Veronika Kronast: Der „Diebstahl“ von Kryptowährungen – strafloses Vermögensdelikt?

Die Autorin ist Studentin der Rechtswissenschaft im 10. Fachsemester (Universität Bayreuth). Der Beitrag ist im Rahmen des studienbegleitenden Seminars „Modern crimes, modern solutions? – Aktuelle Rechtsfragen zu Straftaten und Strafverfolgung aus dem IT-Strafrecht“ bei Prof. Dr. Christian Rückert (Lehrstuhl Strafrecht II - Strafrecht, Strafprozessrecht und IT-Strafrecht) entstanden.

A. Einleitung

Der verbreitete Grundsatz in der Welt der Kryptowährungen „not your keys, not your coins“, deutet auf eine Tatsache hin, die sowohl Fluch als auch Segen für Nutzer ist: Wer Zugriff auf den Schlüssel zu den Kryptowährungseinheiten hat, kann auch über diese verfügen. Dies bietet Kriminellen eine willkommene Möglichkeit, Kryptowährungen zu „stehlen“, da sie durch ihre dezentrale Organisation ohne Banken oder sonstige zentrale Stellen funktionieren und daher weniger abgesichert sind. Über sog. „Kryptodiebstähle“ wird insbesondere deswegen immer wieder medial berichtet, da teilweise bis zu neunstellige Beträge erbeutet werden. So bereicherte sich ein US-Ehepaar mit fast 120.000 Bitcoin im Wert von 3,6 Milliarden US-Dollar, indem es im Februar 2022 einen Hackerangriff auf die Kryptobörse Bitfinex verübte.[1]

Im Folgenden soll die Strafbarkeit des „Diebstahls“ von Kryptowährungen untersucht werden. Dabei werden unterschiedliche Vorgehensweisen der Täter beleuchtet und aufgezeigt, warum der Begriff des „Diebstahls“ womöglich ungenau und an welchen Stellen ein gesetzgeberisches Eingreifen erforderlich ist.

B. Technische Grundlagen

Kryptowährungen sind virtuelle Währungen.[2] Die Bekannteste ist der sog. Bitcoin mit einem Marktwert von 1,3 Billionen Euro.[3] Im Jahr 2024 existieren jedoch über 20.000 weitere Kryptowährungen.[4] Im Unterschied zu anderen Währungen sind Kryptowährungen dezentral organisiert. Das bedeutet, dass keine zentrale Ausgabestelle an dem Prozess der Schöpfung, dem sog. Mining, beteiligt ist.[5] Bei der Kryptowährung Bitcoin basiert das Zahlungssystemviel mehr auf der Blockchain, einer fälschungssicheren, verteilten Datenstruktur, in der Transaktionen öffentlich protokolliert werden.[6] Diese Transaktionen erfolgen Peer-to-Peer, also nicht wie Banküberweisungen über eine zentrale Instanz, sondern zwischen gleichberechtigten Rechnern.[7] Die Teilnehmer agieren innerhalb des Netzwerks ohne Angabe von persönlichen Daten, was ein nahezu anonymes Vorgehen ermöglicht.[8] Zur Nutzung des Netzwerks ist lediglich ein kryptographisches Schlüsselpaar erforderlich, bestehend aus einem öffentlichen Schlüssel, welcher mit einer Kontonummer eines Bankkontos vergleichbar ist, und einem privaten Schlüssel, der dazugehörigen PIN. Jede Transaktion enthält eine digitale Signatur, die von dem privaten Schlüssel generiert wird.[9] Wer Zugriff auf den privaten Schlüssel hat, kann Transaktionen anweisen und somit über die Kryptowährungseinheiten, sog. Token,[10] verfügen. Der private Schlüssel wird meist in einer Wallet gespeichert, welche in digitaler, sog. Online-Wallets, oder analoger Form, sog. Hardware-Wallets, vorliegen kann.[11] Kryptowährungen stellen kein Geld im Rechtssinne dar.[12] Jedoch sind sie als Vermögen

[1] U. S. Department of Justice: Bitfinex Hacker and Wife Plead Guilty to Money Laundering Conspiracy Involving Billions in Cryptocurrency (Pressemeldung vom 3.8.2023), https://www.justice.gov/opa/pr/bitfinex-hacker-and-wife-plead-guilty-money-laundering-conspiracy-involving-billions [Stand: 8.2.2025].
[2] *Djazayeri*, Die virtuelle Währung Bitcoin – Zivilrechtliche Fragestellungen und internationale regulatorische Behandlung, jurisPR-BKR 6/2014 Anm. 1; *Kaulartz*, Die Blockchain-Technologie, CR 2016, S. 474 (474).
[3] extraETF, https://extraetf.com/de/crypto-profile/bitcoin [Stand: 8.2.2025].
[4] *Buhrs*, Digitale Werteinheiten mit ausgeprägten Unterschieden, https://www.finanztip.de/kryptowaehrungen/ [Stand: 8.2.2025].
[5] *Djazayeri*, jurisPR-BKR 6/2014 Anm. 1; *Kütük-Markendorf*, Rechtliche Einordnung von Internetwährungen im deutschen Rechtssystem am Beispiel von Bitcoin, 2016, S. 30 ff.
[6] *Ludes*, Der „Kryptodiebstahl“ – eine Lücke im deutschen Strafrecht?, ZdiW 2022, S. 390 (390); *Siegel* in: Omlor/Link, Kryptowährungen und Token, 2. Auflage 2023, S. 82.
[7] *Börner*, Kryptowährungen und strafbarer Missbrauch, NZWiSt 2018, S. 48 (48); *Beck*, Bitcoins als Geld im Rechtssinne, NJW 2015, S. 580 (581); *Engelhardt/Klein*, Bitcoins – Geschäfte mit Geld, das keines ist, MMR 2014, S. 355 (355).
[8] *Spindler/Bille*, Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, S. 1357 (1359); *Börner*, NZWiSt 2018, S. 48 (49); *Siegel* in: Omlor/Link (Fn. 6), S. 82.
[9] *Schröder/Triantafyllakis*, Kryptowerte in der Insolvenz des Kryptoverwahrers, BKR 2023, S. 12 (13); *Grzywotz/Köhler/Rückert*, Cybercrime mit Bitcoins, StV 2016, S. 753 (754); *Kütük/Sorge*, Bitcoin im deutschen Vollstreckungsrecht, MMR 2014, S. 643 (643).
[10] *Böhm*, Der strafrechtliche Schutz der Inhaberschaft von Kryptowährungseinheiten, S. 92; *Fromberger/Haffke/Zimmermann*, Kryptowerte und Geldwäsche, BKR 2019, S. 377 (377).
[11] *Böhm* (Fn. 10), S. 82, 85.
[12] *Hefendehl* in: MüKo-StGB, Band 5, 4. Auflage 2022, § 263 Rn. 615; *Baier*, Kriminalpolitische Herausforderungen durch Bitcoin und andere Kryptowährungen, CCZ 2019, S. 123 (125).

rechtlich anerkannt[13] und gelten somit auch als Vermögen im strafrechtlichen Sinne, insbesondere im Rahmen des juristisch-ökonomischen Vermögensbegriffs.[14]

C. Prüfung der Strafbarkeit

I. Anknüpfungspunkte an die Strafbarkeit

Um Kryptowährungen zu „stehlen“, ist ein Zugriff auf den privaten Schlüssel erforderlich, mit dessen Hilfe eine Transaktion über die Blockchain ausgeführt und die Token einer anderen Adresse zugeordnet werden können. Somit kann die Tathandlung in zwei Phasen aufgeteilt werden: das Beschaffen des privaten Schlüssels und die Initiierung einer Transaktion, der eigentliche „Diebstahl“ der Token.[15] Darüber hinaus sind weitere Szenarien denkbar, etwa der sog. Adresswechsel, bei dem der Nutzer irrtümlicherweise Token an den Täter überträgt[16] oder der Entzug des Zugriffs auf den privaten Schlüssel.[17] Im Folgenden sollen die letzten beiden Möglichkeiten außer Betracht bleiben, um einen genaueren Blick auf die Erlangung des privaten Schlüssels und das Auslösen einer Transaktion zu werfen.

II. Strafrechtliche Bewertung

1. Beschaffen des privaten Schlüssels

Es sind verschiedene Vorgehensweisen denkbar, wie ein Täter Kenntnis des privaten Schlüssels erlangen kann. Nachfolgend sollen das sog. Phishing, Hacking und das Entwenden der Hardware, auf dem ein privater Schlüssel gespeichert ist, näher beleuchtet werden.

a) Phishing

Beim Phishing erschleicht sich der Täter das Vertrauen des Opfers, sodass es die sensiblen Daten freiwillig preisgibt.[18] Dies kann beispielsweise über das Versenden von E-Mails erfolgen, die den Anschein erwecken, als stammen sie von einem Wallet-Anbieter oder einer Kryptobörse, welche die privaten Schlüssel ihrer Kunden verwalten. Über einen Link wird der Nutzer auf eine gefälschte Webseite geleitet, auf der er aufgefordert wird, seine Zugangsdaten einzugeben.[19]

aa) § 263 I StGB

In Betracht kommt zunächst eine Strafbarkeit wegen Betrugs gemäß § 263 I StGB, denn durch die E-Mail wird beim Opfer bewusst eine Fehlvorstellung darüber hervorgerufen, dass die E-Mail und schließlich auch die Webseite von seinem Wallet-Anbieter stamme. Somit täuscht der Täter über das Vorstellungsbild des Opfers und führt einen Irrtum hervor. Ignoriert das Opfer hingegen die E-Mail, scheidet eine Strafbarkeit mangels Täuschung aus.[20]

Problematischer ist das Tatbestandsmerkmal der Vermögensverfügung. Eine Vermögensverfügung wird definiert als jedes Handeln, Dulden oder Unterlassen, das unmittelbar eine Vermögensminderung herbeiführt.[21]

