen Kryptowährungen auf ein anderes Wallet bei einem externen Anbieter vornehmen. Diese externen Anbieter tragen dann eventuell keine Risiken aus Handelsaktivitäten und sind reine Verwahrer mit einer anderen Risikostruktur.

Zumindest für die Durchführung des Handels ist es aber auf jeden Fall temporär notwendig, die zu handelnden Kryptowährungen bei einem Wallet der Handelsplattform zu verwahren.

In Deutschland sind Anbieter von Wallets und anderer Dienstleistungen in Kryptowährungen wegen der Einstufung als Finanzinstrumente durch die Finanzaufsicht verpflichtet, eine Identifikation der handelnden Personen durchzuführen. Im Interesse aller gesetzeskonformen Nutzer ist dieser Vorgang wichtig, um staatliche Sanktionsmaßnahmen gegen Kryptowährungen allgemein und kriminelle Aktivitäten einzelner Nutzer zu vermeiden. Es muss allerdings darauf hingewiesen werden, dass es jederzeit möglich ist, in Ländern mit anderen Rechtsauffassungen oder Kontrollen Wallets ohne einen Identitäts-Legitimationsprozess (auch KYC-Prozess genannt) zu eröffnen. Damit können Sie als Anleger indirekt dennoch Teil eines Netzwerkes sein, bei dem einzelne Teilnehmer illegale Aktivitäten im Sinne des Geldwäschegesetzes (Geldwäsche, Terrorismusfinanzierung u.a.) vornehmen.

Generell gilt: Sie müssen dem Anbieter von Wallets vertrauen. Sie lassen sich darauf ein, Ihre Vermögensgegenstände bei diesem Anbieter zu verwahren und tragen daher das Risiko, dass der Anbieter aus verschiedenen Gründen in die Insolvenz geht, dass er Ihre Bestände nicht oder nicht ausreichend gegen Zugriff von dritter Seite und damit gegen Betrug und Diebstahl schützt, dass er in illegale Transaktionen verstrickt wird und daher oder auch aus anderen Gründen mit Strafmaßnahmen bis hin zur Schließung der Aktivitäten durch gesetzliche oder aufsichtsrechtliche Maßnahmen rechnen muss. Alle diese Fälle können dazu führen, dass Sie Ihre bei dem Wallet-Anbieter gehaltenen Bestände verlieren. Hier tragen Sie als „**Kontrahentenrisiko**“ das Totalverlustrisiko Ihrer dort gehaltenen Bestände.

Bitte sorgen Sie daher dafür, dass Sie sich ausschließlich auf etablierte Partner mit einer ausreichend guten technischen und finanziellen Basis für die Verwaltung Ihrer Wallets konzentrieren. Verteilen Sie im Zweifel Ihre Vermögen in Kryptowährungen auf mehrere verschiedene Wallet Anbieter, um ein **Klumpenrisiko**, d.h. das Risiko des Ausfalls genau eines Partners, bei dem Ihr gesamtes Vermögen ausschließlich verwahrt wird, zu vermeiden.

### *2.1.1 Identifikationswerkzeuge des Wallets*

Bei der Eröffnung eines E-Wallets gibt es immer zwei wesentliche Bestandteile:

Sie erhalten einen **Public Key** und einen **Private Key** zu jedem Wallet.

Der **Public Key** ist ein öffentlich zugänglicher und damit auch bei allen späteren Transaktionen bekannter und registrierter Schlüssel, der Ihr Wallet innerhalb des Netzwerkes unverkennbar identifiziert. Man könnte den Public Key am besten mit Ihrer **Kontonummer** im klassischen Bankgeschäft vergleichen. Sobald Sie Kryptowährungen transferieren, wird dieser Public Key in den Transaktionscode geschrieben und innerhalb des Transaktionsregisters grundsätzlich unlöschbar eingetragen und dann im Netz an alle Teilnehmer verteilt. Damit lassen sich Transaktionen grundsätzlich innerhalb des Netzes für Ihr Wallet nachvollziehen.

Allerdings kann man diesen Public Key anhand der Transaktionen nicht direkt Ihnen als Person und Anleger zuordnen. Das Kryptonetzwerk ist daher nicht anonym sondern man spricht davon, dass es „**pseudonym**“ ist, da zumindest der Public Key registriert und bekannt ist.

Innerhalb der Transaktion nicht bekannt dagegen ist der einmalig bei Eröffnung eines Wallets generierte und Ihnen mitgeteilte **Private Key**. Der **Private Key** muss auch unbedingt ausschließlich in Ihren Händen bleiben und **darf nicht** befugten **Dritten überlassen** oder zur Kenntnis gebracht **werden**. Der Private Key dient zum **Nachweis Ihres Eigentums** über das Wallet! Wenn die Funktionsweise des Private Keys in das klassische Bankgeschäft übertragen würde, könnte man die Funktion des Private Keys am besten mit einem Zugangspasswort kombiniert mit Pin und Tan übersetzen. Das bedeutet: Wer den Private Key besitzt, weist sich als rechtmäßiger Eigentümer des Wallets aus und kann mit dem Private Key die Übertragung der Kryptowährungen durchführen. **Wer den Private Key besitzt, kann also über die Kryptowährungen verfügen.**

**Sichern Sie** daher den **Private Key** ganz besonders! Es gibt eine Reihe von Sicherheitsmechanismen, die angewandt werden können, um den Key möglichst sicher zu verwahren. Doch Vorsicht: Wenn Sie die Daten zu gut verstecken oder die Informationen in der Zukunft vergessen haben sollten, haben Sie keinen Zugriff mehr auf Ihr Wallet! Es wird geschätzt, dass derzeit 10 bis 20% der im Umlauf befindlichen Kryptowährung „Bitcoin“ auf Wallets schlummern, bei denen der Eigentümer den Private Key entweder verlegt, verloren oder vergessen hat.

Als sichere Variante der Aufbewahrung für Anleger, die Kryptowährungen eher als Wertanlage denn als Zahlungsmittel betrachten, haben sich so genannte **Paper Wallets** herausgestellt.

Dabei wird die **Keys in Papierform** ausgedruckt - entweder als lange Zahlenreihe oder in Form eines so genannten QR Codes. Ein QR Code ist ein Zeichen, mit dem eine Nachricht in optischer Form verschlüsselt wird.

Die Abbildung auf der Folgeseite zeigt einen QR Code.

Dieser QR Code lässt sich mit einfachen Programmen via Mobilfunkgerät oder Computer auslesen:

Abb. 1: Beispiel für einen QR Code mit dem Textinhalt „QR-Code“

Diese Ausdrucke können Sie danach zum Beispiel in einem Safe deponieren, so dass Dritte dort keinen Zugang zu den sensiblen Daten haben. Auch hier müssen Sie sich aber bewusst sein, dass bei der Erstellung des Codes ein Dritter involviert war. Idealer Weise teilen Sie einen Papiercode in 2 Teile und verwahren diese beiden Teile an getrennten Orten auf.

Ob Sie die Daten elektronisch verwahren (auch **E-Wallet** genannt) oder auf Papier ausdrucken: In beiden Fällen tragen Sie Sicherheitsrisiken!

Bei **E-Wallets** sehen Sie sich denselben Risiken ausgesetzt wie bei **Online Banking** Geschäften, schützen Sie daher Ihren Computer vor unbefugten Zugängen und Cyberattacken wie Phishing, Viren oder Trojaner z.B. durch geeignete Maßnahmen.

In ausgedruckter Form (**Paper Wallet**) halten Sie **quasi Bargeld** in der Hand. Auch wenn durch die Eingabe der Daten die Kryptowährung erst wieder digitalisiert werden muss, ist der Verlust des Papieres wie der Verlust von Bargeld zu werten. Auch eine Vernichtung des Papieres durch Brand, Schreddern o.ä. führt zu demselben Ergebnis, als wenn Sie einen Geldschein verbrennen.

**In der Vergangenheit haben sich vor allem die digitalen Brieftaschen als Einfallstor für Hacker erwiesen. Schützen Sie sich immer vor unerlaubtem Eindringen in Ihren Computer. Folgen Sie keinen unbekannten Links, geben Sie Internetadressen immer per Hand ein, um nicht unwissentlich auf falsche Seiten mit betrügerischem Hintergrund gelockt zu werden und seien Sie bei jeder Aktion grundskeptisch und vorsichtig!**

**Denken Sie daran: Für die Sicherheit Ihres Wallets sind Sie selbst verantwortlich! Digitale Kryptowährungen sind leichte und sichere Beute für Hacker. Bei Nutzung von Kryptowährungen sind Sie automatisch im Visier von Betrügern und Sie sollten mindestens Grundkenntnisse in IT Sicherheit haben, wenn Sie sich in Kryptowährungen engagieren!**

## 2.2 Exkurs: Wie entsteht Kryptogeld?

Auch wenn dieser Punkt keine Finanzdienstleistung ist, über die Sie einer Aufklärung bedürfen, so dient dieser Exkurs Ihrem Verständnis der Blockchain Technik und den Zusammenhängen der Kryptowährungen.

Auch wenn nicht alle Kryptowährungen nach demselben Prinzip funktionieren, so ist deren ausgegebene Menge in der Regel doch begrenzt. Bei vielen dieser Kryptowährungen bestehen nicht alle maximal geplanten Währungseinheiten, auch **Coins** genannt, vom ersten Tag an. Da die Kryptowährungen ihren Initiatoren zufolge ja auch einen Inflationsschutz

bieten sollen, haben die Macher der ersten Kryptowährung Bitcoin eine Grundidee aufgenommen anhand derer wir Ihnen die Funktionsweise darlegen wollen:

Um den Wert des Bitcoin zu sichern, bedarf es auf Seiten der Erwerbsinteressenten eines gewissen Aufwands, um den Bitcoin zu erhalten. Analog zu Gold, was auch gemeinhin aufgrund seiner Seltenheit als Inflationsschutz gilt, müssen zum Erhalt von Bitcoins nicht unerhebliche Anstrengungen unternommen werden, damit Bitcoins entstehen. Auch die Produktion von Gold ist aufwändig, man muss in Minen nach Gold schürfen, benötigt dafür Personal und Energie.

Diesen Gedanken haben sich die Schöpfer des Bitcoins zu Eigen gemacht und verlangen vor der Ausgabe neuer Bitcoins einen entsprechenden Aufwand auf Seiten des Interessenten. In Analogität zu einer Goldmine heißt der Vorgang zur Generierung neuer Kryptowährungsanteile daher auch „**Mining**“ oder wird als das „**virtuelle Schürfen**“ von Coins bezeichnet.

Der **Aufwand des Mining** besteht darin, dass mit Hilfe eines besonders ausgestatteten Computers versucht wird, algorithmisch einen **Block** innerhalb der Blockchain logisch richtig und vollständig **zu generieren**. Dabei werden die Zahlenreihen in einem Block der Reihe nach vervollständigt, bis ein Block korrekt erstellt und von anderen Computern innerhalb des Netzwerkes als vollständig und richtig erkannt und damit akzeptiert wird. Es wird also vor allem **Rechenleistung** benötigt, um das Mining durchzuführen. Personen, die das Mining betreiben, werden folgerichtig auch als „**Miner**“ bezeichnet.

Da es weltweit eine Vielzahl von Computern gibt, die diese Blöcke vervollständigen, kommt es häufig zu Mehrfachergebnissen unterschiedlicher Miner. Ein Block kann aber nur von einem Miner erfolgreich erstellt werden. Alle anderen Miner haben ihren Aufwand umsonst betrieben und müssen sich der Vervollständigung des nächsten Blocks zuwenden.

Daher investieren eine Vielzahl von Minern **Zeit und Energie**, die letztlich verloren ist, weil sie den Block nicht rechtzeitig vervollständigen konnten. Gerade dem Thema Energie kommt große Bedeutung zu, da der Dauerbetrieb von Computern, die die Rechenleistungen zur Vervollständigung eines Blocks erbringen, **sehr stromintensiv** und daher auch **teuer** ist.

Es haben sich in der Vergangenheit so genannte „**Miningfarmen**“ etabliert, die an Orten mit günstiger Stromversorgung eine Vielzahl von Computern zum Mining zusammen schließen. In Europa finden sich diese Miningfarmen vor allem auf Island, da die Stromproduktion durch die dort vorhandene geothermische Aktivität sehr günstig ist. Zudem finden sich gerade in China große Serverfarmen.

### *2.2.1 Vergütung für Mining*

Den hohen zeitlichen und finanziellen Aufwand betreiben Miner nicht einfach so – als quasi Vergütung für ihren Aufwand erhalten die Miner im Erfolgsfall nach festgelegten Kriterien neue Bitcoins zugeteilt. Da diese Bitcoins einen Wert haben, den man auf Handelsplattformen realisieren kann, können Miner mit ihrer Tätigkeit Gewinne erzielen. Um aber einer inflationären Erzeugung neuer Bitcoins entgegenzuwirken, haben die Macher des Bitcoins konzeptionell Bremsen eingebaut. Zunächst gibt es eine zeitliche Limitierung, nur etwa alle 10 Minuten wird ein Block vollständig erstellt UND anerkannt. Alle zwischenzeitlichen Ergebnisse anderer Miner sind dann hinfällig.

Darüber hinaus wird die Anzahl der Bitcoins, die zur Belohnung ausgegeben werden, alle 4 Jahre halbiert. Damit werden die letzten Bitcoins im Verhältnis zu den anfangs in höherer

Zahl entstandenen Bitcoins immer wertvoller. Umgekehrt ist im Miningprozess auch in indirektes Wertmodell eingebaut: Ist der Wert von bestehenden Bitcoins so niedrig, dass der Aufwand für ein Mining teurer ist, als einen bestehenden Bitcoin über eine Handelsplattform zu erwerben, so kommen keine neuen Bitcoins mehr hinzu. Erst wenn der Bitcoin Preis wieder höher liegt als der Preis für Rechenleistung und Strom für neue Bitcoins, werden Miner wieder aktiv.

# 3 Vorteile von Kryptowährungen

Es gibt eine Reihe von Argumenten, die für die Nutzung von Kryptowährungen sprechen.

## 3.1 Problemlose Übertragung

Darunter zählt hauptsächlich die barrierefreie Übertragungsmöglichkeit von Kryptowährungen weltweit. Dass eine Übertragung der Kryptowährungen über das Internet zudem auch jederzeit rund um die Uhr möglich ist, während bei Banken häufig Annahme- und Verarbeitungszeiten eine Rolle spielen, versteht sich fast von selbst.

## 3.2 Geringe bis keine Kosten

Bei Übertragungen von Kryptowährungen entstehen im Gegensatz zu klassischen Überweisungen gerade ins Ausland keine hohen Kosten für Überweisungen oder die Einschaltung von Bankenstrukturen notwendig sind.

## 3.3 Hohe Transaktionssicherheit für User und Geschäfte

Der Sicherheitsaspekt, hergeleitet aus der schon geschilderten Blockchain-Technologie mit seiner dezentralen Vernetzung von Millionen Computern im Netz, spielt für viele Nutzer eine große Rolle. Die Eintragung einer jeden Transaktion in einem öffentlich zugänglichen System ist – selbst bei Ausfall einiger oder vieler Computer innerhalb des Systems unkritisch, da alle Informationen auf allen Computern vorhanden sind. Alle Transaktionen sind daher quittiert und bekannt. Diese Transaktionssicherheit ist für alle Beteiligten sehr wertvoll.

## 3.4 Schutz vor Verlust

Der deutsche Name „virtuelles Geld“ sagt schon aus, dass Kryptowährungen nicht physisch existieren. Es gibt also weder Münzen noch Geldscheine. Bei Verlust von Bargeld ist das Geld unweigerlich verloren. Durch die Blockchain Technologie und die dezentrale Vorhaltung aller Transaktionen auf allen vernetzten Computern sind „verlorene“ Kryptowährungen über geeignete Maßnahmen jederzeit wieder herstellbar. Hierzu bedarf es nur der Eingabe von bestimmten verschlüsselten Sequenzen (so genannte „**private keys**“), die der Nutzer bei der Wiederherstellung eingeben muss. Selbst die Zerstörung eines Computers oder einer Festplatte, auf der die Kryptowährungen verwahrt werden, kann durch die Eingabe der private keys von den Auswirkungen auf die Kryptowährungen ungeschehen gemacht werden.

## 3.5 Neutralität

**Kryptowährungen sind unabhängig** von Banken, Staaten oder Organisationen. Durch fehlende staatliche Eingriffe oder Regulation macht das die Kryptowährungen vollkommen autonom von staatlichen Eingriffen oder politischen und wirtschaftlichen Entscheidungen Dritter.

# 4 Nachteile von Kryptowährungen

Es gibt eine Reihe von Nachteilen von Kryptowährungen, die wir Ihnen im Folgenden aufführen:

## 4.1 Geringe Verbreitung

Auch wenn ständig mehr Menschen Kryptowährungen nutzen, ist die weltweite Zahl der Nutzer noch immer relativ gering. Daher ist auch die Zahl von Händlern oder Dienstleistern bislang noch überschaubar, die Kryptowährungen als Zahlungsmittel akzeptieren, auch wenn die Akzeptanz steigt.

## 4.2 Beeinflussbarkeit

Im Vergleich zu den großen Weltwährungen stellen Kryptowährungen nur ein sehr kleines System dar. Das bedeutet auch, dass Einflüsse von außen starke Auswirkungen auf das System haben können. Etwa, wenn ein Spekulant größere Bestände einzelner Kryptowährungen kauft oder verkauft. So kann es zum Beispiel schnell zu sehr hohen und teilweise irrationalen Kursschwankungen bei den Wechselkursen selbst für die Leitwährung der Kryptowährungen Bitcoin kommen.

## 4.3 Ständige Weiterentwicklung

Auch wenn es Kryptowährungen bereits seit einigen Jahren gibt, ist es im Vergleich zu klassischem Geld noch ein junges System, also eine Art von Geld, die es bisher so noch nie gab und deren Akzeptanz in der breiten Bevölkerung noch sehr gering ist. Das System wird daher noch ständig weiterentwickelt.

## 4.4 Technische Risiken

Aufgrund der ständigen Weiterentwicklung der Technik sowie Neuerscheinen weiterer Kryptowährungen bestehen Risiken in der inhaltlichen und technischen Weiterentwicklung von solchen Finanzinstrumenten. Der dezentrale Charakter mit einer open source Technologie führt darüber hinaus zu Diskussionen und Streit der Gesamtheit der Nutzer und Entwickler über die technischen Eigenschaften einer Kryptowährung, was zu Abspaltungen von ursprünglichen mit einer individuellen Kryptowährung verbundenen ideologischen Besonderheiten führen kann.

## 4.5 Hohe Zahl von Kryptowährungen sorgt für Unübersichtlichkeit

Täglich kommen neue Kryptowährungen auf den Markt. Es ist kaum einem Privatanleger möglich, sich die Funktionsweisen und die Sicherheitsaspekte dieser neuen Kryptowährungen anzusehen, geschweige denn sofort oder vollumfänglich zu verstehen. Damit wächst die Gefahr, bei der Auswahl von neuen Währungen auf falsche Kryptowährungen zu setzen.

## 4.6 Systembelastung durch Datenvolumen und Vernetzung

Die Vernetzung aller Computer zur Erhöhung der Transaktionssicherheit hat einen Nachteil: Wenn die Transaktionen zunehmen und alle Transaktionen mit den entsprechenden kryptischen Verschlüsselungen untereinander ausgetauscht werden, so nimmt das Datenvolumen stetig zu und verlangsamt die Kommunikation innerhalb des Netzwerkes. Die Blockchain ist daher ohne weitere Entwicklungen langsam und damit teilweise nicht effizient.

Auch weitere Begrenzungen innerhalb der Systeme sorgen für Kapazitätsengpässe: So ermöglicht die derzeit führende Kryptowährung Bitcoin weltweit maximal sieben Transaktionen pro Sekunde – für das gesamte Netzwerk eines immer weiter wachsenden Netzwerkes! Ethereum, gemessen an der Marktkapitalisierung an zweiter Stelle der Kryptowährungen, liegt bei 15 einfachen Geldtransfers pro Sekunde.

## Tabellarische Gegenüberstellung von Vor- und Nachteilen

In der Tabelle auf der Folgeseite wollen wir Ihnen einige Vor- und Nachteile der Kryptowährungen wertungsfrei und ohne Gewichtung gegenüber stellen. Die Liste erhebt keinen Anspruch auf Vollständigkeit und soll einen Überblick über die typischen Vor- und Nachteile geben. Aufgrund der sich stetig weiterentwickelnden Technik und den damit verbundenen dynamischen Prozessen kann es durchaus möglich sein, dass sich Verschiebungen oder Zu- sowie Abgänge innerhalb der Tabelle ergeben.

| VORTEILE | NACHTEILE |
|---|---|
| frei zugänglich | hohe Volatilität |
| kaum staatliche Kontrolle | fehlender Anlegerschutz |
| dezentral organisiertes Netzwerk | Netzwerk-Übernahme mit Hilfe von Quantencomputern |
| Pseudonymität (Identifikation nur über öffentliche Adresse) | Verschleierung möglicher krimineller Aktivitäten |
| ständige und stetige Verfügbarkeit | starke Konzentration des Besitzes |
| hohe Sicherheit durch Blockchain-Technologie | Überlastung /Trägheit des Netzwerks |
| freie Konvertierbarkeit | Aufbewahrung virtuell mit IT-Risiken |
| teilweise niedrige Transaktionskosten | extremer Energieverbrauch Mining |
| relativ schnelle Transaktionen ggü. Banküberweisungen | Betrugs- und Phishingversuche |
| i.d.R. begrenzte Geldmenge lässt Inflationsschutz erwarten | mögliche gesetzliche Verbote |
| zunehmende Akzeptanz als Bezahl-methode in Realwirtschaft | Hohe Konkurrenz unterschiedlicher Währungen und Techniken |

Abb. 2: Gegenüberstellung von Vor- und Nachteilen von Kryptowährungen

# 5 Zweck von Geschäften in Kryptowährungen

Für den Einsatz von Kryptowährungen gibt es unterschiedliche Motivationen, von denen die Wesentlichsten zu nennen sind:

## 5.1 Durchführung von Finanztransaktionen ohne hohe Kosten und zeitliche oder technische Begrenzungen

Aufgrund der technischen Ausgestaltung und einer direkten Kommunikation zwischen Absender und Empfänger sind Finanztransaktionen, also Bezahlungen, weltweit ohne staatliche oder zentralbankliche Kontrollen und Vorgaben in kürzester Zeit und ohne hohe Kosten möglich. Für einen freien weltweiten Geldverkehr sind Kryptowährungen ideal. Aufgrund der anonymen Transaktionsmöglichkeiten besteht aber die Gefahr von Missbrauch der Zahlungsmöglichkeiten durch Kriminelle, die auf diese Weise Geldwäscheaktivitäten durchführen können. Ebenso können Kryptowährungen zur Bezahlung krimineller Geschäfte dienen wie Drogen- und Waffenhandel. Daher steht insbesondere die Funktion der Bezahlung unter besonderer kritischer Beobachtung durch staatliche Organe und Zentralbanken. Durch die deutsche Einstufung von Kryptowährungen als Finanzinstrumente sind deutsche Dienstleister verpflichtet, nicht nur über eine Genehmigung nach dem Kreditwesengesetz zu verfügen, sondern auch alle damit verbundenen Maßnahmen zur Verhinderung von Geldwäsche zu erfüllen. Dies schließt eine Identifikation der Nutzer (KYC-Prozess) mit ein.

**TIPP:** Auch wenn Nutzer anderer Länder anonym bleiben und die Nutzung von Kryptowährungen zu illegalen Aktivitäten führen können, empfehlen wir deutschen und europäischen Nutzern unbedingt die Einschaltung eines regulierten Dienstleisters. Dies führt zwar zu einer bestimmten Kontrolle, die ursprünglich aufgrund des dezentralen Charakters der Initiatoren nicht gewünscht war. Allerdings fördert die transparente Nutzung von Kryptowährungen die Akzeptanz auf staatlicher Seite und somit den fortdauernden Einsatz von Kryptowährungen im Sinne eines freien, schnellen und kostengünstigen weltweiten Zahlungsverkehrs.

## 5.2 Transaktionssicherheit

Aufgrund des zentralen Buchhaltungscharakters der Blockchain Technologie sind Transaktionen sehr sicher. Im verbundenen Netz der entsprechenden Computer einmal eingetragene Transaktionen können nicht mehr verschwinden. Damit ist für alle Nutzer – sowohl Händler als auch Überweisende – sichergestellt, dass Zahlungen nicht nur wirklich ankommen sondern später auch nicht verschwinden können, wie es im klassischen Bezahlsystem durch Unterschlagung oder technische Maßnahmen erfolgen kann.

## 5.3 Wertanlage und Insolvenzschutz

Kryptowährungen können je nach Ausgestaltung über maximale, systematisch vorgegebenen Höchstmengen verfügen. Damit sind diese Währungen nicht beliebig reproduzierbar und vor allem in der Menge begrenzt. Dies setzt einen Kontrapunkt zu dem bestehenden Geldsystem, bei dem im Wesentlichen das Vertrauen der Geldnutzer in den Wert der Anlage die Kaufkraft bemisst. Die Vergangenheit hat bewiesen, dass die Nutzung der „Geldpresse“, also die permanente Ausgabe neuen Geldes mit einer Geldschwemme zur Inflation führen kann. Kryptowährungen sollen daher einen digitalen Inflationsschutz analog

zur Anlage in Gold ermöglichen. Anleger, die auf diesen Faktor setzen, werden eher langfristige Halter von Kryptowährungen sein, anstatt Kryptowährungen zu Zahlungsverkehrszwecken oder kurzfristigen, spekulativen Transaktionen einsetzen.

### 5.4 Spekulation

Neue Finanzinstrumente, gerade, wenn sie noch nicht weit verbreitet sind und noch über keinen ausgedehnten und liquiden Markt verfügen, ziehen bei entsprechenden Wertentwicklungen Spekulanten an. Daher werden Geschäfte in Kryptowährungen auch in der Hoffnung durchgeführt, einen Gewinn mit dem spekulativen Einsatz zu erzielen. In diesem Fall hat der Erwerber der Kryptowährung weniger ein Interesse, Zahlungsverkehrsleistungen zu nutzen oder einen Insolvenzschutz zu erzielen. Er hat ausschließlich oder überwiegend Interesse daran, kurzfristige Wertsteigerungen zu erzielen. Der Einsatz von derivaten Produkten auf Kryptowährungen, wie zum Beispiel CFDs (Contracts for Difference), erlaubt es Spekulanten neuerdings auch auf fallende Kurse von Kryptowährungen zu setzen, was im direkten Einsatz von Kryptowährungen technisch nicht möglich ist. Dort ist nur der Verkauf bestehender Währungen möglich

## 6 Arten von Geschäften in Kryptowährungen

Nachfolgend Führen wir verschiedene Arten von Geschäften in und mit Kryptowährungen auf:

### 6.1 Direkthandel von Kryptowährungen

Ein Anleger kann Kryptowährungen über Handelsplattformen und überwiegend unregulierte Plattformen im In- und Ausland handeln. Je nach Ausgestaltung der Vorgehensweisen des Handels bedarf es im Inland bestimmter aufsichtsrechtlicher Genehmigungstatbestände der Finanzaufsicht und einer Regulierung des Anbieters nach dem Kreditwesengesetz. Im Ausland fehlen aber häufig solche Regulierungen, so dass der Anleger, der solche Kryptowährungen im Ausland handeln will, einen eigenen Qualitätsprozess starten muss, mit dem er seinen Handelspartner und dessen Sicherheitsmechanismen und finanzielle Stabilität selber prüfen muss.

Anleger können auf diesen Handelsplätzen Kryptowährungen kaufen oder verkaufen. Je nach Ausgestaltung des Handels ist der Handelskontrahent des Anlegers entweder ein anderer Anleger oder aber ein zwischengeschalteter Händler. Im Moment des Handels gehen die wirtschaftlichen Risiken vom Verkäufer auf den Erwerber über. Dies betrifft insbesondere das Risiko des Kurs- bzw. Werteverlustes, den ab diesem Zeitpunkt der Erwerber tragen muss. Steigt eine Kryptowährung nach dem Handel im Kurs, so macht nur noch der Erwerber einen Gewinn, der Veräußerer profitiert nicht mehr von Kursanstiegen.

