

Besondere Risiken von Crypto Assets

Inhalt

1.	Vorläufige Anmerkungen	1
2.	Umfang der Risiken	1
3.	Weitere Informationen und Hinweise.....	1
4.	Definitionen	2
5.	Marktrisiken	2
6.	Kreditrisiken	3
7.	Liquiditätsrisiken	3
8.	Technische und betriebliche Risiken	3
9.	Rechtliche und regulatorische Risiken	5

1. Vorläufige Anmerkungen

- 1.1. Diese Risikobroschüre bietet Kundinnen und Kunden (**Kunde, Sie** oder **Ihr**) einen Überblick über die Risiken im Zusammenhang mit Crypto Assets und den damit verbundenen Dienstleistungen, einschliesslich finanzieller und nicht-finanzieller Risiken (**Broschüre**).
- 1.2. Sofern nicht anders angegeben, gilt diese Broschüre für die Geschäftsbeziehung, die Sie mit einer Gruppengesellschaft der Bitcoin Suisse Gruppe unterhalten, einschliesslich **Bitcoin Suisse AG** und **Bitcoin Suisse (Europe) AG** (zusammen **BTCS**), wobei eine «Gruppengesellschaft» BTCS kontrolliert, von BTCS kontrolliert wird oder unter gemeinsamer Kontrolle mit BTCS steht (zusammen **Gruppengesellschaften**).
- 1.3. Die Broschüre ergänzt und bildet einen integralen Bestandteil der Geschäftsbeziehung und muss in Verbindung mit den entsprechenden Allgemeinen Geschäftsbedingungen (**AGB**) und allen anderen besonderen Vereinbarungen zwischen Ihnen und BTCS gelesen werden, soweit anwendbar. Sofern hierin nicht anders definiert oder aus dem Kontext nicht anders ersichtlich, haben alle Begriffe, die mit einem Grossbuchstaben beginnen, die gleiche Bedeutung wie in den entsprechenden AGB.
- 1.4. BTCS behält sich das Recht vor, diese Broschüre jederzeit anzupassen und zu ändern und Ihnen solche Änderungen gemäss den jeweils geltenden einschlägigen AGB mitzuteilen. Die aktuelle Version dieser Broschüre ist auf www.bitcoinsuisse.com/legal (**Webseite**) verfügbar.
- 1.5. Wenn Sie die Informationen in dieser Broschüre nicht verstehen, holen Sie bitte vor einer Investition oder Transaktion in Crypto Assets fachlichen Rat ein. BTCS ist nicht verpflichtet, Sie über das Eintreten oder das mögliche Eintreten eines der hierin beschriebenen Risiken oder anderer Risiken im Zusammenhang mit Crypto Assets zu informieren.
- 1.6. **Mit Aufnahme der Geschäftsbeziehung erkennen Sie die in dieser Broschüre (Ziffer 5-9) beschriebenen Risiken an und akzeptieren diese. Sie verstehen, dass die Verwirklichung solcher Risiken zu einem vollständigen Verlust der Investition und möglicherweise zu zusätzlichen Verlusten führen kann, die den ursprünglichen Investitionsbetrag überschreiten – abhängig von der Art des Crypto Assets sowie den Besonderheiten der Investitionstätigkeit und des Risikos.**

2. Umfang der Risiken

- 2.1. Sie erkennen an und erklären sich damit einverstanden, dass die Broschüre weder alle verfügbaren Risiken im Zusammenhang mit Crypto Assets abdecken noch eine erschöpfende Darstellung aller Risiken bieten kann, die diese möglicherweise mit sich bringen. Sofern verfügbar, wird empfohlen, sich auch auf die Informationsdokumente zu verlassen, die von Emittenten, Händlern, Finanzdienstleistern, Handelspartnern und anderen Personen bereitgestellt werden, die am Angebot, Vertrieb, Handel und anderen Transaktionen im Zusammenhang mit Crypto Assets beteiligt sind. Solche Informationsdokumente, einschliesslich, aber nicht beschränkt auf, Prospekte, Informationsblätter, White Papers, Factsheets und andere Informationsblätter, enthalten detaillierte Informationen über die Risiken und Kosten, die mit einem bestimmten Crypto Asset oder einer Klasse von Crypto Assets verbunden sind.
- 2.2. Diese Broschüre berücksichtigt nicht Ihre individuellen finanziellen, rechtlichen und steuerlichen Risiken. Für eine umfassende persönliche Beratung zu Ihrer finanziellen Situation wenden Sie sich bitte bei Bedarf an einen Anlageberater, Steuer- oder Rechtsexperten.