(1) Vermögensminderung

Initiiert der Täter eine Transaktion über die Blockchain, so liegt eine Vermögensminderung, bzw. ein Schaden i. S. d. juristisch-ökonomischen Vermögensbegriffs[22] vor,[23] insbesondere seit Kryptowährungen als Wirtschaftsgüter anerkannt sind.[24] Durch das bloße Erlangen des privaten Schlüssels oder der Zugangsdaten zur Online-Wallet mindert der Täter noch nicht das Vermögen des Opfers, da er noch keine Transaktion ausgeführt hat. Jedoch kann im Rahmen der Figur der schadensgleichen Vermögensgefährdung bereits eine konkrete Gefahr des Vermögensverlustes eine Vermögensminderung darstellen. Hierfür muss die Gefahr des Vermögensverlustes so nahe liegen und so groß sein, dass nach wirtschaftlicher Betrachtungsweise in dieser Gefährdung bereits eine

---

[13] BGH Urt. v. 27.7.2017 − 1 StR 412/16 = NStZ 2018, S. 401 (405); *Hefendehl* in: MüKo-StGB (Fn. 12), § 263 Rn. 616; *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung, MMR 2014, S. 75 (77); *Rettke*, Bitcoin und die strafrechtliche Einziehung, NZWiSt 2020, S. 45 (50).
[14] *Böhm* (Fn. 10), S. 166; *Rückert* in: Maume/Maute, Rechtshandbuch Kryptowerte, 2020, § 22 Rn. 4; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, 2019, S. 148.
[15] *Böhm* (Fn. 10), S. 178; *Rückert* in: Maume/Maute (Fn. 14), § 20 Rn. 12.
[16] *Böhm* (Fn. 10), S. 326 ff.
[17] *Böhm* (Fn. 10), S. 334 ff.
[18] *Maihold* in: Ellenberger/Bunte Bankrechts-Handbuch, Band 1, 6. Auflage 2022, § 33 Rn. 49; *Goeckenjan*, Phishing von Zugangsdaten für Online-Bankdienste und deren Verwertung, wistra 2008, S. 128 (129).
[19] *Grzywotz* (Fn. 14), S. 184.
[20] *Gercke*, Die Strafbarkeit von „Phishing“ und Identitätsdiebstahl, CR 2005, S. 606 (607).
[21] BGH Urt. v.11.3.1960 – 4 StR 588/59 = NJW 1960, S. 1068 (1069); BGH Urt. v. 10.8.2016 − 2 StR 579/15 = NStZ 2017, S. 351 (352); OLG Karlsruhe Urt. v. 9.8.2023 – 1 ORs 35 Ss 322/23 = NJW 2023, S. 2894 (2894); *Beukelmann* in: BeckOK-StGB, 60. Edition, Stand: 1.2.2024, § 263 Rn. 31; *Perron* in: Schönke/Schröder StGB, 30. Auflage 2019, § 263 Rn. 55.
[22] *Saliger* in: Matt/Renzikowski StGB, 2. Auflage 2020, § 263 Rn. 155; *Gähler*, Der Gefährdungsschaden im Untreuetatbestand, 2016, S. 37; *Pawlik*, Das unerlaubte Verhalten beim Betrug, 1999, S. 258.
[23] *Böhm* (Fn. 10), S. 198.
[24] BMF, Schr. v. 15.5.2022, IV C 1 – S 2256/19/10003 :001, S. 995; BFH Urt. v. 14.2.2023 – IX R 3/22 = DStR 2023, S. 435 (439).

bezifferbare Verschlechterung der gegenwärtigen Vermögenslage liegt.[25]

(a) Meinungsstand

Ob ein Gefährdungsschaden im zu untersuchenden Fall vorliegt, ist nicht eindeutig geklärt.

Bejahende Stimmen argumentieren, dass das Opfer die alleinige Verfügungsmacht über den privaten Schlüssel verliere und außer eines schnellen Transfers der Token auf eine andere Blockchain-Adresse keine Möglichkeit habe, eine Transaktion des Täters zu verhindern.[26]

Eine andere Ansicht lehnt dagegen einen Gefährdungsschaden ab.[27] Die Transaktion der Token durch den Täter stelle eine weitere Handlung mit einem selbstständigen Willensentschluss dar, den der Täter zwischenzeitlich noch aufgeben könnte. Mithin sei das bloße Phishing der Zugangsdaten noch keine schadensgleiche Gefährdung für das Vermögen.

(b) Stellungnahme

Der BGH hat bisher keinen Fall zum Phishing in Bezug auf Kryptowährungen entschieden. Im Schrifttum werden häufig Parallelen zu den EC-Karten-Fällen gezogen, bei denen der Täter täuschungsbedingt die EC-Karte des Opfers mit dazugehöriger PIN erlangt.[28] Der BGH bejaht hier einen Betrug, nimmt also – wenn auch nicht ausdrücklich – einen Gefährdungsschaden an.[29] Der Täter habe nun ungehinderten Zugriff und müsse nur noch aktiv werden.[30] Wird dieser Gedanke auf den Fall des Phishing von Kryptowährungen übertragen, so hat der Täter mit dem Zugriff auf den privaten Schlüssel bzw. den Zugangsdaten zur Wallet alles, was er zum Auslösen einer Transaktion benötigt. Jedoch ist hierbei zu beachten, dass das Opfer seinen Zugriff auf den privaten Schlüssel nicht verliert. Vielmehr haben nun sowohl Opfer als auch Täter die Möglichkeit, Transaktionen über die Blockchain auszuführen. Dies ist ein entscheidender Unterschied zum EC-Karten Fall, bei dem das Opfer den Besitz an der EC-Karte verliert, also selbst keinen direkten Zugriff – zumindest mithilfe der Karte – auf das Kontoguthaben hat.

Das BVerfG erkennt die Rechtsfigur des Gefährdungsschadens zwar an, mahnt aber, den Tatbestand nicht verfassungswidrig auszuweiten.[31] So wird bereits in den EC-Karten Fällen die Annahme eines Gefährdungsschadens kritisiert.[32] Da das Opfer im zu untersuchenden Fall immer noch Zugriff auf den privaten Schlüssel hat, würde die Annahme einer Vermögensgefährdung, die so nahe liegt, dass bereits ein Schaden bezifferbar ist, über die Grenzen des Bestimmtheitsgebots[33] (Art. 103 II GG) hinausgehen. Zudem würde mit der Bejahung eines Gefährdungsschadens ein Täter, welcher seinen Willen nach dem Erlangen der Zugangsdaten ändert und anschließend keine Transaktion ausführt, mit dem Täter gleichgestellt werden, welcher diese Handlung vornimmt. Aus diesen Gründen ist ein Gefährdungsschaden abzulehnen. Anders wäre das Ergebnis, wenn der Täter den Zugriff des Opfers auf den privaten Schlüssel oder die Online-Wallet verhindert, etwa durch eine Änderung des Wallet-Passworts.

(2) Unmittelbarkeit

In diesen Fällen muss die Vermögensminderung zudem unmittelbar eintreten. Es ist nicht final geklärt, wann eine Unmittelbarkeit vorliegt.

Häufig wird vertreten, dass keine weiteren Zwischenhandlungen seitens des Täters gegeben sein dürfen.[34] Der Betrug benötige in Abgrenzung zum Diebstahl einen „Akt des Gebens“ durch das Opfer. Dies unterstreiche den Selbstschädigungscharakter des Betrugs. [35] Schaffe sich der Täter durch seine Handlung nur die Möglichkeit eine Vermögensminderung oder einen Schaden beim Opfer zu bewirken, sind aber noch weitere Handlungsschritte

---

[25] BGH Urt. v. 9.7.1987 – 4 StR 216/87 = NJW 1987, S. 3144 (3145); BGH Urt. v. 15.12.2006 – 5 StR 181/06 = NJW 2007, S. 782 (786); *Rengier*, Strafrecht Besonderer Teil I, 26. Auflage 2024, § 13 Rn. 210.
[26] *Grzywotz* (Fn. 14), S. 186; *Böhm* (Fn. 10), S. 215.
[27] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 17.
[28] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 16; *Grzywotz* (Fn. 14), S. 185.
[29] BGH Urt. v. 17.8.2004 – 5 StR 197/04 = NStZ-RR 2004, S. 333 (334); BGH Urt. v. 15.1.2013 – 2 StR 553/12, Rn. 2, BGH Urt. v. 16.7.2015 − 2 StR 16/15 = NStZ 2016, S. 149 (152); BGH Urt. v. 9.8.2016 – 3 StR 109/16, Rn. 8.
[30] *Ceffinato*, Vermögensstraftaten um und über das Internet, NZWiSt 2016, S. 464 (466); *Weber*, Phishing: Brauchen wir einen Sondertatbestand zur Verfolgung des Internetphishings?, HRRS 2004, S. 406 (409).
[31] BVerfG Urt. v. 23.6.2010 – 2 BvR 2559/08 = NJW 2010, S. 3209 (3220); BVerfG Urt. v. 7.12.2011 − 2 BvR 2500/09 = NJW 2012, S. 907 (916).
[32] *Bosch*, Computerbetrug mittels einer durch Betrug erlangten EC-Karte, JURA 2016, S. 451 (451); *Popp*, „Phishing“, „Pharming“ und das Strafrecht, MMR 2006, S. 84 (86); *Perron* in: Schönke/Schröder StGB (Fn. 21), § 263 Rn. 64.
[33] BVerfG Urt. v. 21.6.1977 – 2 BvR 308/77 = NJW 1977, S. 1815 (1815).
[34] OLG Saarbrücken Urt. v. 6.10.1966 - Ss 36/66 = NJW 1968, S. 262 (262); *Gercke*, CR 2005, S. 606 (608); *Saliger* in: Matt/Renzikowski StGB (Fn. 22) § 263 Rn. 117.
[35] *Heger* in: Lackner/Kühl/Heger StGB, 30. Auflage 2023, § 263 Rn. 22; *Fischer*, StGB, 71. Auflage 2024, § 263 Rn. 76.

erforderlich, so sei ein Betrug abzulehnen.[36] Nicht geklärt ist, ob die Zwischenhandlungen deliktischer Natur sein müssen.[37]

Im Fall des klassischen Phishing von Online-Legitimationsdaten eines Bankkontos wird das Kriterium der Unmittelbarkeit zumeist abgelehnt.[38] Zum einen trete die Vermögensminderung nicht beim Kunden selbst, sondern zunächst bei der Bank ein.[39] Zum anderen stelle das unbefugte Verwenden der erlangten Daten in Form einer Überweisung einen Computerbetrug gemäß § 263a I StGB dar, womit eine deliktische Zwischenhandlung vorliege.[40]

Zieht man nun eine Parallele zu dem Fall des Phishing von Wallet-Zugangsdaten oder privaten Schlüsseln, so ist zunächst festzustellen, dass anders als im klassischen Phishing die Vermögensminderung bei einer Transaktion der Token beim Opfer selbst eintritt, da im Kryptowährungssystem gerade keine zentrale Instanz ähnlich einer Bank beteiligt ist. Zum anderen stellt das Auslösen einer Transaktion durch den Täter keine deliktische Handlung, wie etwa §§ 263a StGB,[41] dar. Somit liegen zumindest keine Zwischenhandlungen deliktischer Natur vor.