Der Erwerber der Kryptowährung trägt mit Erwerb das komplette Verlustrisiko, dieses ist der Höhe nach auf den eingesetzten Geldbetrag zuzüglich etwaiger Handelsgebühren begrenzt. Eine Nachschusspflicht besteht nicht, jedoch besteht ein Totalverlustrisiko des eingesetzten Geldes.

## 6.2 Einsatz von Derivaten

In einem jungen Marktsegment bilden sich ständig neue Anbieter und auch neue Angebote heraus. Nachdem es zunächst nur möglich war, direkte Investitionen in Kryptowährungen durchzuführen, gibt es nun auch Anbieter, die derivative Produkte mit Hebelwirkung, so genannte CFDs (Contracts for Difference) zum Kauf und Verkauf von Kryptowährungen zur Verfügung stellen. Mit CFDs ist es auch erstmals möglich, auf fallende Kurse von Kryptowährungen zu setzen, ohne diese zu besitzen. Dies wird ermöglicht durch so genannte Short-Produkte.

CFDs sind Verträge, die mit einem Handelskontrahenten, hier dem ausführenden Broker, eingegangen werden. Diese Verträge sehen vor, dass ein Vertragspartner dem anderen Vertragspartner die Wertentwicklung eines Handelsobjektes in Geld ausgleicht. Als Basis für die Wertentwicklung wird ein Finanzinstrument (z.B. der Bitcoin oder eine andere Kryptowährung), das so genannte Underlying, vereinbart. Bei Erwerb eines CFDs handelt der Anleger also nicht das Underlying selbst, sondern ausschließlich dessen Preis und Kursänderungen.

Gebühren, die bei CFD-Geschäften anfallen, sind in der Regel Handelsspreads (Unterschiedsbetrag zwischen An- und Verkaufskursen) sowie gegebenenfalls noch Kontoführungsgebühren, Finanzierungskosten bei Positionen, die über Nacht gehalten werden und eventuell noch Ausführungsprovisionen.

CFDs unterliegen dem so genannten **Hebelrisiko**.

Schätzen Sie als Anleger den Kurstrend falsch ein, so kann dies zu Verlusten führen, die gerade bei Termingeschäften mit Produkten wie CFDs und Hebeleffekten bis hin zu einem Totalverlust führen können
Der Kapitaleinsatz bei CFDs ist nur ein Bruchteil dessen, was der Investor gewöhnlich bei einem direkten Investment zu zahlen hätte. Der Kapitaleinsatz, auch Margin genannt, ist eine Art Pfand und beträgt i.d.R. zwischen 0,25% und 20% der Gesamtposition. Dadurch entsteht eine Hebelwirkung, weil bereits mit kleinem Kapitaleinsatz auf die Wertentwicklung des Gesamtinvestments abgestellt wird. Dieser Hebel, auch „Leverage“ genannt, kann unterschiedlich hoch sein, bei bestimmten, hochliquiden Märkten ist ein bis zu 400-facher Hebel (bei Margin von nur 0,25%) möglich.

Dadurch, dass nur einen Bruchteil des Vertragswertes als Einschuss (Margin) geleistet wird, können Verluste aufgrund der Hebelwirkung weit über diese Einschüsse hinausgehen. Durch die Hebelwirkung des Einsatzes, der nur einen Bruchteil des Kontraktwertes ausmacht, wirken sich Marktbewegungen weit überproportional aus. Bei Erstverlusten und wiederholten Geschäften ist insbesondere unter Berücksichtigung der Kosten die zur Erreichung der Ausgangsposition erforderliche Marktbewegung äußerst unwahrscheinlich. Anfängliche Gewinne ändern hieran nichts. Bei solchen Geschäften handelt es sich daher um reine Spekulationsgeschäfte mit dem höchsten Risiko.

Je niedriger die Margin ist, umso höher ist der Hebel. Je höher der Hebel ist, desto höher der mögliche Gewinn aber eben auch der mögliche Verlust, der bis zu einem Totalverlust führen kann. Eine Nachschusspflicht für CFDs ist in Deutschland verboten. Nachschuss bedeutet, dass Sie aufgefordert werden, neben Ihrem eingesetzten Geld noch weiteres Geld als Sicherheit nach zu investieren. Es ist aber nicht auszuschließen, dass es in anderen Ländern eine Nachschusspflicht bei Verlusten in CFDs gibt, denen Sie sich ausgesetzt sehen.

## 6.3 Optionen und Futures

Zum Zeitpunkt der Auflage dieser Basisinformationen besteht noch keine Möglichkeit, Kryptowährungen an einer deutschen Options- oder Futuresbörse zu handeln. Allerdings ist der Handel in den USA im Dezember 2017 gestartet worden.

In diesem Zusammenhang sei darauf hingewiesen, dass Sie bei Teilnahme an einem solchen Handel insbesondere **Termingeschäftsrisiken** zu tragen haben. Über Termingeschäftsrisiken existiert eine separate Aufklärungsbroschüre, die wir Ihnen bei Bedarf überlassen. Sollten wir Ihnen gegenüber Dienstleistungen mit Termingeschäften erbringen, erhalten Sie die Aufklärungsbroschüre vor Aufnahme unserer Tätigkeit.

## 6.4 Teilnahme an ICOs (Initial Coin Offerings)

2017 erlebten ICOs, die im Zusammenhang mit der Blockchain oder Kryptowährungen stehen unter Besitzern von Kryptowährungen einen regelrechten Boom. Bei ICOs handelt es sich um erstmalige öffentliche Angebote von Coins oder auch Tokens, die in der Regel eine neue Kryptowährung initiieren wollen. Anbieter solcher ICOs nutzen das günstige Kursumfeld für Kryptowährungen, die es ihnen ermöglichen, in kurzer Zeit Emissionen zu begeben, die Millionenwerte erreichen.

Aufgrund des Booms und der Wertsteigerung in Kryptowährungen haben es ICOs daher ermöglicht, unglaubliche Geldmengen einzig und allein mit einer Internetverbindung zusammenzutragen. Mehr als 1,7 Milliarden US-Dollar wurden 2017 bereits durch ICOs zusammengetragen.

Dabei wurde virtuelles Geld in Projektenzusagen investiert. Dies ist zunächst kein unübliches Vorgehen auch in anderen Märkten (Aktienemissionen u.a.). Das Problem mit ICOs aber besteht darin, dass der Markt der Kryptowährungen nach wie vor nicht reguliert ist; es gibt weder Risikobewertungsmechanismen für die angebotenen Projekte noch die Garantie einer Kapitalrendite. Dazu kommt, dass die **Dokumentation für ICOs** noch **keine**n **bekannten Standards** (wie z.B. einem Wertpapierprospekt oder einem Vermögensanlageprospekt) entspricht.

Es ist daher nicht auszuschließen, dass **ICOs** ohne behördliche Genehmigungen durchgeführt wurden und zu **Totalverlust** bei Anlegern führen werden. Ein Anleger verlässt sich daher bei der Teilnahme an ICOs ausschließlich auf das Ehrenwort derjenigen, die das Projekt ins Leben gerufen haben.

Logischerweise garantiert eine Idee der Initiatoren nicht, dass diese auch gut oder umsetzbar ist, dass ein Produkt Gewinn machen oder dass der Initiator die eingenommenen Gelder auch tatsächlich in die Umsetzung des Projekts investieren wird. Damit besteht das Risiko, dass der Investor in ICOs betrogen wird – und sich die Systematiken der Blockchain gegen den Investor wenden, weil die Zahlungsströme eine Rückverfolgung quasi unmöglich machen.

Die deutsche Finanzaufsicht warnt derzeit vor der unkritischen Teilnahme an ICOs mit Blick auf die damit verbundenen hohen Verlust- und Betrugsrisiken. Gleichwohl ist die Teilnahme an ICOs gegebenenfalls finanziell attraktiv. Daher bedarf es im Vorfeld der Teilnahme an einem ICO einer besonders ausführlichen und sorgfältigen inhaltlichen und technischen Prüfung des Vorhabens.

Es gibt sehr viele auf **Betrug** ausgerichtete Kryptowährungs-Emissionen, so genannte „**Schein-Coins**“. Dies sind **Coins**, **welche** nur für einen Vertrieb gemacht wurden und die,

nachdem damit genug Geld eingesammelt wurde, wieder **vom Markt verschwinden**. Dadurch werden viele geschädigte Kunden hinterlassen. Diese Coins werden wahrscheinlich niemals auf einer handelbaren Plattform vertreten sein, da sie einige Richtlinien und Bestimmungen nicht erfüllen können oder wollen.

Auch bereits handelbare Kryptowährungen können aus unterschiedlichen Gründen wieder vom Markt verschwinden.

# 7 Handelsplätze für Geschäfte in Kryptowährungen

Es gibt eine Reihe von privatrechtlich organisierten Handelsplätzen für Kryptowährungen im Wesentlichen im Ausland. Eine offizielle, regulierte Börse gibt es derzeit nicht. Stattdessen werden diese Finanzinstrumente auf nicht regulierten, dezentralen digitalen Börsen gehandelt. Es gibt kein allgemein gültiges Regelwerk für diese Börsen, vielfach gibt es privatrechtliche Regelungen und Allgemeine Geschäftsbedingungen, die eventuell willkürlich und zum Nachteil des Anlegers jederzeit geändert werden können.

Die technischen Voraussetzungen zur Teilnahme am Handel an diesen Handelsplätzen sind unterschiedlich und auch dort gelten keine generellen Regelungen. So müssen Anleger teilweise bei der Handelsplattform elektronische Brieftaschen, so genannte Wallets, unterhalten und können sich keine alternativen Wallet Anbieter aussuchen. Teilweise muss der Anleger auch Gelder auf diese Plattformen überweisen, so dass sich Gelder außerhalb seiner Einflusssphäre befinden.

Ebenso haben alle Handelsplattformen unterschiedliche Eigenkapital- und sonstige finanziellen Ausstattungen, jede Plattform entspricht einem eigenständigen Risiko!

# 8 Risiken von Geschäften in Kryptowährungen

Bitte halten sich dies vor einem finanziellen Engagement in Kryptowährungen immer vor Augen:
Geschäfte in Kryptowährungen bergen **erhebliche Risiken**, die zu einem **Totalverlust** des eingesetzten Kapitals führen können!

Sollten Sie Direktinvestments in Kryptowährungen durchführen, so ist Ihr Risiko auf das eingesetzte Kapital begrenzt. Sofern Sie CFDs auf Kryptowährungen handeln, ist bei deutschen Anbietern eine Nachschusspflicht ausgeschlossen, es ist aber nicht auszuschließen, dass ausländische Anbieter eine Nachschusspflicht verlangen. In diesem Fall könnte das Eingehen von CFD Positionen je nach Kursverlauf der vereinbarten Kryptowährung zu unbegrenzten Risiken führen.

Die Situation kann auch auftreten, wenn Sie an einer derzeitig nur in den USA bestehenden aber zukünftig eventuell auch in Deutschland angebotenen Terminbörse Optionen und Futures auf Kryptowährungen handeln wollen. Diese Verlustrisiken könnten Ihre **finanzielle Leistungsfähigkeit beeinträchtigen oder sogar übersteigen**, was bis hin zu einer persönlichen **Insolvenz** führen könnte. ***Bedenken Sie daher unbedingt vor Abschluss von Geschäften in Kryptowährungen diese Risiken und Gefahren!***

# B Kryptowährungen Übersicht

Wie in einem jungen Markt üblich, gibt es dauernd neue Angebote sowohl was die Anzahl der Handelsplattformen als auch was die Anzahl der angebotenen Kryptowährungen an sich angeht. Zum Zeitpunkt der Auflage dieser Basisinformationen werden mehr als 1.300 Kryptowährungen an über 7.000 internationalen Handelsplätzen gehandelt.

Informieren Sie sich im Vorfeld über die Funktionsweise und die technische Zusammensetzung einer jeden Kryptowährung, die Sie als Anleger aus den unterschiedlichsten Gründen nutzen wollen! Aufgrund der noch unregulierten Funktionsweise sind zentrale Informationen schwerlich erhältlich. Diese Aufgaben erfüllen häufig Internetangebote, die auch weitergehende Daten wir Marktanteile sowie Marktkapitalisierung der einzelnen Kryptowährungen beinhalten. Bitte beachten Sie, dass die Informationsangebote von Dritten zusammengestellt werden und die SCHNIGGE Wertpapierhandelsbank SE über Wahrheitsgehalt und Inhalte der Webseiten keine Angaben machen kann. Bitte berücksichtigen Sie auch, dass jederzeit neue Anbieter mit besseren oder umfangreicheren Informationen auftreten können, so dass Sie regelmäßig durch entsprechende Suchen im Internet Alternativanbieter finden könnten.

Anbieter solcher Informationen sind zum Zeitpunkt der Auflage dieser Basisinformationen beispielsweise:

https://coinmarketcap.com/

https://bitinfocharts.com/index_v.html

https://bitmakler.net/kriptovaluta

https://de.wikipedia.org/wiki/Liste_von_Kryptowährungen

Neben Kryptowährungen, die über eine Handelsplattform zu handeln sind, gibt es eine Vielzahl von Kryptowährungen, die gar nicht über eine Handelsplattform zu erwerben sind. So existieren zum Zeitpunkt der Auflage dieser Basisinformationen über **3.000 verschiedene Kryptowährungen**. Handelbar sind derzeit nur ca. 1.300 Kryptowährungen.

Die bekanntesten und auch akzeptiertesten Kryptowährungen zum Zeitpunkt der Auflage dieser Basisinformationen sind in der Reihenfolge nach Marktkapitalisierung:

**Bitcoin, Ethereum, Bitcoin Cash, Ripple, Dash, Litecoin, Bitcoin Gold, IOTA, Cardano, Monero**.

Von diesen Kryptowährungen hat Bitcoin als ältestes und „Leitwährung“ unter den Kryptowährungen den weitaus größten Marktanteil und Aufmerksamkeit bei Anlegern erhalten. Dies hat auch zu starken Kursanstiegen geführt. Daher weisen wir an dieser Stelle darauf hin, dass gerade der Gedanke der Zahlung mittels Kryptowährungen nicht abhängig ist von der Höhe des Wertes einer Kryptowährung. Zur Vermeidung von Wertverlusten, die sich häufig nach hohen Wertzuwächsen ergeben können, steht es daher Anlegern offen, andere, weit weniger hochpreisige Kryptowährungen zu wählen.

# C Generelle Risiken bei Geschäften in Krypto-währungen

## 1 Technische Risiken

Investoren muss bewusst sein, dass eine Kryptowährung ein digitales und damit virtuelles Finanzinstrument ist. Im Gegensatz zu Wertpapieren oder Bargeld, welches man in den Händen halten kann, ist dies mit Kryptowährungen nicht möglich. Dies birgt für Anleger ganz besondere Risiken, die nicht unbedingt direkt etwas mit den Risiken von Wertentwicklung des Finanzproduktes sondern mit seiner technischen Funktionsweise zu tun haben.

Kryptowährungen funktionieren nach festgelegten, in den meisten Fällen für Alle zugänglichen, Softwareregeln und Algorithmen.

Kommt es zu Fehlern in der Programmierung oder den mit der Kryptowährung verbundenen fest verankerten Regeln kann das den Wertverlust der virtuellen Währung oder die Nicht-Nutzbarkeit der Kryptowährung verursachen.

Ein für Kryptowährungen ebenfalls spezifisches Risiko wäre zum Beispiel der Geldverlust aufgrund einer fehlerhaften Adresse des Empfängers. Im Fall der Kryptowährung Ethereum verlieren Sie Ihr Geld, wenn zum Beispiel die letzte Ziffer der Adresse nicht kopiert wurde.
Für Bitcoin ist dieser Fehler nicht relevant, denn das System verfügt über eine integrierte Adressvalidierung. Auch daran erkennen Sie, dass die Funktionsweise von Kryptowährungen unterschiedlich sein kann.

In einem Fall wie bei Ethereum sind die investierten **Gelder** aller Voraussicht nach **verloren**. Ob und wenn ja gegen wen es für Anleger Ansprüche auf Ausgleich dieses Verlustes gibt, ist absolut offen und es ist nicht auszuschließen, dass niemand die Verluste ausgleicht – entweder aus juristischen Gründen oder aber auch mangels verfügbarer Vermögen der Verursacher.

Ein grundsätzliches Problem: **Blockchain-Technik** ist dezentral und **entwickelt sich** deshalb nur **schwer weiter**.
So ist es nicht besonders einfach, Veränderungen in ein dezentralisiertes Netzwerkprotokoll einzubringen. Der Entwickler kann entweder zwingende Updates für alle Kunden durchführen – obwohl diese Art von Netzwerk nicht wirklich als dezentralisiert gesehen werden kann – oder er muss alle Teilnehmer davon überzeugen, die Veränderungen zu akzeptieren. Sollte ein bedeutender Teil allerdings gegen die Veränderungen stimmen, könnte sich die Gemeinschaft in zwei Nutzergruppen teilen: Die Blockchain würde sich in zwei alternative Blockchains aufteilen, aus der 2 verschiedene Währungen resultieren würden. Diese Aufteilung wird ***„Fork“*** genannt.

Verschiedene Teilnehmer haben in einer Kryptowährung unterschiedliche Interessen. Miner sind daran interessiert, ihre erfolgreichen Miningversucher und damit ihre Vergütung zu steigern. Die Nutzer hingegen möchten weniger für die Übertragung von Kryptowährungen z.B. für Bezahlaktivitäten belastet bekommen. Die klassischen „Fans“ wollen, dass die Kryptowährung bekannter wird - und technische Nerds wollen, dass der Technologie nutzvolle Innovationen hinzugefügt werden.

Zwei der größten Kryptowährungen haben sich bereits geteilt. Bitcoin hat sich aufgeteilt, als sich die Teilnehmer nicht über die Strategie der Erweiterung der Blockgröße einig werden konnten. Bereits davor geschah etwas ähnlich mit Ethereum. Ein Anspruch auf Änderung der Software besteht aber eben nicht sondern muss von einer Mehrheit der

Kryptowährungsnutzer genehmigt werden. Diese veränderte Version muss dann aber von so vielen Anwendern akzeptiert bzw. verwendet werden, dass mehr als die Hälfte der Rechenleistung aller verbundenen Rechner darauf entfällt. Wenn das zu Kryptowährungs-Einheiten führt, die für eine frühere Version der Software nicht mehr gültig sind, wird es als „***Hard Fork"*** bezeichnet.

Kryptowährungen haben nicht überall ausgereifte technische Konzeptionen. Sollten also Fehler bestehen, ohne dass Plausibilitätskontrollen etabliert werden, bestehen ebenso Risiken des Verlustes bzw. der Unbrauchbarkeit. So gibt es Kryptowährungen, die mit nur einer Eingabe einer falschen Ziffer innerhalb eines Blocks der Blockchain komplett unbrauchbar werden. Ohne einen Plausibilitätscheck können sich so schnell Kryptowährungen der totalen Wertlosigkeit ausgesetzt sehen.

Es besteht das theoretische Risiko, dass der Zusammenschluss extremer Rechenleistung (z.B. über Quantencomputer) in der Zukunft einzelne Kryptowährungen oder gar die Gesamtheit aller Kryptowährungen gefährden könnte. Zwar könnte vorher der Algorithmus umgestellt werden, doch ist nicht auszuschließen, dass die nicht rechtzeitig vor einem Angriff umgesetzt wird.

Auch ein Brute-Force Angriff (übersetzt: Angriff mit „roher Gewalt") ist im Bereich des theoretisch Möglichen, hier spricht man von dem Versuch, über das Ausprobieren von Szenarien ein System zu gefährden. Zwar sind beide Varianten ohne wirtschaftlichen Hintergrund weniger wahrscheinlich, aber auch nicht ausschließbar. Derzeit stehen für solche Angriffsvarianten voraussichtlich zu wenig Rechenleistung und Rechnerkapazitäten zur Verfügung.

Während die Funktionsweise der Kryptowährungen mit der Blockchain Technologie verhältnismäßig sicher ist, sind die notwendigen Drittdienstleister bei der Nutzung der Kryptowährungen in der Regel eine besondere Schwachstelle. Wir weisen an dieser Stelle daher explizit und besonders auf die Risiken bei Nutzung von Drittanbietern hin. (Abschnitt D1) Zu den dort behandelten Risiken gehören u.a. Diebstahl, Hackerrisiken, Hard- und Softwarerisiken, organisatorische Risiken sowie z.B. wirtschaftliche Risiken des Partners.

## 2 Rechtliche Risiken

Der rechtliche Status von Kryptowährungen ist noch überwiegend offen. Außer in einer Handvoll Ländern- darunter Bolivien, Bangladesch, Ecuador und Kirgisistan- ist die Verwendung von Bitcoins bzw. Kryptowährungen von Privatpersonen nicht ausdrücklich verboten. Allerdings existiert derzeit kein spezifisches Gesetz in Europa. Es kann **nicht ausgeschlossen** werden, **dass der Besitz**, die Nutzung oder der Handel von Kryptowährungen durch Gesetzgeber **verboten wird**.

Ob und wenn ja wo und wie die Nutzung der einmal erworbenen Kryptowährungen in einem solchen Fall noch möglich ist, ist zum jetzigen Zeitpunkt absolut offen. Anleger müssten in so einem Fall von dem größtmöglichen Risiko, hier dem Totalverlust der Investition, ausgehen!

In China wurde Banken und anderen Finanzinstituten verboten, mit den Kryptowährungen zu handeln. Auch Eingriffe in die Struktur bzw. Verfügbarkeit von Handelsplätzen hat es in der Vergangenheit durch die Schließung solcher Handelsplätze gegeben. Angesichts der zunehmenden Kapitalflucht in unsicheren Ländern wie Venezuela oder Kuba ist eine repressive Regulierung durchaus denkbar.

Auch in China, wo restriktive Kapitalkontrollen herrschen und die Währung eventuell abwertet, ist dies ein realistisches Szenario. Mehr noch: Die größten Serverfarmen, die das Bitcoin-Netzwerk und andere Kryptowährungen unterstützen und sicher machen, stehen in China. Ein plötzlicher Ausfall derselben würde die
Verarbeitung von Bitcoin-Transaktionen oder die von anderen Kryptowährungen über Wochen verlangsamen. Ein solcher Eingriff dürfte mindestens zu wochenlangen Turbulenzen, verbunden mit starken Kursschwankungen bis hin zu massiven Kursverlusten führen.

In **Japan** dagegen ist der Bitcoin als eine Kryptowährung bereits **offiziell anerkanntes Zahlungsmittel**. Hier könnten Änderungen an dem Status auch für massive Verwerfungen sorgen.

# 3 Aufsichtsrechtliche Risiken

Die Freiheit der Dezentralität und die nicht vorhandene Überwachung im Graubereich führt auch u einer Reihe von zusätzlichen und spezifischen Risiken:

## 3.1 Kein Einlagenschutz

Gehen Tauschbörsen in die Pleite, haben Sparer anders als bei Geschäftsbanken keinen Anspruch auf gesetzlichen Einlagenschutz. Das gilt nach den derzeitigen Regeln selbst dann, wenn der betroffene Dienstleister bei einer nationalen Aufsichtsbehörde registriert ist.

## 3.2 Keine Regulierung und Überwachung

Üblicherweise schützen Organisationen wie börsliche Handelsüberwachungen oder eine der deutschen Börsenaufsicht vergleichbare Institution den Anleger vor betrügerischen Aktivitäten im Handel mit Wertpapieren. Eine solche staatliche Überwachung im Sinne der Marktteilnehmer fehlt bei Kryptowährungen. Die bedeutet für den Anleger, der Gefahr von Marktmanipulation durch Absprachegeschäfte, Layering oder anderen in Wertpapiermärkten verbotenen Handlungsweisen ausgesetzt zu sein. Als Layering wird das Befüllen eines Orderbuchs mit Scheinorders bezeichnet, die dem Anleger das Gefühl vermitteln sollen z.B. eine hohe Marktliquidität vorzuspiegeln oder aber Preise dadurch zu beeinflussen.

## 3.3 Keine Beschwerde- oder Sanktionsmöglichkeiten für Anleger

Aufgrund der fehlenden Überwachung und Regulierung sind Aufsichtsbehörden derzeit nicht für Beschwerden der Anleger zuständig. Damit entfallen auch aufsichtsrechtliche Sanktionsmöglichkeiten, von denen der Anleger an regulierten Wertpapiermärkten ansonsten profitieren könnte. So fallen Ombudsmänner oder Schiedsmänner derzeit in der Regel zur Schlichtung aus. Auch börsliche Kontroll- oder Sanktionsmechanismen wie ein Sanktionsausschuss oder Reklamations- und Beschwerderegeln stehen häufig nicht zur Verfügung. Anleger in Kryptowährungen müssen sich daher nicht nur auf einen Totalverlust ihrer Investitionen einstellen sondern auch damit rechnen, dass sie im Nachgang kaum oder nicht vorhandene Reklamationsmöglichkeiten haben werden.

# 4 Marktpreisrisiko

Als **Marktpreisrisiko** wird das Risiko der Preisänderung eines Finanzproduktes, also auch einer Kryptowährung bezeichnet. Das allgemeine Marktrisiko einer Kryptowährung, was auch als systematisches Risiko bezeichnet wird, ist das Risiko einer Preisänderung, die der allgemeinen Tendenz am Markt der Kryptowährungen zuzuschreiben ist und die in keinem direkten Zusammenhang mit der spezifischen Situation einer einzelnen Kryptowährung steht. Dem Marktrisiko unterliegen also alle Kryptowährungen grundsätzlich gleichermaßen. Die Entwicklung aller Kryptowährungen erfolgt dann grundsätzlich parallel innerhalb des Gesamtmarktes. So kann der Kurs einer Kryptowährung sinken, obwohl sich aktuell an der Funktion, der Sicherheit oder sonstiger Faktoren der Kryptowährung nichts geändert hat.
So kann sich eine Veränderung der politischen Situation in einem Land indirekt auf den gesamten Markt der Kryptowährungen auswirken.

Einfluss auf Marktpreise können zudem Risiken aus anderen Bereichen haben. Hier sind vor allem zu nennen:

## 4.1 Zinsänderungsrisiken

Dies sind Risiken, aus denen sich vor allem Auswirkungen auf Währungskursentwicklungen anderer Währungen ergeben, aus denen sich die Attraktivität von Kryptowährungen gegenüber den anderen Währungen ableiten lässt.

## 4.2 Inflationsrisiken

Dies sind Risiken, aus denen sich die Attraktivität von Kryptowährungen mit z.B. maximaler Ausgabeanzahl gegenüber klassischen Währungen ohne Ausgabebegrenzung ableiten lassen.

## 4.3 Aktienmarktrisiken

Dies sind Risiken, bei denen die allgemeine Kursniveauänderung der Aktienmärkte Auslöser für eine Flucht in oder aus den Kryptowährungen sein kann.

Die Maßeinheit für die Schwankungen in Märkten wird **Volatilität** genannt. Je stärker die Volatilität ist, umso stärker sind die Kursschwankungen, d.h. dass die Kurse in beide Richtungen ausschlagen. Je niedriger die Volatilität eines Finanzinstrumentes oder von Märkten ist, umso geringer sind die Kursschwankungen, also umso flacher ist die Kursentwicklung mit nur geringen Ausschlägen. Kryptowährungen verfügen in dem frühen Stadium ihrer Existenz über teilweise beträchtliche Volatilitäten. Kursausschläge von 20% an einem Handelstag sind nicht selten, Kursanstiege von mehreren 100% innerhalb kurzer Zeiträume sind ebenso möglich, wie Kursverluste um mehr als 50%.

Das Marktpreisrisiko wird zudem durch externe Faktoren beeinflusst. Hier sind es vor allem Ereignisse, die auf die Psychologie der Marktteilnehmer Auswirkungen haben.

Bei Kryptowährungen sind dies vor allem Nachrichten aus Politik und Wirtschaft, insbesondere zur Frage der Regulierung von Kryptowährungen durch Staaten und Finanzaufsichten. Ebenso sind Wirtschaftskrisen einzelner Länder Gradmesser für die Flucht aus oder in Kryptowährungen.

Bereits Gerüchte über solche oder andere Entwicklungen können Auswirkungen auf die Marktpreise haben.Zudem können auch andere externe Faktoren Einfluss auf die Stimmung und die Psychologie der Marktteilnehmer haben. Dies könnten sein: Sorgen vor Arbeitslosigkeit, sonstige wirtschaftliche Ereignisse oder individuelle Entscheidungen oder Bewertungen der Anleger.

