Luzerner Kantonalbank

Risikohinweise für Kryptowährungen

Die Risikohinweise zu Kryptowährungen beschreiben die Risiken, die mit der Nutzung der Dienstleistungen der Luzerner Kantonalbank AG (nachstehend Bank genanngt) und den Kryptowährungen verbunden sind. Die Bank empfiehlt jedem Kunden, sich umfassend und über den Inhalt dieses Dokumentes hinaus mit den Risiken von Kryptowährungen zu befassen. Der Kunde trifft eigenverantwortlich seine Anlageentscheidungen zu Kryptowährungen, und ist sich dessen bewusst, dass die Risiken erheblich sind und im schlimmsten Fall zum Totalverlust seiner Investition oder der Kryptowährungen führen können. Die nachfolgend dargestellten, nicht abschliessend aufgezählten Risiken, können sich unvorhergesehen ändern und/oder es können neue (heute unbekannte) Risiken hinzukommen.

1. Technologische Risiken

Die Blockchain Technologie und die darauf aufbauenden Softwareanwendungen wie Smart-Contract-Systeme befinden sich noch in einem frühen Entwicklungsstadium, sind teilweise unerprobt und liegen ausserhalb der Kontrolle oder des Einflusses der Bank. Es gibt keine Garantie oder Gewährleistung dafür, dass die Übertragung, die Nutzung und der Besitz von Kryptowährungen ununterbrochen oder fehlerfrei abläuft, und es besteht ein inhärentes Risiko, dass das zugrundeliegende verteilte Register/Protokoll Schwachstellen, Lücken oder Programmierfehler enthalten können, die unter anderem, den vollständigen Verlust von Kryptowährungen verursachen können, selbst wenn die von der Bank genutzten Systeme korrekt funktionieren. Der Kunde ist sich bewusst, dass es häufig keine natürliche oder juristische Person gibt, die für solche Mängel haftbar gemacht werden kann, da die Funktionsweise der Kryptowährungen auf Open-Source-Software beruht. Technologische Fortschritte in der Entschlüsselung von kryptographischen Protokollen, im Brechen eines Codes oder Quantencomputer in Bezug auf Entschlüsselung, können eine Gefahr für die Sicherheit von Kryptowährungen sein. Kryptowährungen sind zudem häufig den Gefahren von Betrug, Diebstahl und Cyberangriffen ausgesetzt. Aufgrund der zugrundeliegenden Technologie, dass Transaktionen in Kryptowährungen nicht rückgängig gemacht werden können und in der Regel pseudonym erfolgen, sind Kryptowährungen ein attraktives Ziel für kriminelle Aktivitäten.

Weiterentwicklungen jeglicher Art können dazu geeignet sein, dass die zugrundeliegende Technologie der Blockchain oder einer Kryptowährung an Relevanz verliert, veraltet oder ein Risiko beinhaltet, was sich unmittelbar negativ auf den Preis von Kryptowährungen auswirken kann.

Der Kunde ist sich bewusst, dass Kryptowährungen und deren zugrundeliegende Software laufend angepasst werden. Software-Updates können zu hohen Risiken führen. Neben den rein technischen Risiken können Meinungsverschiedenheiten zwischen den Akteuren wie Entwicklern, Minern (Erzeuger von neuen Blöcken in der Blockchain) oder Node-Betreibern (Validatoren von Blockchain-Transaktionen) zu einer Protokolländerung führen, die eine Abspaltung der Kryptowährung zur Folge hat. Forks können den Handel in den betroffenen Kryptowährungen bei der Bank einschränken oder verhindern.

