Kapitel 1: Herausforderungen technischer Begriffsdefinitionen in der MiCAR

Nicholas Stifter/Aljosha Judmayer

Literaturverzeichnis

ACM Symposium on Principles of Distributed Computing 2019 (Tagungsband); *Birman*, The promise, and limitations, of gossip protocols, ACM SIGOPS Operating Systems Review 2007, 8; *Bonneau et al*, Coda: Decentralized cryptocurrency at scale, Cryptology ePrint Archive 2020, Nr 352; *Bonneau et al*, Sok: Research perspectives and challenges for bitcoin and cryptocurrencies, IEEE symposium on security and privacy 2015; *Chaum*, Achieving electronic privacy, Scientific american 1992, 96; *Chaum/Fiat/Naor*, Untraceable electronic cash, Advances in Cryptology – CRYPTO'88 (1990), 319–327; *Chaum/Rivest/Sherman* (Hrsg), Advances in Cryptology: Proceedings of Crypto 82 (1983); Companion Proceedings of the Web Conference 2022 (Tagungsband); Cryptology–CT-RSA 2020: The Cryptographers' Track at the RSA Conference 2020, San Francisco, February 24–28, 2020 (Tagungsband); *Gudgeon et al*, Sok: Layer-two blockchain protocols, Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24 (Tagungsband); IEEE International Conference on E-Commerce Technology 2005 ('CEC'05) (Tagungsband); IEEE symposium on security and privacy 2020 (SP) (Tagungsband); International Conference on High Performance Computing & Simulation 2019 (HPCS) (Tagungsband); International Conference on High Performance Computing & Simulation (HPCS) 2018, (Tagungsband); International Workshop on Web and Internet Economic 2007 (WINE) (Tagungsband); *Judmayer/Stifter/Krombholz/Weippl*, Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms (2017); *Kirchmayr/Miernicki/Weilinger/Wild/Wimmer* (Hrsg), Handbuch Besteuerung von Kryptowährungen (2023); *Law/Sabett/Solinas*, American University Law Review 1996, 1131; *Lehmann/Schinerl*, The Concept of Financial Instruments: Drawing the Borderline between MiFID and MiCAR, EBI Working Paper Series Nr 171; *Malkhi* (Hrsg), Concurrency: the works of Leslie Lamport (2019); *Narayanan/Clark*, 'Bitcoin's academic pedigree. Commun. ACM 2017, 36–45; Network and distributed security symposium 2015 (Tagungsband); *Ovezik/Karakostas/Kiayias*, SoK: A stratified approach to blockchain decentralization, Financial Cryptography and Data Security 2024: Twenty-Eighth International Conference (Tagungsband); *Pease/Shostak/Lamport*, Reaching agreement in the presence of faults, Journal of the ACM (JACM) 1980, 228–234; *Putz*, Der behördliche Zugriff auf Krypto-Assets (Diplomarbeit Linz, 2023); *Saberi/Kouhizadeh/Sarkis/Shen*, Blockchain technology and its relationships to sustainable supply chain management, International journal of production research 2019, 2117–2135; Security Protocols: 15th International Workshop, Brno, Czech Republic, April 18–20, 2007, Revised Selected Papers (Tagungsband); *Stifter et al*, What is meant by permissionless blockchains? Cryptology ePrint Archive (2021).

1. Einleitung

1.1. Ziele und Herausforderungen der MiCAR

1/1 Die Verordnung über Märkte für Kryptowerte (Markets in Crypto-Assets Regulation – „**MiCAR**")[1] soll auf die schnellen technologischen Entwicklungen im Bereich digitaler Finanzmärkte reagieren, um einen gangbaren Rechtsrahmen zu schaffen, der Innovationen zulässt und gleichzeitig Sicherheiten für Anleger und das Finanzsystem als Ganzes bietet.[2] Der Fokus der Ausgestaltung liegt hierbei auf dem **Konzept der Kryptowerte** (Crypto-Assets). Die Verordnung bedient sich dafür einer Reihe von technischen Definitionen und Begriffserläuterungen, um ihren Anwendungsbereich und Ausnahmen davon klarzustellen. Dabei liegt beim Gesetzgeber die Herausforderung darin, die Definitionen so breit zu gestalten, dass die Verordnung mit den schnellen technischen Entwicklungen Schritt halten kann. Gleichzeitig dürfen die Definitionen jedoch nicht zu weit gefasst sein, da sonst diverse Technologien und Konzepte unter die MiCAR fallen könnten, die eigentlich nicht in den vorgesehenen Anwendungsbereich gehören.