Dabei ist nicht klar, welcher Marktteilnehmer welches Ereignis in welche Richtung interpretiert. Ein und dieselbe Nachricht kann dabei unterschiedlich bewertet oder interpretiert werden, weswegen nicht immer von vornherein klar ist, wie sich Märkte daraufhin entwickeln. Rationale und irrationale Faktoren haben daher gleichermaßen Einfluss auf Kursentwicklungen. Allerdings ist der Anleger nicht zwangsläufig in der Lage, diese Faktoren zu erkennen, zu werten und richtig zu interpretieren.

## 5 Risiko der Hebelwirkung

Geschäfte in Kryptowährungen erfordern grundsätzlich einen direkten Kapitaleinsatz der gesamten Anlagesumme. Anzahlungen, die häufig nur einen kleinen Bruchteil des Geschäftsgegenwertes ausmachen, sind bei den typischerweise Kassageschäften nicht einschlägig. Insofern entfällt bei Direktgeschäften in Kryptowährungen das Risiko der Hebelwirkung, auch **Leverage Effekt** genannt. Von einem Leverage Effekt wird gesprochen, wenn die Preisentwicklung der geleisteten Anzahlung zum Erwerb eines Derivates aufgrund der Kursänderung des Basiswertes eine überproportionale Reaktion (hohe Gewinne aber auch Totalverlust) zeigt.

Je größer der Hebel ist, umso risikoreicher ist eine Position, da sie sehr schnell zu einem Totalverlust führen kann. Dabei wird die Reagibilität dieses Effektes als „Leverage Faktor“ bezeichnet, der damit Gradmesser des Risikos einer Hebelposition ist. Dabei ist die Hebelwirkung immer mindestens 1, so dass der absolute Gewinn/Verlust immer größer ist als beim verbundenen Kassageschäft.

Das Hebelrisiko tritt auf, sofern ein Geschäft nicht direkt in einer Kryptowährung erfolgt sondern in CFDs oder auch Optionen und Futures auf Kryptowährungen.

## 6 Risiko von Margin-Zahlungen

Auch das Risiko von Marginzahlungen betrifft das Direktinvestment in Kryptowährungen nicht. Es tritt auf bei indirekten Investments über CFDs sowie Futures und Optionen.

Bei letzteren Produkten erfolgt eine tägliche Gewinn- und Verlustrechnung, die sich auf Basis der Veränderung des Preises im Basiswert ergibt. Somit lässt sich die Margin Zahlung nicht im Vorhinein ermitteln oder abschätzen. Dies führt während der Laufzeit zu starken Schwankungen des Gewinns oder des Verlustes, bevor es am Ende der Laufzeit (Tag der Fälligkeit des Derivates) zu einer Abschlussabrechnung von Gewinn bzw. Verlust kommt. Da die Gewinnschwankung sofort dem Konto gutgeschrieben oder belastet wird, bedeutet eine Gewinnschwankung immer einen Einfluss auf die Liquidität des Anlegers. Je länger die Laufzeit des Derivates ist und je größer die Position in diesem Derivat ist, umso stärker sind die Auswirkungen auf die Liquidität des Anlegers.

Im Extremfall kann bei ungünstiger Kursentwicklung des Basiswertes eine Nachschusspflicht bestehen. In diesem Fall reicht die initial hinterlegte Anzahlungssicherheit, auch **initial margin** genannt, nicht aus, um die variablen Gewinnveränderungen abzufedern. Die variable Gewinnberechnung erfordert die Hinterlegung einer sich ändernden Sicherheit, auch **variation margin** genannt. Das Nachschussrisiko besteht tatsächlich nur bei Options- und

Futurespositionen. In Deutschland besteht das Verbot einer Nachschusspflicht bei CFDs. Sollte der Anleger jedoch CFD Positionen im Ausland eröffnen und halten, kann es auch möglich sein, dass er diesem Schutz nicht unterliegt.

# 7 Liquiditätsrisiko

Unter dem Liquiditätsrisiko wird das Risiko verstanden, dass Positionen nicht, nicht komplett oder nicht zu fairen Marktbedingungen verkauft oder eingegangen werden können. Für ein solches Risiko gibt es verschiedene Gründe, wie einen fehlenden oder eine nicht ausreichende Anzahl von Handelskontrahenten. Aber auch ein Missverhältnis zwischen der Größe der zu handelnden Position im Verhältnis zu dem angebotenen Handelsvolumen kann ein Grund für ein Liquiditätsrisiko sein. Die Schließung oder der temporäre Ausfall von Handelsplätzen führt ebenfalls dazu, dass die Glattstellungsmöglichkeit von Positionen entfallen und der Anleger z.B. seinen Bestand nicht verkaufen kann.

Gerade in jungen Märkten, die noch nicht effizient sind und noch nicht über viele Handelsteilnehmer verfügen oder aber bei denen professionelle Market Maker fehlen, ist das Liquiditätsrisiko sehr hoch. Mangelnde Markttiefen, Anfälligkeit für Kursschwankungen sowie Ordergrößen in Privatanlegervolumina erhöhen ebenso das Liquiditätsrisiko. Selbst das Vorhandensein eines Market Makers ist keine Garantie dafür, dass eine ausreichende Liquidität besteht, da es keine Verpflichtung geben muss, permanent während des gesamten Handels als Liquiditätsspender zu agieren. Zudem ist eine hohe Anzahl verschiedener Handelsplätze, zumal diese noch unreguliert sind, belastend und das Liquiditätsrisiko erhöhend, da die die wenige vorhandene Orderliquidität noch weiter fragmentiert wird.

Hinzu kommt, dass der Handel von Kryptowährungen aufgrund der eingesetzten Technik ohne besondere Handelsunterstützung durch menschliche Unterstützung ein Handel weltweit rund um die Uhr ist. Es ist nicht auszuschließen, dass der Anleger im Zeitpunkt seiner Anlageentscheidung auf einen aus internationaler Sicht gesehen vergleichsweise inaktiven Handelszeit trifft und die Marktliquidität daher auch aus zeitlicher Sicht gering ist.

Auch die für junge Märkte nicht unüblichen technischen Probleme von Handelsplatzbetreibern, die für nicht immer ausreichende Bandbreiten oder technische Verfügbarkeiten sorgen, führen gegebenenfalls im Moment der Ordererteilung zu Nichtausführungen von Orders. Auch Systemstörungen bei anderen mit der Geschäftsabwicklung verbundenen Dienstleister – hier im Besonderen Anbieter von Wallets – führen gegebenenfalls temporär oder dauerhaft zu Problemen bei der Weiterleitung von Orders an die Ausführungsplätze.

# 8 Risiken bei Geschäften an unregulierten Handelsplätzen im In- und Ausland

Der Handel von Kryptowährungen unterliegt nur im Inland einer gewissen aufsichtsrechtlichen Anforderung. Hier muss der Dienstleister, der den Handel durchführt, über aufsichtsrechtliche Genehmigungen nach dem Kreditwesengesetz verfügen. Je nach Ausgestaltung des Handels bedarf es aber keiner weitergehenden Maßnahmen, Marktregelungen oder Handelsordnungen. Zudem fehlt es an analogen Kontrollen der Handelsabläufe, wie man sie in der EU bei der Organisation von Handelsplätzen gewohnt ist. Dazu gehört die Börsenaufsicht, die die Tätigkeit operativ an die Handelsüberwachung einer Börse auslagert.

Ohne solche Institutionen besteht das Risiko, dass manipulative und betrügerische Handelsmachenschaften nicht entdeckt oder auch nicht verfolgt werden. Es ist sogar nicht

auszuschließen, dass die Betreiber von Handelsplattformen Bestandteil von Handelsmanipulationen oder intransparenten Handelsaktionen sind.
Aufgrund der fehlenden Regulierung von Handelsplätzen besteht das Risiko, dass die finanzielle Ausstattung solcher Plattformen nicht dazu geeignet ist, Schadensfälle abzudecken. Ob und wie die technische Ausstattung ausreichend für die sichere Abwicklung von Transaktionen ist, ist für Nutzer nicht immer erkennbar. Auch dahinterliegende Sicherheitskonzepte sind nicht immer offen kommuniziert. Der Anleger ist auf **eigene Recherchen** bei der Bewertung der Seriosität und wirtschaftlichen Stärke der von ihm gewählten Handelsplattform(en) angewiesen.

Ob und wann eine Handelsplattform seriös ist, lässt sich nicht durch nachvollziehbare und für alle Nutzer zugängliche, transparente Qualitätskriterien ermitteln. Vielmehr sind subjektive Meinungen und Einschätzungen bei der Auswahl des Handelspartners notwendig. Die Nutzung einer ausländischen Handelsplattform kann zudem das Risiko beinhalten, dass lokale Behörden die Nutzung der Plattform sowie den Handel und den Transfer der Kryptowährungen bzw. bei Verkauf erlösten Gelder unterbinden. In einem solchen Fall besteht das Totalverlustrisiko.

Anleger sollten bei der Auswahl des Handelsplatzes einige Fragen klären:

**Kann ich auf den Webseiten identifizieren, wer Anbieter des Handelsplatzes ist?** Gibt es Adressen und Angaben zu Verantwortlichen, Adressen und Telefonnummern? Machen Sie durchaus einen Probeanruf oder eine anderweitige Kontaktaufnahme. Falls Sie die Fragen nicht positiv beantworten können, nehmen Sie von der Beauftragung des Handelsplatzes Abstand.

**Verstehe ich das Angebot inhaltlich und was kostet es?** Wenn die Kosten zu hoch oder gar nicht ausgewiesen sind, nehmen Sie von der Beauftragung des Handelsplatzes ebenso Abstand wie im Falle inhaltlicher Unverständlichkeit des Angebotes!

**Wie sieht es mit der Sprache aus, ist diese für mich verständlich, ist sie grammatikalisch richtig oder wirkt sie „dahingeschustert"?** Schlechte, grammatikalisch falsche Inhalte zeugen meist von wenig Professionalität eines Angebotes. Die Beauftragung solcher Handelsplätze mit qualitativ schwachen Webseiten sollte daher möglichst unterbleiben.

**Wo ist der Rechtsstand des Anbieters, also wo ist der Sitz der Handelsplattform?** Habe ich im Zweifel Zugriff auf diesen Staat im Fall von Klagen oder ist der Anbieter vor meinen Ansprüchen geschützt? Die Beauftragung solcher Handelsplätze mit Sitz in kleinen und unregulierten Ländern sollte möglichst unterbleiben. Suchen Sie sich Rechtsräume aus, die mindestens dem Standard Deutschlands entsprechen (EU-Raum, USA, Kanada etc.)

**Gibt es Regeln, die alle Seiten zu befolgen haben?** Dies betrifft sowohl die Abläufe des Handels aber insbesondere auch Handelsregeln, die einen organisierten Markt ausmachen. Die Beauftragung solcher Handelsplätze sollte unterbleiben, wenn es keine Handelsregeln und die Darlegung der Kontrolle dazu gibt.

**Gibt es Sicherheiten** der Handelsplattform oder Dritter für die Abwicklung meiner Geschäfte für den Fall, dass es zu Unstimmigkeiten oder betrügerischen Machenschaften kommt? Gibt es eventuell sogar eine aufsichtsrechtliche Regulierung für den Handelsplatzanbieter?

# 9 Risiko bei kreditfinanzierten Geschäften in Kryptowährungen

Das **Risiko** für Anleger **erhöht sich** überproportional in dem Fall, dass die Finanzierung von Geschäften in **Kryptowährungen auf Kredit** erfolgt. Kommt es nämlich zu einer negativen Kursentwicklung der Anlage, also bei einer gegenläufig der eigenen Erwartung ablaufenden Börsenphase, führt dies zu Verlusten für den Anleger. Der Anleger muss in diesem Fall nicht nur den Verlust, vielleicht sogar den Totalverlust hinnehmen, er muss darüber hinaus auch noch den Kredit sowie dessen Kreditzinsen abtragen.

Der Anleger darf daher nie darauf setzen, dass er Kreditzinsen und die Rückzahlung des Kredites aus zukünftigen Gewinnen seiner Anlage tätigt. Er muss vielmehr damit rechnen, dass er Verlusten ausgesetzt ist und er zusätzlich noch die Kreditvolumina zuzüglich aufgelaufener Zinsen zurückzahlen muss. Daher muss er vor Eingang einer solchen Kreditverbindlichkeit prüfen, ob er in der Lage ist, den Kredit auch im ungünstigen Verlustfall der Anlage aus sonstigen Einkünften oder Vermögen zu tilgen.

Sofern die Spekulation auf Kredit vorgenommen wird, erhöht sich das Verlustrisiko nochmals neben den Marktrisiken um die Kreditkosten. Geschäfte, insbesondere in jungen Finanzinstrumenten wie Kryptowährungen, sollten in keinem Fall durch Kredite finanziert werden, da die Gefahr stark schwankender Preise bis hin zu einem Zusammenbruch des neuen Marktes besteht. Anderenfalls geht der Anleger das Risiko ein, in die **persönliche Insolvenz**situation zu rutschen!

# 10 Einfluss von Kosten auf die Gewinnerwartung

Bei Kauf und Verkauf von Kryptowährungen fallen neben dem aktuellen Kurs der Währung an der jeweiligen Börse auch noch verschiedene Nebenkosten an. Diese können sein: Nutzungskosten von Wallets, Überweisungskosten, sonstige Provisionen und/oder Transaktionskosten der Handelsplattform oder anderer in die Dienstleistung involvierter Firmen oder Personen. Hierzu gehören Provisionen, die entweder als Fixprovision oder volumensabhängige Gebühr erhoben werden können.

Dabei sind die Konditionen und Gebühren je nach Handelsplatz unterschiedlich, da die Plattformen im Wettbewerb zueinander stehen. Auch Drittkosten bei der Orderausführung müssen bei der Kalkulation berücksichtigt werden. Diese Drittkosten können Ihnen entweder von dem Dienstleister direkt oder von der Handelsplattform stellvertretend für weitere Dienstleister belastet werden. Es kann sein, dass alleine die Beauftragung eines Handels bereits eine Gebühr auslöst, zudem ist für die eigentliche Orderausführung eine Gebühr zu erwarten.

Erhobene Gebühren belasten die Wahrscheinlichkeit und Ihre Chancen, aus der Order zu einem späteren Zeitpunkt Gewinne zu erzielen, da die Wertentwicklung für ein profitables Geschäft mindestens dem Einstandspreis zuzüglich der gezahlten Kosten/Gebühren entsprechen muss.

Wichtig: Erteilen Sie Orders nur dann, wenn Sie sich über alle Kosten, Gebühren oder Provisionen informiert haben. Einerseits will man keine unangenehme Überraschung erleben, wenn auf einmal Kosten auf den Anleger zukommen, die man vorher nicht erwartet hat. Zudem kann der Anleger nur in Kenntnis der Gebühren für alle Geschäfte errechnen, ab welchem Zeitpunkt er mit der Gesamtinvestition die Gewinnzone erreicht. Denn nur wenn alle Kosten abgedeckt sind, kann der Anleger einen Gewinn erzielen.

# 11 Steuerliche Risiken

Auch wenn es sich bei Kryptowährungen noch um eine junge Form von Finanzinstrumenten handelt, so ist die steuerliche Bewertung in Deutschland bereits klar geregelt.

## 11.1 Veräußerung

Die **Veräußerung** von Kryptowährungen ist dann **steuerpflichtig**, wenn die Anschaffung und Veräußerung **innerhalb eines Jahres** erfolgt. Hier findet der § 23 EStG Anwendung, welcher auch bei Immobilien greift. Geschäfte werden steuerlich als privates Veräußerungsgeschäft klassifiziert. Dieses private Veräußerungsgeschäft ist dann steuerpflichtig, wenn zwischen Anschaffung und Veräußerung weniger als ein Jahr liegt. Des Weiteren muss die Freigrenze von 600 € überschritten werden. Bei der Freigrenze gilt: Bei Überschreiten der Freigrenze ist der gesamte Betrag zu versteuern. Es handelt sich hierbei also nicht um einen Freibetrag, der per se immer steuerfrei bleibt!

**Steuerfrei** hingegen ist die Veräußerung, wenn zwischen Anschaffung und Verkauf **mindestens ein Jahr** vergangen ist. Zum Nachweis dienen Ihre eigenen Aufzeichnungen, die daher von besonderer Wichtigkeit sind. Gegenüber dem Finanzamt sind Sie hier in der Nachweis- und Mitwirkungspflicht. Daher sollten Sie die wichtigsten Belege immer aufbewahren.

Anders als bei Aktien- oder Zinsgeschäften wird also **keine Abgeltungssteuer** fällig.

## 11.2 Risiko der Doppelbesteuerung bei Auslandsanlagen

Als in Deutschland ansässiger Anleger, der aber eventuell im Ausland handelt oder ausländische Dienstleister nutzt, kann für Sie das Risiko bestehen, dass Steuern im Ausland anfallen, deren Höhe Sie ganz oder teilweise nicht in Deutschland zur Vermeidung einer Doppelbesteuerung anrechnen können.

# D Spezielle Risiken bei Kryptowährungen

Im Grunde genommen haben Kryptowährungen grundsätzlich dieselben funktionalen Prinzipien wie „ursprüngliche“ Zahlungsdienste, so zum Beispiel PayPal. Es geht um die vertrauenswürdige Übertragung von Geldern von Absender zu Empfänger – allerdings ohne zentrale Dienstleister. Daher weisen Kryptowährungen auch grundsätzlich ähnliche Probleme wie klassische E-Zahlungssysteme auf.

Während die für Kryptowährungen überwiegend im Einsatz befindliche Blockchain Technologie aufgrund ihrer hohen Vernetzung und eines Transaktionsregisters mit allen historischen Geschäften relativ sicher ist, sind eine Reihe von Dienstleistern rund um den Handel und die Übertragung sowie die Verwahrung von Kryptowährungen im Einsatz, die sich denselben Risiken ausgesetzt sehen, wie andere Dienstleister der klassischen Finanzdienstleisterwelt (z.B. Banken).

Natürlich können auch Kunden einer traditionellen Bank oder eines Zahlungssystems Schwierigkeiten mit Cyber-Dieben bekommen. Dennoch besteht bei traditionellen Systemen manchmal die Möglichkeit, die Überweisung zu stornieren oder gar rückgängig zu machen. Im Falle der Kryptowährungen ist dieser Schritt allerdings nicht möglich: Was in der Blockchain passiert, bleibt in der Blockchain.
Kommt es bei der klassischen Bank jedoch zu einem Betrug, übernimmt nicht selten die Bank die entstandenen Schäden. Eine Schadensübernahme innerhalb der Kryptowährungen ist jedoch nicht gegeben, es gibt auch keine Entschädigungseinrichtung, wie sie im deutschen Bank- und Wertpapierwesen üblich ist. Allenfalls freiwillige und privatrechtliche Vereinbarungen bzw. Entschädigungen kann es geben.

Dies bedeutet:

**Wo immer Technik im Einsatz ist und es um Vermögensgegenwerte geht, sind Betrüger nicht weit!**

**Sichern Sie sich und Ihre Computerzugänge daher zu allererst gegen betrügerische Einfälle (Viren, Trojaner, Keylogger und andere Instrumente) ab! Da auch eingesetzte Virensoftware selber Einfallstor für jedwede Art von Schadsoftware sein kann, sollten Sie generell mindestens Grundinformationen über IT Sicherheit besitzen.**

**Leider gilt aber auch:**

**Die 100 %-ige Sicherheit gibt es nicht, weder online noch offline. Dessen müssen Sie sich jederzeit und absolut bewusst sein. Ansonsten laufen Sie Gefahr, dass Sie viel Geld – in virtueller oder realer Form – verlieren.**

# 1 Indirekte Risiken durch Dienstleistungspartner

Es gibt zudem auch Risiken, die Sie nicht selber managen können. Diese Risiken betreffen vor allem **Dienstleistungen Dritter**, die im Rahmen von Aktivitäten um Kryptowährungen von jedem Kunden benötigt werden. Diese Dritten könnten Einfallstore für Betrüger sein. Daher muss Ihnen bewusst sein, welche Risiken Sie mit welchen Dienstleistungspartnern eingehen.

## 1.1 Dienstleistungspartner

Als Dienstleistungspartner zu nennen sind beispielsweise:

- **Anbieter von Wallets**
- **Anbieter von Zahlungsdienstleistungen (auch „Exchanger“ genannt)**
- **Handelsplattformen**
- **Vermögensverwalter**

---

**TIPP**: Suchen Sie sich generell möglichst sichere Partner aus. Es kommt nicht immer nur darauf an, Gebühren zu sparen. Sicherheit kostet Geld – die der Anbieter investieren muss in Systeme, Überwachungen, Software. Werden Sie hellhörig, wenn es scheinbar deutlich günstiger geht als bei der Konkurrenz! Dann besteht das Risiko, dass an der Sicherheit gespart wird.

---

Befolgen Sie bitte grundsätzlich die nachbenannten Ratschläge, um Ihre Risiken prinzipiell zu minimieren:

### *1.1.1 Auswahl des Drittanbieters*

Der erste Punkt zum Thema Sicherheit ist die **Auswahl des Anbieters** über den Sie Ihre Aktivitäten abwickeln.

Diese Anbieter müssen vertrauenswürdig sein. Seien Sie sich aber auch darüber bewusst, dass jeder Anbieter Ziel von Hackern werden kann, ganz gleich wie gut und wie vorausschauend er ist.

Vertrauenswürdige Anbieter erkennen Sie häufig an:

- Möglichst aufsichtsrechtlicher Regulierung durch eine Behörde
- Guter Erreichbarkeit von Service und Support
- Sitz in einem Land mit hohem Rechtsschutz
- Häufig von Dritten genannter Partner im Internet (neutrale Foren usw.)*
- Eventuell existieren bereits Bewertungen zu dem Anbieter*
- Hohe Anzahl real existierender User
- Sonstige Versicherungen, Garantien, Entschädigungen im Schadensfall zu Ihren Gunsten

* ziehen Sie bei diesen Punkten bitte in Betracht, dass vermeintlich positive Bewertungen oder Kommentare auch als Werbemaßnahmen oder zur Betrugszwecken erstellt werden können!

### *1.1.2 Vorsicht vor Betrügern*

Bei manchen Anbietern sitzt das Sicherheitsrisiko nicht vor der Firewall, sondern dahinter. Bei diesen Anbietern handelt es sich dann um **SCAM**. Unter SCAM versteht man ein meist groß aufgezogenes Online-Betrugsszenario, das zum Ziel hat, Internet Nutzern reales oder virtuelles Geld zu stehlen. Dabei geht es weniger um direkte Angriffe auf die IT sondern darum, über gezielte psychologische Manipulation Internetnutzer zu schädigen.

Diese Anbieter wollen zum einen Daten abgreifen, die sie verkaufen und darüber hinaus das Geld der Anleger stehlen bzw. veruntreuen.

Um sich vor Online-Betrug zu schützen, helfen keine Programme oder technischen Hilfsmittel. Die Nutzer können sich nur auf sich selbst, ihr Wissen und ihren gesunden Menschenverstand verlassen.

Die Anbieter erkennt man zum Beispiel daran, wie aggressiv sie am Markt auftreten. Diese Betrüger benötigen hohe Reichweiten, um zu existieren. Zudem halten sie den Aufwand gering und nutzen automatisierte Übersetzungsprogramme.

Woran erkennt man betrügerische Anbieter häufig?

- geringe Sicherheit bzw. Verifizierung
- unbekannte Seite im Internet, das bedeutet auch wenig Presse
- wenige Informationen in seriösen Foren
- Hohe Boni bei Mitgliederwerbung
- undurchsichtiges Verdienstsystem
- bemerkenswert unprofessionelle Webseiten mit Rechtschreibfehlern
- Versprechen, die sich außergewöhnlich gut anhören.

Mit diesen Merkmalen lassen sich zwar nicht alle unseriösen Anbieter eliminieren, es ist aber ein Anfang und erstes Selektionskriterium.

Passen Sie zum Schutz vor Hackern auch besonders auf Ihre **Kommunikation** auf!

Sie sollten für jeden Anbieter (Handelsplattform usw.) eine **eigene E-Mail Adresse** einrichten. Mit dieser Maßnahme schützen Sie sich vor negativen Folgen eines Hackerangriffs bei dem Anbieter. Sollte nämlich ein Anbieter gehackt werden, ist das zwar schlimm, aber nicht so schädlich, weil er keinen Zugriff auf die anderen Anbieter hat. Aktivieren Sie hier auch, falls möglich, eine E-Mail-Benachrichtigung bzw. Freischaltung per E-Mail.

### *1.1.3 Keine öffentlichen Computer*

Melden Sie sich **niemals** mit sensiblen Informationen an einem **öffentlichen Computer** an. Diese Computer sind meist voll mit Schadsoftware, die nur darauf warten, dass Sie Ihre Daten eingeben. Nutzen Sie Ihren privaten Computer und sorgen Sie durch geeignete Maßnahmen für eine sichere Kommunikation. Halten Sie Ihre Betriebssoftware stets aktuell. Öffnen Sie keine unbekannten Dateien. Idealerweise führen Sie die Kommunikation zu Kryptodienstleistungen ausschließlich von einem Computer, auf dem sonst keine weiteren Programme oder Mailkommunikation laufen. Um generell Risiken zu vermeiden, loggen Sie sich immer sicher aus!

### *1.1.4 Nutzen Sie 2FA (Zwei-Faktor-Authentifizierung)*

Unter 2FA versteht man eine „Zwei-Faktor-Authentifizierung“. Dabei verlangen verschiedene Dienstleister im Rahmen ihres Services zusätzlich noch ein zweites Sicherheitsmerkmal. Damit haben Sie zum Beispiel auf Ihrem Handy eine App oder einen „Token“, welche regelmäßig Codes generieren. Diese Codes müssen Sie dann zusätzlich zu Ihrem Passwort bei der Identifizierung eingeben, damit Sie Zugriff erhalten.

### *1.1.5 Nutzen Sie sinnvolle Passwörter*

„123456“ oder „start“ sind ebenso wenig gute Passwörter wie Ihr Geburtsdatum. Nutzen Sie daher bitte **unbedingt komplexe Passwörter**!

Es gibt im Internet kostenlose Passwortgeneratoren mit denen Sie schnell und einfach komplexe Passwörter erstellen können. Allerdings birgt dies die Gefahr, dass diese Informationen auch gehacked oder mitverfolgt werden können. Idealerweise suchen Sie sich die Ihr Passwort selbst nach den nachfolgenden Faktoren aus:

„Komplex“ bedeutet, dass ein **Passwort** eine **Kombination** mit einer Reihe der folgenden Bestandteile enthält:

- **Großbuchstaben**
- **Kleinbuchstaben**
- **Zahlen**
- **Sonderzeichen**

Auch hier sollten Sie sicherstellen, für jeden Anbieter und jede E-Mail Adresse ein eigenes Passwort zu verwenden. Sie reduzieren damit die Wahrscheinlichkeit negativer Auswirkungen eines Ausspähens Ihres Passwortes nochmals erheblich. Des Weiteren sollten Sie die **Passwörter** auch **regelmäßig ändern**. Wir empfehlen Ihnen in solch sensiblen Bereichen die regelmäßige Änderung!

### *1.1.6 Schweigen ist Gold*

Oft denkt man immer, dass die Schwachstelle für einen Betrugsversuch ausschließlich bei dem gewählten Dienstleistungsanbieter liegt. Dies ist häufig aber eben nicht immer der Fall – oft ist die Schwachstelle der Nutzer selbst. Sorgloser Umgang mit Technik oder zu großes Mitteilungsbedürfnis sorgen für Risiken! Auch wenn man sich über Gewinne freut: **Erzählen Sie niemandem** von Ihren Kryptowährungen, von Ihren Accounts, von den E-Mail-Adressen, wo Sie die Passwörter aufbewahren und vor allem nicht, wie viel Kryptogeld auf diesen Accounts liegt.

Aufgrund des jungen Marktes gibt es regelmäßig neue Sicherheitsmechanismen (USB-Token, Ledger Speicher u.a.), die Sie ebenfalls für den Gebrauch von Kryptowährungen einsetzen können. Halten Sie sich informiert – **Sie sind Ihre eigene Bank** und tragen daher das Risiko, dass Ihre Bank Opfer eines „Bankraubes“ wird, jederzeit selbst!

### *1.1.7 Nutzer- und Bedienfehler*

Häufig sitzt die Fehlerquelle für Verluste vor dem eigenen Computer – es sind Sie selber, der mit falschen oder unbedachten Handlungen dafür sorgen kann, dass Werte verloren gehen.