3. Weitere Informationen und Hinweise

- 3.1. Die Broschüre «Risiken beim Handel mit Finanzinstrumenten» der Schweizerischen Bankiervereinigung (SBVg) sowie die Broschüre «Risiken im

Effektenhandel» des Liechtensteinischen Bankenverbands können zusätzliche Informationen zu Crypto Assets enthalten.

- 3.2. Kunden wird empfohlen, regelmässig die relevanten Warnhinweise der zuständigen nationalen Behörden zu prüfen, darunter die Eidgenössische Finanzmarktaufsicht (FINMA), die Finanzmarktaufsicht Liechtenstein (FMA) sowie die europäischen Aufsichtsbehörden, insbesondere die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA).

4. Definitionen

- 4.1. **DLT.** Der Begriff «Distributed Ledger Technology» (DLT) ist eine Sammelbezeichnung für Technologien, die eine verteilte Datenbankarchitektur verwenden. Das bedeutet, dass über die ganze Welt verteilte Computer, die auch als «Knoten» bezeichnet werden, mehrere identische Kopien der Datenbank unterhalten und eine Software ausführen, um die Datenbank abzugleichen und zu koordinieren. Das Gegenteil von DLT wäre ein zentraler Server an einem einzigen Standort, der einem Unternehmen oder einer Person gehört.
- 4.2. **Blockchain.** Blockchain ist eine spezielle Art von DLT. Sie beschreibt die Tatsache, dass Daten in Blöcken aufgezeichnet werden, die durch den Einsatz von Kryptographie aneinander gekettet sind. Ein Block besteht aus Transaktionen, die von den Knoten im Netzwerk validiert werden. Wenn ein Block erzeugt wird, wird er in der Regel mit Hilfe einer kryptografischen Hash-Funktion «vervollständigt» (oder «gehasht»), die die Daten aller Transaktionen im Block und einen Verweis auf den vorherigen Block enthält, wodurch eine Kette oder Verbindung zwischen den Blöcken entsteht. Neue Blöcke werden von speziellen Knoten im Netz gefunden und der Kette hinzugefügt, die auch als «Miner» oder «Validatoren» bezeichnet werden.
- 4.3. **Permissionless, private und permissioned verteilte Register.** Bei verteilten Registern kann es sich entweder um «permissionless» (Teilnahme ist möglich für jeden, der über einen Node verfügt), «private» (ein Unternehmen oder eine Person betreibt ein eigenes verteiltes Register für interne Zwecke) oder «permissioned» (Teilnahme durch Einladung und Überprüfung des Teilnehmers möglich) verteilte Register handeln. «Permissionless» verteilte Register verwenden in der Regel öffentliche Blockchains, was bedeutet, dass alle Transaktionen zwischen Blockchain-Adressen für die Öffentlichkeit sichtbar sind. Da die Marktkapitalisierung von Crypto Assets in erster Linie auf jene Crypto Assets zurückzuführen ist, die auf «permissionless» und öffentlichen Blockchains ausgegeben werden, beschreibt diese

Broschüre hauptsächlich die mit solchen Systemen verbundenen Risiken.

- 4.4. **Crypto Assets.** Crypto Assets sind digitale Vermögenswerte, die dezentral oder zentral ausgegeben und über eine Blockchain oder ein anderes verschlüsselungsbasiertes verteiltes Hauptbuch übertragen werden.

