Neue Blockchain-basierte Marktinfrastrukturen: Digital Asset Custody

Die aktuell entstehende, neue Blockchain-basierte Marktinfrastruktur für digitale Assets bietet Unternehmen die Chance, neue, innovative Services zu entwickeln. Das Fundament für diese Dienstleistungen ist die sichere und kundenfreundliche Verwahrung dieser digitalen Vermögenswerte. Rechtliche Aspekte, wie die künftige Lizenzpflicht in Deutschland nach dem Kreditwesengesetz (KWG), die Compliance mit geldwäscherechtlichen Anforderungen und weitere Folgepflichten müssen beachtet werden. Eine Umsetzung kann auf Basis unterschiedlicher technischer Ansätze erfolgen, die allerdings spezifische Hardware- oder Softwarekomponenten erfordern.

Text — Dr. Matthias Hirtschulz, Dr. Marcus Hennig, Dr. Filipp Valovich, Daniel Resas, Dr. Niklas Ulrich

Die Repräsentation von Werten und Rechten auf Blockchain-basierten Systemen[1] („Digital Assets" oder „Crypto Assets") eröffnet vollständig neue Möglichkeiten der Erzeugung, Verwendung und Abwicklung von digital verwalteten Vermögenswerten. Einzelne Unternehmen der Finanzbranche haben den potenziell disruptiven Charakter dieser Entwicklung erkannt und setzen aktuell Projekte in großem Stil um, mit dem Ziel, Digital-Asset-basierte Produkte und Services zu starten.

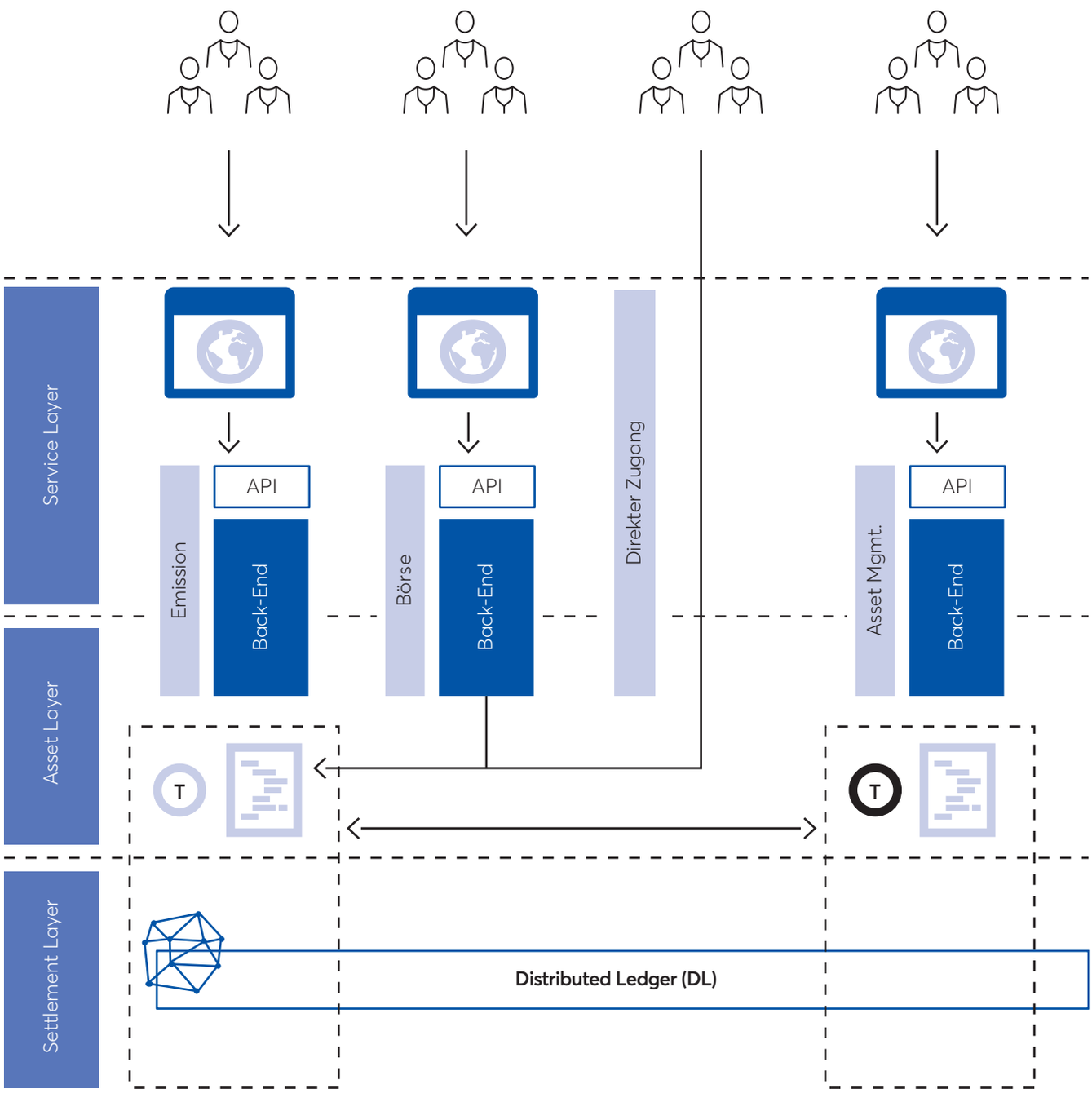
Parallel zur existierenden Marktinfrastruktur für Erzeugung (Primärmarkt), Handel (Sekundärmarkt) und Abwicklung entsteht aktuell eine neue Marktinfrastruktur für Digital Assets. Die klassischen Rollen in der Finanzbranche von Börsen, Banken bis Asset Manager und Verwahrer etc. werden dabei neu verteilt. Eine intensive und rechtzeitige Beschäftigung mit dem Thema ist daher für viele Unternehmen der Finanzbranche unabdingbar und führt oftmals zur Definition einer Digital-Asset-Strategie und der Umsetzung erster Angebote.