Teilweise wird für das Unmittelbarkeitskriterium eine Beurteilung nach der allgemeinen Zurechnungslehre gefordert, da die Bestimmung der Unmittelbarkeit sonst als Notbehelf zur Darstellung des gewünschten Ergebnisses missbraucht würde.[42] Nach dieser Ansicht wäre die Vermögensminderung im zu behandelnden Fall unmittelbar, da die Vermögensminderung nach dem Erlangen der Daten des Opfers kausal auf das vorangegangene Phishing des Täters zurückzuführen und diesem objektiv zuzurechnen ist.

Es ist nicht nachvollziehbar, weshalb bei dem Merkmal der Unmittelbarkeit auf deliktische Zwischenhandlungen des Täters abgestellt wird. So würde es zu willkürlichen Ergebnissen führen, ob eine Strafbarkeit bejaht wird oder nicht, was die unterschiedliche Beurteilung bezüglich des klassischen Phishing und dem Phishing nach privaten Schlüsseln oder Wallet-Zugangsdaten zeigt. Die Anwendung der allgemeinen Zurechnungslehre genügt dem Erfordernis der Unmittelbarkeit nicht, da hier der Selbstschädigungscharakter des Betrugs verkannt wird. Die Handlung des Opfers muss gerade einen „Akt des Gebens“ darstellen und nicht nur dem Täter die Möglichkeit geben, eine Vermögensminderung herbeizuführen. Erlangt der Täter die erforderlichen Daten, um eine Transaktion auslösen zu können, kann er immer noch von der Tat Abstand nehmen oder sonst an der Tat gehindert werden.[43] Ebenso stellt der private Schlüssel gerade nur die Möglichkeit für den Täter dar, durch weitere Zwischenhandlungen eine Vermögensminderung durch eine Transaktion herbeizuführen.

Selbst bei der Annahme einer Vermögensminderung scheitert das Tatbestandsmerkmal der Vermögensverfügung somit an der Unmittelbarkeit.

(3) Zwischenergebnis

Somit scheidet die Strafbarkeit wegen Betrugs aus.

bb) § 263a III StGB

Weiterhin denkbar ist eine Strafbarkeit wegen der Vorbereitung eines Computerbetrugs (§ 263a III Nr. 1, 2 StGB), wenn der Täter Webseiten erstellt oder Phishing-E-Mails verschickt. Das Phishing muss jedoch als objektiven Zweck die Begehung eines Computerbetrugs haben.[44] Durch das Auslösen einer Transaktion verwirklicht der Täter nicht den Tatbestand des § 263a I StGB.[45] Somit scheidet eine Strafbarkeit gemäß § 263a III StGB aus.

cc) § 269 I StGB

Durch das Verschicken der Phishing-E-Mail sowie den Betrieb einer falschen Webseite kommt eine Strafbarkeit gemäß § 269 I StGB in Betracht, soweit er das Opfer über die Identität des Absenders und des Erstellers täuscht und der E-Mail, bzw. der Webseite Urkundenqualität zugewiesen werden kann.[46]

---

[36] *Heger* in: Lackner/Kühl/Heger StGB (Fn. 35), § 263 Rn. 25; *Hefendehl* in: MüKo-StGB (Fn. 12), § 263 Rn. 431.
[37] Bejahend: BGH Urt. v. 29.6.2005 - 4 StR 559/04 = NJW 2005, S. 2789 (2789); BGH Urt. v. 29.6.2005 – 4 StR 559/04 = wistra, 2005, S. 427 (428); BGH Urt. v. 10.8.2016 − 2 StR 579/15 = NStZ 2017, S. 351 (352); OLG Karlsruhe Urt. v. 9.8.2023 – 1 ORs 35 Ss 322/23 = ZWH 2023, S. 309 (310).
[38] *Popp*, Von „Datendieben” und „Betrügern” - Zur Strafbarkeit des so genannten „phishing”, NJW 2004, S. 3517 (3518); *Weber*, HRRS 2004, S. 406 (408); *Popp*, MMR 2006, S. 84 (86); *Graf*, „Phishing“ derzeit nicht generell strafbar!, NStZ 2007, S. 129 (131); *Heghmanns*, Die Strafbarkeit des „Phishing“ von Bankkontodaten und ihre Verwertung, wistra 2007, S. 167 (168), *Goeckenjan*, wistra 2008, S. 128 (130); *Seidl/Fuchs*, Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafänderungsgesetzes, HRRS 2010, S. 85 (86).
[39] *Popp*, MMR 2006, S. 84 (86); *Goeckenjan*, wistra 2008, S. 128 (130).
[40] *Gercke*, CR 2005, S. 606 (608); *Marberth-Kubicki*, Computer- und Internetstrafrecht, 1. Auflage 2005, Rn. 120.
[41] Siehe hierzu Teil C, II, 2., b).
[42] *Stuckenberg*, Zur Strafbarkeit des „Phishing“, ZStW 118 (2006), S. 878 (903); *Pawlik* (Fn. 22), S. 241.
[43] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 17.
[44] Vgl. *Husemann*, Die Verbesserung des strafrechtlichen Schutzes des bargeldlosen Zahlungsverkehrs durch das 35. Strafänderungsgesetz, NJW 2004, S. 104 (108); *Altenhain* in: Matt/Renzikowski StGB (Fn. 22), § 263a Rn. 28.
[45] Siehe hierzu Teil C, II, 2., b).
[46] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 18; *Böhm* (Fn. 10), S. 217; *Grzywotz* (Fn. 14), S. 187.

dd) §§ 202a I, 202b StGB

Denkbar ist eine Strafbarkeit nach § 202a I StGB, da der Täter mithilfe der „gephishten“ Zugangsdaten zur Wallet des Opfers die Zugangssicherung überwindet und so Daten ausspäht, die nicht für ihn bestimmt sind. Jedoch erfolgt die Überwindung der Zugangssicherung durch die Daten, die das Opfer zwar durch Täuschung, aber ansonsten freiwillig herausgibt. Somit scheitert eine Strafbarkeit an dem Merkmal „nicht für den Täter bestimmt“ durch ein tatbestandsausschließendes Einverständnis.[47] Aus demselben Grund scheitert eine Strafbarkeit gemäß § 202b StGB. Die Wallet-Daten werden nicht mithilfe von technischen Mitteln abgefangen, sondern freiwillig durch das Opfer herausgegeben.[48]

ee) § 240 I StGB

Eine Strafbarkeit wegen Nötigung gemäß § 240 I StGB kommt nur dann in Betracht, wenn der Täter in der E-Mail – beispielsweise mit der Sperrung der Wallet – droht.[49]

ff) Weitere Straftatbestände

Im Fall des Phishing von privaten Schlüsseln oder Zugangsdaten zu Online-Wallets kommen über das StGB hinaus weitere Straftatbestände in Betracht. Nutzt der Täter beim Betreiben der falschen Webseite geschützte Logos, so ist eine Strafbarkeit nach §§ 106 ff. UrhG oder § 143 MarkenG denkbar; bei Verstößen gegen das Datenschutzrecht kann § 42 II BDSG einschlägig sein.[50]

b) Hacking

Eine weitere Methode an den privaten Schlüssel des Opfers zu gelangen, ist das Hacking. Dabei wird gegen den Willen des Berechtigten in dessen Computersystem eingedrungen und es werden meist durch eine Schadsoftware Daten ausgespäht, abgegriffen oder manipuliert.[51] Besonders anfällig für Hacking-Angriffe sind Online-Wallets, da sich die Daten auf einem Webserver befinden und diese oft schwächer geschützt sind.[52]

aa) § 202a I StGB

Wallet-Daten, die den privaten Schlüssel beinhalten, stellen Daten i. S. d. § 202a II StGB dar.[53] Bezüglich der Zugangssicherung genügt es, wenn zum Ausdruck kommt, dass ein Interesse an einer Geheimhaltung besteht.[54] Überwindet der Täter durch das Hacking eine Firewall oder ein Antivirenprogramm, so ist dies erfüllt. Umgeht der Täter hingegen mithilfe einer Schadsoftware die Zugangssicherung, so liegt kein Überwinden i. S. d. § 202a I StGB vor.[55]

bb) Weitere Straftatbestände

Löscht der Täter den privaten Schlüssel so macht er sich regelmäßig gemäß § 303a I StGB strafbar.[56] Je nach Schadprogramm ist ebenso eine Strafbarkeit gemäß § 303b I StGB möglich, soweit die Token für das Opfer von wesentlicher Bedeutung sind.[57] Zudem kommt eine Strafbarkeit gemäß § 23 I Nr. 1 GeschGehG in Betracht, wenn die Token und damit der private Schlüssel zu unternehmerischen Zwecken genutzt werden, da der private Schlüssel ein Geschäftsgeheimnis i. S. d. § 2 Nr. 1 GeschGehG darstellen kann.[58]

c) Entwenden der Hardware-Wallet

Eine weitere Möglichkeit des Täters an den privaten Schlüssel des Opfers zu gelangen, ist das Entwenden der Hardware, auf welcher der private Schlüssel gespeichert oder sonst damit verbunden ist. Hardware-Wallets können beispielsweise USB-Sticks oder sonstige Speichermedien sein, es kommen jedoch auch analoge Wallets wie ein Blatt Papier, sog. Paper Wallets,[59] in Betracht. In der Praxis dürfte dieses Vorgehen wohl seltener sein. Dennoch wurde bereits über einen Fall berichtet, in dem ein bayerisches Unternehmen mehr als