1.2. Technische Begriffe und Konzepte in der MiCAR

1/2 In diesem Beitrag werden die wesentlichen technischen Begriffe und Konzepte in der MiCAR beleuchtet und wird auf den aktuellen Stand der Informatik in diesem Bereich aus technischer Sicht eingegangen. Dabei ist das Ziel, den Wortlaut und die verwendeten technischen Begriffe verständlich zu beschreiben und dort, wo es aus unserer Sicht Ambiguitäten oder alternative Interpretationsweisen gibt, darauf hinzuweisen, dass hier Mehrdeutigkeiten bestehen können. Dieser Beitrag soll vor allem Juristen helfen, ein tieferes Verständnis für die Bedeutung der technischen Beschreibungen und Begriffe zu erlangen. Dadurch soll auch ein Bewusstsein dafür geschaffen werden, dass die in der MiCAR verwendeten Begriffe aus technischer Sicht nicht in jedem Fall eindeutig definiert sind und sich daraus in der Praxis durchaus Probleme ergeben können.

1.3. Was in diesem Beitrag nicht im Detail betrachtet wird

1/3 Das Hauptaugenmerk dieses Beitrags richtet sich auf die Analyse und Interpretation der wesentlichen technischen Begriffsbestimmungen in der MiCAR, insbesondere hinsichtlich des Begriffs der Kryptowerte sowie deren zugrundeliegenden Distributed-Ledger-Technologien. In der MiCAR werden aber auch weitere Aspekte behandelt, bei denen eine genauere technische Betrachtung sinnvoll erscheint – die jedoch den Rahmen dieses Beitrags sprengen würden. Darunter fallen beispielsweise:

- Voraussetzungen für die Zulassung zum Handel von Kryptowerten, insbesondere im Kontext der Erstellung eines spezifischen „Kryptowerte-Whitepapers". Dieses Dokument muss zum einen selber gewisse technische Anforderungen erfüllen, beispielsweise maschinenlesbar sein,[3] zum anderen wird vorgeschrieben, dass der Inhalt auch

1 VO (EU) 2023/1114 ABl L 2023/150, 40.
2 Vgl etwa ErwGr 6 MiCAR.
3 Vgl Art 6 Abs 10 MiCAR.

auf technische Aspekte der zugrundeliegenden Technologien eingehen soll – hier bedarf es im Speziellen einer expliziten Darstellung und Quantifizierung im Dokument, wie der angedachte Konsensmechanismus bzw die Transaktionsvalidierung sich auf das Klima und die Umwelt nachteilig auswirken könnte (zB durch den Einsatz von Proof-of-Work).

- Auch die vorgesehenen Verpflichtungen von sogenannten Crypto-Asset Service Providers („**CASPs**"), also Anbietern von Kryptowerte-Dienstleistungen, behandeln zum Teil technische Aspekte. Hierbei bezieht sich die MiCAR insbesondere auch auf technische Vorkehrungen zur Sicherung der Informations- und Kommunikationstechnologie-(„**IKT**")-Infrastruktur, die getroffen werden müssen.

Die MiCAR sieht zudem zusätzlich vor, dass die Europäische Wertpapier- und Markt- **1/4**
aufsichtsbehörde (European Securities and Markets Authority – „**ESMA**") und die Europäische Bankenaufsichtsbehörde (European Banking Authority – „**EBA**") Entwürfe für technische Regulierungs- und Durchführungsstandards im Rahmen der Verordnung ausarbeitet. Hierbei handelt es sich großteils um Aspekte zu den oben genannten Punkten, die dieser Beitrag nicht abdeckt. Zudem ist wichtig zu beachten, dass diese Vorschriften sich häufig nicht auf Technik im Sinne von Technologie beziehen. Stattdessen sollen beispielsweise Formulare und Muster zur Verwendung durch nationale Behörden entwickelt oder Verfahrensvorschriften für Beschwerdeverfahren erarbeitet werden. Viele der Stellen,[4] an denen solche Standards von der MiCAR vorgesehen sind, sind daher nicht unmittelbar für ein tieferes Verständnis der technischen Konzepte in diesem Beitrag relevant. Die zur MiCAR veröffentlichten Konsultationspapiere der ESMA[5] können dennoch eine hilfreiche Quelle bei der Identifikation unklarer technischer Begriffe und Konzepte in der MiCAR darstellen und wurden bei der Erstellung dieses Beitrags ebenso berücksichtigt.

