Vertrauen ist gut, Kontrolle ist besser

Unsere Blockchain Assurance sorgt für beides!

Neue Technologie, neue Geschäftsmodelle, spezifische Risiken - Distributed Ledger-basierte Geschäftsmodelle bringen spezifische Risiken mit sich, die es zu berücksichtigen gilt.

Regulatorische Änderungen durch eWPG & MiCa: Was auf Unternehmen zukommt

Die Distributed Ledger Technologie (DLT) hat in den letzten Jahren zur Entstehung vieler neuer Geschäftsmodelle beigetragen. Einige dieser Geschäftsmodelle, wie die Tätigkeit als Kryptoverwahrer oder die Führung eines Kryptowertpapierregisters nach § 16 eWPG, wurden erst durch Schaffung der gesetzlichen Rahmenbedingungen, insb. durch das Gesetz über elektronische Wertpapiere ermöglicht. Unternehmen, die solche Dienstleistungen erbringen gelten nun als Finanzdienstleistungsinstitute nach § 1 Abs. 1a KWG und müssen folglich gewisse Anforderungen hinsichtlich einer ordnungsgemäßen Geschäftsorganisation sowie eines angemessenen und wirksamen Risikomanagements erfüllen. Auch die MiCa-Verordnung schreibt auf europäischer Ebene vor, dass Anbieter von Krypto-Dienstleistungen strengen organisatorischen Anforderungen unterliegen und über solide interne Kontroll- und Risikobewertungs-mechanismen verfügen müssen.

Ein starkes Risikomanagement und internes Kontrollsystem sind wesentlich für den Erfolg DLT-basierter Geschäftsmodelle.

Risiken durch die Nutzung der Distributed Ledger Technologie

DLT-bezogene Risiken variieren je nach verwendeter DLT-Technologie. Die Herausforderung besteht darin, das Risikomanagement, die Geschäftsorganisation und das interne Kontrollsystem geeignet anzupassen, um die spezifischen Risiken angemessen zu berücksichtigen. Dies gilt sowohl für Start-Ups im Krypto-Sektor als auch für etablierte Unternehmen, die ihre Geschäftstätigkeit in den Krypto-Sektor erweitern möchten. Einige dieser Risiken haben wir in der folgenden Tabelle dargestellt:

Darüber hinaus kommt dem Notfallmanagement für IT-Systeme, das Business Continuity Management sowie einem angemessenen Auslagerungsmanagement bei Krypto-bezogenen Geschäftsmodellen eine wesentliche Bedeutung zu. Es ist davon auszugehen, dass die Aufsichtsbehörden die Entwicklungen im Krypto-Sektor weiter aktiv beobachtet, begleitet und künftig Prüfungen der Angemessenheit der Geschäftsorganisation und des Risikomanagements bei Krypto-Dienstleistern durchführt.

Unterschiedliche DLT bergen individuelle Risiken, die eine differenzierte Betrachtung erfordern. Risiken können dabei der Verlust privater Schlüssel, unsichere Smart Contracts und unzureichende Netzwerksicherheit sein. Unternehmen müssen angemessene Maßnahmen zur Risikominimierung ergreifen.

Wallets & Key Management

Risikotreiber

- Verlust oder Diebstahl von Kryptowerten oder privaten Schlüsseln durch mangelhaftes Berechtigungsmanagement
- Unzureichende Sicherheit bei der Wallet-Verwaltung (z.B. durch angreifbare API-Schlüssel)
- Menschliche Fehler bei der Schlüsselverwaltung

Mitigierende Maßnahmen

- Multi-Signatur-Lösungen für gemeinsame Kontrolle
- Hardware-Sicherheitsmodule für sichere Schlüsselspeicherung
- Verschlüsselung und regelmäßige Sicherheitsüberprüfungen und –updates
- Zugriffskontrollen und Back-up-Verfahren
- Schulungen (z.B. zu Phishing)

Anwendungs- / Smart Contract Security

Risikotreiber

- Potenzielle Schäden durch die Integration mit externen Datenquellen (Oracles) oder dApps
- Sicherheitslücken oder Fehler in Smart Contracts durch Fehler bei der Programmierung (z.B. unautorisierte Transaktionen, Umgehung von Transaktionslimits, mangelnde Verschlüsselung von Private Keys in Smart Contracts)
- Skalierbarkeit und Performance-Probleme von Smart Contracts