---

[47] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 14; *Graf* in: MüKo-StGB, Band 4, 4. Auflage 2021, § 202a Rn. 64; *Popp*, MMR 2006, S. 84 (85); *Graf*, NStZ 2007, S. 129 (131); *Heghmanns*, wistra 2007, S. 167 (169); *Goeckenjan*, Auswirkungen des 41. Strafrechtsänderungsgesetzes auf die Strafbarkeit des „Phishing“, wistra 2009, S. 47 (50).
[48] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 14; vgl. *Weidemann* in: BeckOK-StGB (Fn. 21), § 202b Rn. 9.
[49] Vgl. *Stuckenberg*, ZStW 118 (2006), S. 878 (905); *Seidl/Fuchs*, HRRS 2010, S. 85 (86).
[50] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 18; *Böhm* (Fn. 10), S. 218.
[51] BT Drs. 16/3656 S. 7; *Böhm* (Fn. 10), S. 181; *Ernst*, Hacker und Computerviren, NJW 2003, S. 3233 (3233 f.).
[52] *Grzywotz* (Fn. 14), S. 187; *Dölle*, Fiasco! Kryptobörse Altsbit wälzt Diebstähle auf einzelne Kunden ab, c´t 5/2018, S. 64 (64).
[53] *Böhm* (Fn. 10), S. 183.
[54] BT-Drs. 10/5058, S. 29; *Ernst*, NJW 2003, S. 3233 (3236).
[55] Vgl. BGH Urt. v. 21.7.2015 – 1 StR 16/15 = NJW 2015, S. 3463 (3464); *Grzywotz* (Fn. 14), S. 188.
[56] *Koch* in: Omlor/Link (Fn. 6), S. 882; vgl. *Hilgendorf/Kudlich/Valerius/Eisele*, Handbuch des Strafrechts – Band 6: Teildisziplinen des Strafrechts, § 63 Rn. 122.
[57] *Koch* in: Omlor/Link (Fn. 6), S. 882 f.
[58] *Böhm* (Fn. 10), S. 183 ff; *Kütük-Markendorf* (Fn. 5), S. 112 ff.
[59] *Böhm* (Fn. 10), S. 85; *Rettke*, NZWiSt 2020, S. 45 (48).

eine halbe Million Euro verlor, indem die Täter einen USB-Stick mit einem privaten Schlüssel entwendeten.[60]

aa) § 242 I StGB

Wird eine Hardware-Wallet entwendet, liegt zunächst eine Strafbarkeit wegen Diebstahls gemäß § 242 I StGB nahe. Der objektive Tatbestand dürfte in den meisten Fällen erfüllt sein; insbesondere handelt es sich bei USB-Sticks, Speicherplatten oder Paper-Wallets um körperliche Gegenstände und damit um Sachen i. S. d. § 90 BGB. Im subjektiven Tatbestand ist das Merkmal der Zueignungsabsicht eine Voraussetzung. Diese beinhaltet eine Enteignungs- und Aneignungskomponente.[61] Bezüglich der Enteignung genügt als Vorsatzform dolus eventualis,[62] für die Aneignung ist Absicht, also dolus directus ersten Grades erforderlich.[63]

(1) Handeln ohne Rückführungswillen

Erfolgt die Wegnahme ohne einen Rückführungswillen, so ist sowohl eine Aneignungsabsicht als auch ein Enteignungswille gegeben.[64] Dabei ist es im Ergebnis unerheblich, ob der Täter die Hardware nach Auslesen des privaten Schlüssels selbst weiter nutzt, ohne weitere Nutzung in seinem Besitz behält oder sogar zerstört. Zwar entschied der BGH, dass bei späterer Zerstörung des Trägers eine Aneignungsabsicht nicht unbedingt gegeben ist,[65] stellt aber in einer späteren Entscheidung klar, dass es darauf ankomme, ob der Täter sich die Sache zumindest vorübergehend körperlich und wirtschaftlich einverleiben will.[66] Dem ist zuzustimmen. Bei einem Entwenden der Hardware-Wallet erfolgt die Wegnahme nicht nur, um dem Opfer den Zugriff zu verweigern, sondern vor allem zur Nutzung eigener Zwecke, nämlich dem Auslesen des privaten Schlüssels, um eine Transaktion der dazugehörigen Token auslösen zu können. Eine Aneignungsabsicht kann demnach auch dann bejaht werden, wenn der Täter nach Kopie der auf der Hardware befindlichen Daten kein Interesse mehr an der Hardware hat und diese vernichtet.[67]

(2) Handeln mit Rückführungswillen

Häufig wird es im Interesse des Täters liegen, den Datenträger wieder an das Opfer zurückzuführen, um unauffällig zu handeln und sein wahres Vorhaben zu verschleiern. Bezüglich des Substanzwerts der Hardware scheidet ein Diebstahl aus, da der Täter bei der Wegnahme nicht die Absicht hat, sich die Sache selbst anzueignen.

Zueignungsgegenstand kann jedoch auch der Wert sein, der in der Sache verkörpert ist, konkret also der Wert der Kryptowährungseinheiten. Nach der sog. Vereinigungstheorie[68] kann der Zueignungsgegenstand neben dem Substanzwert der Sache selbst auch der ihr innewohnende Sachwert sein. Bei einem Sparbuch etwa, das mit Rückführungswillen entwendet wird, wird ein verkörperter Wert in Form des Sparguthabens angenommen und eine Zueignungsabsicht bejaht.[69] Eine EC-Karte hingegen verkörpert nicht den auf dem Konto befindlichen Wert, da sie nur wie ein Schlüssel fungiert, welcher Zugang zu dem verwahrten Vermögen ermöglicht.[70]

Wendet man diese Grundsätze auf die Wegnahme einer Hardware-Wallet an, welche den privaten Schlüssel enthält, so ist festzustellen, dass nicht bereits die Sache selbst den wirtschaftlichen Wert darstellt. Ähnlich dem EC-Karten-Fall eröffnet der Datenträger nur die Möglichkeit, auf das Vermögen in Form der Token

---

[60] *Emig*, Polizeipräsidium Oberbayern Süd: Internationale Täter betrügen Geschäftsmann um mehr als eine halbe Million Euro (Pressemeldung vom 2.3.2021) https://www.bka.de/DE/IhreSicherheit/Fahndungen/Personen/UnbekanntePersonen/Betruegerbande_Bayern/Sachverhalt.html [Stand: 8.2.2025].
[61] *Schmidt* in: Matt/Renzikowski StGB (Fn. 22), § 242 Rn. 27; *Rengier* (Fn. 25), § 2 Rn. 89.
[62] *Schmidt* in: Matt/Renzikowski StGB (Fn. 22), § 242 Rn. 28; *Wittig* in: BeckOK-StGB (Fn. 21), § 242 Rn. 39.
[63] BGH Urt. v. 22.3.2012 – 4 StR 541/11 = NStZ-RR 2012, S. 239 (241); *Wittig* in: BeckOK-StGB (Fn. 21), § 242 Rn. 39; *Schmitz* in: MüKo-StGB (Fn. 47), § 242 Rn. 129.
[64] *Grzywotz* (Fn. 14), S. 189; *Koch* in: Omlor/Link (Fn. 6), S. 879.
[65] BGH Urt. v. 14.2.2012 – 3 StR 392/11 = NStZ 2012, S. 627 (627).
[66] BGH Urt. v. 17.10.2019 – 3 StR 536/18 = StV 2020, S. 667 (668).
[67] *Böhm* (Fn. 10), S. 227; *Putzke*, Anmerkung zu einer Entscheidung des BGH, Beschluss vom 14.02.2012 (3 StR 392/11), ZJS 2013, S. 311 (313); *Reinbacher*, Neue Herausforderungen an die Zueignungsabsicht i. S. d. § 242 StGB bei Daten- und Informationsträgern, ZStW 126 (2014), S. 642 (665).
[68] BGH Urt. v. 15.1.1970 – 4 StR 527/69 = NJW 1970, S. 1753 (1754); BGH Urt. v. 10.5.1977 – 1 StR 167/77 = NJW 1977, S. 1460 (1460); BGH, v. 26.9.1984 – 3 StR 367/84 = NJW 1985, S. 812 (812); *Kindhäuser/Hoven* in: NK-StGB, 6. Auflage 2023, § 242 Rn. 78; *Schmitz* in: MüKo-StGB (Fn. 47), § 242 Rn. 138.
[69] *Heger* in: *Lackner/Kühl/Heger* StGB (Fn. 35), § 242 Rn. 23; *Bosch* in: Schönke/Schröder StGB (Fn. 21) § 242 Rn. 50; *Wessels/Hillenkamp/Schuhr*, Strafrecht Besonderer Teil 2, 46. Auflage 2023, § 2 Rn. 179.
[70] BGH Urt. v. 16.12.1987 – 3 StR 209/87 = NJW 1988, S. 979 (979); *Rengier* (Fn. 25), § 2 Rn. 113; *Wessels/Hillenkamp/Schuhr* (Fn. 69), § 2 Rn. 186.

zuzugreifen. Die Hardware selbst ist, anders als eine EC-Karte, nicht zum Auslösen einer Transaktion erforderlich. Dies verdeutlicht umso mehr, dass die Hardware-Wallet keinen Sachwert in Form der Token verkörpern kann. Faktischer Wertträger der Token ist damit nicht einmal der private Schlüssel, sondern die Daten der Blockchain, da hierdurch bestimmten Adressen ein Wert zugewiesen wird.