2. Technische Grundlagen der Distributed-Ledger-Technologie

2.1. Übersicht

In diesem Abschnitt wird eine Einführung in Distributed-Ledger-Technologien („**DLT**") **1/5**
gegeben, um die grundlegenden technischen Konzepte und Herausforderungen zu erläutern, die für das Verständnis der MiCAR notwendig sind. Ein kurzer historischer Überblick zeigt hierbei die Entwicklung von zentralisierten digitalen Zahlungssystemen hin zu dezentralen Systemen. Wesentliche Konzepte wie **Kryptographische Primitive, Konsens-Protokolle** und **Verteilungstransparenz** werden erläutert, um zu illustrieren, wie DLTs eine konsistente und ausfallsichere Systemumgebung gewährleisten. DLTs

4 Ein für die Inhalte dieses Beitrags durchaus interessanter Punkt wird in ErwGr 14 der Verordnung angeführt, bei dem die ESMA beauftragt werden soll *„[…] Leitlinie zu den Kriterien und Bedingungen für die Einstufung von Kryptowerten als Finanzinstrumenten herauszugeben."* Das entsprechende Konsultationspapier ESMA75-453128700-52 vom 29.1.2024 enthält hierbei auch technische Erwägungsgründe und Empfehlungen, die unter anderem eine möglichst technologieneutrale Betrachtung bei der Beurteilung befürworten.

5 ESMA-Homepage, www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica (abgerufen am 30.6.2024).

ermöglichen hierdurch die Umsetzung von digitalen Zahlungssystemen als verteilte Systeme und können so die Zuverlässigkeit und Fehlertoleranz gegenüber zentralistischen Lösungen verbessern. Es soll betont werden, dass verschiedene DLT-Architekturen unterschiedliche technische Ansätze und Sicherheitsmechanismen verwenden können, um Herausforderungen wie das Double-Spending-Problem zu bewältigen. Die gewählten technischen Lösungsansätze können dabei zu unterschiedlichen Systemeigenschaften führen. Dieser Abschnitt soll zudem Bewusstsein dafür schaffen, dass die verwendeten technischen Begriffe nicht immer eindeutig definiert sind und im jeweiligen Kontext betrachtet werden sollten.

2.2. Wesentliche technische Begriffsdefinitionen in der MiCAR

1/6 Ein zentraler Gegenstand der MiCAR sind sogenannte Kryptowerte (Crypto-Assets, oder Cryptoassets). Als solche werden digitale Darstellungen von Werten oder Rechten, welche unter der Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden können, verstanden.[6] Die in der MiCAR genutzte Begriffsdefinition stützt sich hierbei zwar auf eine **(allgemein gehaltene) Charakterisierung und Abgrenzung der zugrundeliegenden Technologien**, genauere technische Eigenschaften dieser Systeme werden jedoch in der Verordnung nicht konkretisiert, wodurch ein erheblicher Interpretationsspielraum entstehen kann, welche Formen von Technologien hier gemeint sein könnten. Dieser Abschnitt soll zum einen wesentliche technische Konzepte diverser Distributed-Ledger-Technologien (DLT) sowie deren grundlegende Eigenschaften kurz erläutern. Zum anderen soll der Leser dafür sensibilisiert werden, dass eine eindeutige technische Abgrenzung zwischen verschiedenen **Ausgestaltungen von digitalen Zahlungssystemen** in der Praxis oft schwierig ist und sich eine allgemein akzeptierte Definition von DLT in der Informatik noch nicht etabliert hat. Somit bietet dieser Abschnitt eine technische Einführung und legt den Grundstein für die weitere Behandlung der spezifischen Begriffsbestimmungen der MiCAR in Abschnitt 3 (→ Rz 1/30)

1/7 Um Unklarheiten im weiteren Verlauf dieses Beitrags zu vermeiden und die verwendete Terminologie zu präzisieren, möchten wir an dieser Stelle kurz erläutern, wie der Begriff „**digitales Zahlungssystem**" im Kontext dieses Beitrags zu verstehen ist. Hierbei handelt es sich um technische Systeme, die eine elektronische Übertragung bzw den Austausch von digitalen Werteinheiten oder anderen Daten, denen ein Wert oder Rechte beigemessen werden können, zwischen Teilnehmern im System ermöglichen. Diese zusätzlich eingeführte Begriffsbestimmung soll jegliche technische Ausgestaltung inkludieren und neben den Distributed-Ledger-Technologien (DLTs) und artverwandten Technologien beispielsweise auch zentralisierte Zahlungssysteme beinhalten. Zum einen wollen wir hiermit einen generischen, technologieneutralen Oberbegriff zur Bezeichnung solcher technischen Systeme einführen. Zum anderen möchten wir bewusst eine Vermischung von technischen Beschreibungen und den technologiebezogenen Rechtsbegriffen der MiCAR vermeiden, die zu Verwechslungen führen könnte.