Damit ist diese Entwicklung nicht nur als disruptiv anzusehen, sondern birgt Chancen für etablierte und lizensierte Unternehmen der Finanzbranche, neue Umsatzpotenziale zu erschließen. Trotz des dezentralisierten Charakters der Blockchain-Technologie wird es nämlich auf absehbare Zeit weiterhin vertrauenswürdiger, lizensierter dritter Parteien bedürfen, die kundenfreundliche und sichere Services bereitstellen.

Das Potenzial der Technologie hat mittlerweile eine beträchtliche Anzahl von Regierungen erkannt. Dazu zählen nicht nur prominente Vorreiter in eher progressiven Jurisdiktionen

1 Im Allgemeinen spricht man von Distributed Ledger Technology (DLT), wobei es sich bei Blockchain nur um eine spezielle Ausprägung handelt. Aus Gründen der Lesbarkeit wird hier nur der Begriff Blockchain verwendet.

Abbildung 1: Blockchain-basierte Marktinfrastruktur für Digital Assets: Silos werden aufgebrochen und Services teilen Business-Logik und Daten



Vorteile

- Geteilte technische Basisinfrastruktur zwischen verschiedenen Services
- Daten- und Logiksilos werden aufgebrochen
- Offene, gemeinsame Infrastruktur fördert Innovation und Wachstum des Ökosystems
- Nutzer sind weniger von einzelnen Anbietern abhängig
- Freier Zugang zur Infrastruktur

wie beispielsweise Liechtenstein, die der Technologie gleich ein umfassendes Gesetz widmen, sondern neuerdings auch die Bundesregierung, die in ihrer Blockchain-Strategie klar Stellung bezieht und sich zur aktiven Förderung der Innovationen auf Basis der Blockchain-Technologie bekennt.

Eine der zentralen Herausforderungen und fundamentaler Bestandteil der neuen Infrastruktur ist die sichere Verwahrung von Digital Assets. Insbesondere im Bereich offener Blockchains kommt der sicheren Speicherung und Verwendung sogenannter kryptografischer privater Schlüssel dabei eine zentrale Bedeutung zu. Der Zugriff auf diese geheimen privaten Schlüssel erlaubt es, Transaktionen auf der Blockchain auszulösen und beispielsweise Assets zu übertragen. Der Verlust oder Diebstahl dieser privaten Schlüssel kann daher im schlimmsten Fall zum unwiederbringlichen, vollständigen Verlust der anvertrauten Werte führen.

Eine der zentralen Herausforderungen und fundamentaler Bestandteil der neuen Infrastruktur ist die sichere Verwahrung von Digital Assets.

Die Bundesregierung ist sich der Bedeutung der Verwahrung von Digital Assets bewusst. Der Bundesrat hat am 29. November 2019 dem von der Bundesregierung eingebrachten Gesetz zur Einführung des sog. „Kryptoverwahrgeschäfts“ als erlaubnispflichtigen Tatbestand im KWG zum 1. Januar 2020 zugestimmt. Der Tatbestand des Kryptoverwahrgeschäfts soll die „Verwahrung, die Verwaltung und die Sicherung von Kryptowerten oder privaten kryptografischen Schlüsseln, die dazu dienen, Kryptowerte zu halten, zu speichern oder zu übertragen, für andere“ erfassen. Kryptoverwahrer könnten damit als Finanzdienstleistungsinstitute vom Gütesiegel der Regulierung profitieren, sofern sie die entsprechenden Zulassungsvoraussetzungen erfüllen.

Im Rahmen des Erlaubnisantrags werden die Aufsichtsbehörden insbesondere den Geschäftsplan und die Organisationsstruktur der Gesellschaft, die Zuverlässigkeit, Eignung und Zeitkapazitäten der Geschäftsleiter, die Führungsstruktur und die finanzielle Solidität der Gesellschaft auf Regulierungskonformität überprüfen sowie eine Kontrolle der Inhaber bedeutender Beteiligungen durchführen. Kryptoverwahrer werden verpflichtet, ein regulatorisches Anfangskapital von mindestens 125.000 Euro zur Verfügung zu stellen. Finanzdienstleistungsinstitute, die außer dem Kryptoverwahrgeschäft keine weiteren Finanzdienstleistungen im Sinne des § 1 Abs. 1a Satz 2 KWG erbringen, wären von den aus der Bankenregulierung bekannten, darüber hinausgehenden Solvabilitätsvorschriften zur Unterlegung von Risiken mit Eigenmitteln befreit. Alle anderen Kryptoverwahrer müssten hingegen voraussichtlich die Solvabilitätsvorschriften einhalten. Hiervon losgelöst müssten in Gruppensachverhalten überdies die maßgeblichen Risikopositionen des Kryptoverwahrers aller Voraussicht nach in die Zusammenfassung der Risikopositionen auf konsolidierter Gruppenebene einbezogen werden.