5. Marktrisiken

- 5.1. **Marktrisiken sind Risiken, dass eine Anlage oder ein Vermögenswert seinen Wert ganz oder teilweise verliert.**
- 5.2. **Aufstrebender Markt.** Der Markt für Crypto Assets befindet sich noch in einer aufstrebenden und reifenden Phase, die mit erhöhter Volatilität und begrenzter Transparenz und Zuverlässigkeit, Ausführungsverzögerungen oder -ausfällen einhergehen kann, die alle potenziell zu Verlusten oder anderen nachteiligen Auswirkungen führen können. Investitionen in Märkte für Crypto Assets werden oft als risikoreicher angesehen als in langjährigen und reiferen Märkten. Darüber hinaus sind die Ausführungsplätze für Crypto Assets in der Regel rund um die Uhr, sieben Tage die Woche und 365 Tage im Jahr geöffnet. Dies bedeutet, dass die Crypto Assets ständigen Marktrisiken ausgesetzt sind, da der Handel nie unterbrochen wird und möglicherweise eine ständige Überwachung durch die Marktteilnehmer erforderlich ist.
- 5.3. **Schwierigkeit, einen fairen Wert zu bestimmen.** Es kann schwierig sein, den fairen Wert eines Crypto Assets vor der Investition zu bestimmen. Crypto Assets unterscheiden sich häufig von herkömmlichen Vermögenswerten in Bezug auf ihre Kapitalstruktur und Cashflows, was die Anwendung herkömmlicher Bewertungsmodelle erschwert. Crypto Assets stellen unter Umständen keine Eigentumsrechte oder Rechte an Cashflows dar, sondern gewähren oft Zugangsrechte zu einem Blockchain-basierten Dienst oder einer Anwendung. In diesem Fall kann es schwierig sein, den Wert der erworbenen Crypto Assets mit dem Wert der Dienstleistung zu vergleichen, für die das Crypto Assets verwendet werden kann. Dies birgt das Risiko, mehr für das Crypto Asset zu bezahlen, als er möglicherweise wert ist.
- 5.4. **Hohe Volatilität.** Der Marktwert von Crypto Assets ist oft volatil. Einige der Gründe für die Volatilität sind die geringe Marktkapitalisierung im Vergleich zu traditionellen Kapitalmärkten, das Risiko plötzlicher regulatorischer Änderungen, Trendzyklen und/oder Abhängigkeiten von der Entwicklung des Marktes für traditionelle Anlagen.
- 5.5. **Verbindung zu traditionellen Finanzinstrumenten.**

Der Wert von Crypto Assets kann sich auf den Marktwert traditioneller Finanzinstrumente stützen, wie z.B. tokenisierte Aktien oder Stablecoins, die an eine Fiat-Währung gekoppelt sind. Solche Crypto Assets können das gleiche oder ein ähnliches Risikoprofil wie das zugrunde liegende, nachgebildete oder gespiegelte traditionelle Finanzinstrument aufweisen und somit die Marktrisiken der traditionellen Märkte übernehmen.

6. Kreditrisiken

- 6.1. **Kreditrisiken sind Risiken, dass eine Partei einer Transaktion nicht in der Lage ist, ihre Verpflichtungen gegenüber ihrer Gegenpartei zu erfüllen.**
- 6.2. **Emittent.** Crypto Assets haben oft keinen Emittenten im herkömmlichen Sinne. Daher ist das Halten der meisten Crypto Assets in Eigenverwahrung nicht mit einem traditionellen Kreditrisiko verbunden. Dennoch kann bei bestimmten Crypto Assets ein Kreditrisiko bestehen, insbesondere in Form des Emittentenrisikos. Insbesondere kann es vorkommen, dass der Emittent eines Crypto Assets die Vermögenswerte nicht an den Käufer ausliefert, was bedeutet, dass das Kreditrisiko zum Tragen kommt.
- 6.3. **Traditioneller Emittent.** Bei traditionell begebenen Finanzinstrumenten, wie etwa einem börsengehandelten Finanzprodukt, das einen Korb von Crypto Assets nachbildet, kann das Gegenparteirisiko auch das Emittentenrisiko des jeweiligen Finanzinstruments umfassen.
- 6.4. **Ausfall der Gegenpartei.** Wenn ein Kunde Dienste eines Krypto-Dienstleisters, wie z.B. einer Krypto-Verwahrstelle oder eines Ausführungsplatzes, in Anspruch nimmt, können Crypto Assets das Ausfallrisiko der jeweiligen Gegenpartei tragen. Das Ausfallrisiko ist die Möglichkeit, dass eine Gegenpartei nicht in der Lage ist, ihren Verpflichtungen nachzukommen. So können beispielsweise Ausführungsplätze nicht in der Lage sein, Abhebungs- oder Abrechnungsanträge ihrer Kunden zu erfüllen. Darüber hinaus kann der Ausfall einer oder mehrerer Gegenparteien Ansteckungseffekte auf andere Krypto-Dienstleister haben und sich somit negativ auf den gesamten Markt für Crypto Assets auswirken, wodurch Markt- und Liquiditätsrisiken entstehen können.
- 6.5. **Keine Einlösung.** Selbst wenn die Crypto Assets an den Käufer geliefert werden, gibt es keine Garantie, dass die Crypto Assets gegen eine Fiat-Währung oder ein herkömmliches Finanzinstrument durch Umtausch beim Emittenten oder einem Dritten eingelöst werden können.