Daher gilt: **Passen Sie** mit Ihren Angaben **bei Überträgen** von Kryptowährungen genau **auf**! Getätigte **Falschüberweisungen** können **nicht rückgängig** gemacht werden!
Folgen Sie keinen Werbelinks und recherchieren Sie vorab gut im Internet über potentielle Anbieter, mit denen Sie zusammen arbeiten wollen. Lassen Sie sich nicht von vermeintlich tollen Angeboten locken und **schalten Sie Ihren gesunden Menschenverstand ein**, indem Sie sich nicht von Gier leiten lassen.

## 1.2 technische Risiken

Auch wenn eine Webseite das Anbieters einen professionellen Eindruck macht und der Auftritt vertrauensvoll wirkt – dies ist keine Garantie dafür, dass die hinter der Webseite liegenden Technologien aktuell und damit risikobegrenzt sind. Die nachfolgenden Risiken liegen in der Regel außerhalb Ihres direkten Einflussgebietes bei Drittanbietern.

### *1.2.1 Risiko Hardware*

So wissen Sie nicht, welche **Qualität** die eingesetzte **Hardware des Anbieters** hat. Gerade die Qualität und die Dimensionierung der Hardware ist aber Garant dafür, dass eine hohe Anzahl von Transaktionen ausfallsicher durchgeführt werden kann. Ist dies nicht gegeben, so besteht das Risiko, dass Sie Aufträge nicht, nicht komplett oder nur mit hohen zeitlichen Verzögerungen platzieren können. In einem solchen Fall tragen Sie das Verlustrisiko aus zwischenzeitlichen Kursänderungen, die zwischen Ihrem eigentlich angedachten Handelszeitpunkt und dem tatsächlichen Handelszeitpunkt entstehen. Dies ist ein Totalverlustrisiko.

### *1.2.2 Risiko Software*

Die **eingesetzte Software** ist wesentlich **für** die **Betriebssicherheit** und den reibungslosen Ablauf verschiedener Transaktionen notwendig. Sollte die Software nicht aktuell gehalten werden, sollte die Software nicht vor Angriffen Dritter sicher gehalten werden oder sollte die Software z.B. durch Aktualisierungen fehlerhaft agieren, besteht das Risiko, dass Sie Aufträge nicht, nicht komplett oder nur mit hohen zeitlichen Verzögerungen platzieren können. In einem solchen Fall tragen Sie das Verlustrisiko aus zwischenzeitlichen Kursänderungen, die zwischen Ihrem eigentlich angedachten Handelszeitpunkt und dem tatsächlichen Handelszeitpunkt entstehen. Dies ist ein Totalverlustrisiko.

### *1.2.3 Risiko Leitungen*

Dienstleister benötigen für Ihre Arbeit **Leitungen ins Internet** oder zu Handelsplattformen. Dies können virtuelle Leitungen oder aber Standleitungen sein. Sollten diese Leitungen ausfallen oder nicht ausreichend für die zu sendenden Informationen dimensioniert sein, so besteht das Risiko, dass Sie Aufträge nicht, nicht komplett oder nur mit hohen zeitlichen Verzögerungen platzieren können. In einem solchen Fall tragen Sie das Verlustrisiko aus zwischenzeitlichen Kursänderungen, die zwischen Ihrem eigentlich angedachten Handelszeitpunkt und dem tatsächlichen Handelszeitpunkt entstehen. Dies ist ein Totalverlustrisiko.

### *1.2.4 Risiko Sicherheitstechnik*

Dienstleister können nur dann sicher agieren, wenn sie sich vor **Angriffe**n **Dritter** schützen. Ob ein Dienstleister seine Hard- und Softwaresysteme durch Firewalls, Überwachungslogiken oder auch andere geeignete Maßnahmen schützt, ist für Sie als Anleger nicht ersichtlich. Sie müssen daher darauf vertrauen, dass entsprechende Sicherheitsmaßnahmen ergriffen werden.
Auch indirekte technische Sicherheitsvorgaben bergen Risiken – so Zugangskontrollen zum Schutz vor unbefugten Eindringlingen in die Räumlichkeiten des Dienstleisters gehören hier zu. Falls solche Schutzmaßnahmen nicht oder nicht ausreichend oder nicht aktuell genug existieren, besteht für Sie ein **Diebstahlrisiko** mit der Möglichkeit eines Totalverlustes.

## 1.3 organisatorische Risiken

Die Branche der Kryptowährungsdienstleister steht in dem Ruf, hemdsärmelig und lax mit Sicherheitsbedenken und organisatorischen Strukturen umzugehen. **Mangelnde Organisation** erhöht für Sie als Anleger das Risiko, dass aufgrund von Fehlplanungen, Fehlorganisation oder nicht bedachter Sachverhalte Verluste erlitten werden. Zu den nachfolgenden Punkten können Sie Ihre Anlagen teilweise bis vollständig verlieren!

Zu **organisatorischen Risiken** auf Seiten der Anbieter gehören beispielsweise:

### *1.3.1 Personalrisiken*

Wichtige Personen, die für den Betrieb notwendig sind, können nicht beim Anbieter gehalten werden, so dass dies negative Auswirkungen auf Arbeitsabläufe und Betriebssicherheit des Anbieters hat.

Darüber hinaus besteht auch ein Diebstahlrisiko INNERHALB der Mitarbeiterschaft der Anbieter. Personen mit Kenntnissen über Sicherheitsstrukturen und Abwicklungspraktiken des Anbieters fällt es häufig leicht, Sicherheitsmaßnahmen – sofern überhaupt vorhanden – zu erkennen und zu umgehen. Der Diebstahl wichtiger Informationen ist damit nicht auszuschließen. Mit diesen wichtigen Informationen könnten sich solche betrügerischen Mitarbeiter Vorteile durch Diebstahl von Kryptowährungen von Anlegern verschaffen.

Der Dienstleister könnte zahlenmäßig nicht ausreichende und fachlich nicht (genügend) qualifizierte Mitarbeiter einsetzen. Der Anleger trägt damit das Risiko keine, keine ausreichende oder keine kompetente Ansprechperson bei dem Anbieter im Falle von Problemen oder Rückfragen zu haben.

### *1.3.2 Fehlendes Vier-Augen-Prinzip*

Bei bestimmten sicherheitsrelevanten Transaktionen kann es sein, dass der Dienstleister kein gegenseitiges Kontrollprinzip eingerichtet hat. Auch dies sorgt dafür, dass das Risiko betrügerischer Handlungen zu Lasten des Anlegers durch nicht ausreichend kontrollierte Mitarbeiter steigt.

### *1.3.3 Fehlende in- und externe Kontrollen*

Als nicht regulierter Bereich sparen sich womöglich Dienstleister die im regulierten Finanzbereich üblichen in- und externen Kontrollstellen. Diese Kontrollstellen sind beispielsweise eine interne Revision, eine Compliance oder eine Wirtschaftsprüfung.

### *1.3.4 Fehlende KYC Prüfung*

Da der Bereich der Dienstleistungen im Ausland keiner Regulierung unterliegt, verzichten Dienstleister häufig auf einen KYC Prozess. Von einem KYC (von **K**now**Y**our**C**ustomer bzw. Kunden-Legitimation) Prozess spricht man, wenn der Dienstleister die Identität des Kunden nach den Vorgaben einer Aufsichtsbehörde prüft. In Deutschland sind Finanzdienstleister und Banken zu einer entsprechenden Prüfung zur Verhinderung von Geldwäsche oder Terrorismusfinanzierung verpflichtet. Auch wenn Kryptowährungen angelegt sind, um staatlichen Einfluss zu verhindern, so dient dieser Prozess allen, um eine sinnvolle Technik von missbräuchlichen und kriminellen Zahlungsaktivitäten frei zu halten. Findet ein solcher KYC Prozess bei dem Anbieter nicht statt, so besteht das Risiko der Schließung durch eine Aufsicht oder den Gesetzgeber, der anschießenden Insolvenz und damit mit dem Risiko des Totalverlustes für den Anleger.

## 1.4 betriebswirtschaftliche Risiken

Wenn Sie einen Anbieter auswählen, wissen Sie häufig nichts über dessen finanzielle Möglichkeiten und das zur Verfügung stehende Haftungskapital. Sie kooperieren demnach mit einem Partner auf reiner Vertrauensbasis und tragen daher auch das Risiko, dass dieses Vertrauen in die finanziellen Fähigkeiten des Dienstleistungspartners enttäuscht wird.

So mussten schon eine Reihe von Dienstleistern, u.a. der ehemals größte Handelsdiensteister Mt. Gox, ohne Entschädigungen für die Anleger ihre Tätigkeiten einstellen.

Prüfen Sie daher vorab möglichst alle Informationen zu Ihrem Dienstleistungspartner, das beinhaltet neben der Frage der verantwortlichen Personen und des Sitzes der Gesellschaft auch eine Prüfung der Bilanzen oder sonstiger Angaben, die Ihnen ein Gefühl von der wirtschaftlichen Größe des Partners vermitteln.

Kommt das Partnerunternehmen in wirtschaftliche Schwierigkeiten z.B. durch einen der oben genannten Schadensfälle aufgrund Betrugs dritter Seiten, besteht die Gefahr, dass Sie als Anleger Ihre Kryptowährungen und damit Ihr angelegtes Vermögen teilweise oder komplett verlieren.

# 2 Spezielle Risiken bei der Vermögensverwaltung

Beauftragen Sie einen Vermögensverwalter mit der Umsetzung einer Anlagestrategie in Kryptowährungen, so tragen sie neben dem Risiko, dass die Anlagestrategie nicht wirksam ist, also Verluste erwirtschaftet, vor allem ein mit dem Vermögensverwalter verbundenes **operationelles Risiko**. Von operationellen Risiken wird gesprochen, wenn **Risiken außerhalb** typischer **unternehmerischer Risiken** auftreten.

Solche Risiken können sein:

- Organisatorische Schwachstellen
- Kommunikative Schwachstellen
- Schwachstellen in Kontrollmechanismen
- Fahrlässiges oder vorsätzliches „menschliches Versagen“
- Fehlerhafte Arbeitsanweisungen u.v.m.

Bei Auftreten solcher Risiken führt dies in der Regel zu hohen finanziellen Schäden – sowohl bei dem Dienstleister als auch gegebenenfalls bei den betroffenen Kunden.
Ein wesentliches Risiko bei der Vermögensverwaltung tritt aufgrund der besonderen technischen Konstruktion der Kryptowährungen auf. Bei einer klassischen Vermögensverwaltung eröffnet der Anleger bei einer Bank ein Konto und Depot. Auf dieses Konto und Depot hat der Vermögensverwalter nur insoweit Zugriff, als dass er Dispositionen, also Käufe und Verkäufe, zu Gunsten bzw. zu Lasten des Kundendepot und –kontos vornehmen darf. Die Abhebung von Geld oder die Möglichkeit, Wertpapierverkäufe zu eigenen Gunsten vorzunehmen, sind dem Vermögensverwalter nicht möglich.

Bei der Vermögensverwaltung in Kryptowährungen dagegen sieht der Grundsatz vor, dass der Vermögensverwalter für den Anleger entweder ein Wallet eröffnet und führt oder aber zumindest so führt, dass er Transaktionen, also den Kauf oder Verkauf verschiedener Kryptowährungen, durchführt. Dies setzt voraus, dass der Vermögensverwalter auch Zugriff auf die persönliche Wallet-Identifikation, den Private Key, hat. Die Eigentümerschaft eines Wallets wird durch den Private Key nachgewiesen. Hat ein Dritter diesen Key, so besteht die Möglichkeit, dass dieser Dritte über die kompletten Kryptowährungen verfügt und diese nicht verfolgbar auf eigene Wallets überträgt.

Bei der Einrichtung eines Wallets für den Kunden oder im weiteren Verlauf bei Transaktionen kann es vorkommen, dass Sicherheitsmechanismen des Vermögensverwalters umgangen werden. Sofern sich nur ein Mitarbeiter in den Besitz des Private Keys des Anlegers bringt, könnte er diese Informationen speichern und für den Diebstahl der betreuten Vermögen sorgen.

Darüber hinaus besteht das Risiko, dass die Aufbewahrung der Private Keys einzelner oder aller Anleger von Dritten – z.B. durch Einbruch oder durch betrügerische IT-Maßnahmen (Trojaner, Phishing, Viren o.ä.) – gestohlen werden. Auch in diesem Fall besteht das Risiko, dass die Gelder verloren sind. Daher besteht in diesem Punkt trotz aller organisatorischen Maßnahmen des Vermögensverwalters im Gegensatz zu einer klassischen Vermögensverwaltung ein Totalverlustrisiko.

# 3 Spezielle Risiken bei CFDs auf Kryptowährungen

Beim Handel mit CFDs in Kryptowährungen müssen Sie sich bewusst sein, dass diese Finanzinstrumente an nicht regulierten, dezentralen digitalen Handelsplätzen gehandelt werden.
Somit hängen die Preisbildung und die Kursbewegungen der Kryptowährungen allein von den internen Regeln der jeweiligen digitalen Börse ab, und diese Regeln können sich jederzeit und ohne Ankündigung ändern. Dies führt im Tagesverlauf oft zu sehr hohen Kursschwankungen bei den Kryptowährungen, die im Vergleich zu anderen Finanzinstrumenten deutlich höher ausfallen können.
Durch den Handel von CFDs in Kryptowährungen akzeptieren Sie deshalb ein deutlich höheres Risiko auf den Verlust Ihrer investierten Beträge, zu dem es innerhalb sehr kurzer Zeit aufgrund plötzlicher negativer Kursbewegungen bei den Kryptowährungen kommen kann.

CFD Anbieter leiten ihre Markt- und Kursdaten zu den Kryptowährungen von den digitalen, dezentralen Börsen ab, an denen die Kryptowährungen gehandelt werden. Aufgrund der fehlenden Regulierung solcher Börsen können die Marktdaten- und Kurs-Feeds, die von solchen Börsen bereitgestellt werden, den internen Regeln und Praktiken solcher Börsen unterliegen. Diese Regeln und Praktiken können sich deutlich von den Regeln und Praktiken, die von regulierten Börsen eingehalten werden, unterscheiden.

Insbesondere sollten Sie sich bewusst sein, dass die Regeln für die Preisbildung an den Kryptowährungsbörsen keiner Regulierungsaufsicht unterliegen und von der entsprechenden digitalen Börse nach eigenem Ermessen jederzeit geändert werden können. Ebenso können diese digitalen Börsen den Handel aussetzen, andere Maßnahmen ergreifen, die zu einer Aussetzung oder Einstellung des Handels an solchen Börsen führen können, oder der Kurs- und Marktdaten-Feed könnte dem Handelsanbieter kurzfristig oder längerfristig nicht mehr zur Verfügung stehen. Solche Faktoren können sich stark negativ auf die vom Anleger gehaltenen offenen Positionen auswirken und bis hin zum kompletten Verlust seiner gesamten investierten Beträge führen.

Wenn es zu einer zeitweiligen oder dauerhaften Störung oder Einstellung des Handels an einer digitalen Börse kommt, können CFD Anbieter ihre Bewertungslogiken einstellen, ändern und nur den letzten verfügbaren Kurs heranziehen. Es ist eventuell nicht möglich, gehaltene Positionen zu schließen, abzuwickeln oder Guthaben, das im Zusammenhang mit einer solchen Position steht, auszuzahlen, bis der Handel an der jeweiligen digitalen Börse – sofern überhaupt- wieder aufgenommen wird.

Der Anleger muss akzeptieren, dass es im Fall einer Wiederaufnahme des Handels an entweder der entsprechenden ursprünglichen digitalen Börse oder deren Nachfolgerbörse oder sogar einer alternativen neuen Börse zu einer deutlichen Kursdifferenz (Preisgapping) kommen kann. Dies kann sich auf den Wert der gehaltenen CFD-Positionen des Anlegers in der entsprechenden Kryptowährung auswirken und zu deutlichen Zuwächsen oder Verlusten führen. Falls der Handel nicht wieder aufgenommen wird, verliert der Anleger unter Umständen sein gesamtes Investment.

Sofern die Verpflichtung auf eine ausländische Währung oder Rechnungseinheit lautet oder das Konto in ausländischer Währung geführt wird, erhöht sich das Verlustrisiko nochmals um das Währungsrisiko.

Verluste, die der Anleger möglicherweise aufgrund des Handels von CFDs in Kryptowährungen erleidet, sind gegebenenfalls in Abhängigkeit des Sitzes des Handelspartners nicht durch die Schutzvorkehrungen, die im Rahmen des Einlagensicherungsfonds verfügbar sind, gedeckt.

Eine fehlende Regulierung des Handelspartners kann dazu führen, dass eventuell vom Anleger eingereichte Beschwerden oder eventuelle Streitigkeiten, die sich zwischen ihm und dem Handelspartner in Verbindung mit dem Handel von CFDs in Kryptowährungen ergeben könnten, nicht gültig sind und vom Ombudsmann oder einer anerkannten Schlichtungsstelle des Landes mangels Zuständigkeit zurückgewiesen werden.

Auch wenn in Deutschland ein Verbot der Nachschusspflicht für CFD-Produkte besteht, trägt der Anleger zumindest für sein eingesetztes Kapital in CFDs auf Kryptowährungen das Totalverlustrisiko. Aufgrund der starken Schwankungen in Kryptowährungen und der mit CFDs verbundenen Hebelung der Einsätze besteht das außerordentlich hohe Risiko eines Totalverlustes. Damit übersteigt das Risiko der Anlage in CFDs auf Kryptowährungen die ohnehin schon vorhandenen Risiken bei der Anlage in CFDs auf andere Produkte bei weitem. Seien Sie sich dieses enormen Risikos unbedingt bewusst und investieren Sie nur Beträge, deren Totalverlust Sie wirtschaftlich verkraften können!

**Verfügen Sie bitte über angemessene Rücklagen in anderen Anlagen, und investieren Sie nur einen überschaubaren Teil Ihres Vermögens, dessen Verlust Sie aushalten können, in Risikoanlagen!**

# 4 spezielle Risiken beim Handel mit Kryptowährungen

Im Folgenden führen wir weitere Risiken in Bezug auf den Handel von Kryptowährungen auf:

## 4.1 Schließung des Handelsplatzes

Wenn Plattformen etwa aufgrund technischer Probleme zusammenbrechen, verlieren Anleger regelmäßig ihr Geld. Besonders tückisch ist es, dass Tauschbörsen gerade bei Kurseinbrüchen oft vom Netz gehen, sodass viele Kryptowährungs-Inhaber in solchen Momenten keine Chance mehr haben, Verluste zu minimieren. Das Schließen von Handelsplätzen ist in der Vergangenheit bereits mehrfach vorgekommen und Nutzer hatten das Nachsehen.
Das – temporäre oder dauerhafte- Schließen von Handelsplätzen führt für den Anleger zu hohen Risiken bis hin zum Totalverlust. Dabei ist es gleichgültig, ob die Schließung aus Kapazitätsgründen, aus Gründen einer technischen Störung oder aus gesetzlichen Gründen wie ein angeordnetes Handelsverbot erfolgt.

## 4.2 Betrug und Diebstahl

Handels- und Tauschplattformen werden immer wieder Opfer von Hackerattacken, bei denen Interneträuber virtuelle Beute machen und die Kryptowährungs-Nutzer um ihre Investitionen prellen. Kommt es zu einem Diebstahl der zur Übertragung wichtigen Informationen, so können Betrüger auf die von der Plattform gehaltenen oder in Abwicklung befindlichen Kryptowährungen zugreifen und auf ihre eigenen Wallets übertragen. Damit trägt der Anleger bei einer solchen Handelsplattform das Totalverlustrisiko.

## 4.3 Übermittlungsrisiken

Für die Nutzung einer Handelsplattform ist es notwendig, dass der Anleger mit der Handelsplattform in Kontakt tritt, um einen Auftrag zu platzieren. Es kann sein, dass die Handelsplattform zwar erreichbar ist, aber der Anleger selber keinen Zugriff auf einen Internetzugang hat. In einem solchen Moment ist er grundsätzlich davon abgeschnitten, mit Aufträgen agieren zu können. Kommt es in einem solchen Zeitraum zu einer ungünstigen Kursentwicklung, so droht dem Anleger für seine Positionen ein Totalverlust.

## 4.4 Abwicklungsrisiken

Für die Abwicklung von Kryptowährungen gibt es kein standardisiertes Abwicklungsvorgehen. Ein allgemein gültiges Clearingsystem wie es an klassischen Börsen teilweise sogar länderübergreifend installiert ist, gibt es für Kryptowährungen nicht. Daher ist es häufig erforderlich, die Abwicklung über klassische Überweisungen durchzuführen. Dies ist sowohl zeitintensiv, kostenintensiv als auch risikobehaftet, da innerhalb des Überweisungsvorganges durch Phishing oder andere betrügerische Maßnahmen versucht werden kann, den Geldstrom abzufangen und umzuleiten.

Zudem kann ihr Vertragspartner bei Abschluss des Geschäftes eventuell nicht über die finanziellen Mittel verfügen, die dieser zur Begleichung der Transaktion benötigt. Je nach Handelsplatz und Handelsregeln kann es daher passieren, dass Ihre zunächst unter Vorbehalt stehende Transaktion endgültig storniert wird. Dabei spielt es keine Rolle, ob der

Handelspartner ein anderer Privatkunde ist oder aber ein von der Börse eingesetzter Market Maker, der auf eigene Rechnung und Risiko Kryptowährungen an- und verkauft.

Sobald die Handelsplattform Bestandteil der Abwicklung wird, z.B. weil dort Transaktionen über zentrale, der Handelsplattform zuzurechnende Wallets durchgeführt werden, tragen Sie zudem das Risiko, dass während der Abwicklungsphase die Handelsplattform in wirtschaftliche Schwierigkeiten und in die Insolvenz gerät. In einem solchen Fall wie auch in allen anderen genannten Fällen droht Ihnen als Anleger ein Totalverlustrisiko.

## 4.5 Glattstellungsrisiken

Aufgrund eines noch jungen Marktes von Kryptowährungen mit **hohen Volatilitäten** kann es sehr realistisch sein, dass in manchen Marktphasen **keine Marktliquidität** besteht. Das bedeutet, dass Sie für Ihren Verkauf keine Abnehmer oder nur auf einem niedrigeren Kursniveau finden. Umgekehrt kann es sein, dass Sie unbedingt Kryptowährungen erwerben wollen, Sie aber keinen Vertragspartner finden, der Ihnen die Kryptowährungen verkaufen oder allenfalls zu höheren Kursen verkaufen will. Auch ein Market Maker – sei es als Bestandteil der Handelsplatzorganisation oder auf freiwilliger Basis – kann seine Tätigkeit temporär oder dauerhaft einstellen.
**Sie finden** in solchen Fällen **keinen Kontrahenten** für Ihre Handelsaktivitäten. Sie tragen damit das Risiko, dass Sie Ihre Positionen nicht oder nicht zu den gewünschten Kursen handeln können. Damit verbunden ist ein Totalverlustrisiko, falls Sie vor einer Wertlosigkeit nicht verkaufen können.

## 4.6 Verwahrungsrisiken

Falls Sie die Kryptowährungen in einem eigenen Wallet verwahren, tragen Sie alle Risiken insbesondere des Diebstahls des Private Keys, mit denen die Eigentümerschaft der Kryptowährungen nachgewiesen wird. Ist dieser Private Key verloren, ist auch das verwahrte virtuelle Geld verloren. Selbst, wenn Ihnen der Private Key nicht gestohlen wurde und Sie haben ihn nur verloren oder vergessen, so können Sie auf die Kryptowährungen nicht mehr zugreifen.

Auch wenn Sie mit einer Handelsplattform kooperieren, so ist es nicht ausgeschlossen, dass diese Plattform eigene Wallets unterhält. Wenn Sie nach dem Erwerb von Kryptowährungen diese Wallets der Handelsplattform nutzen, tragen Sie das Risiko, dass die Verwahrmöglichkeit der Handelsplattform gekapert wird. Ein solcher Hackerangriff kann über technische Manipulationen ebenso erfolgen wie über menschliche Aktivitäten betrügerischer, eventuell sogar bewusst eingeschleuster, Mitarbeiter bei einer solchen Handelsplattform.

Im Gegensatz zu der Verwahrung von Wertpapieren, die in Deutschland eine Bankdienstleistung ist (Depotverwahrung) und die höchste aufsichtsrechtliche Regulierung beinhaltet, ist die Verwahrung der Finanzinstrumente derzeit regulierungsfrei für jeden Anbieter möglich. Damit fehlen die Qualitätsmerkmale der Bankregulierung für z.B. Aktien und Anleihen bei Kryptowährungen vollkommen. Hinzu kommt, dass Wertpapierbestände im Fall der Insolvenz einer Bank an die eigentlichen Depotinhaber herausgegeben werden müssen. Im Falle der Insolvenz eines Handelsplatzbetreibers mit eigenen Wallets besteht dieser Herausgabeanspruch der eigentlichen Kryptowährungsinhaber nicht. In einem solchen Fall besteht das Risiko, dass die dort verwalteten Kryptowährungsbestände des Anlegers verloren sind, er trägt also das Totalverlustrisiko.

Auf jeden Fall bestimmt sich die Vorgehensweise im Fall der **Insolvenz eines ausländischen Handelsplatzes nach den örtlichen Rechtsvorschriften**. Auch vor diesem Hintergrund kommt dem Sitz einer Handelsplattform eine wesentliche Bedeutung zu. Nicht rechtssichere Jurisdiktionen sollten daher möglichst gemieden werden.

---

**TIPP**: Bitte berücksichtigen Sie auch, dass gerade mit dem Wandel der gesellschaftlichen Strukturen in so genannten Schwellenländern -oder auch Emerging Markets genannt- oftmals tiefgreifende Veränderungen der jeweiligen Rechtsordnungen verbunden sind. Dies hat nicht nur konkreten (meist negativen) Einfluss auf die rechtliche Einordnung von Kryptowährungen in diesen Ländern sondern auch auf die Verfolgung und Durchsetzung möglicher Rechtsansprüche gegen z.B. Handelsplatzbetreiber in diesen Ländern.

---

# E Was Sie bei Geschäften in Kryptowährungen beachten sollten

Im folgenden Kapitel erläutern wir Ihnen, welche besonderen Umstände und Zusammenhänge bei der Erteilung von Kauf- und Verkaufsorders in Kryptowährungen bzw. in Derivate oder CFDs auf Kryptowährungen auftreten, die Sie beachten sollten.

Da es derzeit in Deutschland noch keine Futures und Optionen auf Kryptowährungen gibt, wird dieser Bereich derzeit noch nicht behandelt. Allerdings ein derartiger Handel in den USA im Dezember 2017 gestartet worden.

Daher konzentriert sich dieses Kapitel im Wesentlichen auf die bereits jetzt vorhandenen Produkte im CFD Handel sowie den direkten Handel von Kryptowährungen auf Handelsplätzen.

Bitte beachten Sie: Es gibt **derzeit keine Börse nach deutschen** oder europäischen **Standards** für Kryptowährungen. **Es fehlen** sowohl ein öffentlich-rechtlicher **Börsenbetreiber**, eine **Börsenaufsicht**, eine **Handelsüberwachung** als auch **Handelsregeln** einer Börsenordnung. Damit bestehen derzeit an keinem Handelsplatz auch nur annähernd analoge Sicherungsmechanismen für Marktteilnehmer oder für Handelskunden, wie sie im deutschen Börsenwesen vergleichbar wären.

Bei Aufträgen, die Sie an **ausländischen Handelsplätzen** erteilen, gelten die dortigen Rechtsvorschriften und privatrechtlichen Handelsregeln, die von Handelsplatzbetreiber zu Handelsplatzbetreiber unterschiedlich sein können. Es ist zu erwarten, dass selbst innerhalb eines Landes und Rechtsraums unterschiedliche Handelsregeln und Handelsbedingungen bestehen, so dass Sie Ihre Kenntnisse der Regeln und Usancen eines Handelsplatzes nicht zwangsläufig auf andere Handelsplätze desselben Landes übertragen können.

## 1 Geschäfte mit CFDs auf Kryptowährungen

CFDs sind bilateral Verträge zwischen Ihnen als Anleger und einem Vertragspartner auf der anderen Seite. Der englische Begriff „**C**ontract **f**or **d**ifference“ war namensgebend für das Produkt, welches auf Deutsch „Differenzkontrakt“ heißt. Ursprünglich stammt das Produkt aus England, da damit die dortigen Steuerregeln umgangen werden konnten. Im Gegensatz zu Aktiengeschäften fielen die als „Stempelsteuer“ genannten Steuern bei dem Verkauf von Aktien nicht an.