6 Vgl Art 3 Abs 1 Nr 5 MiCAR.

2.3. Digitale Zahlungssysteme sind keine neue Erscheinung

Die grundlegende Idee, mittels technischer Protokolle,[7] die auf kryptographischen Verfahren[8] und (verteilten) Algorithmen basieren, digitale Zahlungssysteme zu realisieren, ist hierbei **aus Sicht der Informatik kein neuartiges Konzept**. Bereits in den 80er Jahren wurden erstmals solche Systeme nicht nur wissenschaftlich beschrieben,[9] sondern auch technisch entwickelt.[10] Ein wesentliches Merkmal solcher frühen digitalen Zahlungssysteme ist die (technische) Notwendigkeit einer zentral betreibenden Instanz, um die Konsistenz und Sicherheit des Systems zu gewährleisten.[11] Hierdurch erklärt sich teilweise auch der wissenschaftliche Fokus in diesen Designs auf die Verwendung von kryptographischen Verfahren zur Verbesserung und Wahrung der Privatsphäre bei Zahlungen zwischen Teilnehmern, wie beispielsweise **Blindsignaturen**.[12] Auch hinsichtlich der abzubildenden digitalen Repräsentation von Werten findet sich in frühen technischen Designs häufiger die (implizite) Annahme, dass die Systeme Formen von (Zentral-)Bank-verwaltetem E-Geld verwenden und keine eigenständigen digitalen Werte einführen.[13] **1/8**

Der Begriff Kryptowert hat sich erst in den letzten Jahren als breiter Sammelbegriff etabliert, um unterschiedlichste Formen und technische Ausgestaltungen digitaler Repräsentationen von Werten und Rechten zu umfassen. In der (technischen) Literatur finden sich demnach auch diverse andere Bezeichnungen wie beispielsweise „**electronic cash**", „**e-money**" und „**cryptocurrency**", die im Kontext von digitalen Zahlungssystemen verwendet werden. Insbesondere der Terminus „**Kryptowährung**" hat, aufgrund der Konnotation mit Bitcoin, stark an Popularität gewonnen und ist häufig anzutreffen. Eine exakte Abgrenzung und Differenzierung der genauen Bedeutung dieser einzelnen Begriffe ist hierbei jedoch oft schwierig und kann mitunter zu Missverständnissen bei der Interpretation führen.[14] Gerade hinsichtlich des Begriffs der Kryptowährung besteht teilweise eine implizite Annahme, dass die technischen Komponenten ähnliche Eigenschaften wie Bitcoin[15] aufweisen. Die Praxis zeigt jedoch, dass der Begriff auch für andere Systemarchitekturen häufig Verwendung findet und nur schwer zu charakterisieren ist. **1/9**

Die (pseudonyme) Veröffentlichung des Bitcoin-Whitepapers[16] 2008 und der Start des Bitcoin-Netzwerks 2009 können als wesentliche Meilensteine in der Entwicklung von **1/10**

7 In der Informatik versteht man unter dem Begriff „Protokoll" ein Regelwerk, welches das Verhalten und die Kommunikation zwischen elektronischen Geräten, beispielsweise Computern, genau spezifiziert.

8 Hierbei handelt es sich um kryptographische Verfahren, die über eine einfache Kommunikationsverschlüsselung zwischen Teilnehmern hinausgehen.

9 *Chaum/Fiat/Naor*, Untraceable electronic cash, Advances in Cryptology—CRYPTO'88 (1990), 319–327; *Chaum* in *Chaum/Rivest/Sherman*, Advances in Cryptology: Proceedings of Crypto 82, 199–203.

10 DigiCash, World's first electronic cash payment over computer networks, 27.5.1994, https://chaum.com/wp-content/uploads/2022/01/05-27-94-World_s-first-electronic-cash-payment-over-computer-networks.pdf (abgerufen am 30.6.2024).

11 *Law/Sabett/Solinas*, How to make a mint: the cryptography of anonymous electronic cash, American University Law Review 1996, 1131.

12 *Chaum* in *Chaum/Rivest/Sherman*, Advances in Cryptology: Proceedings of Crypto 82, 199–203.

13 *Chaum*, Scientific american 1992, 96–101.

14 *Stifter/Judmayer/Putz/Brameshuber/Weippl* in *Kirchmay/Miernicki/Weilinger/Wild/Wimmer*, Handbuch Besteuerung von Kryptowährungen 33.

15 Der Begriff Kryptowährung wird oft im Kontext von digitalen Zahlungssystemen verwendet, die dezentral mittels (zumeist Proof-of-Work basierten) Blockchain-Technologien betrieben werden.

16 *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system (2008), https://bitcoin.org/bitcoin.pdf (abgerufen am 21.7.2024).

digitalen Zahlungssystemen gesehen werden. Hierbei konnte demonstriert werden, dass eine **dezentrale Emission von Kryptowerten** und die **dezentrale Verarbeitung und Absicherung von Transaktionen über diese Kryptowerte** nicht nur theoretisch möglich, sondern auch in der Praxis prinzipiell umsetzbar ist. Seit dem Erscheinen von Bitcoin ist hierbei nicht nur das (wirtschaftliche) Interesse an den vom System verwalteten Kryptowerten stetig gewachsen (→ Rz 2/9 ff), auch auf technischer Seite war es ein Anstoß für weitere Entwicklungen und Forschung.[17] Dadurch sind teilweise Jahrzehnte alte Konzepte wieder in den Fokus der Wissenschaft gerückt.[18]