7. Liquiditätsrisiken

- 7.1. **Liquiditätsrisiken sind Risiken, dass der Kauf oder Verkauf eines Vermögenswerts gegen eine Fiat-Währung einen Einfluss auf den Preis des betreffenden Vermögenswerts haben kann. Wenn es beim Kauf oder Verkauf eines Vermögenswerts keine Preisauswirkungen gibt, ist der Vermögensinhaber keinem oder nur einem geringen Liquiditätsrisiko ausgesetzt.**
- 7.2. **Unreife Marktstruktur.** Die Märkte für Crypto Assets sind im Allgemeinen im Vergleich zu traditionellen Märkten unterkapitalisiert, da in der Regel weniger Marktteilnehmer auf diesen Märkten aktiv sind. Der Handel mit Crypto Assets kann an verschiedenen Arten von Ausführungsplätzen erfolgen, einschliesslich, aber nicht beschränkt auf zentrale Börsen, dezentrale softwarebasierte Plattformen und Peer-to-Peer-Marktplätze. Die Fragmentierung der Ausführungsplätze kann zu Illiquidität führen, was wiederum Preisschwankungen bei Crypto Assets zur Folge haben kann, wodurch der Kauf und Verkauf von Crypto Assets für den Vermögensinhaber schwierig oder sogar unmöglich wird.

8. Technische und betriebliche Risiken

- 8.1. **Technische und operationelle Risiken sind Risiken, die mit der Unangemessenheit oder dem Versagen von Verfahren, Menschen, Technologien und Systemen oder mit externen Ereignissen zusammenhängen.**
- 8.2. **Forks.** Eine Blockchain-Gabelung beschreibt ein Ereignis, das zu zwei sich widersprechenden Versionen der ursprünglichen Blockchain führt. Es gibt viele Gründe für eine Abspaltung, z.B. eine Änderung des Protokollcodes oder eine ungeplante Inkonsistenz des Protokollcodes aufgrund eines Softwarefehlers. Bei Unstimmigkeiten über eine Protokollaktualisierung kann sich ein Blockchain-Netzwerk in zwei Gruppen aufspalten, was zu mindestens zwei verschiedenen Blockchains und Netzwerken führt. Nach einer Abspaltung sind die Crypto Assets der ursprünglichen Blockchain auch auf der neuen Blockchain vorhanden. Im Falle einer Abspaltung kann es zu erheblichen Preisschwankungen kommen, die zu einer vorübergehenden Aussetzung des Handels, zu Cyberangriffen auf die Inhaber von Crypto Assets oder zu nachteiligen Auswirkungen auf die Funktionalität oder Konvertierbarkeit führen, was eine vollständige oder teilweise Verringerung des Werts der betroffenen Crypto Assets zur Folge haben kann.
- 8.3. **Replay-Angriffe.** Das Auftreten von Forks kann zu Replay-Angriffen durch Dritte führen. Replay-Angriffe finden statt, wenn Transaktionen in Crypto

Assets auf einer kürzlich «geforkten» Blockchain technisch gesehen auf beiden oder mehreren Blockchains gültig sind. Daher kann eine dritte Partei eine frühere Transaktion, die auf der alten Blockchain durchgeführt wurde, böswillig auf der neuen Blockchain wiederholen, was dazu führt, dass dieselbe Anzahl von Einheiten auch auf der neuen Blockchain übertragen wird.