Was zunächst als Steuerwerkzeug etabliert wurde, hat sich in den letzten gut 15 Jahren zu einem eigenständigen Produktsegment entwickelt.

CFDs können Sie nicht nur bei ausländischen Brokern kaufen und verkaufen, seit einigen Jahren bieten auch etablierte deutsche Banken ihren Kunden eine Handelsmöglichkeit in CFDs an.

Aufgrund der Ausgestaltung der Produkte als Derivate mit teilweise sehr hoher Hebelwirkung sorgt das Produkt gerade bei unerfahrenen Anlegern, die dadurch angelockt werden, dass sie mit nur niedrigem finanziellem Aufwand hohe Gewinne erzielen können, für großes Interesse. Auf die mit der Hebelwirkung verbundenen Risiken bis hin zum Totalverlust hatten wir Sie bereits hingewiesen, wollen dies aber an dieser Stelle nochmals ausdrücklich wiederholen.

Das extreme Risiko **kann** grundsätzlich **zu** einer **Nachschusspflicht führen**, d.h. der Anleger muss bei ungünstiger Kursentwicklung im Extremfall weitere Gelder über seinen Handelspreis hinaus einschießen bzw. nachliefern. Die deutsche Finanzaufsicht hat es Anbietern von CFDs verboten, von deutschen Anlegern eine Nachschusspflicht über das eingesetzte Kapital hinaus zu verlangen. Damit ist der maximale Verlust auf das eingesetzte Kapital begrenzt. Der **Anleger trägt** jedoch ein **Totalverlustrisiko** auf das eingesetzte Kapital.

## 1.1 Handel

Aufträge zum Handel von CFDs können Sie Ihrem Broker oder Ihrer Bank – sofern diese das Produkt CFD im Handelsangebot hat – über Online-Mechanismen oder auch telefonisch erteilen.

Der **Handel von CFDs** in Deutschland findet **an keiner Börse** statt, sondern wird als **bilateraler Vertrag zwischen Ihnen und** einem vorher benannten **Handelspartner** abgeschlossen. Daher bieten die beauftragten Broker oder Banken Ihnen in der Regel eine eigene Handelssoftware oder aber den Zugang zu einer Handelssoftware an, über die mit dem CFD-Anbieter kommuniziert wird.

Über diese Plattform können Sie Kauf- und Verkaufsorders erteilen. Ob und wenn ja in welchen Zeiten Sie Zugang zu der Ordererteilungsmöglichkeit haben, hängt von dem jeweiligen Bank- und Brokerpartner ab. Unabhängig von der Frage, ob und wann Sie Orders über das System der Bank erteilen können, beschränkt sich Ihre tatsächliche Handelsmöglichkeit auf den Zeitraum, in dem Ihr Handelskontrahent Ihnen als Handelspartner zur Verfügung steht. Häufig ist dies abhängig von einzelnen Assetklassen, auf die sich die CFDs beziehen.

So findet der Handel in Währungen häufig 7 Tage in der Woche an jeweils 24 Stunden statt, andere Wertpapiere dagegen werden Ihnen nur zu den originären Handelszeiten dieser Wertpapiere an ihrer Heimatbörse zum Handel angeboten.
Ähnlich verhält es sich bei Kryptowährungen. Hier referenzieren CFD-Anbieter bei ihrer Preisgestaltung auf Referenzhandelsplätze. Sind diese Referenzhandelsplätze jedoch geschlossen oder bieten dem CFD Anbieter außerhalb ihrer Kernhandelszeiten keine ausreichende Markt- und Handelsliquidität, besteht für Sie als Anleger keine Handelsmöglichkeit. Die **Handelszeit verschiedener Produkte kann** daher selbst bei einem Anbieter **variieren**.

Da unterschiedliche CFD Anbieter auf unterschiedliche Referenzhandelsplätze zugreifen, kann über die Handelszeit keine generelle Aussage getroffen werden. Dies ist demnach von CFD-Anbieter zu CFD-Anbieter individuell verschieden und muss vor der Beauftragung dieses Handelspartners auf Übereinstimmung mit Ihren Handelszeitenwünschen abgeglichen werden.

Die CFD Anbieter organisieren ihre Handelsregeln individuell und selbständig. Daher kann es möglich sein, dass vor dem Handelsbeginn noch eine **Orientierungsphase** für Sie als Anleger vor Aufnahme des Handels besteht. Diese **Pre-Trading Phase** ermöglicht es Ihnen in der Regel, einen Eindruck von der Marktlage zu erhalten, da die Anbieter meist indikative Quotes, also An- und Verkaufsangebote, veröffentlichen. Während der Pre-Trading Phase können Sie als Anleger nicht direkt handeln!

CFD Anbieter schließen daran häufig eine **Opening Phase** (Eröffnungs-Zeitfenster) an. Im Gegensatz zu klassischen Börsen, die diese **Eröffnungsphase** dazu nutzen, für bestehende Orderungleichgewichte (zu viele Verkäufer bei zu wenigen Käufern oder zu viele Käufer

ohne ausreichende Verkäufer) dem Markt ausreichend Zeit zu geben, diese Verschiebungen durch das Einstellen von Orders auszugleichen, sorgt diese Opening Phase des CFD Anbieters häufig nur für einen Handelsstopp, bis die Opening Phase an der jeweiligen Heimatbörse des betroffenen Wertpapieres beendet ist.

Danach beginnt dann auch bei dem CFD Anbieter grundsätzlich die reguläre und übliche Handelszeit, in der Sie als Kunde fortlaufend CFDs gegen Ihren Handelskontrahenten handeln können. Diese Phase wird auch **Trade Phase** oder **fortlaufende Handelszeit** genannt.

Während all dieser Phasen können Sie üblicherweise Orders erteilen, streichen oder hinsichtlich Stückzahl, Limit oder Gültigkeit ändern. Zu einer **Ausführung** Ihrer im Markt befindlichen Orders kann es aber **nur innerhalb** der **Trade Phase** kommen.

Vereinzelt bieten CFD Broker noch eine **Post-Trading Phase**, auch **Nachhandelszeit** genannt, an. In dieser Zeit können wiederum keine Geschäfte mehr getätigt werden, es können aber bereits für den Folgetag Orders eingegeben werden. Danach werden die Systeme häufig für einzelne Assetklassen bis zum erneuten Start komplett gesperrt, hier ist dann Ihrerseits keine Aktion mehr möglich.

---

**TIPP:** Bitte beachten Sie: Das Einstellen von Orders **nach Handelsende** ist mit großen Risiken verbunden. In einem ohnehin hoch spekulativen Produkt, welches massive Hebelrisiken beinhaltet, ist es ein weiteres Risiko, dass Sie auf Nachrichten und Bewegungen, die sich bis zum Handelsstart des Folgetages ergeben, nicht mehr reagieren können. Selbst wenn es Ihnen theoretisch möglich wäre, am Folgetag vor Handelseröffnung in der Pre-Trading Phase Orders zu löschen, so besteht das Risiko, dass Sie aus den verschiedensten Gründen (persönliche Gründe, technische Gründe etc.) entgegen Ihrer Erwartung keinen Zugriff mehr aus das System erhalten. Wir empfehlen Ihnen daher ausdrücklich, nur Orders in dem Moment einzustellen, wo Sie sich zu einer Aktion entscheiden. Ebenso raten wir Ihnen, dass Sie sich aktiv um Ihre Position bis zur Schließung derselben kümmern und nicht zwischenzeitlich abwesend sind.

---

## 1.2 Auftragsarten

CFD Anbieter gestatten Ihnen systematisch grundsätzlich die selben Auftragsarten, die Sie auch an vielen normalen Börsen gewohnt sind. Da diese Anbieter jedoch mit eigenen Systemen arbeiten, offeriert man Ihnen als Kunden häufig noch zusätzliche Ordermöglichkeiten, die in klassischen, regulierten Wertpapierbörsen nicht möglich sind.

Prinzipiell stehen Ihnen die folgenden Auftragsarten zur Verfügung:

- unlimitierte Orders
- limitierte Orders
- Stop-Orders

### *1.2.1 Unlimitierter Auftrag*

Ein Auftrag, der sofort ausgeführt werden soll sowie den nächstmöglichen und bestmöglichen Preis erzielen soll, wird als **unlimitierter Auftrag** oder **„market" Order** bezeichnet. Orders können auch noch mit einem Gültigkeitshinweis versehen werden, in liquiden Märkten sind diese Gültigkeitshinweise grundsätzlich jedoch nicht notwendig.

---

**TIPP**: Wir empfehlen Ihnen jedoch grundsätzlich, keine unlimitierten Orders im CFD Bereich zu erteilen. Es ist nicht auszuschließen, dass Ihr Handelspartner temporär und längerfristig keine Preise stellt, die Handelsspreads verbreitert werden oder technische Störungen auftreten. Wenn Sie unlimitierte Orders erteilen, kann es passieren, dass der bestmögliche Preis zum Handelszeitpunkt dann ein ganz anderer Preis ist, als Sie zum Zeitpunkt der Ordererteilung vermutet haben. Noch risikoreicher wird es für Sie, sofern Sie unlimitierte Orders mit einer theoretisch längeren Gültigkeit laut der nachfolgenden Erklärung versehen.

---

Mögliche **Gültigkeitsvorgaben** Ihrerseits sind:

- **Order gültig bis auf Widerruf / gtc (Good Till Cancelled)**

Eine gtc Order ist ein Auftrag, der solange gültig ist, bis Sie als Kunde ihn zurückziehen, also widerrufen. Wird der Auftrag nicht ausgeführt, behält er demnach so lange Gültigkeit, bis Sie ihn explizit wieder streichen. Wie lange die längste Laufzeit der Order sein kann, ist abhängig von Ihrem CFD Anbieter, in der Regel sind die Orders zeitlich begrenzt bis

a) Laufzeitende eines CFD-Kontrakts, sofern es keine open end / unbegrenzten CFDs sind
b) bis zum Jahresende oder
c) bis maximal 1 Jahr nach Orderaufgabe

- **Order gültig bis zu einem bestimmten Tag / gtc (Good Till Date)**

Eine gtd Order ist ein Auftrag, der so lange gültig ist, bis der Tag erreicht ist, den Sie vorgegeben haben. Mit Ablauf des von Ihnen angegebenen Datums erlischt Ihre Order automatisch, ohne dass Sie noch einmal aktiv werden müssen, sofern die Order nicht vorher ausgeführt wurde.

Grundsätzlich gilt:

**Unlimitierte Orders ohne** eine explizite **Gültigkeitsvorgabe** Ihrerseits **sind nur** für den jeweiligen **Ordererteilungstag gültig**. Kommt es an diesem Tag nicht zu einer Ausführung, so wird Ihr Auftrag automatisch gelöscht.

### *1.2.2 Limitierter Auftrag*

Von einem limiterten Auftrag spricht man, wenn Sie Ihrer Order ein **Preislimit** mitgeben. Im Fall der **Kauforder** ist dies der **maximale Preis**, den Sie bereit sind zu bezahlen. Im Fall einer **Verkaufsorder** entspricht Ihr Limit dem **Mindestpreis**, den Sie erzielen wollen. Können Sie günstiger erwerben oder teurer verkaufen, so erhalten Sie den für Sie besseren Preis. Ihr Limit ist daher nur eine Obergrenze zum Schutz davor, dass Sie bei Marktstörungen, bei verbreiterten Spreads, Handelsstops oder so genannten Flashtrades –

hier spricht man von irrationalen oder nachrichtlich ausgelösten extremen Kursschwankungen innerhalb einer kurzen Zeitspanne – vor unerwarteten Handelspreisen geschützt sind.

**Ohne** weitere Angaben zur **Gültigkeit sind** auch **limitierte Orders** grundsätzlich nur am Tag der Orderaufgabe gültig (**tagesgültig**).

Darüber hinaus können auch limitierte Orders mit zusätzlichen Gültigkeitsangaben, hier Orders **gtc** und **gtd** (siehe unter 1.2.1 / unlimitierte Orders) versehen werden.

Bei **limitierten Orders** können Sie zudem **Vorgaben** hinsichtlich des **Umfang**es der gewünschten **Orderausführung** machen:

- **„ganz oder gar nicht" Order / fok (Fill Or Kill)**

Bei dieser Form des limitierten Auftrags möchten Sie, dass Ihre **Order sofort und** dann auch nur **mit** der von Ihnen **gewünschten Stückzahl komplett ausgeführt** wird. Ist das nicht möglich, wird Ihre Order gar nicht ausgeführt.

- **„sofort oder löschen" Order / ioc (Immediate Or Cancel)**

Bei dieser Form des limitierten Auftrages möchten Sie, dass Ihre Order sofort bis zu der von Ihnen vorgegebenen Maximalstückzahl ausgeführt wird. Sie akzeptieren dann auch Teilstückzahlen auf Ihre Order, nehmen also das, was Sie in dem Moment an Stückzahl erzielen können. Die restliche Order über den nicht ausgeführten Teil der gewünschten Stückzahl wird dann umgehend gelöscht.

### *1.2.3 Stop-Orders*

Eine Stop-Order dient der Absicherung von Positionen oder dem bewussten Eingehen von Positionen ab Erreichen eines bestimmten Kursniveaus.

Es wird dabei zwischen der Kauf- und Verkaufsseite unterschieden, zudem gibt es zwei Arten von Stop-Orders. Bei **Kauforders** spricht man von einer **Stop-Buy** Order, bei **Verkaufsorders** dagegen von **Stop-Sell** Orders. Die Funktionslogik ist jedoch einheitlich: Eine Stop-Order wird Ihrerseits mit einem so genannten **Stop-Limit** versehen, Ihre Order ist dann zwar gültig, jedoch **nur inaktiv** im Markt.
Wird während des Handels in dem Ihre Order betreffenden Produkt der von Ihnen als Stop-Limit angegebene Preis erreicht (auch **„Trigger"-Preis** oder Auslösungspreis genannt), so wird Ihre **Order aktiviert** und damit **aktiv** im Markt.

Es wird zwischen zwei Arten der Stop-Orders unterschieden:

- **Stop-Order unlimitiert**

In diesem Fall wird Ihre Stop Order mit Erreichen des Trigger Preises aktiviert und automatisch zu einer unlimitierten Order.

**TIPP:** Durch diese Funktionsweise ist nicht garantiert, dass Sie als Ausführungspreis auch den von Ihnen vorgegebenen Trigger-Preis erhalten. Sie erhalten grundsätzlich den nächsten Preis, der nach dem Trigger-Preis erzielbar ist. Dieser Preis nach der Auslösung kann aber ganz anders sein als der Preis, den Sie als Auslösungspreis angegeben haben. Gerade, wenn eine psychologische wichtige Marke als Auslösungslimit vorgegeben wurde (z.B. eine glatte 100er Zahl wie 200 Euro), ist davon auszugehen, dass viele Marktteilnehmer gleichlautende Stop-Limite erteilt haben. In diesem Fall erzeugen viele Stop-Limite einen starken Druck auf den Markt und der nächste Kurs weicht wegen hoher Stückzahlen deutlich vom Auslösungslimit ab. Setzen Sie daher keine Stop-Limite bei „runden" Zahlen.

- **Stop-Limit Order**

Eine Stop-Limit Order enthält zwei Limite, die Sie vorgeben müssen. Neben dem Auslösungslimit (Trigger-Limit) gibt man noch ein normales Limit ein. Das zweite Limit fungiert dann analog zu einer limitierten Order an der Börse. Das bedeutet: Ihre Order ist zunächst bis zum Erreichen des Trigger-Preises inaktiv und wird dann aktiviert. Aber anstatt dass Ihre Order damit als eine unlimitierte Order aktiv wird, wird Sie mit dem zweiten von Ihnen vorgegebenen Limit in den Markt eingestellt.

Dies hat zwar den Vorteil, dass Sie kein Risiko unkalkulierbarer Preisänderungen nach dem Auslösungslimit tragen. Allerdings hat dies den Nachteil, dass Sie sich nicht sicher sein können, dass Sie damit auch eine Änderung Ihrer gehaltenen Position erreichen. Wird Ihr zweites Limit nicht erreicht, so behalten Sie Ihre ursprüngliche Position nämlich bei, bis Ihr Limit erreicht wird.

Gerade vor dem Hintergrund eines eigentlich erhofften Verlustschutzes kann daher eine Stop-Limit Order risikoreich sein, wenn man nicht weiß, welchen Verkaufspreis man wirklich erzielt.

**Funktionsbeispiel:**

Sie haben CFDs in der Gattung Siemens über 100 Stück.
Der Börsenkurs ist 150 Euro. Bei Unterschreiten der Marke von 145 Euro für die Siemens Aktie rechnen Sie damit, dass ein Abwärtstrend eingeläutet ist. Um sich vor fortlaufenden Verlusten innerhalb des Abwärtstrendes zu schützen, erteilen Sie eine Stop-Order und geben als Auslösungslimit den Preis von 145 Euro mit.

Bei einer normalen Limit Order würde Ihre Order sofort ausgeführt, da der Börsenkurs bei 150 Euro liegt und Sie nur 145 Euro mindestens erzielen wollen. Die Stop-Order bleibt aber inaktiv und schlummert.
Steigt der Börsenkurs von Siemens weiter an, freut Sie das als Anleger, es gibt für Sie erst einmal keinen Grund für eine Aktivität. Die Stop-Order schlummert weiter im Hintergrund.
Falls der Kurs aber doch auf 145 Euro fallen sollte, greift Ihr Stop-Limit, wird also „getriggert". Damit wird also Ihre Order nach dem Erreichen des Kurses von 145 als unlimitierte Order aktiviert.
Nach dem Kurs von 145 ist der nächste Preis 144 Euro. Zu diesem nächsten Preis von 144 Euro wird daher Ihre Order ausgeführt.

### *1.2.4 Ordersonderformen*

Es gibt eine Reihe von Ordersonderformen, die Ihnen individuell von Ihrem CFD Broker angeboten werden können. Dabei kann hier aufgrund der Individualität keine Aussage getroffen werden, dass Ihr Broker diese Sonderformen auch anbietet. Ebenso kann an der Stelle keine Vollständigkeit der Ordersonderformen garantiert werden. Informieren Sie sich daher bitte unbedingt im Vorfeld, welche Ordertypen Ihr Broker noch anbietet und welche Funktionsweisen damit verbunden sind!

Exemplarisch für Sonderformen der Orders seien daher benannt:

- **Trailing Orders**

Börsen arbeiten in Trends. Anleger wollen häufig von einem Trend möglichst langfristig profitieren. Wenn sich Börsenkurse aber bewegen, müssten Sie permanent ihre Orders anpassen. Daher bieten verschiedene CFD Broker Trailing Orders an. Bei diesen Orders ziehen die ursprünglich von Ihnen erteilten Limite in einem bestimmten vorher festgelegten Verhältnis immer und automatisch mit, ohne dass Sie manuell aktiv werden müssen.

Bitte rufen Sie sich das vorherige Beispiel von Siemens in Erinnerung. Dort lag der Börsenkurs bei 150 Euro und Ihr Stop-Limit bei 145 Euro. Bei einer Trailing Order geben Sie nun vor, dass sie bei einem Kursanstieg von Siemens um 5 Euro auch Ihr Stop-Limit um 5 Euro erhöht. Das bedeutet: Erreicht der Börsenkurs von Siemens 155 Euro, passt sich Ihr Stop-Limit automatisch von 145 auf 150 Euro nach oben an. Sie können daher von Kursanstiegen theoretisch unendlich profitieren, ohne zu früh verkauft zu haben. Erst wenn der Aufwärtstrend bricht und die Kurse fallen, greift Ihr Stop-Limit.
Broker können Ihnen statt absoluten Euro-Werten für die Limitänderungen auch Prozentzahlen anbieten. Daher lautet dann Ihre Vorgabe: Steigt der Kurs um x%, ziehe mein Limit ebenfalls um x% nach.

- **oco-Orders (One cancels the Other)**

Bei dieser Form von Orders erteilt der Anleger direkt zwei, sich aber gegenseitig bedingende Orders. Es kommt nur die Order zur Ausführung, deren Limit zuerst erreicht ist.

Auch hier ist der Grundgedanke, dass der Anleger zwar Kursanstiege erwartet, er aber gleichzeitig vor Kursverlusten geschützt sein möchte.
Er erteilt daher z.B. zwei gleichzeitige Verkaufslimite, eines davon für den Fall, dass sein Kursziel für die Anlege erreicht ist, das andere Verkaufslimit jedoch für den Fall, dass seine Meinung falsch ist und der Kurs fällt. In diesem Fall möchte er seine CFDs gerne auch zu einem niedrigeren Kurs verkaufen.
Wenn eine der beiden Orders ausgeführt wird, wird der zweite Bestandteil der Order automatisch gelöscht. Es kann also nur entweder der eine oder der andere Orderbestandteil ausgeführt werden.

Auch hier bedienen wir uns wieder des Siemens-Beispiels:

Der Anleger hat die Siemens CFDs zum aktuellen Kurs von 150 erworben und erwartet, dass der Kurs auf 160 Euro steigt. Gleichzeitig sorgt er sich davor, dass der Kurs nachhaltig fallen könnte, wenn er unter 145 Euro rutscht. Daher erteilt er eine oco-Order zum Verkauf seines Bestands mit folgenden Parametern: 160 und 145 Euro.
Steigt der Kurs nun auf 160 Euro, bevor er die 145 Euro erreicht hat, wird sein Verkauf bei 160 Euro ausgeführt. Da sein Bestand ja nun verkauft ist, wird automatisch der zweite Orderbestandteil über den Verkauf zu 145 Euro gelöscht.

Fällt der Kurs während der Ordergültigkeit dagegen zuerst auf 145 Euro, ohne dass vorher der Kurs von 160 Euro erreicht wäre, wird der Orderbestandteil im Verkauf zu 145 Euro ausgelöst. Der zweite Orderteil zu 160 Euro wird dann gestrichen.

**Beide Formen bieten Ihnen als Anleger weitere Schutzmechanismen, um Sie vor fortlaufenden Verlusten im Falle einer Fehlinterpretation der Marktentwicklung zu bewahren.**

---

**TIPP:** Nutzen Sie gerade bei CFDs als Produkte mit Hebelwirkungen konsequent die Möglichkeiten, Ihre Positionen zu schützen. Die konsequente Anwendung von Stop-Orders ist unbedingt notwendig, damit Ihr eingesetztes Kapital nicht verloren ist.

---

### *1.2.5 Preisermittlung bei CFDs*

Bei Preisen in CFDs handelt es sich nicht um Börsenpreise sondern um zivilrechtlich zwischen Ihnen und Ihrem Broker vereinbarte Preise. Es gibt keine Handelsüberwachung im Sinne einer stattlichen Überwachung. Ebenfalls gibt es keine Börsenaufsicht. Alle Sicherungsmaßnahmen bzw. Handelsregeln sind in der Regel privatrechtlicher oder freiwilliger Natur. Meist überwachen interne (Compliance-) Abteilungen das ordnungsgemäße Zustandekommen von Handelskontrakten zwischen Ihnen und Ihrem Broker. Dies sind interne Abteilungen Ihres Brokers, deren Mitarbeiter von dem Broker bezahlt werden. Ob und wenn ja in welchem Umfang diese Compliance Abteilungen dieselben Tätigkeiten mit derselben Effektivität durchführen wie eine staatliche Handelsüberwachung muss bezweifelt werden.

Der Handel zwischen Ihnen und dem Market Maker kommt durch Angebot und Annahme zustande. Meist übermittelt der Broker indikative An- und Verkaufspreise über sein System, zu welchem Sie als Kunde Zugang erhalten. Wenn Sie eine Order aufgrund dieser Preisinformation erteilen, wird dies als Angebot Ihrerseits gewertet. Der Broker kann sich dann entscheiden, ob er dieses Angebot annimmt oder nicht.

Kommt es zur Annahme des Angebotes, wird automatisiert ein Vertrag zwischen Ihnen abgeschlossen. Der Vertrag sieht vor, dass sich beide Handelsteilnehmer, also Sie als Anleger und der Market Maker einen täglichen Ausgleich der erzielten Kursunterschiede gewähren. Sie erhalten also nicht das jeweilige Wertpapier sondern nur einen Differenzanspruch.

Die Funktionsweise sei noch einmal am Beispiel von Siemens dargelegt:
Sie kaufen Siemens zu einem Kurs von 150 als CFD über 1.000 Stück. Am Ende des Tages liegt der Kurs bei 149,50 Euro. Dies bedeutet einen Verlust von 0,50 Euro je Aktie für Sie. Da sie ein CFD über 1.000 Aktien abgeschlossen haben, beläuft sich der gesammelte Verlust auf 0,50 Euro x 1.000 Aktien, demnach 500 Euro. Der mit dem Broker geschlossene Vertrag auf Differenzausgleich verpflichtet Sie nun, die Differenz dem Broker auszugleichen. Diesen Betrag von 500 Euro belastet der CFD Broker daher nun Ihrem Konto.

Am Folgetag steigt der Kurs auf 151 Euro. Dies ist ein Kursunterschied von 1,50 Euro je Aktie. Nun ist der Broker Ihnen gegenüber zum Ausgleich dieser Differenz verpflichtet und schreibt Ihrem Konto 150 Euro x 1.000 Aktien, demnach 1.500 Euro gut.

Sie haben damit nicht nur die Belastung über 500 Euro vom Vortag ausgeglichen sondern zudem noch einen weiteren Ertrag erzielt.

### *1.2.6 Hebeleffekt*

In diesem Zusammenhang ist noch einmal wichtig, Sie auf den **Hebeleffekt** und die damit verbundenen **dramatischen Risiken** bis hin zum **Totalverlust** Ihres eingesetzten Kapitals hinzuweisen. Normalerweise müssten Sie zum Erwerb von 1.000 Aktien der Siemens AG bei einem Preis von 150 Euro je Aktie den Betrag von 150.000 Euro aufwenden.
Bei CFDs ist vereinbarungsgemäß nur eine Anzahlung notwendig. Der CFD Broker verlangt – in Abhängigkeit des CFD Produktes – teilweise nur Anzahlungen von 1% des ausmachenden Betrages.

Im konkreten Fall würde dies bedeutet:
Auf die eigentliche Investitionssumme von 150.000 Euro für 1.000 Aktien Siemens mit Preis von 150 Euro müssten Sie nur 1% oder 1.500 Euro als Anzahlung leisten.

Im vorgenannten Beispiel würden Sie bei einem Verlust von 500 Euro zum ersten Handelstag bereits 33,33% oder ein Drittel Ihres Einsatzes verloren haben.
Mit dem Kursgewinn des Folgetages würden Sie zu Ihrem Einsatz von 1.500 Euro noch den Gewinn von 1.000 hinzu gebucht erhalten. Dies entspräche auf den Einsatz von 1.500 Euro einem Gewinn von 66,66% oder zwei Dritteln des eingesetzten Kapitals.

Diese Relationen sollen Ihnen vor allem vor Augen führen, wie schnell und mit welcher dramatischen Art sich bereits kleine Kursunterschiede auf Ihr eingesetztes Kapital auswirken. Gerade in Kombination mit den massiven Volatilitäten in Kryptowährungen, also den teilweise massiven untertägigen Kursschwankungen von bis zu 25%, ist dieses Totalverlustrisiko kein theoretisches sondern ein sehr realistisches und valides Risiko!

# 2 Geschäfte an Handelsplätzen für Kryptowährungen

Aufträge zum Kauf oder Verkauf von Kryptowährungen können Sie nicht über Ihre Bank erteilen. Vielmehr benötigen Sie einen Internetzugang mit Leitungszugang (LAN, WLAN, UMTS oder anderen Techniken) und eine direkte Verbindung zu einer Handelsplattform, über die Sie Ihre Kryptowährungen kaufen und verkaufen wollen. Ebenso benötigen Sie mindestens bei der Handelsplattform eine elektronische Geldbörse, ein Wallet, um Ihre Währungen eingebucht zu bekommen.

Es gibt an diesen Handelsplattformen grundsätzlich keine unterschiedlichen Marktsegmente, die Funktionsweisen und Handelsregeln gelten in der Regel produktübergreifend über alle Handelsprodukte gleichermaßen. Manche Handelsplätze bieten nur den Handel in Bitcoin, der Erst- und Leitwährung innerhalb der Kryptowährungen an. Andere wiederum bieten zudem den Handel in anderen Kryptowährungen an. Zum Zeitpunkt der Auflage dieser Basisinformationen werden 1.300 Kryptowährungen an Handelsplätzen weltweit gehandelt.