Als Finanzdienstleistungsinstitute müssen die Kryptoverwahrer zudem geldwäscherechtliche Vorkehrungen treffen. Dies setzt das Vorhalten eines wirksamen Risikomanagements voraus, d. h. die Durchführung einer Risikoanalyse für das eigene Geschäft sowie die Schaffung interner Sicherungsmaßnahmen (z. B. Ausarbeitung einer Anti-Money Laundering (AML)-Policy, Einhaltung von Know-your-Customer-(KYC)-Pflichten, Bestellung eines Geldwäschebeauftragten etc.).

Sowohl im institutionellen Bereich als auch im Kontext von Privatanlegern stehen Nutzer und Dienstleister daher vor der Herausforderung, wie die Verwahrung rechtlich und technisch bewerkstelligt werden kann.

> **Kryptoverwahrer könnten damit als Finanzdienstleistungsinstitute vom Gütesiegel der Regulierung profitieren, sofern sie die entsprechenden Zulassungsvoraussetzungen erfüllen.**

Digital Asset Custody als Geschäftsmodell

Die Custody-Lösung selbst kann zunächst als reine Stand-alone-Lösung angeboten werden und/oder als Basis dienen, um diese in eigene oder andere externe Digital Asset Services zu integrieren. Mögliche Kundengruppen ergeben sich dann aus diesen Ansätzen. Beispielhaft seien folgende mögliche Kundengruppen genannt:

- High Net Worth Individuals (HNWI)
- Family Offices
- Privatkunden
- Digital Asset Funds
- Emittenten von Digital Assets
- Regulierte Handelsplätze für Digital Assets
- Weitere (regulierte) Anbieter von Digital Asset Services (z. B. Emissionsplattformen)

Jede dieser Kundengruppen wird unterschiedliche Anforderungen an die Ausgestaltung eines konkreten Serviceangebots haben. Während bestimmte Digital Asset Funds aus institutioneller Sicht beispielsweise regulatorische Anforderungen bzgl. der Auslagerung der Verwahrung erfüllen müssen (so z. B. die von einer erlaubnispflichtigen Kapitalverwaltungsgesellschaft verwalteten alternativen Investmentfonds (AIFs)) und garantierte Serviceleistungen fordern (Service Level Agreements, SLAs), steht bei Privatkunden eher eine hohe Benutzerfreundlichkeit im Fokus. Eine detaillierte Analyse der jeweiligen Kundenanforderungen ist daher je nach Zielgruppe notwendig, beispielsweise ist oft eine Abwägung hinsichtlich der Sicherheit und der Benutzerfreundlichkeit der Prozesse zu treffen.

Rechtlich haben Marktteilnehmer Spielraum bei der Entwicklung verschiedener Geschäftsmodelle (z. B. Kombination von einem multilateralen Handelssystem (MTF) mit dem Kryptoverwahrgeschäft). Das noch im Gesetzgebungsverfahren vorgesehene Trennungsgebot, demzufolge ein Finanzdienstleistungsinstitut neben dem Kryptoverwahrgeschäft keine andere erlaubnispflichtige Tätigkeit nach dem KWG hätte ausüben dürfen, wurde schlussendlich aufgegeben.

Eine weitere Dimension der Ausgestaltung einer Custody-Lösung sind die zu verwaltenden Digital Assets. Man kann in diesem Zusammenhang zunächst zwischen einfachen und komplexen Digital Assets unterscheiden. Einfache Digital Assets besitzen neben der reinen Übertragbarkeit keine weiteren (komplexen) Eigenschaften oder Funktionalitäten. Beispiel hierfür wären native Kryptowährungen wie Bitcoin oder Ethereum.[2] Diese Kryptowährungen werden im finanzaufsichtsrechtlichen Kontext als sogenannte Payment-Token bezeichnet. Bei der Verwahrung einfacher Digital Assets sind die wesentlichen umzusetzenden Services:

- Sichere Verwahrung der privaten Schlüssel
- Transaktionsausführung, d. h. Ein- und Auszahlungen
- Buchführung über die Bestände
- Reporting

Bei einigen der aktuell im Fokus stehenden Blockchain-Technologien ermöglichen sogenannte Smart Contracts die Strukturierung prinzipiell beliebig komplexer Assets. Für Token, die konventionelle Wertpapiere repräsentieren (sog. Security Token), können beispielsweise Cashflow-Strukturen abgebildet werden. Diese und andere Funktionen müssen auf der Seite des

2 Zukünftig könnten bei Ethereum durch Umstellung auf den sogenannten Proof-of-Stake-Konsensmechanismus allerdings weitere Funktionalitäten (Staking) hinzukommen.

Verwahrers dann unterstützt werden und beim Kunden „ankommen". Perspektivisch kommen daher insbesondere für Security Token klassische Asset-Servicing-Dienstleistungen hinzu.