1/11 Als **quelloffene Software** ermöglichten Adaptionen und Änderungen des Bitcoin-Protokolls zudem die schnelle Entwicklung zahlreicher neuer Systeme. Mittlerweile gibt es tausende eigenständige Projekte, die unterschiedlich stark auf den fundamentalen technischen Konstrukten von Bitcoin aufbauen und verschiedene Zielsetzungen verfolgen. Während Bitcoin primär als Zahlungssystem konzipiert wurde, erweitern Plattformen wie Ethereum dessen Funktionsumfang und ermöglichen durch Konzepte wie Smart-Contracts zahlreiche Anwendungsmöglichkeiten, die über einen unmittelbaren Transfer von Kryptowerten zwischen Nutzern hinausgehen.[19]

1/12 Im Kontext von Bitcoin und der Proof-of-Work-(„PoW")-basierten Blockchain-Technologie[20] ist es essentiell zu erwähnen, dass auch andere technische Konstruktionen und Protokolle aus dem Bereich der Verteilten Systeme[21] sich als **Grundlage für digitale Zahlungssysteme** eignen. Selbst für dezentrale Protokolle existieren Lösungen, die sich teilweise deutlich vom Design einer klassischen Blockchain-Technologie, wie sie Bitcoin verwendet, unterscheiden. Mit der Bezeichnung **Distributed-Ledger-Technologie** hat sich diesbezüglich ein **Überbegriff** etabliert, der diesen Umstand bewusst unterstreichen soll und ein breites Spektrum an technischen Lösungen impliziert. DLTs können demnach als Technologien und Methoden verstanden werden, mit denen verteilte Systeme umgesetzt werden können, während die (Proof-of-Work)-Blockchain-Technologie eine Unterkategorie von DLT ist.

2.4. Wesentliche Kryptographische Primitive

1/13 Bevor im weiteren Verlauf des Abschnitts auf technische Aspekte wie die Transaktionsverarbeitung (→ Rz 1/42 ff), Datenstrukturen (→ Rz 1/45 ff) und Konsens-Protokolle (→ Rz 1/48 ff) näher eingegangen werden kann, gilt es zuerst, wesentliche kryptographische Bausteine, sogenannte Primitive, zu beschreiben, die praktisch in allen DLTs und den meisten digitalen Zahlungssystemen Verwendung finden. Hierbei ist es essenziell, den Leser vor möglichen Begriffsverwirrungen oder Fehlannahmen in diesem Kontext

17 *Bonneau et al*, Sok: Research perspectives and challenges for bitcoin and cryptocurrencies, IEEE symposium on security and privacy 2015, https://ieeexplore.ieee.org/document/7163021 (abgerufen am 22.7.2024).

18 *Narayanan/Clark*, Bitcoin's academic pedigree, Commun. ACM 2017, 36–45, https://doi.org/10.1145/3132259 (abgerufen am 21.7.2024).

19 *Stifter/Schindler/Judmayer*, Blockchain – Anwendungsformen (2024), https://360.lexisnexis.at/d/lexisbriefings/blockchain_anwendungsformen/h_80004_630884878022479727 7_c915ebcbf2 (abgerufen am 21.7.2024).

20 *Judmayer/Stifter/Krombholz/Weippl*, Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms 15–50.

21 Hier insbesondere sogenannte Byzantine-Fault-Tolerant-(BFT)-Protokolle.

zu bewahren, die in der Praxis leider immer wieder vorkommen. Insbesondere die Annahme, DLTs würden bei der Transaktionsverarbeitung oder im Rahmen des Konsens-Protokolls auf **kryptographische Verschlüsselungsverfahren** setzen, ist in den überwiegenden Fällen falsch![22] Korrekterweise finden bei DLTs hauptsächlich **(asymmetrische) digitale Signaturverfahren** Verwendung. Grundlegende Konzepte der asymmetrischen Kryptographie werden nachfolgend in (→ Rz 1/16 ff) erläutert.