Darüber hinaus gibt es verschiedene Angriffsvektoren, welche die Verarbeitung von Transaktionen respektive Blocks auf der Blockchain stören oder verzögern können. So ist es möglich, dass die Blockchain der zugrundeliegenden Kryptowährung mit Transaktionen überflutet werden kann, weshalb es zu einer verlangsamten Verarbeitungszeit der Transaktionen auf der Blockchain kommt. Da die Kunden in der Regel mit der Bank als Eigenhändlerin handeln, übernimmt die Bank bei Käufen und Verkäufen der Kunden regelmässig das Risiko einer verzögerten Übertragung der Kryptowährungen auf der Blockchain. Sollte der Übertrag von Kryptowährungen jedoch im erheblichen Mass gestört sein, behält sich die Bank das Recht vor, die Kundentransaktionen zu stornieren. Hierzu gehören auch Szenarien, die Abzielen, die Kontrolle über die Blockchain zu übernehmen, beispielsweise mittels eines 51% Angriffs, in dem die Angreifer 51% der Rechenleistung kontrollieren oder zentrale Punkte einer Blockchain Infrastruktur (Miner, Nodes, usw.) angreifen und so in der Lage sein könnten, den Transfer von Kryptowährungen zu verlangsamen, zu verunmöglichen oder im schlimmsten Fall durch Betrug und Diebstahl in den Besitz von Kryptowährungen zu kommen. In der Regel haben solche Ereignisse auch negative Auswirkungen in das Ver-

trauen in Kryptowährungen und in deren Eigenschaften als Tausch- und Wertaufbewahrungsmittel, selbst wenn die gehandelten Kryptowährungen oder Bestände der Bank nicht betroffen sein sollten. Der Kunde ist sich dessen bewusst, dass dies negative Auswirkungen auf den Preis bis hin zum Totalverlust seiner Anlage in Kryptowährungen und deren Handelbarkeit haben kann.

2. Regulatorische und rechtliche Risiken

Obwohl in der Schweiz bereits ein Regulierungsrahmen unter anderem in der Form der "Mantelverordnung zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register" existiert, können zukünftige weltweite oder internationale Regulierungen oder Branchenstandards Auswirkungen auf die Dienstleistungen der Bank für Kryptowährungen haben. Es ist möglich, dass gesetzliche oder regulatorische Änderungen schwerwiegende Auswirkungen auf die von der Bank genutzten Systeme haben und infolgedessen zu einer Einschränkung oder Beendigung bestimmter Dienstleistungen für Kryptowährungen führen kann. Im Extremfall könnten neue Regularien die Handelbarkeit und die Übertragung von Kryptowährungen wesentlich einschränken oder sogar verbieten. Der Kunde ist sich dessen bewusst, dass die Nutzung der Dienstleistungen für Kryptowährungen rechtlichen, regulatorischen sowie auch steuerlichen Unsicherheiten und somit mit Risiken verbunden ist.

3. Markt- und Liquiditätsrisiken

Kryptowährungen sind hochvolatil, d.h. Preise von Kryptowährungen können sich erheblich ändern, selbst innerhalb eines Tages. Investitionen in Kryptowährungen sind generell hochspekulativ. Die vergangene Wertentwicklung einer Kryptowährung lässt keine Rückschlüsse auf die zukünftige Wertentwicklung zu. Kryptowährungen existieren erst seit kurzer Zeit, was zu einem gegenüber traditionellen Finanzinstrumenten deutlich höheren Risikoprofil in Bezug auf technologische, regulatorische und sonstige Risiken einhergeht. Der Kunde ist sich bewusst, dass aufgrund des dezentralen Charakters von Kryptowährungen nicht im gleichen Masse durch Zentralbanken, Aufsichtsbehörden oder sonstigen Institutionen beaufsichtigt sind und daher diese auch nicht eingreifen können, um den Wert von Kryptowährungen zu stabilisieren oder irrationale Wertentwicklungen zu verhindern oder zu vermindern. Der Kunde nimmt dies in Kauf, wenn er auf die Dienstleistung zugreift und diese nutzt. Das Risiko eines erheblichen oder vollständigen Wertverlusts von Kryptowährungen besteht somit zu jeder Zeit. Stablecoins können zusätzlich zu erheblichem oder vollständigem Wertverlust führen, wenn die Preisbindungen an den abgebildeten Vermögenswerten (Peg) unterschritten werden (z.B. aufgrund technischer, regulatorischer oder Marktrisiken sowie mangelhafter Preisbindungsmechanismen oder Sicherheiten).