Sowohl Payment- als auch Security Token stellen ab 1. Januar 2020 sog. Kryptowerte (eine neue Kategorie der Finanzinstrumente im KWG) im Sinne des Kryptoverwahrgeschäfts dar. Aus der Begründung des Gesetzentwurfes ergibt sich jedoch, dass das Kryptoverwahrgeschäft subsidiär sein soll gegenüber dem auf Verwahrung von Wertpapieren angelegten Depotgeschäft (§ 1 Abs.1 Satz 2 Nr. 5 KWG) und dem eingeschränkten Verwahrgeschäft für AIFs (§ 1 Abs. 1a Satz 2 Nr. 12 KWG). Mit anderen Worten ergibt sich folgende Systematik der Verwahrtatbestände: Token, die konventionelle Wertpapiere repräsentieren, sollen nicht in den Anwendungsbereich des neu eingefügten Kryptoverwahrgeschäfts fallen. Derzeit erfordert der für das Depotgeschäft maßgebliche Wertpapierbegriff allerdings noch die papierurkundliche Verbriefung der Wertpapiere. Das bedeutet, dass tokenisierte Wertpapiere vorübergehend noch vom Tatbestand des Kryptoverwahrgeschäfts erfasst wären. Die Blockchain-Strategie der Bundesregierung sieht aber mit der beabsichtigten Öffnung des deutschen Rechts für elektronische Wertpapiere und der entsprechenden Anpassung des Depotrechts Abhilfe vor. Diese Öffnung ist zunächst auf elektronische Schuldverschreibungen beschränkt. Ein Referentenentwurf hierzu dürfte noch bis Ende 2019 veröffentlicht werden. Die Einführung der elektronischen Aktie und elektronischer Investmentfondsanteile soll ausweislich der Blockchain-Strategie der Bundesregierung erst im nächsten Schritt geprüft werden.

Über die bereits genannten Eigenschaften hinaus kommen Funktionen hinzu, die man aus der klassischen Verwahrung nicht kennt und die Blockchain-spezifisch sind. Wir fassen diese Sachverhalte unter dem Begriff „Blockchain Servicing" zusammen.[3]

Zunehmend rücken auch Themen in den Fokus, die in der klassischen Welt der Prime Brokerage zugeordnet werden. Dazu gehört beispielsweise die Leihe oder grundsätzlich die Möglichkeit, Digital Assets im Rahmen von „Decentralized Finance"(DeFi)-Anwendungen zu nutzen. Darüber hinaus gibt es kundengruppenspezifische Anforderungen, beispielsweise OTC Trades sicher durchführen zu können, der direkte Anschluss an Handelsplätze oder ein (Lese-) Zugriff für dritte Parteien (z. B. Fund Administrator).

Zusammengefasst kommen neben den oben erwähnten Kernangeboten möglicherweise (in weiteren Ausbaustufen) folgende Services hinzu:

- Asset Servicing für Security Token und andere komplexe Digital Assets
- Blockchain Servicing
- Prime Brokerage Services
- Weitere (kundengruppenspezifische) Services

Damit geht eine Verwahrung von Digital Assets weit über die rein technisch sichere Speicherung von privaten Schlüsseln hinaus und eröffnet neben dem Kernangebot weitere Services und Erlöskomponenten. Im Rahmen einer Gesamtstrategie für Digital Assets kommt dieser Komponente oftmals strategische Bedeutung zu und sie ist auf kurz- bis mittelfristige Sicht kein Commodity-Service. Da über die Verwahrlösung die direkte technische und prozessuale Verbindung zur Blockchain besteht, hängen weitere Digital Asset Services oft von der Verwahrlösung ab. In einem sich extrem schnell verändernden Umfeld kann dann die Kontrolle über die Verwahrlösung zum Wettbewerbsvorteil werden.

Neben dem grundsätzlichen Serviceangebot stellt sich die Frage, welche Arten der Verwahrung aus Kundensicht möglich sind. Technologisch kann man hier hinsichtlich der Walletstruktur zwischen einer „Segregated Wallet" und einer „Omnibus Wallet" unterscheiden. Auf der Ebene der Blockchain erhält bei der Segregated Wallet jeder Kunde eigene Wallets. So können die für diese Kunden verwahrten Assets direkt auf der Blockchain nachvollzogen werden, wenn die zur Wallet gehörige Adresse bekannt ist.

Bei der Omnibus Wallet hingegen werden innerhalb einer Wallet Digital Assets von mehreren Eigentümern verwaltet. Die entsprechenden Eigentumsverhältnisse werden dann separat („off-chain") festgehalten. Dieses Konzept ist

Wallet
Ein Wallet ist eine digitale Brieftasche und besteht aus einer Sammlung von Blockchain-Adressen, die Assets empfangen und transferieren können. Eine Custody-Lösung verwaltet solche Wallets für ihre Kunden, indem sie die den Adressen zugehörigen privaten Schlüssel erzeugt, sicher verwahrt und zum Signieren von Transaktionen verwendet.