Ein weiteres zentrales kryptographisches Primitiv, das in digitalen Zahlungssystemen Verwendung findet, sind sogenannte **kryptographische Hashfunktionen** (siehe → Rz 1/27 ff). Diese werden informell gerne mit der Metapher eines digitalen Fingerabdrucks beschrieben, welche auf einer abstrakten Ebene durchaus hilfreich sein kann, um wesentliche Aspekte zu versinnbildlichen. Dennoch sollten die konkreten kryptographischen Annahmen und technischen Eigenschaften von Hashfunktionen bei einer tieferen Betrachtung der technischen Materie von digitalen Zahlungssystemen hinreichend bekannt sein, um Fehler zu vermeiden. So wird zB manchmal in der Literatur fälschlicherweise beschrieben, dass Hashfunktionen genutzt werden, um Daten zu verschlüsseln**.** **1/14**

Abschließend wird in (→ Rz 1/34 ff) auf das Konzept von sogenannten **(electronic) Wallets** (Deutsch: elektronische Geldbörsen) eingegangen. Dieser Begriff wurde in der technischen wissenschaftlichen Literatur schon im Kontext von frühen digitalen Zahlungssystemen wie David Chaums e-Cash in den 1980er Jahren diskutiert.[23] Im Allgemeinen handelt es sich hierbei um eine Kombination aus Lösungen zur sicheren Verwahrung und Verwaltung von kryptographischem Schlüsselmaterial, wie etwa private Schlüssel von asymmetrischen Signaturverfahren, sowie Mechanismen und Hilfsmittel für die Interaktion mit digitalen Zahlungssystemen. Ein in diesem Kontext häufig anzutreffendes Missverständnis ist die Annahme, dass die durch das Wallet verwalteten Kryptowerte tatsächlich lokal auf dem Gerät, auf dem die Wallet-Software ausgeführt wird, gespeichert sind**.**[24] **1/15**

2.4.1. Asymmetrische Kryptographie

Asymmetrische kryptographische Verfahren, auch als **Public-Key-Kryptographie** bezeichnet, sind eine zentrale technische Komponente digitaler Infrastrukturen, einschließlich digitaler Zahlungssysteme. Im Gegensatz zu symmetrischen kryptographischen Verfahren, bei denen die Teilnehmer für Verschlüsselung oder Authentifizierung denselben geheimen Schlüssel teilen, wird bei der asymmetrischen Kryptographie ein Schlüsselpaar verwendet, das aus einem öffentlichen Schlüssel (englisch: *public key*) und einem privaten Schlüssel (englisch: *private key*) besteht. **1/16**

Symmetrische Verschlüsselungsverfahren haben den Nachteil, dass der geheime Schlüssel zunächst sicher zwischen den beteiligten Parteien verteilt werden muss. Dies **1/17**

22 *Stifter/Judmayer/Putz/Brameshuber/Weippl Blockchain-Babel*, Herausforderungen bei der Entwicklung präziser Begrifflichkeiten zwischen Recht und Technik im Kontext von Kryptowährungen und Distributed-Ledger-Technologien in *Kirchmayr/Miernicki/Weilinger/Wild/Wimmer* (Hrsg), Handbuch Besteuerung von Kryptowährungen (2023).

23 *Even/Goldreich/Yacobi, Y.*, Electronic Wallet, in *Chaum, D.* (eds) Advances in Cryptology (1984), https://doi.org/10.1007/978-1-4684-4730-9_28.

24 Vgl *E. Putz/N. Stifter/E. Weippl*, Rechtliche Lücken bei der Sicherstellung von Kryptowerten in SPWR 2024, DOI 10.52018 / SPWR-24H00-B008, 62.

ist besonders problematisch, wenn die Parteien vorher noch nicht miteinander interagiert haben und daher nicht auf bereits bestehende sichere Kommunikationskanäle zurückgreifen können. Trotzdem sind symmetrische Verfahren, unter anderem aufgrund ihrer Effizienz, weiterhin weit verbreitet, insbesondere in Szenarien mit wenigen Teilnehmern oder in geschlossenen Systemen, wo sichere Schlüsselverteilungen einfacher realisierbar sind, wie beispielsweise Zugangsschlüssel für lokale WLAN-Netzwerke. Ein gängiger Ansatz ist zudem, dass anfangs über ein asymmetrisches Verfahren ein symmetrischer Schlüssel zwischen den Teilnehmern generiert wird und im weiteren Verlauf dann symmetrische Verschlüsselung verwendet werden kann.

1/18 Die Verwendung von **asymmetrischer Kryptographie** beantwortet jedoch nicht automatisch die Frage, ob ein bestimmter öffentlicher Schlüssel tatsächlich dem gewünschten Kommunikationspartner zugeordnet ist. Dieses Problem ist besonders relevant, da eine falsche Zuordnung von Schlüsseln dazu führen könnte, dass vertrauliche Informationen an unbefugte Dritte gelangen, beispielsweise durch Man-in-the-Middle-(MITM)-Angriffe.[25] In der Praxis werden sogenannte Public Key Infrastructures (PKIs) verwendet, um dieses Problem zu lösen. Eine PKI basiert auf vertrauenswürdigen Instanzen, sogenannten Zertifizierungsstellen (Certificate Authorities, CA), die die Zuordnung von öffentlichen Schlüsseln zu deren Besitzern überprüfen und bestätigen. Diese Instanzen stellen digitale Zertifikate aus, die garantieren sollen, dass ein bestimmter öffentlicher Schlüssel tatsächlich der angegebenen Person oder Institution gehört. So wird ein zusätzlicher Vertrauensanker geschaffen, der die Sicherheit eines Einsatzes asymmetrischer Kryptographie in großen Netzwerken verbessert. Beispielsweise wird im Rahmen der eIDAS-Verordnung als Beweggrund angeführt, dass auf europäischer Ebene eine PKI geschaffen werden muss, um *„die grenzüberschreitende Interoperabilität elektronischer Signaturen zu gewährleisten und die Sicherheit von Transaktionen, die über das Internet ausgeführt werden, zu erhöhen."*[26]