## 2.1 Handel

Der Handel an den Handelsplätzen ist nicht einheitlich geregelt. Stattdessen gibt es eine Reihe von unterschiedlichen Herangehensweisen mit unterschiedlichen Verhaltensweisen:

### *2.1.1 Vermittlung*

Manche Handelsplatzbetreiber vermitteln ausschließlich zwischen Käufern und Verkäufern. Sollten keine Orders dritter Käufer oder Verkäufer vorliegen, so können Sie für Ihre Orders dann eventuell keine Kontrahenten finden. Juristisch ist Ihr Handelskontrahent dann eine andere Privatperson, die Sie jedoch nicht direkt kennen. Sie können daher weder feststellen, wer dieser Kontrahent ist, noch ob dieser lautere Absichten hat oder Bestandteil eines kriminellen Geldwäscherings. Ebenso können Sie keine Bonitätsprüfung dieses Handelskontrahenten vornehmen. Sie müssen sich daher darauf verlassen, dass die Sicherungsmaßnahmen der Handelsplattform greifen.

### *2.1.2 Market Making*

Der Handelsplatzbetreiber agiert selber oder aber eine dritte Person oder Firma als Market Maker. Ein Market Maker stellt auf eigenes Risiko und eigene Rechnung An- und Verkaufspreise in Kryptowährungen und erwartet sich aus der Differenz zwischen An- und Verkaufsaktionen einen Ertrag. Das Risiko auf Ihrer Seite liegt darin, dass der Market Maker die Geschäfte mit Ihnen nicht mehr erfüllen kann und der Handel damit effektiv nicht mehr abgewickelt werden kann. Sie sind nicht in der Lage, die finanzielle Bonität und die organisatorische Aufstellung dieses Market Makers zu prüfen und müssen sich daher auf die Sicherungsmaßnahmen der Handelsplattform verlassen. Agiert die Handelsplattform zugleich als Market Maker auf der Plattform tragen Sie nicht nur das organisatorische Risiko der Handelsplattform selber sondern zudem das wirtschaftliche und organisatorische Risiko der Market Making Aktivitäten.

### *2.1.3 Preisbildung*

Der Handel von Kryptowährungen findet ausschließlich auf elektronischem Wege statt. Ein Präsenzhandel ist derzeit nicht möglich. Damit treffen Aufträge von Anlegern auf elektronischem Wege bei dem Handelsplatz ein und ein Computer führt die Aufträge nach bestimmten Logiken (Vermittlung/Market Making) aus.

Die Festlegung der Handelszeiten obliegt dabei dem Handelsplatzbetreiber und kann von Handelsplatz zu Handelsplatz unterschiedlich sein. Es gibt auch hier keinerlei einheitliche Handhabung und daher muss dies ebenso wie die unterschiedlichen Handelsregeln individuell bei Ihrer Auswahl eines Handelsplatzes berücksichtigt werden.

Die Kursbildung wird von keiner stattlichen Handelsüberwachung überwacht. Ob sich die Preisfeststellung an die selbst auferlegten Regeln hält, ist daher für Sie nicht erkennbar!

## 2.2 Auftragserteilung

Ob ein Handelsplatz ausschließlich Kauf- und Verkaufsaufträge unlimitiert oder mit Limit zulässt oder ob auch andere Aufträge möglich sind, ist individuell abhängig von dem jeweiligen Handelsplatz.

Als Ordermöglichkeiten grundsätzlich denkbar sind:

Käufe und Verkäufe

- mit Limit
- ohne Limit
- Stop-Order (Stop-Limit oder unlimitiert)
- Orders mit Gültigkeiten
- Orders mit Stückzahlrestriktionen (fok bzw. ioc)

Informieren Sie sich daher unbedingt vorab, welche Ordertypen und Ordermöglichkeiten Ihnen der von Ihnen gewählte Handelsplatz offeriert.

## 2.3 Abrechnung

Bei dem Handel von Wertpapieren Sind Sie es gewohnt, eine Wertpapierabrechnung zu erhalten. Unabhängig von der Frage, ob die Handelsplattform für Ihre Rechnung ein Geschäft vermittelt oder als Market Maker ein Festpreisgeschäft abschließt: Ob eine Handelsplattform Ihnen eine Abrechnung über ein entsprechendes Geschäft in Kryptowährungen erstellt und überlässt ist individuell von der von Ihnen gewählten Handelsplattform abhängig. Informieren Sie sich daher unbedingt vorab bei dem jeweiligen Handelsplatz, ob er eine solche Abrechnung erstellt. Insbesondere vor dem Hintergrund der steuerlichen Betrachtung ist es unbedingt notwendig, dass Sie zumindest eine Transaktionsübersicht in Ihren Kryptowährungsgeschäften erhalten, um nachweisen zu können, dass Sie eventuell über die steuerlichen relevanten Fristen hinaus aktiv waren oder sich noch innerhalb der Freigrenzen bewegen. Generell haben Geschäfte in Kryptowährungen steuerliche Auswirkungen, die jedoch nicht Bestandteil der Abrechnung sind.

Es kann sein, dass die üblichen Angaben, die Sie in Deutschland bei einer Wertpapierabrechnung gewohnt sind, komplett fehlen. Klären Sie daher unbedingt im Vorfeld

mit dem vom Ihnen ausgewählten Handelspartner ab, ob und wenn ja in welchem Umfang er Ihnen eine entsprechende Abrechnung zukommen lässt. Inhalte einer Abrechnung für Wertpapiere, wie Sie in Deutschland üblich sind, erfahren Sie auf der Folgeseite.

Solche Angaben sind beispielsweise:

- Geschäftsart (Kauf/Verkauf)
- Gehandeltes Produkt (Kryptowährung)
- Stückzahl
- Geschäftsgegenwert und Währung
- Ausführungskurs
- Valutatag (Tag der Erfüllung von Lieferung und Zahlung des Gegenwertes)
- Handelszeit und Handelsort (Börse oder Handelsplatz)
- Art des Geschäftes (Kommissions- oder Festpreisgeschäft)
- Handelsentgelt (Provision des Ausführungsplatzes) sowie
- Drittkosten

## 2.4 Risiken bei Abwicklung von Orders in Kryptowährungen

Bei der Abwicklung von Orders in Kryptowährungen haben wir bereits einige Risiken aufgeführt und wollen diese noch einmal aufführen:

### *2.4.1 Übermittlungsrisiko*

Da Orders in Kryptowährungen nicht mündlich erteilt werden sondern nur systematisch erfasst werden, sind die Übermittlungsrisiken nicht auf Versprechen oder falsches Hören von Aufträgen bezogen. Vielmehr betreffen die Übermittlungsrisiken auf andere Faktoren:

- Fehleingaben
    - z.B. das Verwechseln von Kauf oder Verkaufsaufträgen
    - z.B. die Fehleingabe von Limiten
    - z.B. das Verwechseln der gewünschten Handelswährung
    - z.B. die Fehleingabe von gewünschten Volumina
    - z.B. die Fehleingabe bei der Angabe von Gültigkeiten
- fehlende Marktzugriffe
    - z.B. weil Ihr Zugang ins Internet nicht arbeitet
    - z.B. weil Ihr Computer defekt ist
    - z.B. weil Sie erkrankt sind oder andere persönliche Gründe Sie am Handel hindern

Beachten Sie bitte, dass es eine Reihe von nicht kalkulierbaren Risiken gibt, die Sie daran hindern, eine Order an einem Handelsplatz zu platzieren. Im Extremfall können Sie nicht mehr agieren und sind mit Ihrer Handelswährung komplett abhängig von der Marktentwicklung. Dieses Risiko kann zu einem Totalverlust führen.

### *2.4.2 Fehlende Marktliquidität*

Sie haben den Wunsch, dass Ihre Order jederzeit bei entsprechendem Limit ausgeführt wird. Sie sind dabei jedoch davon abhängig, dass Sie für Ihren Handelswunsch eine entsprechende Gegenseite finden. Dabei ist es unerheblich, ob diese entsprechende Handelsgegenseite von einem anderen Anleger oder von einem professionellen Market Maker zur Verfügung gestellt wird. Es ist nicht oder nicht immer sichergestellt, dass Sie zum Zeitpunkt Ihres Handelswunsches immer ein entsprechendes Gegenangebot vorfinden. Besteht keine Nachfrage oder kein Angebot in der von Ihnen gewünschten Kryptowährung, so können Sie Ihren Bestand nicht oder nicht sofort verkaufen oder kaufen. Damit zieht sich ein Handelswunsch teilweise länger hin als gedacht und gewünscht. Ebenso können hohe Ungleichgewichte zwischen Ihrer Order und den Volumina der Gegenangebote auftreten. Diese Ungleichgewichte haben – insbesondere bei unlimitierten Aufträgen – teilweise massive negative Auswirkungen auf den Kurs. Zudem kann Ihre Order bei hohen Volumina dazu führen, dass sich die Kurse nicht über Ihr Limit bewegen können, bis Ihre Order abgearbeitet ist.

### *2.4.3 Preisrisiko*

Kryptowährungen haben eine **extreme Volatilität**. Der **Bitcoin**, erste und auch Leitwährung der Kryptowährungen, hat an manchen Tagen **Schwankungsbreiten** (Volatilitäten) von **mehr als 25%.**
Sollten Sie Aufträge erteilen, ist es daher nicht unrealistisch, dass zwischen dem Zeitpunkt der Auftragserteilung und der späteren Ausführung aus verschiedenen Gründen (Leitungsverzögerungen, Handelsschwankungen usw.) so viel Zeit vergeht, dass sich der Kurs am Handelsplatz zu Ihrem Nachteil massiv verändert.

---

**TIPP**: Wir raten Ihnen daher unbedingt, dass Sie bei Orders immer **mit Limiten agieren** und nicht unlimitiert kaufen und verkaufen wollen. Bitte **bewahren Sie** darüber hinaus **kühlen Kopf**. Kryptowährungen sind verhältnismäßig neue Finanzinstrumente. In den letzten Jahren ist es zu einem Run auf diese Finanzinstrumente mit entsprechender Auswirkung auf die Kurse gekommen. Kursanstiege von 1.000 Prozent waren keine Seltenheit. Dies hat dazu geführt, dass auch unerfahrene **Anleger unkritisch** in der Hoffnung auf eine Fortsetzung der Kursgewinne versuchen, Kryptowährungen zu kaufen.

Bitte rufen Sie sich in Erinnerung, wie sich die Kurse am **Neuen Markt** entwickelt haben. Anleger sind scharenweise in diese Aktien geströmt und haben für **astronomische Marktbewertungen** gesorgt. Im Anschluss sind diese Kurse teilweise wieder um 99% gefallen. Trotz aller Unterschiede der Kryptowährungen zu Aktiengesellschaften, der Zahlungsfunktion und dem Inflationsschutz ist es nicht auszuschließen, dass sich eine **Blase** aufbaut, die einmal platzen und damit zu **massive**n **Kursverluste**n führen könnte.

Springen Sie deshalb nicht hinterher, wenn Ihr Preislimit überschritten wurde. **Es ist besser, auf Kursgewinne zu verzichten, weil der Preis bereits zu weit gelaufen ist, als später reale Kursverluste zu erleiden.** Bedenken Sie, dass es **kein faires Bewertungsmodell** für Kryptowährungen gibt sondern sich der **Preis** ausschließlich **nach Angebot und Nachfrage** richtet. Welcher Wert einer Kryptowährung demnach zugebilligt wird, ist individuell unterschiedlich und kann sich vor allem von einem Moment zum nächsten Moment verändern.

---

### *2.4.4 Handelsunterbrechungen*

Wenn Plattformen etwa aufgrund technischer Probleme zusammenbrechen, verlieren Anleger regelmäßig Geld, da ihnen der Zugriff auf ihre Bestände und damit ein Handel nicht möglich ist. Besonders tückisch ist es, dass Handelsplätze gerade bei Kurseinbrüchen oft vom Netz gehen, so dass viele Kryptowährungs-Inhaber in solchen Momenten keine Chance mehr haben, Verluste zu minimieren. Das Schließen von Handelsplätzen ist in der Vergangenheit bereits mehrfach vorgekommen und Nutzer hatten das Nachsehen. Gerade in Phasen mit Flashtrades, starken und irrationalen Kurseinbrüchen, werden Handelsplätze ohne Vorankündigung einfach geschlossen und dem Anleger eine Reaktionsmöglichkeit entzogen. Die vorgenannten Unterbrechungen dienen häufig ausschließlich zum Schutz der Handelsplattformen oder sind durch deren unzureichenden technischen Investitionen verursacht.

Das – temporäre oder dauerhafte- Schließen von Handelsplätzen führt für den Anleger zu hohen Risiken bis hin zum Totalverlust. Dabei ist es gleichgültig, ob die Schließung aus Kapazitätsgründen, aus Gründen einer technischen Störung oder aus gesetzlichen Gründen wie ein angeordnetes Handelsverbot erfolgt.

Solche vorgenannten Handelsunterbrechungen sind anders zu bewerten als so genannte Kursaussetzungen an den Wertpapierbörsen. Von Kursaussetzungen spricht man, wenn zum Schutz der Anleger und zur allgemeinen Gleichbehandlung und Orientierung ein Handel temporär suspendiert wird.

### *2.4.5 technische Risiken*

Bei der Ordererteilung bestehen hohe Risiken, da sich die gesamte Kommunikation ausschließlich online über Computer abspielt. Das macht diesen Bereich – in Kombination mit den hohen Gegenwerten – zu einem attraktiven Ziel für Betrüger. Diese versuchen über Trojaner, Viren, Phishing, sonstige Malware oder SCAM Aktivitäten dem Inhaber von Kryptowährungen oder von Walletbetreibern bis hin zu den Handelsplattformanbietern zu schaden.

Dabei werden Sie z.B. auf eine betrügerische Webseite umgeleitet, die den Eindruck einer offiziellen Identität macht. Folgen Sie daher keinen Links aus dem Internet sondern geben die Adresse eines Partners ausschließlich manuell ein.

Schützen Sie sich generell mit entsprechenden Sicherheitsmaßnahmen wie jederzeit aktuell gehaltenen Virenprogrammen. Öffnen Sie keine unbekannten Programme, insbesondere keine Anhänge von Mails. Berücksichtigen Sie bitte, dass selbst das Surfen im Internet und der Besuch einzelner Webseiten sowie das Anklicken von vermeintlich sicheren Bestandteilen wie Fotos dazu führen kann, dass Sie sich ein Schadprogramm aufladen, welches Sie bestehlen soll. Nutzen Sie idealer Weise einen Computer losgelöst von allen anderen Anwendungen ausschließlich zum Handel Ihrer Kryptowährungen.

### *2.4.6 Abwicklungsrisiken*

Für die Abwicklung von Kryptowährungen gibt es kein standardisiertes Abwicklungsvorgehen. Ein allgemein gültiges Clearingsystem wie es an klassischen Börsen teilweise sogar länderübergreifend installiert ist, gibt es für Kryptowährungen nicht. Daher ist es häufig erforderlich, die Abwicklung über klassische Überweisungen durchzuführen. Dies ist sowohl zeitintensiv, kostenintensiv als auch risikobehaftet, da innerhalb des

Überweisungsvorganges durch Phishing oder andere betrügerische Maßnahmen versucht werden kann, den Geldstrom abzufangen und umzuleiten.

Zudem kann ihr Vertragspartner bei Abschluss des Geschäftes eventuell nicht über die finanziellen Mittel verfügen, die dieser zur Begleichung der Transaktion benötigt. Je nach Handelsplatz und Handelsregeln kann es daher passieren, dass Ihre zunächst unter Vorbehalt stehende Transaktion endgültig storniert wird. Dabei spielt es keine Rolle, ob der Handelspartner ein anderer Privatkunde ist oder aber ein von der Börse eingesetzter Market Maker, der auf eigene Rechnung und Risiko Kryptowährungen an- und verkauft.

Sobald die Handelsplattform Bestandteil der Abwicklung wird, z.B. weil dort Transaktionen über zentrale, der Handelsplattform zuzurechnende Wallets durchgeführt werden, tragen Sie zudem das Risiko, dass während der Abwicklungsphase die Handelsplattform in wirtschaftliche Schwierigkeiten und in die Insolvenz gerät. In einem solchen Fall wie auch in allen anderen genannten Fällen droht Ihnen als Anleger ein Totalverlustrisiko.

# 3 Risiken bei taggleichen Geschäften (so genanntem „Day Trading“)

Der barrierefreie Zugang zu Handelsmöglichkeiten bequem vom heimischen Computer aus, ohne eigene Börsenzulassung, ohne sonstige aufsichtsrechtlichen Voraussetzungen hat dazu geführt, dass ehemals Banken und sonstigen Profis vorbehaltene Handelsmechanismen nun auch Privatanlegern zur Verfügung stehen. Der klassische Eigenhandel der Banken gehört nun auch zu den Möglichkeiten, die Privatanlegern offenstehen. Dieser so genannte **Intraday-Handel** oder auch **Day-Trading** bezeichnet den taggleichen Handel von Finanzinstrumenten mit dem Ziel, aus dem Handel heraus Gewinne zu erzielen. Unabhängig von der Frage, ob Sie nur kleine und kurzfristige Schwankungen ausnutzen oder größere Tagesgewinne erzielen wollen, müssen Ihnen die **besonderen Risiken das Day Tradings** bewusst sein.

**Ohne in den einzelnen Punkten noch einmal explizit darauf hinzuweisen, unterliegen Sie in allen Fällen einem sehr hohen finanziellen Risiko und Sie müssen sich darüber im Klaren sein, dass Sie Ihr gesamtes eingesetztes Kapital verlieren können.**

## 3.1 sofortige Ertragswirkung

Jeder Handel, den Sie in der Absicht zur Erzielung kurzfristiger Kursgewinne durchführen, steht unter dem Risiko, dass Sie Verluste erleiden, wenn sich Ihre kurzfristige Erwartung nicht erfüllt. Der Grund für den Nichteintritt Ihrer Erwartung ist dabei unerheblich. Dies können drittinduzierte Nachrichten z.B. aus der Politik sein, allgemeine Marktentwicklungen, individuelle Entwicklungen des von Ihnen gewählten Produktes oder einfach nur eine falsche Markttendenz. Müssen Finanzinstrumente wie Kryptowährungen zur Verlustbegrenzung oder zur Vermeidung von Risiken durch das Halten von **Positionen über Nacht** (**overnight-Risken**) verkauft werden, obwohl Ihre Tendenz falsch war, führt dies zu Verlusten. Sie haben durch die sofortige Glattstellung der Position keine Chancen mehr, von Kursanstiegen über Nacht zu profitieren. Mit dem Verkauf fixieren Sie Ihr Handelsergebnis, die **Glattstellung hat eine sofortige Ertragswirkung.**

## 3.2 professionelle Konkurrenz

Im Tageshandeln stehen Sie in der Konkurrenz zu **professionellen Marktteilnehmern** wie Banken, Brokern und anderen Kapitalsammelstellen. Diese Marktteilnehmer haben gegebenenfalls eine **konträre Auffassung** zu Ihrer Handelsstrategie und verfolgen eigene Interessen, sind eventuell besser informiert und vor allem finanzstärker, so dass sie auch eine längere Verlustphase aushalten können.

## 3.3 systematische Konkurrenz

Sie konkurrieren zudem gegen Handelsplattformbetreiber oder CFD Anbieter, die eigene Interessen verfolgen. Deren Interessen liegen darin, ihren Ertrag zu vergrößern. Da Sie als Anleger deren Handelskontrahenten sind, liegt es nahe, dass eine Ertragssteigerung auf Seiten des Anbieters unter anderem auch dadurch zustande kommt, dass Sie als Anleger weniger verdienen. Zwar haben seriöse Anbieter ein Interesse daran, dass Sie als Kunde lange erhalten bleiben, aber von Ihren Handelsaktivitäten sollen Sie einen Ergebnisbeitrag für den Kooperationspartner liefern. Aus Sicht des Anbieters sollen Sie idealer Weise immer Gewinne machen, diese Gewinne sollen aber möglichst durch eigene Kosten oder Aktivitäten weitestgehend abgeschöpft werden. So werden Sie als „lebender Ertragslieferant“ kontinuierlich benutzt.

Diese Haltung schließt nicht aus, dass in verschiedenen Konstellationen versucht wird, durch Einstellung von Systemen oder Handelsspreads die eigenen Erträge zu Ihren Lasten zu optimieren. So können die Handelsspreads verbreitert werden oder Ihnen schlechtere Preise für einzelne Seiten gestellt werden. Auch das temporäre Einstellen von Market Making Aktivitäten oder auch das Einstellen von Handelsaktivitäten während hochvolatiler Phasen (Flashtrading) zum eigenen Schutz ginge zu Ihren Lasten. In solchen Phasen können Sie Ihre Bestände nicht handeln.

## 3.4 notwendige Kenntnisse

Vor dem Daytrading in Kryptowährungen müssen Sie sich unbedingt **vertiefte Kenntnisse über** die Eigenschaften von **Kryptowährungen**, ihre technischen und risikobehafteten Besonderheiten aneignen. Zudem sind entsprechend **detaillierte Kenntnisse** ebenfalls notwendig im Bereich von **Handelsstrategien, Handelstechniken, Funktionsweise von derivativen Finanzinstrumenten.** Da der Bereich Kryptowährungen und insbesondere die Handelspartner nicht reguliert sind, ist es zudem noch unbedingt erforderlich, dass Sie sich über Ihre **Handelskontrahenten** sowie deren **Handelsregeln, Usancen, wirtschaftlichen Fähigkeiten und Überwachungs- und (freiwilligen) Entschädigungsregelungen informieren**.

## 3.5 Erhöhung Verlustwahrscheinlich durch Kreditaufnahme

Sollten Sie erwägen, zum Intraday Handel **Kredite** aufnehmen zu wollen, so berücksichtigen Sie bitte, dass **zusätzliche Kosten** zur Aufnahme von Krediten entstehen, die Sie mit Ihrem Handel ebenfalls erwirtschaften müssen. Dazu gehören neben **einmaligen Einrichtungskosten** für einen Kredit vor allem die **laufende**n **Zinskosten**. Beachten Sie bitte darüber hinaus: Die Rückzahlungsverpflichtung für einen Kredit trifft Sie unabhängig vom Erfolg der mit dem Kredit durchgeführten Handelsaktivitäten. Erleiden Sie also **Verluste** im Tageshandel, die bis hin zu einem Totalverlust nicht nur des Eigenkapitals sondern auch des mit den Kreditmitteln eingesetzten Kapitals führen können, müssen Sie **dennoch** den **Kredit mit** den entsprechenden **Zinsen zurückführen**.

## 3.6 Kostenbelastung

Der **Handel** von Finanzinstrumenten **kostet Geld**. Entweder Sie müssen eine **Provision** zahlen oder aber Sie verlieren den **An- und Verkaufsspread** beim Handel der Finanzinstrumente. Je häufiger Sie handeln, umso höher sind diese Kosten. Um insgesamt erfolgreich zu handeln, müssen Ihre **Ergebnisse über den Kosten** liegen. Je mehr Sie traden, umso höher wird die Summe, die Sie erfolgreich ertraden müssen, um die Kosten zu decken.

Wenn Sie regelmäßig und viel handeln, können diese Gebühren und Kosten im Verhältnis zum eingesetzten Kapital unverhältnismäßig hoch sein.

## 3.7 Unkalkulierbare Verluste bei Derivaten sowie hochvolatilen Produkten

Kryptowährungen haben sich in der Preisentwicklung als hoch volatil, also mit hohen Preisausschlägen versehen gezeigt. Damit steigt das Risiko, dass Sie zu einem falschen Zeitpunkt innerhalb der volatilen Handelsphase disponiert haben könnten. Zudem sorgt die Hebelwirkung bei derivaten Produkten wir CFDs für ein hohes Verlustrisiko. Hohe Handelsaktivitäten fördern das Risiko, dass die mit dem Hebel verbundenen Risiken valide

werden und Sie Ihr eingesetztes Geld bei falscher Tendenz verlieren. Auch wenn Sie bei CFDs keine Nachschusspflicht in Deutschland haben, so kann es sein, dass dies bei Anbietern im Ausland dennoch gefordert wird.

Die Kombination von hochvolatilen Produkten mit Derivaten und anderen Hebelprodukten potenziert die Risiken zudem.

Mit Beginn des Handels in Termingeschäften wie Futures auf Bitcoin oder andere Kryptowährungen in den USA im Dezember 2017, tragen Sie dort bei solchen Geschäften zudem das Nachschussrisiko, welches dazu führt, dass Sie im Extremfall über Ihr eingesetztes Kapital hinaus noch Gelder nachliefern oder alternative Sicherheiten stellen müssen.

## 3.8 Risiko durch Drittbeeinflussung

Es besteht das hohe Risiko, dass Sie sich durch Eigenlektüre von Internetseiten, Foren und anderen Medien, die über Börsenentwicklungen berichten, stark in Ihrem Verhalten und Ihrer Handelsstrategie beeinflussen lassen. Das führt dazu, dass Sie eventuell von einer einmal geplanten Handelsüberlegung abweichen oder gar abrücken und sich dies zu Ihrem Nachteil entwickelt.

Falls Sie als Daytrader in einem Büro arbeiten, in dem andere Personen ebenfalls im Handel aktiv sind, dann besteht das Risiko, dass Sie sich in Ihrer Meinung durch den Austausch mit den anderen Personen beeinflussen lassen. Dieses Risiko besteht allerdings auch, wenn Sie sich mit nicht professionellen Marktteilnehmern unterhalten. Wir wiederholen an dieser Stelle noch einmal unseren Rat, sich durch Dritte in der Meinung nicht beeinflussen zu lassen, insbesondere nicht die Sorge zu haben, dass Sie nicht mehr rechtzeitig vor weiteren Kurssteigerungen in dem Markt einsteigen zu können. Bewahren Sie ruhigen Kopf!

# F Fachwortverzeichnis

**51% Attacke**
Hinter dieser Bezeichnung versteckt sich eine Möglichkeit der Manipulation eines →Kryptowährung Netzwerks. Dabei liefert entweder ein →Miner alleine oder eine →Mining-Gruppe mehr als 50 Prozent des betreffenden Netzwerkes für die Währung. Dies ermöglicht ihnen theoretisch das Manipulieren des Netzwerks und die Kontrolle über selbiges. So könnten hierbei Aktionen wie das Behindern einer →Transaktionsbestätigung, das mehrfache Ausgeben eines →Coins oder auch das Hindern vom →Mining anderer User durchgeführt werden. Je kleiner die Währung und das zugehörige Netzwerk, desto größer ist das Risiko einer 51% Attacke. Bei größeren →Kryptowährungen (z.B. →Bitcoin) würde für eine solche Attacke eine enorme Rechenleistung benötigt werden, was sie unwahrscheinlicher macht.

**Adresse**
Die Adresse ist der öffentliche Teil einer Transaktion von →Kryptowährungen. Will ein Anleger eine Zahlung in →Kryptowährung empfangen, gibt man für diese Transaktion seine Adresse heraus. Zudem ist sie Bestandteil des →Public Keys, also der Signierung von einzelnen Transaktionen. Die Adresse ist bei → Bitcoin ein sogenannter →Hash-Wert und besteht aus alphanumerischen Zeichen, welche als →QR-Code dargestellt werden können. Eine andere Bezeichnung für die Adresse ist auch → Public Key.

**Altcoin**
Unter dem Sammelbegriff Altcoin werden alle digitalen Währungen bezeichnet, die es neben der Initital- und Leitwährung →Bitcoin noch gibt. Es handelt sich dabei um „alternative Coins“.

**ANN**
Announcement, also Ankündigung. Als Beispiel werden neue →Kryptowährungen häufig mit dem Themennamen “[ANN] CryptowährungX” in Foren angekündigt.

**Anteilskapital Token siehe → Equity Token**

**ASIC**
Die Abkürzung ASIC steht für Application Specific Integrated Circuit. Dahinter verbirgt sich ein Silikonchip, der ausschließlich für einen einzelnen Vorgang produziert wird. Im Zusammenhang mit den →Bitcoin wird ein ASIC für das →SHA-256 Hashing genutzt. Mit ihm lassen sich besonders effizient weitere →Bitcoins →minen.