3 Zu diesen Sachverhalten gehören beispielsweise Airdrops, Staking, Hard Forks oder Voting.

u. a. bei zentralisierten[4] Handelsplätzen für Digital Assets üblich. Im Gegensatz zu Segregated Wallets muss hier bei einem Eigentumsübergang keine Blockchain-Transaktion ausgelöst werden, wenn die Digital Assets von Verkäufer und Käufer in derselben Omnibus Wallet verwaltet werden.

Welchen Einfluss bestehende aufsichtsrechtliche Vorgaben wie die MaDepot (Mindestanforderungen an die ordnungsgemäße Erbringung des Depotgeschäfts und den Schutz von Kundenfinanzinstrumenten für Wertpapierdienstleistungsunternehmen) auf die Anforderungen für die Verwahrung elektronischer Wertpapiere haben, wird sich in der Praxis noch zeigen müssen. Als sicher dürfte gelten, dass eine vergleichbare individuelle Zuordnung der Kundenbestände gewährleistet sein muss. Ob dies die Verwendung von Omnibus Wallets grundsätzlich ausschließt, ist damit aber noch nicht zwingend gesagt. Klärungsbedürftig sind auch die Implikationen für die Verwahrung sonstiger Crypto-Assets, die keine Wertpapierqualität besitzen.

Schließlich kann hinsichtlich des Sicherheitsniveaus der Wallets unterschieden werden. Man spricht hier von sogenannter „Hot Storage", „Warm Storage" oder „Cold Storage". Von Letzterer spricht man, wenn die Speicherung der privaten Schlüssel besonders sicher in einem sogenannten „air-gapped" System abgelegt ist, d. h. dauerhaft vom Internet getrennt ist und der Zugriff physikalisch und durch strenge Prozesse abgesichert ist. Diese Cold Storage dient insbesondere der langfristigen sicheren Speicherung. Im Gegensatz dazu spricht man von Hot Storage, wenn das entsprechende Signierungssystem dauerhaft mit dem Internet verbunden ist und somit ohne manuelle Prozesse eine sofortige Transaktionsausführung und eine höhere Verfügbarkeit der Digital Assets ermöglicht. Die sogenannte „Warm Storage" ist ein Kompromiss aus beiden Extremen, die hohe Verfügbarkeit der Digital Assets mit erhöhter Sicherheit ggü. einer reinen Hot-Storage-Lösung verbindet.

Nach der Gesetzesbegründung für das Kryptoverwahrgeschäft umfasst der Tatbestand mit dem Begriff „Sicherung" sowohl die als Dienstleistung erbrachte digitale Speicherung der privaten kryptografischen Schlüssel Dritter, als auch die Aufbewahrung physischer Datenträger (z. B. USB-Stick, Papier), auf denen solche Schlüssel gespeichert sind. Die bloße Zurverfügungstellung von Speicherplatz, z. B. durch Webhosting- oder Cloudspeicher-Anbieter, ist hingegen nicht tatbestandsmäßig, solange diese ihre Dienste nicht ausdrücklich für die Speicherung der privaten kryptografischen Schlüssel anbieten. Nicht erfasst ist auch die bloße Bereitstellung von Hard- oder Software zur Sicherung der Kryptowerte oder der privaten kryptografischen Schlüssel, die von den Nutzern eigenverantwortlich betrieben wird, soweit die Anbieter keinen bestimmungsgemäßen Zugriff auf die damit gespeicherten Daten haben.

Insgesamt muss abgewartet werden, wie Aufsicht und Gerichte den „bestimmungsgemäßen Zugriff" interpretieren werden. Sachgemäß wäre es, wenn die bloße Zurverfügungstellung eines Smart Contracts, der Kryptowerte im Rahmen eines Plattformgeschäftsmodells nach vordefinierten Regeln automatisch verarbeitet (z. B. zum Zwecke des Settlements lediglich kurzfristig zwischenspeichert), nicht die vorgenannte Schwelle des bestimmungsgemäßen Zugriffs überschreiten würde.

Technische Umsetzung

Um eine Custody-Lösung umzusetzen, muss man einerseits eine technische Lösungsarchitektur und andererseits die notwendigen Geschäftsprozesse implementieren. Abbildung 2 zeigt die grundlegenden Komponenten einer möglichen IT-Architektur.

Endnutzer greifen auf die Dienste der Custody-Lösung beispielsweise mit einer Web-Applikation (User Interface, UI) zu, wohingegen Benutzer wie Asset Manager oder Börsenplätze die Dienstleistungen über eine Applikationsschnittstelle (API) in ihre Systemlandschaft integrieren.

Zur Abbildung der Businesslogik des Verwahrers müssen bestimmte Servicekomponenten in der Lösungsarchitektur implementiert werden. Dies kann zum Beispiel mithilfe von Mikroservices geschehen, die über ein Nachrichtenbussystem gesteuert werden.