- 8.4. **Verlust der privaten Schlüssel.** Der Zugang zu und die Nutzung einer Blockchain basiert auf der Public-Key-Kryptografie, die ein Paar privater und öffentlicher Schlüssel verwendet. Ohne den privaten Schlüssel kann ein Nutzer nicht auf die Blockchain und damit auf die Crypto Assets zugreifen. Private Schlüssel können auf verschiedenen Medien gespeichert werden, z.B. auf Papier, in Software- oder Hardware-Brieftaschen oder bei einem Krypto-Verwahrer. Diebstahl, Verlust, Zerstörung, Hacking oder andere Gründe, die dazu führen, dass der private Schlüssel nicht mehr verfügbar oder erkennbar ist, können zum dauerhaften Verlust der entsprechenden Crypto Assets führen
- 8.5. **Hacking.** Böswillige Dritte können Methoden und Mittel einsetzen, um Zugang zu privaten Schlüsseln zu erhalten. So können beispielsweise private Schlüssel, Seed-Phrasen oder relevante Passwörter, die per E-Mail übermittelt oder in einer Textdatei auf einem ungeschützten Computer gespeichert werden, von Dritten abgefangen und gelesen und zur Kontrolle der Blockchain-Adresse verwendet werden. Dies kann zu einem Totalverlust der Crypto Assets führen
- 8.6. **Hashing- und Verschlüsselungsalgorithmen.** Ein Hashing-Algorithmus ist eine mathematische Funktion, die aus Eingabedaten auf konsistente Weise einen eindeutigen Text ableitet. Crypto Assets und ihre Protokolle können nicht standardisierte, neuartige, veraltete oder fehlerhafte Hashing-Algorithmen verwenden, die zu Schwachstellen führen können, die den Wert der betreffenden Crypto Assets beeinträchtigen. Darüber hinaus können Protokolle Verschlüsselungsalgorithmen verwenden, die sich als fehlerhaft oder veraltet erweisen oder nur einen schwachen Schutz gegen böswillige Dritte bieten, was dazu führt, dass solche Algorithmen kompromittiert werden. Diese Risiken können besonders relevant werden, wenn die Möglichkeiten des Quantencomputings zunehmen.
- 8.7. **Verwendung von falschen Blockchain-Adressen.** DLT-Transaktionen werden an eine vom öffentlichen Schlüssel abgeleitete Blockchain-Adresse gesendet. Wenn eine falsche Adresse verwendet wird, kann es unmöglich sein, den Absender oder Empfänger zu identifizieren und die Transaktion rückgängig zu machen. Kunden, die beabsichtigen, Crypto Assets bei einem Krypto-Dienstleister zu hinterlegen, wird empfohlen, nur die ihnen mitgeteilten Blockchain-Adressen zu verwenden.
- 8.8. **Keine Möglichkeit, Gelder abzulehnen.** Wenn eine Transaktion an eine Blockchain-Adresse durchgeführt wird, kann der Eigentümer der Adresse Transaktion nicht ablehnen und somit den Erhalt von Crypto Assets nicht verhindern. Dies birgt das Risiko, Crypto Assets unfreiwillig zu erhalten und zu halten.
- 8.9. **Abhängigkeit von Dritten.** Die Ausführung und Abrechnung von Transaktionen mit Crypto Assets kann von den Spezifikationen des jeweiligen DLT abhängen, einschliesslich der Beteiligung von Dritten an dem jeweiligen Netzwerk, wie Minern oder Validatoren. Verzögerungen oder Ausfälle bei der Ausführung, Verarbeitung oder Abrechnung von Transaktionen können möglicherweise zu Verlusten oder anderen nachteiligen Auswirkungen für die Nutzer des Netzwerks führen, wie z.B. Wartezeiten bei der Einzahlung von Crypto Assets bei einem Krypto-Dienstleister oder bei Abhebungen von diesem.
- 8.10. **Unfähigkeit, Rechte auszuüben und Chancen wahrzunehmen.** Crypto Assets können ihren Inhabern rechtliche oder tatsächliche Rechte und Möglichkeiten einräumen. Zu den Rechten und Möglichkeiten kann die Verwendung als Zahlungsmittel oder als Beteiligung an Proof-of-Stake-Blockchain-Protokollen oder die Ausübung von Governance-bezogenen Rechten in Bezug auf die Entwicklung eines Blockchain-Protokolls gehören. Je nachdem, wie und wo die Crypto Assets gelagert oder verwendet werden, kann der Inhaber diese Rechte möglicherweise nicht ausüben oder diese Möglichkeiten nicht wahrnehmen.
- 8.11. **Angriffe auf den Konsens.** Ein dezentraler Konsens ist erforderlich, um Transaktionen und Blöcke zu validieren und die Blockchain zu sichern. Die Validierung kann Rechenleistung (Proof-of-Work), einen Einsatz (Proof-of-Stake) oder eine andere Form des Nachweises erfordern, je nach dem anwendbaren Konsensmechanismus. Es kann daher für einen Teilnehmer mit erheblicher Rechenleistung oder substanzieller Beteiligung möglich sein, den Konsensmechanismus effektiv zu manipulieren. Eine solche zentralisierte Macht kann zu verschiedenen Arten von Angriffen führen, z.B. zur doppelten Ausgabe von Crypto Assets oder zur Zensur von Transaktionen Dritter.
- 8.12. **Schwachstellen in intelligenten Verträgen.** Die Existenz, Funktionalität und Übertragbarkeit von Crypto Assets kann von intelligenten Verträgen abhängen, die auf der Blockchain eingesetzt werden.

Intelligente Verträge basieren auf Computercode, dessen Ausführung durch einen Nutzer oder einen anderen intelligenten Vertrag ausgelöst wird. Die Interaktionen mit intelligenten Verträgen können oft sehr komplex und meist unumkehrbar sein. Der Computercode kann fehlerhaft sein oder gehackt werden, oder er kann vom Bereitsteller oder einer anderen Person geändert werden, indem bestehende intelligente Verträge aktualisiert oder ersetzt werden. Die Logik intelligenter Verträge kann von Dritten ausgenutzt werden, z.B. durch Manipulation von Off-Chain-Preisorakeln, die falsche Daten in einen intelligenten Vertrag einspeisen. Die Nutzung eines intelligenten Vertrags hängt potenziell davon ab, dass das zugrunde liegende Netz verfügbar und nicht überlastet ist.