**ASIC – Miner**
Ein Asic Miner arbeitet mit→ ASIC-Chips welche speziell für das →Mining mit →SH256 entwickelt worden sind. Diese Chips zeichnen sich durch besonders hohe Leistung und niedrigen Stromverbrauch im Vergleich zu anderen Chips wie CPU und GPU aus. Mit einem ASIC Miner lassen sich somit alle SH256 Coins →minen. Ein ASIC Miner kann besonders effizient →Kryptowährungen →minen. So genannte →Scrypt-Coins können jedoch nicht mit einem ASIC Bitcoin Miner gemined werden – hierzu bedarf es spezieller ASIC Scrypt Miner.

**ATM**
Im englischsprachigen Raum wird ein Geldautomat als ATM bezeichnet. ATM ist eine Abkürzung für Automatic Teller Machine. Ein „teller“ bedeutet übersetzt „Schalterbeamter“, womit ATM quasi für einen virtuellen Schalterbeamten steht. Während früher Geldautomaten ausschließlich für →Fiatwährungen existierten, gibt es mittlerweile auch ATM für → Kryptowährungen. Dabei können Euro oder US Dollar in verschiedene → Kryptowährungen getauscht und auch wieder zurück getauscht werden.

**Bagholder**
Als Bagholder werden User bezeichnet, die →Coins in ihrem → Wallet für einen längeren Zeitraum halten.

**Basiswert**
Der Basiswert (oder auch Underlying genannt) ist der Gegenstand, auf den sich ein → Derivat bezieht. Als Derivat sind im Zusammenhang mit dem Basiswert → CFDs oder → Optionen zu nennen. Die Wertentwicklung des → Derivats bezieht sich immer auf die Wertentwicklung des jeweiligen Basiswertes. Handelt der Anleger ein → CFD auf → Bitcoin, so ist der → Bitcoin als der Basiswert anzusehen.

**Bestätigung**
Jede Transaktion von →Kryptowährungen wird durch das Netzwerk bestätigt. Eine Bestätigung im Zusammenhang mit →Bitcoin bedeutet, dass die Transaktion durch das Netzwerk verifiziert wurde und sich nur noch schwer rückgängig machen lässt. Die Transaktion wird im →Block gespeichert und ist damit in diesem gesichert. Bei größeren Transaktionen sichert jede weitere Bestätigung die Transaktion zusätzlich.

**Bitcoin**
Der Bitcoin ist die erste und populärste → Kryptowährung. Nach aktueller Marktkapitalisierung ist es zudem die größte digitale → Kryptowährung. Hinter einem Bitcoin verstecken sich Transaktionen, die per Algorithmus auf digitalem Weg dezentral zwischen den Nutzern des Netzwerks ausgetauscht werden.

**Block**
Als Block wird der Datensatz innerhalb einer →Blockchain bezeichnet, in welchem die noch ausstehenden Transaktionen enthalten sind. Er gilt als Bestätigung dieser Transaktionen. Durch das → Mining entstehen neue Blöcke. Die Anzahl der Blöcke ist ein Maß dafür, wie lange das Netzwerk bereits existiert. Je mehr Blöcke existieren, umso länger gibt es das Netzwerk bereits.

**Blockchain**
Eine Blockchain ist eine Datenbank, die über ein Netzwerk von vielen einzelnen Nutzern verteilt ist. So sind alle Transaktionen an vielen verschiedenen Orten gleichzeitig gespeichert. Ihre Integrität ist durch die Speicherung von Hashwerten des jeweils vorangegangenen Datensatzes gesichert. Entstanden ist sie als technische Grundlage für →Kryptowährungen wie →Bitcoin. Inzwischen existieren zahlreiche Weiterentwicklungen der ursprünglichen Blockchain-Technologie. Diese ermöglichen über →Kryptowährungen hinaus zahlreiche Anwendungen im Bereich Lizenz-Management, Versicherungswirtschaft, Logistik oder ID-Management. Die Stärke der Blockchain liegt in einfachen Transaktionen, die das Blockchain-Netzwerk validiert - beispielsweise in rechenintensiven Verfahren mittels →Proof-of-Work. Die Mehrheit der Rechenleistung entscheidet darüber, welche Version der Blockchain korrekt ist. Das schützt sie vor Manipulationen und vertrauenswürdige Intermediäre wären zur Durchführung einer Transaktion nicht mehr erforderlich. Die Blockchain, (oder übersetzt Blockkette), enthält dabei alle Blocks, die bisher erzeugt wurden. In ihr sind alle bisher getätigten Transaktionen festgeschrieben, sodass genau nachvollzogen werden kann, wie viel einer Kryptowährung welcher Adresse gehört. Obwohl die Blockchain-Technologie ganz ursprünglich für die Kryptowährungen entwickelt wurde, lässt sie sich in vielen unterschiedlichen Bereichen sinnvoll einbringen wie beispielsweise bei → Smart Contracts.

**Block Reward**
Erarbeitet ein →Miner einen neuen →Block erhält er eine sogenannte Block Reward. Der Block Reward halbiert sich bei → Bitcoin in bestimmten Abständen. Diese Form von Belohnung treibt vor allem → Miner an, über ihre zur Verfügung gestellte Rechenleistung neue Kryptowährungseinheiten zu → minen.

**BOINC**
Die **B**erkeley **O**pen **I**nfrastructure for **N**etwork **C**omputing, kurz BOINC, ist eine Plattform für verteiltes Rechnen. Beispielsweise laden Forschungsgruppen in kleinen Paketen Teile ihrer Forschung hoch, die noch ungelöst sind. Der Nutzer zu Hause kann sich diese Pakete herunterladen, vom PC lösen lassen und das Resultat wieder hochladen. Auch hier spielt der Gedanke der Dezentralität und der gegenseitigen Unterstützung eine große Rolle.

**Brute-Force Angriff**
Bezeichnet einen mit massiver „technischer Gewalt“ gestarteten Angriff auf ein System. Hierbei ist im Zusammenhang mit Kryptowährungen z.B. ein (z.B. durch kriminelle Bot-Netze initiierter) Zusammenschluss von Rechnerleistungen zum Knacken von Algorithmen oder anderen Attacken gemeint.

**BTC**
BTC ist eine geläufige Abkürzung für eine Bitcoin-Einheit. Es ist ebenfalls das Kürzel für → Bitcoin an einem Kryptowährungshandelsplatz.

**CFD**
Ein CFD ist in der Finanzwelt die Abkürzung für Contract for Difference, was auf Deutsch Differenz-Kontrakt bzw. Differenz-Geschäft bedeutet. Mit Differenz ist der Unterschied zwischen Kaufkurs und Verkaufskurs der grundliegenden Position (→ Basiswert) gemeint. Ein CFD ist ein → Derivat. Anstatt den Basiswert direkt zu handeln, handelt der CFD Anleger nur noch den Anspruch auf finanziellen Ausgleich einer Wertentwicklung des → Basiswertes. Dies führt in Verbindung mit meist nur geringen Anzahlungen zu einem hohen Kursrisiko aufgrund des → Hebeleffektes.

**Client**
Ein Client ist im Allgemeinen ein Programm, also eine Software. Ein Client kann sowohl auf einem mobilen Endgerät, einem Computer oder auch einem Laptop installiert werden. Der Client ermöglicht den Zugriff auf ein Netzwerk. Der Nutzer des Clients stellt automatisch auch einen → Node, einen Netzwerkknoten, dar.

**Cloud Mining**
Will man →Bitcoins – oder eine andere →Kryptowährung – erzeugen, muss man über Rechenleistung verfügen. Hier hat man als Nutzer zwei Möglichkeiten: 1) Der Nutzer kann sich eigene sogenannte → Mining Hardware anschaffen oder aber 2) die benötigte Rechenleistung in einer Cloud mieten oder kaufen. Gängige Methode ist dabei für die meisten Nutzer das Mieten in der Cloud. Hier wird den Nutzern von den Anbietern die benötigte Infrastruktur geliefert. Der Anbieter betreibt zudem die Mining-Hardware, so dass der User ohne großen eigenen Aufwand mit dem →Mining starten kann.

**Coin**
Das Wort Coin stammt aus dem englischen Sprachraum und bezeichnet dort grundsätzlich den Begriff einer Geld-Münze. Im Bereich der → Kryptowährungen steht Coin aber als Kurzform einer virtuellen Währung

**Decentralized autonomous organizations / DAO (siehe → Smart Contracts)**

**Dapp**
Dapps sind dezentralisierte Apps, die durch das Netzwerk-Prinzip der →Blockchain möglich werden. Jede Dapp besteht je nach Anwendungsfall aus sich selbst ausführbaren Codes, den sogenannten →Smart Contracts.

**Derivat**
Dieser aus dem Lateinischen stammende Begriff (derivare = ableiten) beschreibt eine Gruppe von Finanzinstrumenten, die hochrisikoreich sind. Dabei handelt man nicht den eigentlichen Handelsgegenstand (wie Aktien, Anleihen oder Kryptowährungen) sondern nur eine „Ableitung“ dieses Handelsgegenstandes. Es handelt sich dabei um →Termingeschäfte, die mit besonders hohen Risiken verbunden sind (→ Hebeleffekt oder auch Leverage).

**Dev**
Kurzform für “Developer” (übersetzt: Entwickler). Dahinter stehen in der Regel die Personen, die eine Kryptowährung und die zugehörige Softwarelogiken entwickelt haben

**Dezentrales System**
Die Haupteigenschaft der → Blockchain ist ihre Funktion als dezentrales System. Das bedeutet, dass es statt einem zentralen Netzwerk ein sogenanntes → Peer-to-Peer-Netzwerk ist. Die gesamten Daten werden gleichberechtigt zwischen allen Usern geteilt. Das Transaktionsregister, auch als → distributed ledger bezeichnet, ist dabei auf alle Knoten (oder →Nodes) des gesamten Netzwerks verteilt. Alle Nutzer verfügen über die gleichen Rechte und einen gleichberechtigten Zugriff auf die Informationen. Bei jeder Transaktion werden die dazugehörigen Informationen in jedem Knoten gespeichert. Das dezentrale System schützt sich auf diese Weise gegen Manipulationen. Durch seine selbstverwaltende Funktion ist es zudem deutlich geschützter gegenüber Machtmissbrauch als herkömmliche Systeme.

**Diensttoken (→ siehe Utility Token)**

**Difficulty**
Der Begriff Difficulty oder auch Mining Difficulty fällt im Zusammenhang mit dem Hashen eines neuen Blocks. Dabei steigt die Difficulty mit der Rechenleistung des Kryptowährungsnetzwerkes. Sprich: Je höher die Rechenleistung des Kryptowährungsnetzwerks, desto höher die Mining Difficulty. Da das Netzwerk lebendig ist, bleibt auch der Wert der Difficulty in Bewegung.
Die Schwierigkeit beim Hashen eines Blocks hängt damit zusammen, wie viele → Hashes maximal in einem Transaktionsblock erlaubt sind. Wenn die Anzahl an Hashes geringer ist, wird das Erzeugen eines Hashes schwieriger. Durch den Popularitätsgewinn von → Bitcoin steigt die Netzwerkleistung durch mehr Miner und damit steigt zugleich die Schwierigkeit.

**Distributed Computing, DC**
Das Distributed Computing, verteiltes Rechnen, nutzt die Rechenleistung vieler an einem Netzwerk beteiligten Einzelrechner, anstatt zentral auf einem großen Server Berechnungen anzustellen.

**Distributed Ledger Technology (DLT)**

Jegliches dezentrale und digital geführte Kontenbuch wird unter dem Oberbegriff Distributed Ledger Technology zusammengefasst. Den Begriff gibt es dementsprechend bereits länger als die Blockchain Technologie. Eine → Blockchain ist so nur eine von unterschiedlichen DLTs. Allerdings unterscheidet sich die Blockchain durch ihre Komplexität von anderen DLTs, die einen anderen Rahmen benötigen, um funktionieren zu können. Die → Blockchain hingegen ist so komplex gebaut, dass sie autonom und in sich geschlossen agieren kann.

**Doppelausgabe / Double Spending**
Bei vielen Nutzern besteht die Angst vor einer Manipulation der → Blockchain, beispielsweise durch das sogenannte Double Spending. Dabei wird vom User versucht, die gleichen Bitcoins parallel an unterschiedliche Empfänger zu verteilen. Diese Doppelausgabe von Bitcoins wird jedoch durch unterschiedliche Sicherheitsmechanismen erschwert. Zum einen wären dabei das Bitcoin Mining und zugleich auch die Beschaffenheit der Blockchain mit ihren Rückversicherungen. An diesen Kontrollen scheitern die Versuche von Double Spending in der Regel. Eine Garantie auf das Greifen der Sicherheitsmechanismen gibt es jedoch nicht.

**Equity Token**
Der Equity Token oder auch Anteilskapital Token ist ein Finanzierungsinstrument zur Kapitalbeschaffung eines Unternehmens. Sein Zweck besteht in einer Wertsteigerung und ist somit vergleichbar mit einer Aktie. Man könnte es auch als Kapitalbeteiligung an einem Unternehmen sehen. Mit einem Equity Token hat man somit Stimmrechte.

**Exchange/Börse**
Als eine Exchange wird eine zentrale Stelle bezeichnet, an welcher sowohl Währungen als auch Güter gehandelt werden können. Synonym für ein Exchange wird auch der Begriff Börse, Bitcoin-Börse oder Krypto-Börse verwendet. Hier können die digitalen Währungen untereinander getauscht werden, sowie in die sogenannten → Fiat-Währungen umgetauscht werden. Es gibt jedoch derzeit in Deutschland keine offizielle Börse nach dem Börsengesetz, so dass der Begriff Börse irreführend ist.

**Faucet**
Als ein Bitcoin Faucet wird eine Internetseite bezeichnet, auf welche man für das Besuchen der Seite oder das Ausfüllen von Captchas → Bitcoins oder Anteile geschenkt bekommt. Im Grunde ist Faucet eine Marketingmaßnahme für neue Währungen, um auf diese Weise neue Interessenten zu gewinnen. Bei den etablierteren → Kryptowährungen werden Faucets ebenfalls eingesetzt. Diese werden über Werbegelder finanziert.

**Fiat Geld/ Fiat-Währungen**
Als Fiat-Währungen, Fiat Geld oder Fiat Currencies werden im Zusammenhang mit → Kryptowährungen alle staatlichen und von Notenbanken herausgegebenen Währungen bezeichnet. Es handelt sich dabei um Objekte ohne intrinsischen Wert (ohne echten eigenen Wert), welche als Tauschmittel dienen. Beispiele für Fiat-Geld sind Euro oder auch Dollar, sprich, unsere klassischen Währungen. Letztlich sind auch die → Kryptowährungen als Untersparte des Fiat-Geldes zu verstehen, da auch ihnen ein materieller Gegenwert fehlt. Trotz dessen sind mit dem Begriff Fiat-Währungen in der Regel die klassischen Währungen gemeint, und die Kryptowährungen laufen eher in Abgrenzung unter ihrem eigenen Begriff.

**Fork**
Übersetzt bedeutet dieser Begriff Abspaltung und er bezeichnet dementsprechend eine kritische Situation bei den Kryptowährungen. Es kann bei einer Transaktion zu einer Spaltung kommen und damit zu einer Fork. Die Spaltung des Netzwerks bedeutet in seiner Konsequenz, dass das Protokoll der Blockchain nicht mehr abwärtskompatibel ist. Abwärtskompatibel sind die Versionen untereinander nur dann, wenn die Informationen aus den älteren Versionen mit den neuen Versionen übereinstimmen. Bei einer Hard Fork im Zusammenhang mit Bitcoins wird es danach notwendig, dass jegliche Software aktualisiert wird, damit die verschiedenen Systeme weiterhin zusammenarbeiten können.

**FUD (Fear, Uncertainty and Despair)**
Bedeutet Angst, Unklarheit und Verzweiflung. Wir in Bezug auf Anleger benutzt, ohne sich schlau zu machen über eine digitale Währung, investieren. Wenn eine Kryptowährung dann an Wert verliert oder aber sogar komplett untergeht, verweist man oft mit dem Wort FUD auf Foren oder Social Media Links. FUD wird auch als Synonym verwendet, wenn bei Anlegern Angst verbreitet wird, damit der Gerüchtestreuer aus der Angst der Anleger profitieren kann. Da → Kryptowährungen nicht reguliert und überwacht sind, können Akteure mit betrügerischer Absicht häufig erfolgreich und sanktionslos versuchen, solche Gerüchte zu streuen

**Genesis Block**
Der Genesis Block bildet die Grundlage für alle folgenden → Blocks des Systems → Bitcoin. Bei jeder Kryptowährung gibt es einen eigenen Genesis Block.

**Hash**
Generell ist ein Hash ein Code, der kryptografisch aus einem Datensatz errechnet werden kann. Dieser Hash ist einzigartig und für jeden Datensatz unterschiedlich, es kann aber nicht auf den ursprünglichen Datensatz zurückgeschlossen werden. Damit können z.B. innerhalb kurzer Zeit zwei Datensätze auf Gleichheit überprüft werden. Im Fall der Kryptographischen Währungen spricht man von einem Hash, den die Netzwerkknoten im → Proof of Work ermitteln müssen.

**Hash Rate**
Mit dem Begriff Hash Rate wird die Maßeinheit für die Rechenkraft des gesamten Netzwerks für Bitcoins bezeichnet. Das bedeutet, dass sich anhand der Hash Rate ablesen lässt, wie viele Berechnungen innerhalb einer Sekunde durchgeführt werden können. Diese Berechnungen sind aus sicherheitstechnischen Gründen wichtig für die Funktion des Bitcoin-Netzwerks. Beträgt die Hash Rate des Netzwerks so zum Beispiel 12 TH/s, werden 12 Billionen Berechnungen pro Sekunde durchgeführt.

**Hebeleffekt**
→ Derivate unterliegen einem Risiko des Hebeleffektes. Im Gegensatz zu einem direkten Erwerb des → Basiswertes sind Derivate nur Anzahlungen auf den späteren Erwerb eines Finanzinstruments. In Bezug auf die Anzahlung fallen Kursschwankungen prozentual wesentlich höher aus als auf den eigentlichen → Basiswert. Damit partizipiert der Derivateinhaber überproportional von Kursgewinnen oder Kursverlusten des eigentlichen Basiswertes. Dieses besondere Risiko wird als Hebeleffekt oder auch Leverage-Effekt bezeichnet.

**ICO (Initial Coin Offering)**
Übersetzt bedeutet es so viel wie „erstmaliges Münzangebot". In der Welt der → Kryptowährungen dient ein ICOals Finanzierungsphase für ein Projekt, das auf der → Blockchain Technologie beruht.

**Identity-Management**
Identity-Management ist neben den → Kryptowährungen der zweite große Hype innerhalb der →Blockchain. Experten glauben, dass mithilfe der Technologie auch der Verifizierungprozess im Internet vereinfacht werden kann. Anstatt sich beispielsweise in Onlineshops jedes Mal mit E-Mail-Adresse und Passwort einzuloggen, könnte in Zukunft eine einzelne digitale Identität für Transaktionen und Identifizierungen genügen. Prüfungen wären in Echtzeit möglich und das Betrugsrisiko würde sinken.

**ITO (Initial Token Offering)**
Alternativer Begriff für → ICO.

**Konsensverfahren**
Das Konsensverfahren ist der entscheidende Baustein, um die → Blockchain vor Manipulationen zu schützen. Es verhindert, dass ein Teilnehmer einen Wert mehrfach nutzt - also beispielsweise einen Betrag mehrfach transferiert, obwohl er nur einmal vorhanden ist. Das Konsensverfahren löst dieses "Double-Spending-Problem": Erst wenn die Mehrheit der angeschlossenen → Nodes sich über die Schaffung eines bestimmten neuen → Blocks einig ist, wird dieser validiert und an die zuvor erstellten Blöcke angehängt.

**Kryptographie**
Auch dieser Begriff stammt es aus der Mathematik und bezeichnet ein Fachgebiet von ihr. Bei diesem geht es darum, wie man durch mathematische Beweise Sicherheit herstellen kann. Dieser Bereich wird bereits in Bereichen wie dem Bankwesen oder dem Online-Handel genutzt. Kryptopgraphie wird bei den → Bitcoins zum Schutz der → Wallets und der → Blockchain allgemein angewendet. So wird durch Kryptographie ausgeschlossen, dass ein Nutzer → Bitcoins aus einer fremden → Wallet ausgibt. Sie kann dabei zudem zur Verschlüsselung eingesetzt werden. Die → Blockchain wird mittels Kryptographie vor Manipulationen durch User oder Externe geschützt.

**Kryptowährung**
Kryptowährung ist der Sammelbegriff für die neuen und digitalen Formen von Währung. Im deutschen Sprachraum wird teilweise auch von Kryptogeld gesprochen. Umgangssprachlich steht das Wort →Coins synonym für Kryptowährungen. Kryptowährungen sind eine moderne Unterform der → Fiat-Gelder, sprich der Währungen, die keinen materiellen Gegenwert aufweisen. Ihren Namen verdanken sie der zugrunde liegenden → Kryptographie. Diese wird bei Kryptowährungen angewendet, um ein sicheres digitales und dezentrales Zahlungssystem zu ermöglichen. Anders als bei den klassischen Währungen werden die Kryptowährungen durch private Nutzer geschöpft und unterliegen damit nicht der Einflussnahme einer Institution wie der Zentralbank. Seit 2009 gibt es mit dem → Bitcoin die erste öffentlich zugängliche Kryptowährung. Seitdem folgten mehr als 3.000 unterschiedliche Kryptowährungen.

**Kursausschlag (siehe → Volatilität)**

**Ledger**
Ledger bezeichnet das Kontenbuch oder auch das Transaktionsverzeichnis bei den →Kryptowährungen. An dieser Stelle werden jegliche Informationen rund um die Transaktionen gespeichert. In vielen Fällen wird nicht von einem schlichten Ledger gesprochen sondern von einem → Distributed Ledger. Dies bedeutet, dass die Kontenbücher ebenfalls an unterschiedlichen Stellen gespeichert sind, sprich „verstreut" sind. Auf diese Weise sind die Angaben des Ledgers weiterhin gesichert.

**Lending**
Zur Erhöhung der Abwicklungsgeschwindigkeiten kann man einem Handelsplatz seine dort gehaltenen → Kryptowährungen als „Kredit" geben. Nach Ablauf der vereinbarten Laufzeit erhält der Verleiher seine → Kryptowährungen und die verdienten Zinsen zurück. Wichtig: Der Verleiher trägt das Risiko, dass derjenige, dem er seine → Coins verliehen hat, während der Laufzeit insolvent wird.

**Liquidität**
Im Bezug auf Finanzmärkte wird der Begriff Liquidität im Sinne einer Marktliquidität genutzt. Ein Markt, indem viele Käufer und Verkäufer aktiv sind und damit eine jederzeitige Handelbarkeit von Positionen gegeben ist, bezeichnet man als „liquide Märkte", dagegen sind Märkte, in denen kaum Akteure zu verzeichnen sind und bei denen schon kleine Orders für hohe → Volatilitäten sorgen, so genannte „illiquide Märkte".

**Margin**
Eine Margin ist eine Sicherheitsleistung, die zur Abdeckung von mit Geschäften in Terminmärkten (→ Optionen, Futures und →CFDs) verbundenen Risiken zu hinterlegen sind.

**Marktkapitalisierung**
Als Marktkapitalisierung wird der Gesamtwert aller ausgegebenen → Coins einer → Kryptowährung multipliziert mit dem aktuellen Marktkurs bezeichnet. Je höher die Marktkapitalisierung ist, umso mehr → Coins sind entweder im Umlauf oder aber umso höher ist der aktuelle Marktpreis.

**Marktliquidität (siehe → Liquidität)**

**Marktusance (siehe → Usance)**

**Mining**
Ein häufig verwendeter Begriff im Zusammenhang mit Kryptowährungen ist das Mining. Bitcoins und andere Kryptowährungen werden nicht durch Notenbanken, sondern durch „Mining" generiert. Auch hinter diesem Begriff versteckt sich ein mathematischer Vorgang. Die Computer Hardware wird bei Transaktionen aktiv und prüft und bestätigt die verschiedenen Transaktionen. In rechenintensiven Schritten werden die unterschiedlichen Transaktionen zusammengefasst und damit validiert. Jeder →Block wird mit einem → Hash-Wert versehen und an den vorhergehenden → Block angehängt. Hierbei entsteht eine chronologische und lineare Verkettung der →Blocks. Dieser Vorgang dient einer optimierten Sicherheit des Netzwerks und wird als → Mining bezeichnet. User müssen an diesem Vorgang nicht teilnehmen.

Für Bitcoin Mining wird Rechenkraft und damit verbunden Klimatisierung und Strom benötigt. Aus diesem Grund gewährt das Netzwerk den Usern, die sich am notwendigen → Mining beteiligen, sogenannte Transaktionsgebühren für von ihnen bestätigte Bitcoin-Transaktionen. Diese Belohnungen werden je nach der geleisteten Rechenarbeit der User gestaffelt. Der Vorgang wird häufig auch mit dem deutschen Wort „schürfen" übersetzt und verwendet.

**Mining Pool.**
Es gibt einige → Kryptowährungen, die mehr Rechenleistung zum → Minen benötigen als andere Coins. Der → Miner benötigt dort z.B. mehrere Giga Hash an Rechenleistung. Da nicht jeder → Minder über entsprechende Kapazitäten verfügt, gibt es die Möglichkeit, sich in Mining Pools zusammen zu schließen. Man investiert zusammen, um größere Rechner zu betreiben. Diese stehen in großen klimatisierten Hallen und verbrauchen viel Strom. Letzteres hat zu viel Kritik am Vorgang des → Minings aus Nachhaltigkeitsgesichtspunkten geführt. Der Vorteil für den einzelnen Nutzer ist, dass er ohne großen Aufwand anteilig am → Mining beteiligt wird. Denn gerade für gewöhnliche User kann der Aufwand des klassischen → Minings in keinem lohnenswerten Verhältnis zum Ertrag des →Minings stehen.

**Mist**
Mist (aus dem Englischen für Nebel) ist ein Internet-Browser mit integriertem → Wallet für →Kryptowährungen. Technisch fußt der Browser auf der Ethereum-Blockchain, so dass Entwickler in der Lage sind, dezentralisierte Apps (→ Dapps) in einem Webinterface laufen zu lassen. Zu den ersten Anwendungen sollen ein Messaging-Protokoll und ein Filesharing-Dienst gehören.

**Node**
Als ein Node wird ein Knotenpunkt innerhalb des Netzwerks bezeichnet. Teilweise wird synonym auch der Begriff → Client genutzt. Jeder User kann seinen Rechner zu einem Node des Netzwerks machen. Auf diese Weise wird der Rechner ein vollwertiger Bestandteil des Blockchain-Netzwerks und speichert die → Blockchain. Bei allen nachfolgenden Transaktionen werden die Angaben hierzu von jedem Node empfangen, geprüft und weitergesendet. Bei diesem Vorgang kontaktieren sich die Nodes untereinander automatisch und validieren auf diese Weise die Informationen. Die Nodes müssen sich untereinander für diesen Vorgang nicht vertrauen, da stets Prüfsummen enthalten sind und somit konsistente Daten sichergestellt werden.

**Option**
Eine Option ist eine Vereinbarung von zwei Parteien zu einem Erwerb bzw. Verkauf eines bestimmten Finanzinstruments. Diese Vereinbarung ist ein Recht, was einseitig eingeräumt wird: Der Inhaber des Rechtes hat die Möglichkeit, innerhalb eines festgelegten Zeitraumes (Laufzeit) zu einem bei Vertragsabschluss festgelegten Preis eine ebenfalls fest definierte Menge an dem gewählten Basisinstrument zu kaufen oder zu verkaufen. Der Inhaber des Rechts kann das Recht ausüben oder auch verfallen lassen, eine Pflicht, dies auszuüben hat er also nicht. Im Gegensatz zu der o.g. so genannten amerikanischen Option hat der Rechteinhaber bei einer europäischen Option nur die Möglichkeit, sein Recht an einem bestimmten Tag auszuüben.

**Orphan**
Als Orphan (übersetzt „Waise“) ist ein Block, der nicht gültig ist. Beispielsweise ist ein Block, der auf einer → Fork erzeugt wurde, ein Orphan.