1/19 An dieser Stelle möchten wir nun die Verfahren für Public-Key-Verschlüsselung und digitale Signaturen nochmals technisch präzisieren,[27] bevor im Anschluss (→ Rz 1/20 f) die Anwendung asymmetrischer Kryptographie im Kontext von DLT diskutiert wird. Für tiefere Einblicke in die mathematischen und technischen Grundlagen der (asymmetrischen) Kryptographie verweisen wir den geneigten Leser an entsprechende Fachliteratur.[28, 29]

2.4.1.1. Public-Key-Verschlüsselung

1/20 Die Kernidee der asymmetrischen Kryptographie, die erstmals in den 1970er Jahren entwickelt wurde,[30] besteht darin, dass zwei Parteien ein gemeinsames Geheimnis erzeugen können, ohne dass sie hierfür zuvor einen geheimen Schlüssel ausgetauscht haben müs-

25 *Conti, M., Dragoni, N., & Lesyk, V.*, A survey of man in the middle attacks, IEEE communications surveys & tutorials, 18(3), 2027-205(2016)1.
26 Vgl ErwGr 7 VO (EU) 910/201.
27 Siehe *Judmayer/Stifter/Krombholz/Weippl*, Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms (2017) 11ff
28 *Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A.*, Handbook of applied cryptography (2018).
29 *Katz, J., & Lindell, Y.*, Introduction to modern cryptography: principles and protocols (2007).
30 *Diffie, W., & Hellman, M. E.*, New directions in cryptography, in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman* (2022) pp 365–390.

sen. Dies wird allein durch die Nutzung öffentlich zugänglicher Informationen – den öffentlichen Schlüsseln – ermöglicht. So kann beispielsweise ein Absender eine Nachricht an den Empfänger verschlüsseln, indem er lediglich den öffentlichen Schlüssel des Empfängers kennt. Nur der Empfänger, der im Besitz des entsprechenden privaten Schlüssels ist, kann die Nachricht entschlüsseln.

Ein **Public-Key-Verschlüsselungsschema** wird als ein Tripel effizienter Algorithmen $\varepsilon = (G, E, D)$ definiert, wobei: **1/21**

- **G** ein Schlüsselgenerierungsalgorithmus ist, der keine Eingabe benötigt und ein Schlüsselpaar (pk, sk) ausgibt. pk wird als öffentlicher Schlüssel bezeichnet und kann öffentlich geteilt werden. sk wird als privater (geheimer) Schlüssel bezeichnet und sollte geheim gehalten werden.

$$\text{Formal: } (pk, sk) \leftarrow G().$$

- **E** ein Verschlüsselungsalgorithmus ist, der als Eingabe einen öffentlichen Schlüssel pk sowie eine Nachricht $m \in M$ erhält und einen Chiffretext $c \in C$ ausgibt, der unter dem öffentlichen Schlüssel pk verschlüsselt wurde.
- **D** ein (deterministischer) Entschlüsselungsalgorithmus ist, der als Eingabe einen privaten Schlüssel sk sowie einen Chiffretext $c \in C$ erhält und entweder die ursprüngliche Nachricht $m \in M$ ausgibt, falls die richtigen Schlüssel verwendet wurden, oder andernfalls ein Fehlerzeichen $\perp$.

$$\text{Formal: } m \leftarrow D(sk, c).$$

Daraus folgt, dass, wenn die jeweiligen Operationen umkehrbar sind, für jedes Schlüsselpaar $\forall (pk, sk)$ aus G gilt: $\forall m \in M : D(sk, E(pk,m)) = m$.