- 8.13. **Dezentrales Finanzwesen (DeFi).** Die Nutzung von DeFi-Anwendungen wie dezentralen Börsen oder Kreditvergabeplattformen kann besondere Risiken mit sich bringen, unter anderem Risiken im Zusammenhang mit intelligenten Verträgen, betrieblicher Sicherheit, wie die Verwendung von Admin-Schlüsseln durch die Entwickler oder eine andere Person, um eine DeFi-Anwendung zu steuern, Abhängigkeiten von anderen Komponenten und intelligenten Verträgen von DeFi, die Nutzung externer (Off-Chain-)Daten durch Orakel, verstärkte illegale Aktivitäten und Skalierbarkeitsprobleme.
- 8.14. **Schwachstellen in Open-Source-Software.** Crypto Assets basieren in der Regel auf Open-Source-Software, die frei zugänglich ist und von jedermann jederzeit kopiert, verwendet oder verändert werden kann. Obwohl die Entwicklung von Open-Source-Software viele Vorteile haben kann, können Fehler, Schwachstellen und absichtlich eingebaute Fehlfunktionen vorhanden sein und die Sicherheit von Crypto Assets beeinträchtigen, wenn man sie hält oder mit ihnen Transaktionen durchführt. Die Entwicklung von Open-Source-Software kann jederzeit eingestellt werden, was auch die langfristige Sicherheit von Crypto Assets beeinträchtigen kann.
- 8.15. **Sperrfristen für Einsätze.** Je nach Proof-of-Stake-Blockchain-Protokoll kann es Sperrfristen geben, während derer Nutzer keinen Zugang zu den von ihnen eingesetzten Crypto Assets haben. Dies kann zu einer vorübergehenden Illiquidität solcher Crypto Assets führen. Kunden von Einsatzdienstleistern können ebenfalls von Sperrfristen betroffen sein, wenn sie diese Anbieter mit dem Einsatz ihrer Crypto Assets beauftragen.
- 8.16. **Sanktionen und Slashing beim Staking.** Proof-of-Stake-Blockchain-Protokolle können «Sanktions- und Slashing-Mechanismen» enthalten, um Ausfallzeiten von Validatoren zu verhindern und

Fehlverhalten zu sanktionieren, wodurch die Stabilität und Sicherheit des Netzwerks gefördert werden soll. Wenn ein Validator für eine gewisse Zeit offline ist, sich unehrlich verhält oder anderweitig gegen die Protokollregeln verstösst, kann er das Risiko eingehen, seine Staking-Belohnungen – ob bereits verdient oder nicht – und/oder einen Teil der im Protokoll eingesetzten Crypto Assets zu verlieren, was potenziell zu einem vollständigen Verlust der Crypto Assets führen kann. Auch Kunden von Staking-Dienstleistern können von solchen Sanktionen und Slashing betroffen sein, wenn sie diese mit dem Staking ihrer Crypto Assets beauftragen.

- 8.17. **Datenschutz.** Nutzer erlaubnisfreier Blockchains sollten sich darüber im Klaren sein, dass jede Übertragung von Crypto Assets in einem öffentlichen verteilten Transaktionsregister aufgezeichnet wird und daher von Dritten, die nicht an der Übertragung beteiligt sind, eingesehen werden kann. Solche Informationen können von Dritten verarbeitet, ausgenutzt oder missbraucht werden. Es kann für Dritte möglich sein, eine Beziehung zwischen einer Blockchain-Adresse und der Identität ihres Besitzers zu rekonstruieren.

9. Rechtliche und regulatorische Risiken

- 9.1. **Rechtliche und aufsichtsrechtliche Risiken sind Risiken, dass eine unsichere rechtliche Behandlung oder eine Änderung der geltenden Gesetzgebung eine Anlage oder einen Vermögenswert wesentlich beeinträchtigen kann.**
- 9.2. **Rechtliche Unwägbarkeiten.** Der rechtliche und regulatorische Rahmen für Crypto Assets kann in vielen Ländern noch unsicher sein, und Crypto Assets können in diesen Ländern unterschiedlichen rechtlichen und regulatorischen Vorschriften unterliegen. Insbesondere kann es nach geltendem Recht unklar sein, wer welche Rechte in Bezug auf Crypto Assets hat, einschliesslich Eigentumsrechte. Die uneinheitliche Behandlung und die potenziellen rechtlichen Massnahmen setzen die Inhaber von Crypto Assets sowie die Anbieter von Krypto-Dienstleistungen dem Risiko aus, dass die geltenden Gesetze nicht eingehalten werden und/oder die Rechte nach diesen Gesetzen nicht durchsetzbar sind, was sich letztlich auf den Wert des Crypto Assets auswirken kann.
- 9.3. **Kein gesetzliches Zahlungsmittel oder Unmöglichkeit der Einlösung.** Nutzer sollten sich darüber im Klaren sein, dass Crypto Assets, insbesondere Zahlungen-Token, weniger Rechtssicherheit bieten können als traditionelle Fiat-Währungen. Es besteht in der Regel keine Verpflichtung, Crypto Assets als Zahlungsmittel zu akzeptieren, da sie kein