**Peer-to-Peer (Abk.: P2P)**
P2P ist die geläufige Abkürzung für den Begriff „Peer To Peer“. Bei einem „Peer To Peer“-System interagiert jedes Individuum des Systems direkt und unmittelbar mit den anderen Individuen des Systems. Alle Individuen sind dabei gleichberechtigt. Sie können die Dienste des Netzwerks sowohl in Anspruch nehmen als auch zugleich diese Dienste zur Verfügung stellen. Auf das Bitcoin-System bezogen, meint dies, dass jede Transaktion von jedem Nutzer an alle anderen Nutzer übermittelt wird. Durch diese Beschaffenheit wird eine dritte und überprüfende Instanz wie eine Bank für die Sicherheit des Systems überflüssig.

**Permissioned Ledger**
Dies ist ein genehmigungspflichtiges Kontenbuch. Bei diesem benötigt der User eine Autorisierung, um auf das Transaktionsverzeichnis zugreifen zu können. Dementsprechend gibt es bei einem Permissioned Ledger einen oder mehrere User, welche es nutzen und darüber entscheiden, welche anderen Nutzer die Daten einsehen dürfen. Dies hat den Vorteil, dass ausschließlich verifizierte User die Daten verwalten können und die Transaktionsgeschwindigkeit durch diese Begrenzung deutlich höher ist. Der Konsens-Mechanismus ist bei einem Permissioned Ledger deutlich einfacher als bei einer offenen → Blockchain. Durch diese Einfachheit kann das Tempo der Transaktionen gesteigert werden. Bisher setzen vor allem Regierungsinstitutionen sowie private Unternehmen bei der Nutzung auf die sogenannten Permissioned Ledger. Auf diese Weise verfügen sie über eine höhere Kontrolle hinsichtlich ihrer Daten sowie ihrer Transaktionen.

**Phishing**
Der Begriff Phishing ist die Adaption des englischen Wertes für „angeln/fischen“ also fishing. Unter Phishing versteht man daher das „Angeln“ nach Passwörtern mit Ködern. „Phisher“ fangen dabei persönliche Daten von Internetnutzern ab. Dies geschieht meistens über E-Mails und gefälschte Internetadressen, wo vor allem das Design einer originalen Website nachgeahmt wird. Nutzer sollen so auf die betrügerischen Webseiten gelockt und angestiftet werden, ihre sensiblen Daten dort einzugeben. Das Ziel der Initiatoren solcher Attacken ist es, die Nutzerdaten zu missbrauchen und somit Kontoplünderungen zu begehen. Um kein Phishing Opfer zu werden, überprüfen Sie deshalb immer die Internetadresse, auf der Sie sich befinden, doppelt. Folgen Sie vor allem keinen Links aus dem Internet, die Sie zum Besuch auf eine Webseite einladen, da Sie damit unbemerkt auf einer Betrugsseite landen können. Geben Sie daher die Webadresse von Hand in Ihren Browser ein.

**Proof of Developer (Abk.: PoD)**
Bedeutet Beweis des Entwicklers. Der → Bitcoin ist eine → Kryptowährung, die einen anonymen Entwickler hat. So weiß man bis heute nicht genau, wer unter dem Pseudonym Satoshi Nakamoto steckt. Das ist ein Beispiel dafür, dass → Kryptowährungen mit anonymen Initiatoren funktionieren können. Doch mit der Euphorie um → Kryptowährungen gibt es immer wieder Betrüger, die anonym → Kryptowährungen initiieren, das Projekt einstellen und mit dem vereinnahmten Geld zu verschwinden. Um vor solchen → Scam Aktivitäten zu schützen, gibt es mehrere Dienste, die die Identität eines Entwicklers bestätigen. Dies Bezeichnet man dann als Proof of Developer. Sie schützt in einem gewissen Maße vor betrügerischen Kryptowährungen, indem man genau nachvollziehen kann, wer hinter der Entwicklung eines Konzeptes und der Kryptowährung steckt.

**Ponzi Scheme / Ponzi Betrugsmasche**
Betrugsmasche, die nach dem ersten großen Betrüger mit diesem Vorgehen, Carlo (Charles) Ponzi, benannt wurde. Dabei wird Geld mit einem Gewinnversprechen von neuen Anlegern eingesammelt. Fordern Anleger ihre Gelder ein, werden diese nicht aus tatsächlich erzielten Gewinnen ausbezahlt sondern aus den Einzahlungen neuer Anleger. Dies schafft vermeintlich Vertrauen und lockt weitere Einzahler an. Das System funktioniert meist solange, bis eine Vielzahl von Investoren ihre Einlagen zurück erhalten wollen, dann bricht das gesamte System zusammen und Anleger bleiben auf ihren Verlusten sitzen. Das System ist einem Schneeballsystem ähnlich, allerdings stehen hier häufig Personen als vermeintlich vertrauenswürdige Partner im Fokus. Ein Beispiel für eine Ponzi Masche ist das Vorgehen von Betrüger Madoff in den USA.

**Proof of Stake (Abk.: PoS)**
Bei dem Proof of Stake handelt es sich um einen alternativen Mechanismus zum klassischen → Proof of Work. Die Proof of Stake soll dabei weniger Rechenleistung nutzen und so die Zyklen der Blockerzeugung verkürzen. Beim Proof of Stake entsteht eine Abhängigkeit zwischen der Wahrscheinlichkeit der Blockerzeugung durch einen User und seinem wertmäßigem Anteil am Netzwerk. Dadurch werden die Prozesse insgesamt vereinfacht und beschleunigt. Da es bei dem aktuellen Proof of Stake noch deutliche Sicherheitsprobleme gibt, wird dieser Ansatz weiterentwickelt.

**Proof of Work (Abk.: PoW)**
Der Proof of Work gewährleistet die Sicherheit des Systems ohne eine dritte Instanz. Er ist dabei jedoch ressourcenbelastend durch seine rechenintensiven unterschiedlichen Arbeitsschritte, welche die Sicherheit gewährleisten. Bei diesem Prozess wird eine Vielzahl von Daten zwischen den unterschiedlichen → Nodes im System verschickt und validiert. Ein Betrug wäre hierbei nur dann möglich, wenn ein User mehr als 50 Prozent der Rechenleistung innehielte und sein System permanent schneller arbeitet als die Systeme der anderen User → 51% Attacke. Beide Punkte zusammen sind relativ unmöglich zu erreichen. Weitere Schwierigkeit der Manipulation liegt in dem Umstand, dass die → Nodes sich untereinander nicht vertrauen und die Daten aus diesem Grund stets überprüft werden. Neben dem gängigen Proof of Work-Verfahren gibt es weitere Ansätze der Datenkontrolle.

**Private Key**
Der Private Key wird bei der ersten Installation eines jeden → Wallets generiert und ist so etwas wie der Generalschlüssel. Er gewährt Zugriff auf die im Wallet hinterlegten → Kryptowährungen und sollte stets sicher aufbewahrt werden. Denn wer den Private Key zum → Wallet verliert, hat keinen Zugriff auf seine → Kryptowährungen mehr. Ähnlich einer TAN-Liste oder der Geheimzahl für ein klassisches Bankkonto darf ein solcher privater Schlüssel niemals weitergegeben werden. Wer dieses Risiko des Verlustes oder Vergessens minimieren will, muss eine Recovery-Phrase anlegen. Dies entspricht im Grunde einem Daten-Backup. Verliert man den Private Key, kann dieser über die entsprechende Recovery-Phrase wiederhergestellt werden. Allerings bedeutet jede Speicherung auch eine Vergrößerung des Diebstahl oder Betrugsrisikos.

**Public Key**
Der Public Key (oder auch → Adresse) wird benötigt, um im Bitcoin-Netzwerk Bitcoinzahlungen zu empfangen bzw. zu senden. Hier ein Beispiel: „1Pdh123FYpDCmP67PWgvXYr4PL3zVLmiF8“

**QR-Code**
Ein QR-Code ist eine Art Bild, welches aus einem Muster aus Punkten und Balken besteht – hinter diesem Muster lassen sich technisch Information speichern. Durch ein Handy mit Kamera und QR-Code-App lassen sich die gespeicherten Informationen auslesen. Man kann z.B. eine Bitcoin-Adresse (→ Public Key) in einem QR-Code speichern. Diese Form der Darstellung erleichtert gerade das Erfassen der Bitcoin-Adresse per Smartphone.

**Ring-Signatur:**
Eine Ring-Signatur ist eine bestimmte Art einer digitalen Signatur, die von jedem Mitglied einer Gruppe ausgeführt werden kann, das über den jeweils entsprechenden Schlüssel verfügt. Eine der Sicherheitseigenschaften einer solchen Signatur ist, dass es rechnerisch nicht möglich ist festzustellen, welcher der jeweiligen Schlüssel verwendet wurde, um die Signatur zu erzeugen. Der Name Ring-Signatur kommt aus der ringförmigen Struktur des Signaturalgorithmus.

**Satoshi**
Als Satoshi wird die kleinste Einheit der → Bitcoins bezeichnet. Der Name ist als Hommage an den Gründer der Bitcoins, Satoshi Nakamoto, zu verstehen. Ein Satoshi ist ein Millionstel eines → Bitcoins, sprich: 0.00000001 BTC.

**Scam**
Als Scam werden betrügerische Aktivitäten bezeichnet, bei denen dem Nutzer vorgegaukelt werden soll, dass er in attraktive, sichere oder gewinnversprechende Projekte investiert. Dabei wird häufig viel Werbung gemacht, ohne dass wirklich Interesse besteht, das angepriesene Projekt zu betreiben. Es geht ausschließlich darum, z.B. über soziale Netzwerke Investoren anzulocken und dann mit den Geldern von der Bildoberfläche zu verschwinden. Scam ist kein ausschließliches Kryptowährungsphänomen, aber aufgrund der grundsätzlichen Anonymität und der Verlockung auf hohe Kursgewinne ist der Kryptowährungsbereich derzeit sehr anfällig für solche betrügerischen Aktivitäten.

**Schneeballsystem, siehe → Ponzi Scheme**

**Schürfen (siehe → Mining)**

**Scrypt**
Bei den → Bitcoins wird als Mining Algorithmus → SHA256 verwendet. Eine Alternative dazu stellt der Mining Algorithmus Scrypt dar, welches zum Beispiel bei der Kryptowährung „Litecoins“ zum Einsatz kommt. Scrypt hat dabei einen eigenen → Proof-of-work-Algorithmus, welcher von Colin Percival erdacht wurde. Es ist speicheraufwendig konzipiert, um → Brute-Force-Angriffe zu erschweren.

**SegWit – Segregated Witness**
Als SegWit wird ein Update des Bitcoin Core Quellcode bezeichnet. Dabei handelt es sich um die populärste Software in Bezug auf die → Bitcoins. Die SegWit wurde entwickelt, um der Transaktionsverformbarkeit entgegenzuwirken. Dabei handelt es sich um eine Sicherheitslücke, die zwar für den User nicht unmittelbar gefährlich ist und dennoch bereits mehrfach ausgenutzt wurde. Aus diesem Grund schritten die Core Entwickler zur Tat und entwickelten die SegWit. Neben der Transaktionsverformbarkeit wird bei der SegWit jedoch zudem an anderen Problemen wie der Skalierbarkeit der → Blockchain gearbeitet. So wurde SegWit bereits bei der Kryptowährung Litecoin erfolgreich implementiert. Dies lässt hoffen, dass SegWit die lang erwartete Lösung der Skalierungsprobleme der → Bitcoins ist.

**SHA-256**
Hinter diesem Kürzel verbirgt sich der Begriff Secure Hash Algorithm 256. Es handelt sich um eine kryptographische Funktion. Auf ihr basiert das sicherheitsrelevante → Proof-of-Work-System der →Blockchain. Die Ziffer 256 führt aus, wie die Länge des Algorithmus in Bit ist.

**Signatur**
Es ist möglich einer Bitcoinüberweisung eine Signatur zu geben. Diese ist vergleichbar mit dem Überweisungszweck einer SEPA-Überweisung im klassischen Banksystem. Dazu kann beispielsweise als Text vereinbart werden: „Ich, Vorname Nachname habe 10 BTC an die Adresse 1abc… überwiesen“
Mit dieser Signatur hat man einen unveränderbaren Klarnamen-Nachweis innerhalb einer ansonsten grundsätzlich kryptisch anonymen und dezentralen Struktur.

**Smart Contracts**
Smart Contracts gehören zu den Einsatzmöglichkeiten der Blockchain Technologie. Ein Smart Contract ist ein Programm, das einen Vertrag abbildet oder die Abwicklung eines Vertrages technisch unterstützt. In diesem Programm sind Bedingungen vordefiniert und können so Aktionen automatisch auslösen, wenn diese Bedingungen erfüllt werden. Hierdurch wird ein Grundstein gelegt für eine Vertragsdurchführung ohne menschliche Kontrollen. Interessant sind die Smart Contracts für viele unterschiedliche Bereiche wie Versicherungen oder allgemeiner Handel. Smart Contracts bilden dabei erst den Anfang einer neuen Entwicklung hin zu sogenannten Decentralized autonomous organizations (abgekürzt: DAO). Dies sind auf einer Blockchain basierende und autonom handelnde Unternehmen, welche keinerlei menschliche operative Eingriffe mehr benötigen. Die Kontrolle geschieht durch Algorithmen.

**Sniper Wallet**
Als Sniper Wallet wird eine → Wallet bezeichnet, die auf besonders schnelle Transaktionen ausgerichtet ist. Sinn dieser Wallets ist es, sich bei einem → ICO quasi „vorzudrängeln“ und früher an ein Investment zu kommen. Erzielt wird die Schnelligkeit, indem das sogenannte „Gas limit“ erhöht wird – also die maximalen Gebühren für die Transaktion. Kritiker bezeichnen dies auch moderne Form der Bestechung: Wer bereit ist, mehr zu zahlen, wird in der Bearbeitung priorisiert.

**Tokens**
Tokens erhält man bei einem → ICO im Tausch gegen einen bestimmten Betrag einer → Kryptowährung. Jeder Token ist vergleichbar mit einem digitalen Coupon, der beispielsweise zur Teilhabe an einem Unternehmen berechtigt. Gewinnt das Unternehmen später an Wert, steigt auch der Wert des Tokens – wie bei einer Aktie.

**Unpermissioned Ledger**
Bei einem Unpermissioned Ledger kann jeder User frei auf die Blockchain zugreifen. Für diesen Zugriff ist keine Erlaubnis nötig. Jeder User kann hierbei gleichberechtigt Transaktionen tätigen und Daten zu der Blockchain hinzufügen. Niemand kann bei dieser Blockchain das Ausführen von Transaktionen verhindern, da die Blockchain niemanden gehört und alle Nutzer gleichberechtigt sind. Wenn die Transaktion verifiziert werden kann, so wird sie ausgeführt.

**Usance**
Als Usance werden feste, nicht unbedingt in schriftlichen Regelwerken fixierte, Handelsbräuche an einem bestimmten Handelsplatz bezeichnet. Usancen können von Land zu Land und zusätzlich noch Marktplatz zu Marktplatz unterschiedlich sein.

**Utility Token**
Utility Token Besitzer können mit diesen Token zukünftig Zugang zu einem Service erwerben. Utility Token gewähren dem Benutzer Zugriff auf ein bestimmtes Produkt oder eine Dienstleistung, d.h. Utility Token haben einen speziellen zukünftigen Nutzen.

**Volatilität**
Dieser Begriff steht für Kursausschläge eines Finanzinstruments. Dabei bezeichnet die Volatilität die Schwankungsintensität eines Finanzinstruments. Je höher die Volatilität ist, umso stärker schwankt ein Finanzinstrument. Bei diesem Indikator werden historische Daten eines Marktes oder eines einzelnen Finanzinstrumentes nach statistischen Verfahren bewertet.

**Wallet**
In einem Wallet können → Kryptowährungen verwaltet, versendet und empfangen werden. Jedes Wallet verfügt über eine individuelle → Adresse, eine Art Transaktionsnummer, die für den Versand und den Empfang einer → Kryptowährung notwendig ist. Damit übernimmt ein Wallet im Bereich der → Kryptowährungen die Funktion einer elektronischen Brieftasche. Ein Wallet kann entweder als Paper Wallet, online oder über Hardware-Lösungen betrieben werden. Gleichzeitig ist das Wallet der Client, der den das Wallet ausführenden Rechner zum Teil des Coin Netzwerkes macht, zum → Node.

**Whales**
Als Whales (Wale) werden Personen bezeichnet, die sehr viele Münzen einer → Kryptowährung besitzen. Solche Nutzer mit vielen Anteilen können den Markt an der Börse sehr zum Schwanken bringen, wenn sie kaufen oder verkaufen. Gerade → Miner mit ihren in der Vergangenheit geschürften → Kryptowährungen stehen unter dem Verdacht, große Positionen von → Coins angehäuft zu haben, deren Verkauf einmal gravierende negative Auswirkungen auf die Kursentwicklung haben könnten.

**White Paper**
Als ein White Paper wird ein Dokument bezeichnet, welches im Grunde der Öffentlichkeitsarbeit dient und einen Einblick in eine neue Idee im IT-Bereich gibt. Der Begriff ist dabei dem politischen Weißbuch entlehnt. In einem White Paper werden die Leistungen, die Technik sowie die Standards einer Idee grundlegend erklärt. Im Jahr 2008 wurde unter dem Pseudonym Satoshi Nakamoto das Bitcoin White Paper veröffentlicht. In diesem White Paper wurden das System und das Protokoll für die Bitcoins genau beschrieben. Die meisten Gründer einer Kryptowährung nutzen ein White Paper, um ihre Idee publik zu machen. Sie erklären in ihm die spezifischen Eigenschaften der Währung und die Ziele der Währung oder ihres Unternehmens. Ein White Paper steht der Öffentlichkeit allgemeinzugänglich offen. Somit kann sich jeder Nutzer oder Interessent über Inhalte aber auch strategische Ausrichtungen/Ziele einer Kryptowährung informieren.

**Work Unit (Abk.: WU)**
Eine Work Unit, oder Arbeitseinheit, ist meist ein Teil eines größeren numerischen Problems. → BOINC Nutzer zum Beispiel laden diese kleinen Einheiten herunter, lösen diese mit ihrem Rechner, und laden die Lösung dann wieder hoch. Das Gesamtproblem wird dann mithilfe der einzelnen kleinen Lösungen gelöst.

# G Beispiele für Schadensfälle „Kryptowährungen“

**Die nachfolgende, nicht abschließende Liste der Betrugsversuche, Schadensfälle oder Insolvenzen im Bereich von Kryptowährungen soll Ihnen einen Eindruck davon geben, wie risikoreich der Handel, der Besitz und die Verwahrung von Kryptowährungen tatsächlich sind. Schäden haben zu Insolvenzen und zu temporären Schließungen geführt mit Totalverlusten für die Anleger geführt.**


- Am 15. August 2010 wurde der bisher schwerste Softwarefehler im Bitcoin-System entdeckt und behoben. Grundsätzlich wird geprüft, ob die Summe der Ausgänge einer Transaktion die der Eingänge nicht überschreitet. Eine eigens präparierte Transaktion führte aufgrund eines Fehlers zu einer nicht geprüften negativen Gesamtsumme, so dass die Transaktion als gültig akzeptiert wurde und zu einer Gutschrift von 184 Milliarden Bitcoin (BTC) führte. Für die Behebung war es notwendig, das Netzwerk umgehend zu stoppen und ein eilig erzeugtes Update zu verteilen. Die ungültige Transaktion wurde aus der Blockchain entfernt.

- Am 13. Juni 2011 erklärte der Nutzer „Allinvain“, dass bei einem Einbruch in seinen Computer ein Betrag von 25.000 BTC entwendet wurde (zu diesem Zeitpunkt umgerechnet 502.750 USD). Das gestohlene Guthaben wurde vom Dieb unerkannt wieder in den Kreislauf zurück gemischt

- Am 19. Juni 2011 verschaffte sich ein Angreifer bei der größten Onlinebörse Mt.Gox Zugriff auf ein Konto mit einem Guthaben von etwa 500.000 BTC (zu diesem Zeitpunkt rund 8,75 Mio. US-Dollar). Der Angreifer platzierte eine Verkaufsorder mit einem Volumen von 100.000 BTC zum Preis von 1 Cent pro Bitcoin, bei einem Marktpreis von rund 17 US-Dollar. Das Angebot erfüllte sämtliche offenen Kaufgesuche und führte zu einem kurzzeitigen Zusammenbruch des Handels. Der Handel bei Mt. Gox und der zweitgrößten Börse TradeHill wurde infolgedessen vorläufig ausgesetzt, die Preise kehrten jedoch nach Minuten zu ihren vorherigen Niveaus zurück. Zudem wurden auch Passwörter und Mailadressen ausgespäht und im Internet veröffentlicht.

- Am 26. Juli 2011 informierte der Betreiber der damals drittgrößten Tauschbörse Bitomat.pl, dass es aufgrund eines Datenverlustes zum Verlust von Bitcoin-Einlagen der Kunden in Höhe von 17.000 BTC (zum Zeitpunkt rund 170.000 €), gekommen sei.

- Am 11. August 2011 kündigte die japanische Betreiberfirma von Mt. Gox, Tibanne, überraschend an, den Dienst Bitomat.pl zu übernehmen und die Nutzer in die eigene Nutzerbasis zu integrieren. Dabei würden die Guthaben der Nutzer vollständig übernommen. Die Einlagen der Nutzer würden durch Mt. Gox ausgezahlt und es werde weiterhin möglich sein, polnische Złoty durch lokale polnische Banktransfers ein- und auszuzahlen.

- Im August 2011 verkündete der E-Wallet-Dienst MyBitcoin.com, gehackt worden zu sein, und stellte daraufhin seinen Dienst ein. Die Kunden erhielten knapp die Hälfte ihrer Einlagen wieder. Dieser Dienst stellte Nutzern eine Online-Wallet zur Verfügung, was allerdings bedeutete, dass – wie bei Tauschbörsen ebenfalls – sämtliche dort gespeicherten Beträge dem Dienst anvertraut wurden. Schon zuvor war kritisiert worden, dass der Dienst mit einer Postfachadresse an einem Offshore-Finanzplatz praktisch anonym geführt wurde.

- Am 1. März 2012 wurden bei einem Einbruch auf acht Kundenkonten auf Server des Cloud-Providers Linode Wallet-Daten im Gegenwert von 40.000 BTC (damals rund 150.000 €) ausgespäht. Zu den Kunden gehörten Dienstleister und Bitcoin-Börsenbetreiber. Verantwortlich für den Einbruch war ein Fehler in der Managementsoftware des Cloud-Servers, ein Verschulden der Kunden wurde nicht ermittelt.

- Am 12. Mai 2012 wurde bekannt, dass bei einem Einbruch in Server der Bitcoin-Börse Bitcoinica 18.547 BTC (damals rund 87.000 USD) entwendet wurden. Als Ursache wurde ein unzureichend gesicherter E-Mail-Server angegeben. Am 30. Juli erfolgte ein dritter Zwischenfall, bei dem in den Mt.Gox-Account von Bitcoinica eingebrochen wurde und 40.000 BTC verloren gingen. Nachdem Transaktionen aus diesem Guthaben auf den Eigentümer Zhou Tong zurückgeführt worden waren, gab dieser an, den gestohlenen Betrag vom Dieb zurückerhalten zu haben. In der Folge wurde am 1. August 2012 die Liquidation von Bitcoinica bekannt gegeben.

- Etwa am 18. August 2012 brach das bisher größte Schneeballsystem „Bitcoin Savings and Trust“ zusammen, welches von einem Individuum mit dem Pseudonym Pirateat40 initiiert wurde. Den „Investoren“, die vorher von zahlreichen Forennutzern vor dem offensichtlichen Ponzi-Schema gewarnt worden waren, waren Gewinne bis zu 7 % wöchentlich in Aussicht gestellt worden. Der gesamte Schaden wird auf bis zu 500.000 BTC geschätzt.

- Am 22. Dezember 2012 erklärte der Betreiber der auf Spendenbasis angebotenen Tauschbörse bitmarket.eu über das Forum bitcointalk, dass er (entgegen dem Versprechen eines Treuhanddienstes) mit den Einlagen der Nutzer spekuliert und Einlagen bei der Börse Bitcoinica angelegt habe, die sich Anfang August für zahlungsunfähig erklärte. Insgesamt habe er dabei rund 20.000 BTC, entsprechend rund 200.000 EUR, verloren. Da er kein eigenes Vermögen habe, sei er nicht in der Lage, die Einlagen der Nutzer zurückzuzahlen. Der Dienst war – ebenfalls Anfang August – vom Initiator an den Programmierer der Website übertragen worden.

- Am 11. März 2013 kam es aufgrund eines Softwarefehlers zu einer Abspaltung (Fork) der Blockchain.. Bis auf neu geschöpfte Geldeinheiten gingen keine Transaktionen oder Guthaben verloren. Um sicherzustellen, dass keine Coins in beiden Blockchains gleichzeitig gezielt ausgegeben werden konnten (Double Spend Attacke), suspendierten die Börsen kurzzeitig die Annahme von Bitcoin-Einzahlungen.

- Am 3. April 2013 wurde Instawallet, ein web-basierter Wallet-Anbieter, gehackt und über 35.000 Bitcoins entwendet (zum damaligen Zeitpunkt etwa 4,6 Mio. USD). Der Dienst wurde daraufhin eingestellt.

- Am 17. April 2013 wurde die damals viertgrößte Börse BitFloor geschlossen, da die Konten durch die US-amerikanische Bank des Unternehmens gesperrt wurden und keine ausreichende Liquidität mehr vorhanden war.

- Am 2. Mai 2013 verkündete CoinLab, das erste fremdfinanzierte Bitcoinunternehmen, dass es Mt.Gox wegen Vertragsverletzung auf Schadensersatz i. H. v. 75 Mio. USD verklagen werde und die Geschäftsbeziehungen eingestellt wurden.

- Am 15. Mai 2013 beschlagnahmte das Ministerium für Innere Sicherheit der Vereinigten Staaten Konten der Onlinebörse Mt.Gox beim Zahlungsdienstleister Dwolla, da Mt.Gox es versäumt hatte, sich in den USA als Zahlungsdienstleister zu registrieren.

- Anfang Februar 2014 wurden zahlreiche Bitcoin-Börsen, darunter Mt.Gox, Bitstamp und BTC-e, Opfer von Angriffen von Botnetzen, bei dem Versuch einen bekannten Programmfehler auszunutzen. Daraufhin stellten etliche Börsen, darunter auch die größte deutsche Bitcoin-Plattform *bitcoin.de* vorübergehend die Auszahlungen ein.

- Ende Februar 2014 berichtete die Presse über eine Unerreichbarkeit der Bitcoin-Börse Mt.Gox, der die Insolvenzanmeldung in Japan und den USA folgte. Mt.Gox erklärte gegenüber einem US-Gericht, dass rund 850.000 Bitcoins verloren gegangen seien, wovon 750.000 Bitcoins den Anlegern und 100.000 Bitcoins der Handelsplattform selbst zuzuordnen sind.

- Die wichtigste Bitcoin-Börse Bitfinex stellte nach der Entdeckung von Diebstahl von 120.000 Bitcoins mit einem Gegenwert von rund 65 Millionen Dollar (58 Mio. Euro) Anfang August 2016 den Betrieb vorläufig ein.

- Am 21. Juni 2017 kam es zu einem Flash Trade in Ethereum, die den Kurs von 300 US Dollar bis auf 13 US Dollar gedrückt hat. Die Betreiberbörse GDAX führte den Kursrutsch auf Margin Calls und ausgeführte Stopp Orders aus und beschloss trotz fehlendem eigenen Verschulden, die Anleger zu entschädigen. An anderen Marktplätzen gab es diese Kursverluste zunächst nicht, weswegen der

Handelsplatzbetreiber GDAX in die Kritik kam, den Handel zum Schutz aller Anleger nicht ausgesetzt zu haben, bis sich die Kurs an anderen Handelsplätzen angeglichen hätten. Aufgrund des dramatischen Kursverlustes von weit über 90% setzen auch andere Handelsplätze ihren Handel aus.

- Die slowenische Handelsplattform für Cyber-Währungen „Nice Hash“ meldete Anfang Dezember 2017 den Diebstahl von etwa 4700 Bitcoin durch Hacker. Der Gegenwert lag zu dem Zeitpunkt bei 68 Millionen US-Dollar.

Quelle: Wikipedia

Bitte beachten Sie: Diese Liste von Schadensfällen zeigt, dass Sie als Nutzer oder aber eine mit Ihnen in einem Geschäftsverhältnis stehende Handelsplattform o.ä. hohen Betrugs- und Diebstahlrisiken ausgesetzt sind. Letztlich tragen Sie das Risiko des Verlustes, Diebstahls oder Betrugs grundsätzlich selber.