Mitigierende Maßnahmen

- Durchführung von Sicherheitsaudits, Code-Reviews und Penetrationstests
- Automatisierte Testverfahren und kontinuierliche Programmcodeverbesserungen
- Bug-Bounty-Programme und Zusammenarbeit mit Sicherheitsexperten
- Überwachung der Leistung und Optimierung der Smart Contracts

Netzwerk-Sicherheit und andere Sicherheitsthemen

Risikotreiber

- Unzureichender Schutz gegen 51%- oder Eclipse-Attacken sowie Blockchain-DoS-Angriffe durch Spam-Transaktionen
- Mängel in der Netzwerkarchitektur erzeugen Schwachstellen (z.B. single point of failure durch Hosten des gesamten Netzwerks in einer Cloud)
- Man-in-the-Middle-Angriffe
- Änderungen im DLT-Protokoll

Mitigierende Maßnahmen

- Anti-DDoS Lösungen einsetzen (z. B. Firewalls, Lastverteilung, geografische Redundanz)
- Intrusion-Detection- und Prevention-Systeme, Netzwerksegmentierung, VPNs
- Verschlüsselung, starke Authentifizierung, sichere Kommunikationsprotokolle

Vertrauen schaffen in DLT-basierte Geschäftsmodelle

Inzwischen sollte jedem, der sich mit der Distributed Ledger Technologie auseinandersetzt klar sein: nur weil die Blockchain in der Theorie fälschungssicher ist, heißt das nicht, dass grundlegende Prinzipien des Risikomanagements nicht beachtet werden müssen. Risikomanagement, Governance und internes Kontrollsystem dienen auch nicht nur der Erfüllung regulatorischer Anforderungen. Vielmehr sind sie essenziell, um Vertrauen bei Kunden, Geschäftspartnern und anderen Stakeholdern zu schaffen und somit ein wichtiger Baustein für den Geschäftserfolg.

Unsere Services

Gern unterstützen wir Sie bei der Überprüfung, Optimierung und Überwachung Ihrer DLT-bezogenen Geschäftsprozesse und Kontrollen. Unsere umfassenden und maßgeschneiderten Lösungen umfassen Risk Assessment und Compliance Checks, Smart Contract Audits sowie Trust-as-a-Service Dienstleistungen. So helfen wir Ihnen dabei das Vertrauen von Investoren, Kunden und Regulierungsbehörden zu gewinnen und zu erhalten.

DLT Risk Assessment & Compliance Check

Im Rahmen des DLT Risk Assessments begleiten wir Sie bei der:

- Erfassung der DLT-bezogenen Risiken unter Berücksichtigung Ihres konkreten Geschäftsmodells und Ihrer Geschäftsprozesse mit Hilfe des Deloitte Crypto Risk Frameworks
- Identifizierung von Lücken zwischen der vorhandenen Governance, dem Risikomanagement und dem internen Kontrollsystem und den Anforderungen der relevanten Regularien (z.B. MaRisk, BAIT, MiCa).
- Erarbeitung und Implementierung risikomitigierender Maßnahmen und Schließung identifizierter Gaps.

Gern unterstützen wir Sie auch bei der Vorbereitung von Audits oder aufsichtlichen Prüfungen.

Smart Contract Audits

Wir kombinieren einen Software-basierte Smart Contract Analyse mit einem manuellen line-by-line Code Review und fassen die Ergebnisse für Sie in einem umfassenden Audit Report zusammen.

Trust as a Service

Durch unsere langjährige Erfahrung als Treuhänder und unabhängiger Dritter in Kapitalmarkttransaktionen kombiniert mit unserer Expertise im DLT-Bereich können wir Risiken für Transaktionsparteien reduzieren und Vertrauen schaffen, z.B. durch das Halten von Sicherheiten oder das Herbeiführen von Abstimmungen.

Contact us:

Martin Flisgen
Partner | Digital/AI Controls/ Algorithms
Tel: +49 211 8772-4034
E-Mail: mflisgen@deloitte.de

Heiko Jacob
Partner | IT & Specialized Assurance (Industry)
Tel: +49 211 8772-3433
E-Mail: hejacob@deloitte.de

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited ("DTTL"), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die "Deloitte-Organisation"). DTTL (auch "Deloitte Global" genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter www.deloitte.com/de/UeberUns.Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeiterinnen und Mitarbeiter liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 415.000 Mitarbeiterinnen und Mitarbeiter von Deloitte das Leitbild "making an impact that matters" täglich leben: www.deloitte.com/de. Diese Veröffentlichung enthält ausschließlich allgemeine Informationen. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited ("DTTL"), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (insgesamt die "Deloitte Organisation") erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen. Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeitenden oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbständige und unabhängige Unternehmen.