Es lässt sich zusammenfassen, dass die Token keinen innewohnenden Sachwert der Hardware-Wallet darstellen. Das kurzzeitige Entwenden dieser stellt damit lediglich eine straflose Gebrauchsanmaßung dar.[71]

(3) Zwischenergebnis

Entwendet der Täter eine Hardware-Wallet mit einem darauf gespeicherten, privaten Schlüssel, so macht er sich nur strafbar, wenn er bei der Wegnahme keinen Rückführungswillen hat. Der entzogene Wert ist jedoch nur der Substanzwert, also etwa der Wert des USB-Sticks oder des Papiers. Diese dürften in vielen Fällen wohl geringfügige Sachen i. S. d. § 248a StGB darstellen und somit nur auf Antrag verfolgt werden.

bb) § 303a I StGB

Entzieht der Täter die Hardware und damit die darauf gespeicherten Daten, ist eine Strafbarkeit gemäß § 303a I Var. 2 StGB möglich, indem er rechtswidrig Daten unterdrückt.[72] Nach überwiegender Auffassung genügt selbst das nur vorübergehende Entziehen aus dem Zugriff des Berechtigten für ein Unterdrücken.[73] Die Gegenansicht argumentiert, dass das StGB, wie etwa bei § 242 StGB, keine bloße Sachentziehung kenne und ein strafbares Unterdrücken somit dauerhaft sein müsse.[74] Dem ist entgegenzuhalten, dass die Norm das Interesse des Verfügungsberechtigten vor einer beeinträchtigten oder beseitigten Verwendbarkeit der Daten schützt.[75] Schon eine kurzzeitige Datenunterdrückung beeinträchtigt die Verwendbarkeit und kann einen erheblichen Schaden anrichten. Entzieht der Täter die Hardware auch nur vorübergehend, macht er sich somit regelmäßig gemäß § 303a I Var. 2 StGB strafbar.

cc) § 202a I StGB

In Einzelfällen kann der Täter durch das bloße Entwenden der Hardware wegen des Ausspähens von Daten i. S. d. § 202a I StGB strafbar sein. Denn bereits durch die Erlangung des Datenträgers selbst, verschafft sich der Täter Zugang zu den Daten.[76] Dabei muss eine Zugangssicherung überwunden werden. Ein Tresor oder ein anderes geschlossenes Behältnis können eine solche Sicherung darstellen.[77] Der private Schlüssel muss in Form von Daten i. S. d. § 202a II StGB vorliegen, also auf einem Datenträger gespeichert sein. Das Entwenden eines auf einem Papier aufgedruckten Schlüssels, stellt damit kein Ausspähen von Daten dar.

Das zeitlich später erfolgende Auslesen des privaten Schlüssels ist wiederum ein Ausspähen von Daten, wenn beispielsweise Passwörter oder sonstige Verschlüsselungen überwunden werden.[78] Liegt der private Schlüssel hingegen in analoger Form vor, etwa auf einem Papier gedruckt, so kommt eine Strafbarkeit gemäß § 202 I, II StGB in Betracht, soweit das Schriftstück – etwa in einem Brief – verschlossen ist.[79]

2. Transaktion selbst

Der eigentliche „Diebstahl“ stellt das Auslösen einer Transaktion auf der Blockchain mithilfe des zuvor erlangten privaten Schlüssels dar, wodurch der Täter die Token auf einen anderen öffentlichen Schlüssel transferiert und damit dem Opfer entzieht.

a) § 242 I StGB

Aufgrund der häufigen Formulierung des „Diebstahls“[80] von Kryptowährungen ist der Gedanke an eine Strafbarkeit gemäß § 242 I StGB naheliegend. Dazu müssten Token „Sachen“ i. S. v. § 90 BGB, also körperliche Gegenstände, sein. Virtuelle Währungseinheiten sind gerade nicht körperlich. So liegen sie nicht einmal als konkrete Datenmenge vor, lediglich ihre

[71] *Böhm* (Fn. 10), S. 231.
[72] *Böhm* (Fn. 10), S. 235.
[73] AG Frankfurt/M. Urt. v. 1.7.2005 2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, S. 863 (868); *Weidemann* in: BeckOK-StGB (Fn. 21), § 303a Rn. 11; *Frank*, „You’ve got (Spam-)Mail, CR 2004, S. 123 (125); *Jüngel/Schwan/Neumann*, Das Abfangen von E-Mails nach § 303a StGB, MMR 2005, S. 820 (821).
[74] *Altenhain* in: Matt/Renzikowski StGB (Fn. 22), § 303a Rn. 8; OLG Frankfurt/M. OLG Frankfurt/M. Urt. v. 22.5.2006 - 1 Ss 319/05 = MMR 2006, S. 547 (551).
[75] BT-Drs. 10/5058 S. 34; *Wieck-Noodt* in: MüKo-StGB, Band 6, 4. Auflage 2022, § 303a Rn. 2.
[76] *Altenhain* in: Matt/Renzikowski StGB (Fn. 22), § 202a Rn. 7; *Eisele* in: Schönke/Schröder StGB (Fn. 21), § 202a Rn. 18; anders *Weidemann* in: BeckOK-StGB (Fn. 21), § 202a Rn. 18; *Vassilaki*, Das 41. StrÄndG – Die neuen strafrechtlichen Regelungen und ihre Wirkung auf die Praxis, CR 2008, S. 131 (132).
[77] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 19; *Böhm* (Fn. 10), S. 236.
[78] *Grzywotz* (Fn. 14), S. 192; *Böhm* (Fn. 10), S. 237 f.
[79] *Grzywotz* (Fn. 14), S. 192; *Böhm* (Fn. 10), S. 237.
[80] Vgl. *Dölle*, Wie Cracker Millionen in Kryptowährungen stehlen, c’t 6/2020, S. 32 (32); Koch in: Omlor/Link (Fn. 6), S. 877; *Börner*, NZWiSt 2018, S. 48 (50).

Transaktion wird als Teil der Blockchain gespeichert.[81] Kryptotoken stellen demnach keine Sachen i. S. d. § 90 BGB dar.[82] Aufgrund des Analogieverbots (Art. 103 II GG)[83] kann keine Auslegung, die über den Wortlaut „Sache“ hinausgeht, angenommen werden. Mangels tauglichen Tatobjekts scheitert daher eine Strafbarkeit gemäß § 242 I StGB.[84]

b) § 263a I StGB

Die Handlung kann jedoch wegen Computerbetrugs gemäß § 263a I StGB strafbar sein.

aa) Datenverarbeitungsvorgang

Unter einer Datenverarbeitung ist jeder automatisierte Vorgang zu verstehen, bei dem durch Aufnahme von Daten und ihre Verknüpfung nach Programmen Arbeitsergebnisse erzielt werden.[85] Durch das Auslösen einer Transaktion mithilfe des privaten Schlüssels, wird eine Verarbeitung im Netzwerk angestoßen und diese wird von Minern in einen neuen Transaktionsblock aufgenommen. Somit liegt eine Datenverarbeitung vor.[86]

bb) Tathandlung

Das Verwenden unrichtiger oder unvollständiger Daten (§ 263a I Var. 2 StGB) scheidet bei einer Transaktion durch den Täter mithilfe des entwendeten privaten Schlüssels aus, da der private Schlüssel als Datum objektiv richtig und vollständig ist. In Betracht kommt die unbefugte Verwendung von objektiv richtigen Daten, § 263a I Var. 3 StGB.

(1) Meinungsstand

Ob das Auslösen einer Transaktion mithilfe eines „fremden“ privaten Schlüssels eine unbefugte Verwendung darstellt, ist umstritten. In der Rechtsprechung wurde bisher wohl nur ein Urteil bezüglich des „Diebstahls“ von Kryptowährungen gefällt. Ein ehemaliger Systemadministrator einer bayerischen Firma, welche Server und Software für Kryptowährungshandel und die Verwaltung von Kryptowährungseinheiten anbot, transferierte 29,6 Bitcoins an eine eigene Bitcoin-Adresse.[87] Das AG München bejahte hier – jedoch ohne Begründung – einen Computerbetrug. Somit ist anzunehmen, dass das AG München in der Tathandlung eine unbefugte Datenverwendung sah.

Im Schrifttum wird zum Teil ebenso eine unbefugte Verwendung in dem Auslösen einer Transaktion gesehen.[88] Der erbeutete Schlüssel stelle eine Legitimation von Transaktionen dar und nur derjenige sei befugt, der das Schlüsselpaar erzeugt hat.[89] Es bestehe eine faktische Berechtigung, welche bei einer Transaktion konkludent miterklärt werde.[90]

Eine andere Ansicht lehnt eine unbefugte Datenverwendung gänzlich ab.[91] So beinhalte der private Schlüssel keinerlei Information über die Berechtigung des Nutzers. Geprüft werde nur, ob der verwendete private Schlüssel der Richtige ist und zu dem öffentlichen Schlüssel passe.

(2) Stellungnahme

Es gibt verschiedene Ansätze, dem Merkmal „unbefugt“ zu begegnen.