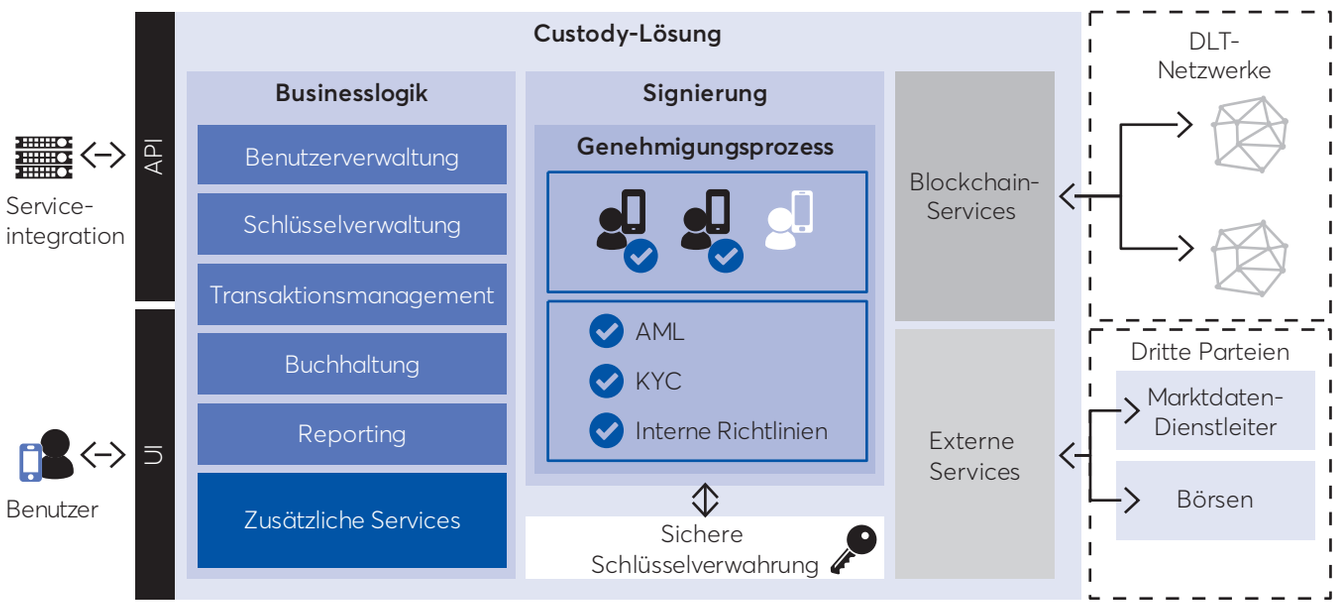
Wie bereits eingangs erwähnt, erlaubt der Zugriff auf den privaten Schlüssel Kontrolle über die Digital Assets. Insofern kommt der Signierungs-

Air-Gap
Das Verwenden eines Air-Gaps (dt. "Luftspalt") hat das Ziel, eine sicherheitskritische Hardware-Komponente von der übrigen IT-Infrastruktur physisch abzukoppeln, sodass diese Hardware-Komponente insbesondere vom Internet getrennt und damit vor Angriffen aus dem Netz geschützt ist.

Mikroservices
In der Software-Entwicklung spricht man von einer Mikroservice-Architektur, wenn eine Software in einzelne unabhängige Komponenten zerteilt ist. Diese Komponenten interagieren miteinander, z. B. mithilfe einer zentralen Orchestrierungssoftware. Dieser Ansatz ist sinnvoll, wenn einzelne Service-Komponenten im operationellen Prozess möglichst leicht austauschbar sein sollen.

4 Im Gegensatz zu sogenannten dezentralisierten Handelsplätzen ("DEX"). Matching und Execution findet hier komplett in klassischen IT-Systemen statt, so dass ein Großteil der heutigen Handelsvolumina sich nicht in Blockchain-Transaktionen niederschlägt.

Abbildung 2: High-Level-Architektur für eine Custody-Lösung



komponente und damit der sicheren Verwahrung des privaten Schlüssels eine entscheidende Rolle zu, die im Folgenden näher beleuchtet wird.

Der private Schlüssel sollte derart gespeichert werden, dass er sowohl vor internen als auch vor externen Attacken geschützt ist. Zu keinem Zeitpunkt sollte der private Schlüssel für Angriffe im Speicher von Hardwarekomponenten exponiert werden, die nicht speziell gesichert sind. Beispielsweise würde bereits ein kurzzeitiges Laden des privaten Schlüssels in den Speicher eines Servers ermöglichen, diesen zu stehlen und damit Zugriff auf die dazugehörigen Digital Assets zu erlangen. Für die Signierung existieren verschiedene technische Lösungen, die von Hardware- bis Softwarelösungen reichen und teilweise auch kombiniert werden.

Grundsätzlich ist es möglich, die Infrastruktur, auf der die Signierung läuft, durch ein Air-Gap physisch wie auch logisch von der im Internet stehenden Infrastruktur zu trennen. Damit steht man vor der Herausforderung, die unsignierte und später signierte Transaktion über das Air-Gap an die an das Internet angebundene Infrastruktur zu übertragen. Die Möglichkeiten reichen hier von akustischen bis optischen Datenübertragungsverfahren.