2.4.1.2. Digitale Signaturen

Ein weiteres wesentliches Anwendungsgebiet asymmetrischer Kryptographie sind digitale Signaturverfahren. Solche Signaturverfahren ermöglichen es einem Unterzeichner S, der einen öffentlichen Schlüssel pk eingerichtet hat, eine Nachricht mit dem zugehörigen privaten Schlüssel sk so zu „signieren", dass jeder, der pk kennt (und weiß, dass dieser öffentliche Schlüssel von S eingerichtet wurde), überprüfen kann, dass die Nachricht von S stammt und während der Übertragung nicht verändert wurde. Es ist wichtig zu beachten, dass im Gegensatz zur Public-Key-Verschlüsselung, wo andere Teilnehmer dem Empfänger (verschlüsselte) Nachrichten senden, im Kontext digitaler Signaturen der Eigentümer des öffentlichen Schlüssels selbst als der Absender agiert.[31] **1/22**

Ein **digitales Signaturverfahren** wird als ein Tripel effizienter Algorithmen $\varsigma = (G, S, V)$ definiert, wobei: **1/23**

- **G** ein Schlüsselgenerierungsalgorithmus ist, der keine Eingabe benötigt und ein Schlüsselpaar (pk, sk) ausgibt. pk wird als öffentlicher Schlüssel bezeichnet und kann öffentlich geteilt werden. sk wird als privater (geheimer) Schlüssel bezeichnet und sollte geheim gehalten werden.

31 Die angeführte Beschreibung folgt im Wesentlichen *Katz, J., & Lindell, Y.*, Introduction to modern cryptography: principles and protocols, Chapman and hall/CRC (2007) 439 ff.

Formal: (pk, sk) ← G ()

- **S** ein Signaturalgorithmus ist, der als Eingabe einen privaten Schlüssel sk sowie eine Nachricht m∈ M erhält und eine Signatur σ ∈∑ ausgibt, die zusammen mit der Nachricht öffentlich kommuniziert werden kann.

  Formal: S : σ ← E (sk, m).

  V ein (deterministischer) Verifikationsalgorithmus ist, der als Eingabe einen öffentlichen Schlüssel, pk eine Nachricht m ∈ M sowie eine Signatur σ ∈∑ erhält und entweder „accept" (gültig) oder „reject" (ungültig) ausgibt, je nachdem, ob die Signatur σ für die Nachricht m korrekt ist.

  Formal: {accept, reject} ← V (pk, m, σ).

  Daraus folgt, dass eine vonS generierte Signatur von V akzeptiert wird, wenn (pk,sk) ein gültiges Schlüsselpaar ist. Das bedeutet: ∀m ∈ M : V (pk, m, S (sk,m)) = accept

1/24 Generell lassen sich mittels asymmetrischer Verschlüsselungsverfahren durch kleinere Anpassungen auch digitale Signaturverfahren realisieren. So kann zum Beispiel mit dem RSA-Kryptosystem[32] sowohl verschlüsselt als auch digital signiert werden. Im Umkehrschluss gilt dies jedoch nicht! **Nicht alle digitalen Signaturverfahren sind auch unmittelbar für Verschlüsselung geeignet**.[33] Bei den **im Kontext von DLT häufig anzutreffenden Signaturverfahren**, wie zB Implementierungen des Elliptic Curve Digital Signature Algorithm (ECDSA), zB, secp256k1 in Bitcoin und Ethereum, **bedarf es zusätzlicher kryptographischer Verfahren**, wie die Verwendung von Elliptic Curve Diffie-Hellman (ECDH) oder Elliptic Curve Integrated Encryption Scheme (ECIES)[34], **um auch eine Verschlüsselung zu ermöglichen**.

2.4.1.3. Anwendungen asymmetrischer Kryptographie in DLT

1/25 In den überwiegenden Fällen finden in DLT[35] hauptsächlich digitale Signaturverfahren eine breite Anwendung, wohingegen (**asymmetrische**) **Verschlüsselungsverfahren nur in Ausnahmefällen** eingesetzt werden. Insbesondere im Kontext der Transaktionserstellung und Verarbeitung (siehe auch Rz 1/13) werden digitale Signaturen verwendet um sich gegenüber dem System zu authentifizieren und zB die Verfügungsmacht über Kryptowerte zu begründen, dh mittels Signaturen wird überprüft, ob der Ersteller einer Transaktion überhaupt die jeweils notwendigen Berechtigungen für die darin enthaltenen Anweisungen hat. Dies hilft auch zu verdeutlichen, warum insb bei möglichst dezentral gestalteten DLT-Systemen eine verschlüsselte Kommunikation schwer umzu-

32 *Rivest, R. L., Shamir, A., & Adleman, L.*, A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM (1978), 21(2), 120–126.

33 Laut rennomiertem Kryptograph *Yehuda Lindell* ist eine verallgemeinerbare generische Transformation asymmetrischer Signaturverfahren hin zu Verschlüsselungsverfahren nicht möglich, siehe https://crypto.stackexchange.com/a/91723.

34 *Gayoso Martínez, Víctor & Hernandez Encinas, Luis & Sánchez Ávila, Carmen*, A Survey of the Elliptic Curve Integrated Encryption Scheme, Journal of Computer Science and Engineering (2010) 2. 7–13.

35 Für den breiter gefassten Begriff der digitalen Zahlungssysteme lässt sich diese Verallgemeinerung schwieriger rechtfertigen.