Nach subjektiver Auslegung sind alle Verhaltensweisen erfasst, die nicht dem tatsächlichen oder mutmaßlichen Willen des Verfügungsberechtigten entsprechen.[92] Im zu untersuchenden Fall ist jedoch nicht klar, auf welchen Willen abzustellen ist. Anders als etwa eine Bankkarte mit PIN ist der private Schlüssel keiner konkreten Person über ein Vertragsverhältnis zugeordnet. Derjenige, der Zugang zu dem privaten Schlüssel hat, kann Transaktionen auslösen. Der private Schlüssel stellt damit kein personalisiertes Zahlungsauthentifizierungsinstrument dar.[93] Zwar geschieht die Transaktion meist gegen den Willen desjenigen, der zuvor

---

[81] *Böhm* (Fn. 10), S. 95.
[82] *Boehm/Pesch*, MMR 2014, S. 75 (77); *Djazayeri*, jurisPR-BKR 6/2014 Anm. 1; *Spindler/Bille*, WM 2014, S. 1357 (1359); *Engelhardt/Klein*, MMR 2014, S. 355 (357); *Kütük-Markendorf* (Fn. 5), S. 81; *Zickgraf*, Initial Coin Offerings – Ein Fall für das Kapitalmarktrecht?, AG 2018, S. 293 (301); *Walter*, Bitcoin, Libra und sonstige Kryptowährungen aus zivilrechtlicher Sicht, NJW 2019, S. 3609 (3610); *Stepanova/Kissler*, Der Kryptoverwahrvertrag aus zivilrechtlicher Sicht, BKR 2023, S. 735 (736).
[83] BVerfG Urt. v. 10.1.1995 – 1 BvR 718/89, 719/89, 722/89, 723/89 = NJW 1995, S. 1141 (1141); BVerfG Urt. v. 23.6.2010 – 2 BvR 2559/08 = NJW 2010, S. 3209 (3211).
[84] *Ludes*, ZdiW 2022, S. 390 (391); *Böhm* (Fn. 10), S. 244.
[85] BT-Drs. 10/318, S. 21; *Schmidt* in: BeckOK StGB (Fn. 21), § 263a Rn. 7.
[86] *Böhm* (Fn. 10), S. 254; *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, Rn. 1056.
[87] AG München Urt. v. 23.7.2020 – 1123 Ls 630 Js 1517/18 (unveröffentlicht); Generalstaatsanwaltschaft Bamberg, Pressemeldung vom 27.6.2019, https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/presse/2019/11.php [Stand: 8.2.2025].
[88] *Koch* in: Omlor/Link (Fn. 6), S. 887; *Grzywotz* (Fn. 14), S. 193.
[89] *Koch* in: Omlor/Link (Fn. 6), S. 886 f.
[90] *Grzywotz* (Fn. 14), S. 194.
[91] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 22; *Böhm* (Fn. 10), S. 267; *Ludes*, ZdiW 2022, S. 390 (393).
[92] BGH Urt. v. 10.11.1994 – 1 StR 157/94 = NJW 1995, S. 669 (670); BayObLG Urt. v. 28.8.1990 – RReg. 4 St 250/89 = NJW 1991, S. 438 (440); LG Bonn Urt. v. 18.6.1999 – 32 Qs 144–99 = NJW 1999, S. 3726 (3726); *Scheffler/Dressel*, „Unbefugtes“ Verwenden von Daten beim Computerbetrug, NJW 2000, S. 2645 (2646).
[93] *Böhm* (Fn. 10), S. 256 f.

Zugriff auf den privaten Schlüssel hatte, jedoch lässt sich grundsätzlich keine Inhaberschaft an Kryptotoken konstruieren.[94]

Die computerspezifische Auslegung nimmt eine unbefugte Verwendung von Daten nur an, wenn sich der entgegenstehende Wille des Berechtigten in der Programmgestaltung niedergeschlagen hat und diese mit ordnungswidriger Einwendung auf den Ablauf des Computerprogramms überwunden wird.[95] Im Prozess einer Transaktion wird lediglich geprüft, ob der private Schlüssel der Richtige ist, nicht ob der Anwendende zum Auslösen einer Transaktion berechtigt ist, daher wäre das Vorgehen des Täters nicht unbefugt.

Die betrugsspezifische Auslegung orientiert sich an § 263 StGB. Demnach ist eine Datenverwendung unbefugt, wenn die Handlung gegenüber einem Menschen als Täuschung anzusehen wäre.[96] Das Abheben von Geld mithilfe einer fremden EC-Karte wäre dann unbefugt, wenn anstatt des Geldautomaten ein Bankmitarbeiter getäuscht worden wäre.[97] Anders als die Bankangestellten einer Bank gibt es im Kryptowährungssystem niemanden, der die Berechtigung desjenigen prüft, der eine Transaktion auslöst. In Betracht könnten die Miner kommen, die aber wiederum aufgrund der Signierung nur die Richtigkeit des privaten Schlüssels prüfen und eben nicht die Berechtigung. Selbst bei dem Bestehen eines absoluten Rechts an Token liegt keine unbefugte Datenverwendung vor, da im Algorithmus nur die kryptographische Gültigkeit geprüft wird.[98]

Die Auslegungen kommen jeweils zu dem gleichen Ergebnis. Eine unbefugte Datenverwendung ist somit abzulehnen. Aus demselben Grund scheitert eine Strafbarkeit wegen sonstiger unbefugter Einwirkung auf den Ablauf gemäß § 263a I Var. 4 StGB.[99]

cc) Zwischenergebnis

Eine Strafbarkeit nach § 263a I StGB scheidet aus.

c) §§ 269 I, 270 StGB

Durch die vom Täter ausgelöste Transaktion kann eine Strafbarkeit wegen der Fälschung beweiserheblicher Daten gemäß §§ 269 I, 270 StGB in Betracht kommen. Nach Verifizierung durch die Miner wird jede Transaktion zu einem Teil der Blockchain; somit wird sie gespeichert.[100] Die durch den Täter ausgelöste Transaktion müsste bei ihrer Wahrnehmung eine Urkunde i. S. d. § 267 I StGB darstellen. Eine Urkunde ist jede verkörperte menschliche Gedankenerklärung (Perpetuierungsfunktion), die zum Beweis im Rechtsverkehr geeignet und bestimmt ist (Beweisfunktion) und ihren Aussteller erkennen lässt (Garantiefunktion).[101]

Durch das Initiieren einer Transaktion wird eine menschliche Gedankenerklärung mit dem Inhalt abgegeben, dass eine bestimmte Anzahl von Token auf eine andere Adresse transferiert werden soll. Diese Transaktion wird daraufhin in der Blockchain gespeichert. Somit liegen sowohl Beweis- als auch Perpetuierungsfunktion vor. Die Garantiefunktion hingegen ist problematisch. Fraglich ist, ob bei einer Transaktion mithilfe des privaten Schlüssels der Aussteller erkennbar ist. Zum Teil wird diese Frage bejaht.[102] Sinn und Zweck der Ausstellererkennbarkeit sei es, dass sich der Rechtsverkehr darauf verlasse, dass die abgegebene Erklärung von einer identifizierbaren Person stamme, die für sie eintreten möchte. Die Kryptowährungsadresse genüge den Anforderungen an die Identifizierbarkeit, da jeder private Schlüssel nur einer Person zugeordnet sei. Zudem sei die Zuordnung einer Adresse zu einer Identität mit Zusatzinformationen, z. B. über Foren oder weitere Transaktionen möglich.[103]

---

[94] *Böhm* (Fn. 10), S. 118 f.; *Drogemüller*, Blockchain-Netzwerke und Krypto-Token im Internationalen Privatrecht, 2023, S. 76 ff; *Djazayeri*, jurisPR-BKR 6/2014 Anm. 1; *Boehm/Pesch*, MMR 2014, S. 75 (78); *Kuhlmann*, Bitcoins – Funktionsweise und rechtliche Einordnung der digitalen Währung, CR 2014, S. 691 (695); *Omlor* in: Omlor/Link (Fn. 6), S. 286.
[95] OLG Celle Urt. v. 11.4.1989 – 1 Ss 287/88368 = NStZ 1989, S. 367 (367); LG Freiburg Urt. v. 17.4.1990 – IV Qs 33/90 = NJW 1990, S. 2635 (2636); LG Ravensburg Urt. v. 27.8.1990 – Qs 206/90 = StV 1991, S. 214 (215); *Neumann*, Anmerkung zu BGH, Beschluss vom 10.11.1994 – 1 StR 157/94, StV 1996, S. 375 (375).
[96] *Schlüchter*, Zweckentfremdung von Geldspielgeräten durch Computermanipulation, NStZ 1988, S. 53 (59); BGH Urt. v. 22.11.1991 – 2 StR 376/91 = NStZ 1992, S. 180 (180); OLG Köln Urt. v. 9.7.1991 – Ss 624/90 = NJW 1992, S. 125 (126); BGH Urt. v. 22.1.2013 – 1 StR 416/12 = NJW 2013, S. 2608 (2610); OLG Hamm, Urt. v. 7.4.2020 − 4 RVs 12/20 = NStZ 2020, S. 673 (674).
[97] BGH Urt. v. 21.11.2001 – 2 StR 260/0 = NJW 2002, S. 905 (906); *Altenhain*, Der strafbare Mißbrauch kartengestützter elektronischer Zahlungssysteme, JR 1997, S. 752 (758).
[98] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 22.
[99] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 22.
[100] *Grzywotz* (Fn. 14), S. 196; *Koch* in: Omlor/Link (Fn. 6), S. 888.
[101] BGH Urt. v. 3.7.1952 – 5 StR 151/52 = NJW 1952, S. 1104 (1104); BGH Urt. v. 18.6.1953 – 3 StR 166/53 = NJW 1953, S. 1519 (1520); OLG München Urt. v. 5.1.2010 – 5 St RR 354/09 = NStZ-RR 2010, S. 173 (173); *Weidemann* in: BeckOK-StGB (Fn. 21), § 267 Rn. 3.
[102] *Koch* in: Omlor/Link (Fn. 6), S. 890; *Grzywotz* (Fn. 14), S. 197.
[103] *Grzywotz* (Fn. 14), S. 196 f.; *Spindler/Bille*, WM 2014, S. 1357 (1359).