Die Verbindung zu den Blockchain-Netzwerken erfolgt mithilfe eines Blockchain-Services, welcher die folgenden Funktionen erfüllt:

- Kommunikation mit den Blockchain-Nodes
- Versendung von signierten Transaktionen
- Abfrage der Bestände der verwalteten Adressen
- Lauschen auf relevante Ereignisse und ggf. Weiterleitung zur Weiterverarbeitung an die Businesslogik

Die Anbindung von Drittanbietern, wie z. B. Börsenplätzen und Marktdaten-Diensten z. B. für Wechselkurse, erfolgt über die Komponente Externe Services. Wechselkurse werden insbesondere für die Bestimmung von Grenzwerten von Transaktions-Restriktionen benötigt. Man stelle sich hier etwa einen nutzerspezifischen maximalen Auszahlungsbetrag pro Tag vor, der im Sinne des Risikomanagements in Euro bemessen wird.

Herausforderungen in der Umsetzung

Eine wesentliche Herausforderung bei der Umsetzung besteht darin, einen Genehmigungsprozess für eine Transaktion direkt und sicher mit der Erstellung einer Signatur für die Transaktion zu verknüpfen. Mit anderen Worten: Eine Transaktion wird dann und nur dann signiert, wenn der Genehmigungsprozess stattgefunden hat. Für

eine Technologie wie Secure Multi-Party Computation (MPC) ist die Verknüpfung zwischen Signierung und Geschäftsprozess durch das zugrunde liegende kryptographisch abgesicherte Protokoll gegeben, d. h. eine Transaktion wird nur dann signiert, sofern ein mit den Schlüsselteilen verknüpfter Geschäftsprozess stattgefunden hat. Bei Hardware-Sicherheitsmodulen (HSMs) hingegen wird eine Kopplung mit dem Geschäftsprozess z. B. mittels Multi-Signature Authorization (MSA) realisiert. Erst wenn eine bestimmte Anzahl an „off-chain"-Signaturen vorliegt, wird eine „on-chain"-Signatur mit dem im HSM liegenden privaten Schlüssel erzeugt. Die Schwierigkeit besteht darin, einen eventuell flexiblen Geschäftsprozess mit einer fixen Anzahl an Signierungsschritten für die MSA zu kombinieren. Die für die Signierung benötigten Schlüssel müssen sicher gespeichert und vor Zugriffen geschützt werden. Für dedizierte Hardware, die z. B. Shamir's Secret Sharing verwendet, kann man ähnlich wie bei MPC einen Geschäftsprozess mit der Signierung verknüpfen, verliert jedoch an Flexibilität und Sicherheit. Zum einen ist eine Änderung des Geschäftsprozesses sehr aufwendig, zum anderen ist es nicht weniger aufwendig, automatische Prüfungen zu integrieren. Ein Nachteil aus der Perspektive der Sicherheit ist es, dass die Schlüsselteile zum Signieren kurzzeitig zusammenkommen müssen und damit der private Schlüssel, wenn auch nur kurzzeitig, exponiert ist.

Secret Sharing
Secret Sharing ist ein kryptographisches Verfahren zum Aufspalten eines Geheimnisses. So teilt ein 2-von-3 Secret-Sharing-Verfahren einen privaten Schlüssel in drei Teile, sodass einerseits nur zwei dieser Teile ausreichen, um den privaten Schlüssel zu rekonstruieren. Andererseits liefert die Kenntnis eines einzigen Teils keinerlei Erkenntnis über den privaten Schlüssel. Im Gegensatz dazu führt eine simple Teilung des privaten Schlüssels in drei Teile („abc" wird in „a", „b" und „c" zerteilt) dazu, dass der Verlust eines Teils den Verlust des privaten Schlüssels bewirkt und dass ein Angreifer mit Kenntnis von zwei Teilen den privaten Schlüssel leichter berechnen kann.

Zusätzlich muss der Genehmigungsprozess so konzipiert werden, dass dieser wenig Angriffsfläche bietet. Der Genehmigungsprozess sollte idealerweise zum einem aus einem manuellen Zustimmungsprozess durch ein Quorum bestehen, z. B. zwei von drei Teilnehmern autorisieren die Transaktion, und zum anderen aus einem automatischen Autorisierungs-Prozess, der die Transaktion auf Übereinstimmung mit den geltenden Regeln und Richtlinien überprüft:

- AML- und KYC-Regeln
- Intern festgelegte Richtlinien

Je größer das zur Genehmigung einer Transaktion erforderliche Quorum ist, desto niedriger ist die Erfolgs-Wahrscheinlichkeit eines Angriffs. Um den Genehmigungsprozess zu kontrollieren und damit die über den privaten Schlüssel verknüpften Digital Assets, müsste ein möglicher Angreifer eine Vielzahl an Quorum-Teilnehmern kompromittieren. Dem steht die Verwendbarkeit des Systems gegenüber. An dieser Stelle ist eine Abwägung zwischen Risiko und geschäftlichen Interessen nötig.

Insofern kommt der Signierungskomponente und damit der sicheren Verwahrung des privaten Schlüssels eine entscheidende Rolle zu.

Da die Entwicklung von Blockchain-Protokollen aktuell und in naher Zukunft starken Änderungen unterliegt, ist es strategisch wichtig, eine Custody-Lösung so aufzubauen, dass sie weitgehend Blockchain-unabhängig funktioniert. Native Blockchain-Lösungen für sichere Transaktionsfreigaben wie Multi-Signature sind dagegen hochspezifisch für unterschiedliche Blockchains. Die Unterstützung zusätzlicher Blockchains und Digital Assets kann je nach System schwierig sein. Z. B. werden HSMs mit der Unterstützung bestimmter Signatur-Algorithmen ausgeliefert. Falls der vom Verwahrer verwendete HSM über keine Unterstützung für einen Signatur-Algorithmus einer bestimmten Blockchain verfügt, kann der Verwahrer diese Blockchain nicht verwenden und entsprechend keinen Service dafür anbieten.