Beim Handel von Kryptowährungen können Situationen begrenzter bis hoher Illiquidität eintreffen. Im Gegensatz zu traditionellen Vermögenswerten, an denen sich die Liquidität am Hauptbörsenplatz bündelt, ist der Handel von Kryptowährungen über verschiedene Kanäle verteilt. Geringe Liquidität zeigt sich in einem erhöhten Risiko von schnellen und hektischen Preisbewegungen, in einem grösseren Spread zwischen dem An- und Verkaufskurs und/oder in einer grösseren Anzahl von Ablehnungen von Orders. Die Preisstellungen der Bank für ihre Kunden hängen auch davon ab, inwieweit andere Markteilnehmer bereit sind, für die Bank Preise zu stellen. Der Kunde ist sich bewusst, dass es in bestimmten Marktsituationen schwierig oder gar unmöglich sein kann, bestehende Position zu liquidieren oder generell zu handeln.

Kryptowährungen sind üblicherweise nicht an einem regulierten Handelsplatz kotiert oder zum Handel zugelassen. Zudem unterliegen die Emittenten und die Besitzer der Kryptowährungen nicht den gleichen Regulierungen und Transparenzpflichten wie börsenkotierte Aktiengesellschaften. Häufig besitzen wenige natürliche oder juristische Personen einen Hauptanteil der handelbaren Kryptowährungen. In der Regel können die Halter dieser grossen Anteile ohne über ihre Handelsaktivitäten in den Kryptowährungen berichten zu müssen, direkt am Handel teilnehmen und den Preis der Kryptowährungen sehr stark beeinflussen. Die Preise für Kryptowährungen können zudem äusserst anfällig für Nachrichten und Kommentare in den sozialen Medien sein, ohne dass die Benutzer der Plattformen bekannt sind und somit für Missinformationen oder für marktmissbräuchliches Verhalten belangt werden können. Der Kunde ist sich daher dessen bewusst, dass die Preisbildung von Kryptowährungen anfällig für marktmissbräuchliches Verhalten wie Betrug oder Insiderhandel sein kann.

4. Gegenpartei-Risiken

Die Bank übernimmt in ihrer Rolle als Eigenhändlerin die Gegenparteirisiken für ihre Hedging Aktivitäten. Die Bank übernimmt jedoch keine Verantwortung für Gegenpartei-Risiken aus Kryptowährungen, die durch eine Währung oder einen anderen Vermögenswert gleich welcher Form (z.B. Stablecoins) besichert, gedeckt oder an sie gekoppelt sind oder dies vorgeben zu sein. In der Regel ist es nicht

möglich zu überprüfen, ob diese Vermögenswerte tatsächlich (gültig und durchsetzbar) besichert, gedeckt oder gekoppelt sind und ob der Inhaber einer solchen Kryptowährung einen rechtlichen oder faktischen Anspruch oder ein Recht auf diese besicherten, gedeckten oder gekoppelten Vermögenswerte im Insolvenzfall des Emittenten hat.

5. Verlustereignisse

Kryptowährungen unterliegen der Gefahr eines Verlustereignisses, wie einem kompromittierten Vorfall (z.B. ein System manipuliert, angegriffen oder gestört wird), der unmittelbar von der Bank und/oder dem Technologie-Provider und/oder Unterverwahrer gehaltenen Kryptowährungen aus welchem Grund auch immer (z. B. Hacking, Diebstahl, Betrug, Cyberangriff, Protokollanpassungen oder Abspaltung eines Protokolls („Fork" oder ähnlich Hardfork, Softfork)) oder dem Verlust des privaten Schlüssels (z.B. Private Key).