Führt man sich die Grundsätze der Garantiefunktion vor Augen, so ergibt sich ein anderes Ergebnis. Demnach muss sich schon aus der Erklärung selbst der Aussteller ermitteln lassen – ohne Nachforschungen oder unter Zuhilfenahme außerhalb der Erklärung liegender Umstände.[104] Zwar ist es wohl möglich, eine Kryptoadresse einer identifizierbaren Person zuzuordnen, indem weitere Transaktionen überwacht werden, jedoch sind hierfür weitere Informationen erforderlich, die über den Informationsgehalt der konkreten Transaktion hinausgehen. Zudem ist es möglich, dass die Token mehrerer Personen bei einer gemeinsamen Kryptoadresse hinterlegt sein können oder eine Person mehrere Adressen erstellt und nutzt, womit nicht unbedingt eine Person identifiziert werden kann.[105] Auch die digitale Signatur weist lediglich darauf hin, dass der richtige private Schlüssel verwendet wurde und hat keinen Aussagegehalt über die Person des Ausstellers.[106] Im Rahmen des § 269 I StGB müssen im Gesamtsystem getroffene Vorkehrungen eine Identifizierung ermöglichen, wenn der Aussteller nicht unmittelbar gespeichert ist.[107] Dies ist im Kryptowährungssystem gerade nicht der Fall. Zu keinem Zeitpunkt müssen die Nutzer persönliche Daten preisgeben.[108] Aufgrund der fehlenden Urkundenqualität scheidet eine Strafbarkeit nach §§ 269 I, 270 StGB aus.

d) § 303a I StGB

Möglich ist jedoch eine Strafbarkeit wegen Datenveränderung i. S. d. § 303a I StGB, indem der Täter eine Transaktion auf der Blockchain auslöst. Als Tatobjekt kommen lediglich die Daten, welche durch die Transaktion der Blockchain angehängt werden, infrage, da die Token selbst nicht als Datum, sondern als Datensatz mit einem zugeordneten Wert vorliegen.[109]

aa) Tathandlung

Ein Löschen von Daten liegt nicht vor. Die Token werden mit einer Transaktion zwar einer anderen Kryptoadresse zugeordnet, jedoch gehen dabei nicht die Daten der Blockchain verloren.[110] Auch ein Unterdrücken oder Unbrauchbarmachen scheidet aus. So hat das Opfer jederzeit die Möglichkeit selbst eine Transaktion auszuführen. Ein Verändern von Daten liegt vor, wenn eine inhaltliche Umgestaltung der Daten erfolgt und sie deshalb einen anderen Informationsgehalt aufweisen.[111] Wenn eine neue Transaktion ausgelöst wird, wird diese in einem neuen Block der Blockchain gespeichert. Mithin wird der Informationsgehalt der Blockchain durch die Transaktion geändert. Teilweise wird angenommen, dass dies bereits ein Verändern i. S. d. § 303a I StGB darstelle.[112] Dem ist jedoch entgegenzuhalten, dass keine bestehenden Daten verändert werden, sondern lediglich neue Daten zur Blockchain hinzugefügt werden.

bb) Eigentümerähnliche Verfügungsbefugnis

Ob tatsächlich eine Tathandlungsvariante des § 303a I StGB vorliegt, kann jedoch dahinstehen, soweit eine weitere Voraussetzung des Tatbestands verneint wird. In Betracht kommt das ungeschriebene Tatbestandsmerkmal der eigentümerähnlichen Verfügungsbefugnis, welches der „Fremdheit“ in § 303 I StGB entspricht. Damit § 303a StGB dem Bestimmtheitserfordernis des Art. 103 II GG genügt, sind daher nur solche Daten erfasst, welche einer eigentümerähnlichen Verfügungsbefugnis unterstehen, da sonst eine Veränderung eigener Daten strafbar wäre.[113] Es gibt verschiedene Ansätze diesem Merkmal zu begegnen. So wird vereinzelt für eine Zuordnung von Daten nach dem UrhG argumentiert.[114] Andere Stimmen wollen eine Zuordnung der Daten über sachenrechtliche Grundsätze bezüglich des Datenträgers annehmen.[115] Eine weitere Ansicht stellt auf den Skribenten des Skripturakts der Daten ab.[116] Diese Auffassungen sind im vorliegenden Fall nicht zielführend. Zwar löst derjenige, der Zugriff auf den privaten Schlüssel hat, eine Transaktion aus, jedoch werden die Transaktionsdaten selbst erst von Minern in der Blockchain gespeichert und somit

---

[104] *Heine/Schuster* in: Schönke/Schröder StGB (Fn. 21), § 267 Rn. 17; *Erb* in: MüKo-StGB (Fn. 12), § 267 Rn. 19; *Erb* in: MüKo-StGB (Fn. 12), § 269 Rn. 11; *Puppe/Schumann* in: NK-StGB (Fn. 68), § 267 Rn. 77.
[105] *Grzywotz/Köhler/Rückert*, StV 2016, S. 753 (755).
[106] *Kütük/Sorge*, MMR 2014, S. 643 (643).
[107] *Heger* in: Lackner/Kühl/Heger StGB (Fn. 35), § 269 Rn. 6; *Weidemann* in: BeckOK-StGB (Fn. 21), § 269 Rn. 6; *Welp*, Strafrechtliche Aspekte der digitalen Bildverarbeitung (II), CR 1992, S. 354 (360).
[108] *Ludes*, ZdiW 2022, S. 390 (391).
[109] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 24; *Böhm* (Fn. 10), S. 301.
[110] *Grzywotz* (Fn. 14), S. 198.
[111] BGH Urt. v. 27.7.2017 − 1 StR 412/16 = NStZ 2018, S. 401 (403); *Weidemann* in: BeckOK-StGB (Fn. 21), § 303a Rn. 15.
[112] *Grzywotz* (Fn. 14), S. 199; *Böhm* (Fn. 10), S. 307.
[113] OLG Nürnberg Urt. v. 23.1.2013 – 1 Ws 445/12 Rn. 11; *Weidemann* in: BeckOK-StGB (Fn. 21), § 303a Rn. 5; *Lenckner/Winkelbauer*, Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG (III), CR 1986, S. 824 (828).
[114] *Goeckenjan* in: LK-StGB, 13. Auflage 2023, § 303a Rn. 12; *Abdallah/Gercke/Reinert*, Zur Strafbarkeit von Kopierschutzmaßnahmen auf Audio-CDs gemäß § 303a StGB, HRRS 2003, S. 134 (138 ff.).
[115] *Kargl* in: NK-StGB (Fn. 68) § 303a Rn. 7; *Hecker* in: Schönke/Schröder StGB (Fn. 21), § 303a Rn. 3.
[116] BayObLG Urt. v. 24.6.1993 – 5 St RR 5/93 Rn. 24; OLG Nürnberg Urt. v. 23.1.2013 – 1 Ws 445/12 Rn. 14; *Welp*, Datenveränderung (§ 303a StGB) – Teil 1, Jur 1988, S. 443 (447).

verändert.[117] Eine Verfügungsbefugnis hinsichtlich der Transaktionsdaten ist ohnehin nicht konstruierbar.[118] Eine Strafbarkeit gemäß § 303a I StGB scheidet somit aus.

e) § 266 I StGB

Besonders praxisrelevant sind Fälle, in denen der private Schlüssel durch einen Dienstleister verwaltet wird und diese Position ausgenutzt wird, um sich zu bereichern. So wurde 2021 über die türkische Kryptobörse Thodex medial berichtet, auf der mehr als 400.000 Nutzer knapp 2 Milliarden US-Dollar investierten und plötzlich keinen Zugriff mehr auf ihre Kryptowährungsbestände hatten.[119] Der Geschäftsführer von Thodex hatte seine Position ausgenutzt und sich bereichert. Nach deutschem Recht kommt in solchen Fällen der Tatbestand der Untreue (§ 266 I StGB) in Betracht. Insbesondere das Merkmal der Vermögensbetreuungspflicht ist von Bedeutung. Dabei muss die Vermögensbetreuung den wesentlichen Inhalt des Vertrags darstellen und von einer gewissen Selbstständigkeit geprägt sein.[120]

Kryptobörsen ermöglichen ihren Kunden den Tausch von Token untereinander.[121] Bei einer strafrechtlichen Bewertung ist zu differenzieren: Während zentralisierte Kryptobörsen ähnlich wie Banken die Kontrolle über die Transaktionen und die privaten Schlüssel ihrer Nutzer haben, behalten bei dezentralisierten Börsen (DEX) die Kunden die Kontrolle über ihre Schlüssel und Token und sie könnten direkt mit anderen Nutzern handeln.[122]

Bezüglich der DEX ist eine Vermögensbetreuungspflicht abzulehnen, da die Börse zu keinem Zeitpunkt Zugriff auf das Vermögen ihrer Kunden oder den privaten Schlüssel hat. Bei zentralen Kryptobörsen ist das Ergebnis zunächst nicht eindeutig. Da sie ähnlich einer Bank agieren, kann die Rechtsprechung zur Vermögensbetreuungspflicht einer Bank gegenüber ihren Kunden herangezogen werden. So wurde eine Vermögensbetreuungspflicht im Falle einer einfachen Kontoverwaltung, etwa bei Spar- oder Girokontoverträgen, regelmäßig verneint.[123] Da Kryptobörsen und Wallet-Anbieter im Grunde nur die privaten Schlüssel und damit die Token verwalten, ist die Rechtsprechung zur einfachen Kontoverwaltung anzuwenden und eine Vermögensbetreuungspflicht auch bei zentralisierten Kryptobörsen abzulehnen.[124]

Eine andere Beurteilung ergibt sich im Falle einer qualifizierten Vermögensbetreuung, wenn etwa ein Vermögensverwalter die volle Kontrolle über den privaten Schlüssel ausübt und zudem über Transaktionen selbstständig entscheidet.