Weitere Herausforderungen für die Entwicklung und den Betrieb einer Custody-Lösung liegen im Management der Sicherheitsrisiken und in der Breite an Funktionalität. Als regulierte Finanzdienstleistungsinstitute müssten Kryptoverwahrer die Mindestanforderungen an das Risikomanagement (MaRisk (BA)) und die bankaufsichtlichen Anforderungen an die IT (BAIT) einhalten. Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich dann insbesondere an den Geschäftsaktivitäten sowie der Risikosituation zu orientieren. Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen u. a. die Integrität und die Verfügbarkeit der

Daten sicherstellen. Für IT-Risiken sind mithin angemessene Überwachungs- und Steuerungsprozesse einzurichten, die insbesondere die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung entsprechender Maßnahmen zur Risikobehandlung und -minderung umfassen.

Am sichersten wäre es, den privaten Schlüssel abzulegen und nie zu verwenden. Erst die Zurverfügungstellung setzt den Schlüssel potenziell einem Risiko aus. Typische Risiken sind u. a.:

- Verlust des privaten Schlüssels und damit einhergehend der verwahrten Digital Assets.
- Cyber-Angriff auf die Infrastruktur des Verwahrers: Der Service wird vorübergehend außer Betrieb gesetzt, was zu Geschäftsausfällen führt.
- Physische Attacken: Angreifer bricht ein und zwingt Mitarbeiter zur Herausgabe der Schlüssel.
- Attacken über Online-Kanäle, die Zugriff auf den privaten Schlüssel erlauben, insbesondere relevant bei Hot Storage.
- Inside Job durch kompromittierte Mitarbeiter, z. B. „Bad Admins“, die Zugriff auf private Schlüssel oder Teile davon haben.

Das Management solcher Risiken ist komplex und unabdingbar für eine Custody-Lösung. Es umfasst unter anderem:

- Sichere Replikation der privaten Schlüssel.
- Trennung von Verantwortlichkeiten, so dass die Kompromittierung einzelner Mitarbeiter wenig Auswirkung hat.
- Absicherung von operativen Räumen, z. B. Zugang mittels biometrischer Daten.
- Verwendung sicherer Kommunikationsprotokolle zwischen einzelnen Servicekomponenten. Zusätzlich kann die Integrität von Nachrichten zwischen Services durch digitale Signaturen sichergestellt werden.
- Abstellung von Internet-Konnektivität einzelner IT-Komponenten.

Fazit

Eine sichere, kundenfreundliche und Blockchainagnostische Verwahrlösung für Digital Assets mag eine technische Herausforderung darstellen. Deren Bewältigung ist aber insbesondere mit Blick auf die strategische Bedeutung der Verwahrlösung, die Abhängigkeit weiterer Digital Asset Services von dieser und die damit einhergehenden Umsatzpotenziale lohnenswert. Die künftige Kryptoverwahrlizenz nach dem KWG gewährleistet mit dem Label der Regulierung einen besonderen Vertrauensschutz und stellt damit eine große Chance, insbesondere im institutionellen Kontext, dar. ▪

Dr. Matthias Hirtschulz
ist Senior Manager bei d-fine und leitet die dortige Blockchain Practice.

Er verantwortet unterschiedlichste Blockchain-Projekte z. B. in den Bereichen Enterprise Blockchain, Markinfrastrukturen für digitale Assets oder Tokenization.

Dr. Marcus Hennig
ist Manager bei d-fine und und betreut verschiedene Blockchain-Projekte.

Nachdem er einige Jahre als Naturwissenschaftler in diversen Forschungszentren gearbeitet hat, startete er seine Karriere als Berater in der Finanzindustrie. Aktuell hilft er Kunden bei der Umsetzung von Blockchain-Projekten mit Schwerpunkt auf Crypto Custody.

Dr. Filipp Valovich
ist Consultant bei d-fine und Experte für Kryptographie und Blockchain.

Als Unternehmensberater arbeitet er derzeit schwerpunktmäßig an Crypto-Custody-Lösungen und an industriellen Blockchain-Use-Cases.

Daniel Resas
ist Rechtsanwalt bei Schnittker Möllmann Partners.

Er leitet die Blockchain & Digital Assets Praxis der Kanzlei und berät verschiedene Marktteilnehmer zu Blockchain-basierten Geschäftsmodellen und Transaktionen. Daneben ist er Senior Research Fellow an der Wharton School und Mitbegründer unterschiedlicher internationaler Arbeitsgruppen zu Regulierungsthemen im Blockchain-Kontext.

Dr. Niklas Ulrich
ist Rechtsanwalt bei Schnittker Möllmann Partners.

Er berät Fondsmanager, Investoren sowie Kredit- und Finanzdienstleistungsinstitute im Kontext Blockchain-basierter Geschäftsmodelle zu Fragen des Investment- und Bankaufsichtsrechts.