gesetzliches Zahlungsmittel sind und nicht von einer Zentralbank oder Regierung ausgegeben werden. Darüber hinaus kann es vorkommen, dass von privaten Marktteilnehmern ausgegebene Stablecoins aufgrund einer unzureichenden oder illiquiden Deckung nicht oder nicht in vollem Umfang einlösbar sind.

9.4. **Sich ändernde Gesetzgebung und Aufsichtspraxis.**

Die rechtliche und regulatorische Landschaft in Bezug auf Crypto Assets in und ausserhalb der Schweiz entwickelt sich ständig weiter und verändert sich. Regierungsbehörden können in ihrem Zuständigkeitsbereich Crypto Assets klassifizieren oder bestehende Klassifizierungen ändern. Dies kann dazu führen, dass ein Crypto Asset von einem Ausführungsplatz gestrichen oder von einem Krypto-Dienstleister nicht mehr zum Handel angeboten wird, oder dass die mit Crypto Assets verbundenen Rechte nicht mehr gesetzlich anerkannt werden. Wenn Länder den Handel und/oder das Halten von Crypto Assets verbieten oder einschränken, kann dies dazu führen, dass solche Crypto Assets nicht mehr verkauft und/oder gehalten werden können, was letztlich ihren Wert beeinträchtigt.

9.5. **Begrenzte Transparenz, unangemessene Werbung und eingeschränkter Anlegerschutz.**

Crypto Assets sind möglicherweise nicht an einem regulierten Handelsplatz gelistet oder zum Handel zugelassen, und ihre Emittenten sind unter Umständen nicht verpflichtet, Informationen offenzulegen, die für Investitions- oder andere Entscheidungen relevant sind. Einige Crypto Assets und verwandte Produkte können aggressiv beworben werden, wobei Informationen verwendet werden, die verwirrend, unvollständig, ungenau und teilweise absichtlich irreführend sind – insbesondere in sozialen Medien, wo Influencer Anreize erhalten können, bestimmte Crypto Assets zu bewerben. Inhaber von Crypto Assets profitieren möglicherweise nicht von denselben Regeln und Vorschriften, die für börsennotierte Unternehmen und/oder auf traditionellen Märkten zum Schutz von Anlegern gelten.

9.6. **Klassifizierung.** Je nach den geltenden Gesetzen und Vorschriften können Crypto Assets unterschiedlich eingestuft werden, was dazu führt, dass für sie, für die Inhaber solcher Crypto Assets oder für Dienstleister, die sie ihren Kunden anbieten, unterschiedliche Regeln gelten. Krypto-Dienstleister können Crypto Assets je nach den spezifischen Umständen klassifizieren oder regelmässig neu klassifizieren. Dies kann dazu führen, dass sie ihren Kunden solche Crypto Assets nur noch eingeschränkt oder gar nicht mehr anbieten. Dies kann insbesondere dann der Fall sein, wenn neue Umstände den

Anbieter dazu veranlassen, ein Zahlungs-Token als Asset-Token neu zu klassifizieren.

9.7. **Tokenisierung.** Wenn Crypto Assets dazu bestimmt sind, gesetzliche Rechte und/oder Pflichten zu begründen, zu verankern oder zu repräsentieren, kann die rechtliche Wirksamkeit eines solchen Konstrukts in den potenziell relevanten Rechtsordnungen, einschliesslich der Rechtsordnung des Emittenten oder des Inhabers des betreffenden Crypto Assets, unterschiedlichen Regelungen unterliegen. Es besteht das Risiko, dass die Tokenisierung der zugrundeliegenden Rechte und/oder Pflichten und/oder die Übertragung solcher Rechte und/oder Pflichten durch Übertragung eines Crypto Assets nicht rechtswirksam ist und dass die Crypto Assets folglich nicht die erwarteten Rechte und/oder Pflichten beinhalten, was zu einem vollständigen oder teilweisen Wertverlust der jeweiligen Crypto Assets führen kann.

9.8. **Behandlung im Konkursfall.** Die Behandlung von Crypto Assets im Falle eines Konkurses oder eines ähnlichen Ereignisses unterliegt nach Schweizer Recht besonderen Bestimmungen. Während die jüngste Gesetzgebung die Rechtssicherheit verbessert hat, ist noch offen, wie die neuen Bestimmungen im Falle eines Konkurses eines Krypto-Verwahrers in der Praxis angewendet werden.

9.9. **Risiko eines missbräuchlichen Marktverhaltens.** Traditionelle Märkte und Handelsplätze unterliegen einem hohen Mass an Vorschriften, die darauf abzielen, faire und transparente Märkte zu fördern. Der Markt für Crypto Assets ist noch im Entstehen begriffen und unterliegt einem unterschiedlichen Mass an Regulierung. Daher halten sich nicht alle Marktteilnehmer an Standards, die mit den Marktverhaltensregeln traditioneller Märkte vergleichbar sind, mit denen Betrug, Marktmanipulation und Insiderhandel verhindert werden sollen, einschliesslich neuer Formen von Marktmissbrauch, die möglicherweise nur in Kryptomärkten existieren.

9.10. **Risiko betrügerischen und sonstigen böswilligen Verhaltens.** Der Markt für Crypto Assets zieht nachweislich betrügerische und böswillige Akteure an, die Marktteilnehmende auf unterschiedliche Weise ins Visier nehmen können – etwa durch das Hacken ihrer IT-Infrastruktur, einschliesslich Wallet-Software, durch das Täuschen zur Preisgabe vertraulicher Informationen, durch den Missbrauch ihrer Zugangsdaten und Identitäten oder durch das Vortäuschen von Handlungen, die nicht real oder plausibel sind («Social Engineering»). Zahlreiche gefälschte Crypto-Asset-Schemes, Hacks und Betrugsmaschinen existieren, und Anleger sollten sich bewusst sein, dass deren einziger Zweck darin

besteht, sie mit verschiedenen Methoden – einschliesslich sogenannter «Pump-and-Dump»-Strategien – um ihr Geld zu bringen.

- 9.11. **Gesetzliche Verpflichtungen.** Sich ändernde rechtliche und regulatorische Rahmenbedingungen können dazu führen, dass Crypto Assets oder Transaktionen von den Behörden in jeder Rechtsordnung zu einem bestimmten Zeitpunkt anders behandelt oder eingestuft werden. Abhängig von ihrem Wohnsitz können Nutzer unterschiedliche rechtliche Verpflichtungen im Zusammenhang mit dem Besitz, Kauf oder Verkauf von Crypto Assets oder der Nutzung bestimmter Dienstleistungen in Bezug auf Crypto Assets haben. Solche Verpflichtungen können rechtliche und regulatorische Verpflichtungen, steuerliche Verpflichtungen oder andere Anforderungen umfassen. Die Nichteinhaltung dieser Verpflichtungen kann zu rechtlichen Massnahmen und Sanktionen, einschliesslich strafrechtlicher Sanktionen, führen oder die Inhaber von Crypto Assets anderweitig beeinträchtigen.
- 9.12. **Verdorbenere Vermögenswerte.** Transaktionen mit Crypto Assets auf öffentlichen Blockchains können zu früheren Blockchain-Adressen und durch forensische Untersuchungen potenziell zu ihren Eigentümern zurückverfolgt werden. Crypto Assets, die kriminellen Aktivitäten zuzuordnen sind, können daher von Krypto-Dienstleistern und/oder Behörden als verdorben angesehen werden. Infolgedessen laufen Crypto Assets unter Gefahr, beschlagnahmt oder zumindest von Gerichten unbrauchbar gemacht zu werden, was den Wert der betreffenden Crypto Assets beeinträchtigen kann.
- 9.13. **Aufsichtsrechtliche Massnahmen.** Crypto Assets, ihre Emittenten oder Entwickler, Nutzer, Ausführungsplätze, Krypto-Dienstleister oder andere in der Branche tätige Parteien können aufsichtsrechtlichen Untersuchungen, Anordnungen oder anderen Massnahmen unterliegen, die möglicherweise zu einem vollständigen oder teilweisen Verlust des Wertes von Crypto Assets führen oder die Fähigkeit beeinträchtigen können, sie Kunden anzubieten, oder sich anderweitig auf Inhaber solcher Vermögenswerte auswirken können. Solche Massnahmen können auch den Handel und/oder das Halten von Crypto Assets verhindern, einschränken oder verbieten.