3. Bewertung der aktuellen Rechtslage

Zusammenfassend lässt sich sagen, dass das Beschaffen des privaten Schlüssels nur bedingt und vor allem wegen Datendelikten (§§ 202a ff. und §§ 303a ff. StGB) strafbar und die Transaktion der Token selbst nicht strafbar ist. Werden die Token von einer Kryptobörse verwaltet, besteht ein Schutz vor Zugriffen Dritter von außen, da aufgrund der eindeutigen Zuordnung der Token zu einem Kundenkonto eine Berechtigung besteht. Nutzen die Vertreter von Kryptobörsen jedoch ihre Position aus und bereichern sich an dem Vermögen ihrer Kunden, so ist dieses Vorgehen wiederum nicht strafbar.

Bisher wurden in der Rechtsprechung nur vereinzelt Urteile zur Strafbarkeit des „Kryptodiebstahls“ gefällt. Bei einem Urteil des AG Münchens wurde die Strafbarkeit des unberechtigten Transfers von Token angenommen, dieses Ergebnis jedoch kaum rechtlich begründet.[125] Im März 2024 verurteilte das LG Traunstein zwei Polizeibeamten als Täter, bzw. Teilnehmer einer Untreue, da diese im Zuge von Ermittlungen Hardware-Wallets entwendeten und sich später daran bereichern.[126] Wie der BGH die aufgeworfenen Fragen beantworten wird, bleibt abzuwarten. Fest steht, dass die aktuelle Rechtslage den Fall der nicht berechtigten Transaktion fremder Token nicht ausreichend abdeckt. Das verwirklichte Unrecht ist mit dem Fall eines Betrugs oder dem eines Diebstahls vergleichbar, da das Opfer hier ebenso Vermögenswerte verliert. So kommt zwar eine Strafbarkeit aufgrund von Datendelikten in Betracht, diese liegt jedoch mit einer Höchststrafe von 3 Jahren

---

[117] *Böhm* (Fn. 10), S. 303.
[118] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 24; *Ludes*, ZdiW 2022, S. 390 (393).
[119] *Stöckel*: Gründer einer Kryptobörse zu 11.196 Jahren Haft verurteilt, https://www.golem.de/news/thodex-gruender-einer-kryptoboerse-zu-11-196-jahren-haft-verurteilt-2309-177532.html [Stand: 8.2.2025].
[120] BVerfG Urt. v. 23.6.2010 – 2 BvR 2559/08 = NJW 2010, S. 3209 (3214); BGH Urt. v. 11.12.2014 – 3 StR 265/14 = NJW 2015, S. 1618 (1619); *Wittig* in: BeckOK-StGB (Fn. 21), § 266 Rn. 15; *Rengier* (Fn. 25), § 18 Rn. 18 f.
[121] *Fromberger/Haffke/Zimmermann*, BKR 2019, S. 377 (378).
[122] *Bonset*: Exchange und DEX: Was ist der Unterschied zwischen zentralen und dezentralen Kryptobörsen?, https://t3n.de/news/unterschied-zentrale-dezentrale-kryptoboerse-1362957/ [Stand: 8.2.2025]; *Hoch* in: Maume/Maute (Fn. 14), § 7 Rn. 23.
[123] OLG München Urt. v. 30.11.2009 – 5 St RR 357/09 = wistra 2010, S. 155 (157); OLG Düsseldorf Urt. v. 4.11.1994 – 1 Ws 807 - 809/94 = wistra 1995, S. 72 (73); *Kindhäuser/Hoven* in: NK-StGB (Fn. 68), § 266 Rn. 57.
[124] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 20.
[125] AG München Urt. 23.7.2020 – 1123 Ls 630 Js 1517/18 (unveröffentlicht).
[126] Traunsteiner Tagblatt: Untreue, Verwahrungsbruch und Geldwäsche, https://www.traunsteiner-tagblatt.de/region/landkreis-traunstein_artikel,-untreue-verwahrungsbruch-und-geldwaesche-_arid,860117.html [Stand: 8.2.2025].

Freiheitsstrafe deutlich unter der Strafandrohung der §§ 242 I, 263 I StGB von bis zu fünf Jahren. Den Token wohnt zudem meist ein hoher Vermögenswert inne. So ist beispielsweise ein Bitcoin aktuell um die 93.000 € wert.[127] Es ist daher im Schrifttum zu Recht von einer ungewollten Strafbarkeitslücke die Rede.[128]

D. Überlegungen de lege ferenda

Diese Schutzlücke wurde schon mehrfach erkannt und im Zuge dessen ein neuer Straftatbestand im StGB gefordert.[129] Bisher wurden im Schrifttum zwei Gesetzesvorschläge vorgebracht.

I. Bisherige Gesetzesentwürfe

So formulierte *Rückert* 2020 einen Entwurf des möglichen Tatbestands § 242a StGB.[130] Strafbar soll demnach derjenige sein, der sich als Nichtberechtigter Daten verschafft, die zum unmittelbaren Zugriff auf Vermögenswerte geeignet und bestimmt sind, um sich oder einem Dritten diese zu verschaffen.

Zuletzt brachte *Böhm* einen Gesetzesentwurf für einen neuen § 248d StGB ein.[131] Hierbei wird nach Abs. 1 bestraft, wer fremde Kryptowerte einem anderen in der Absicht entzieht, diese sich oder einem Dritten rechtswidrig zuzueignen. Zusätzlich wird in Abs. 4 eine Strafschärfung genannt, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt oder Kryptowerte von mehr als 50.000 Euro entzieht. Die Qualifikation des Abs. 5 bestraft einen Täter, der die Tat als Mitglied einer Bande und gewerbsmäßig begeht.

II. Vergleich

1. Verortung im Gesetz

Bei einem Vergleich der beiden Gesetzesentwürfe fällt zunächst auf, dass sie an unterschiedlicher Stelle ins Gesetz angeordnet werden. Während *Rückert* den Tatbestand unmittelbar nach dem Diebstahl § 242 StGB anordnet, reiht *Böhm* ihn unter denselben Abschnitt des StGB, jedoch an den Schluss hinter § 248c StGB, dem Entziehen elektrischer Energie. Da die Inhaberschaft von Kryptotoken eine gewisse Ähnlichkeit zum Sacheigentum darstellt,[132] ist einer grundsätzlichen Verortung im 19. Abschnitt des StGB zuzustimmen. Eine Verortung der Norm bei den Datendelikten §§ 202a ff. StGB oder §§ 303a ff. StGB scheint zunächst ebenso plausibel, jedoch ist das hauptsächlich zu sanktionierende Unrecht des „Kryptodiebstahls“ keine Datenmanipulation oder das Verletzen des persönlichen Lebens- und Geheimbereichs, sondern der Entzug eines Vermögenswertes.

2. Tathandlungen

Ebenso unterscheiden sich die Tathandlungen der beiden Gesetzesentwürfe. Während *Rückert* an das Verschaffen der Daten, um Zugriff auf Vermögenswerte zu haben, anknüpft, stellt *Böhm* direkt auf den Entzug von fremden Kryptowerten ab. Problematisch erscheint das Merkmal der „Fremdheit“ der Kryptowerte. Wie *Böhm* selbst feststellt, gibt es noch keine zivilrechtliche Zuordnung von Kryptowährungseinheiten.[133] Aus diesem Grund ist eine zivilrechtliche Einordnung zur Auslegung des Straftatbestandes unumgänglich.

Rückert nutzt den Begriff der „Daten“. Im Strafrecht existiert kein einheitlicher Datenbegriff. Ein Verweis auf die Legaldefinition des § 202 II StGB bleibt aus, daher muss ein eigener Datenbegriff zugrunde gelegt werden. Aufgrund des Sinn und Zwecks der Strafnorm müssten alle möglichen Darstellungen des privaten Schlüssels gemeint sein, welche sowohl digital als auch analog vorliegen können.[134] Täter müsste ein „Nichtberechtigter“ sein. Die Berechtigung bezieht sich hierbei nicht auf die Kryptwährungseinheiten selbst, sondern auf den privaten Schlüssel. Während eine Inhaberschaft an Token kaum zu konstruieren ist, ist dies bei einem privaten Schlüssel schon eher der Fall. So könnte bei einem auf einer Hardware gespeicherten Schlüssel der Eigentümer dieser berechtigt sein. Im Falle einer Online-Wallet wäre der Wallet-Inhaber Berechtigter des Zugriffs auf den privaten Schlüssel.

3. Strafschärfung und Qualifikation

Während *Böhms* Entwurf in Abs. 4 zwei Strafschärfungstatbestände und in Abs. 5 eine Qualifikation vorsieht, fehlen solche Sanktionierungen in *Rückerts* Gesetzesvorschlag.

III. Stellungnahme

Da eine Inhaberschaft an Kryptowerten nicht zu konstruieren ist, überzeugt *Rückerts* vorgeschlagene Tathandlung, welche bereits an die erste Tatphase, dem Beschaffen der Daten, anknüpft und

[127] Gold.de, https://www.gold.de/kurse/bitcoinpreis/ [Stand: 8.2.2025].
[128] *Böhm* (Fn. 10), S. 344; vgl. *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 25.
[129] *Ludes*, ZdiW 2022, S. 390 (393); *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 25; *Böhm* (Fn. 10), S. 345.
[130] *Rückert* in: Maume/Maute (Fn. 14), § 22 Rn. 25.
[131] *Böhm* (Fn. 10), S. 351.
[132] *Böhm* (Fn. 10), S. 352.
[133] *Böhm* (Fn. 10), S. 354.
[134] *Böhm* (Fn. 10), S. 348.

somit auch die Strafbarkeit dieser Phase mit abdeckt. Ebenso ist der Anwendungsbereich weiter, wenn allgemein auf „Vermögenswerte“ anstatt auf „Kryptowerte“ abgestellt wird. So sind weitere Vermögenswerte umfasst, welche in Zukunft entwickelt werden. Das aktuelle Aufkommen von sog. „AI-Coins“, welche auf eine Kombination aus Blockchain und Künstlicher Intelligenz setzen,[135] zeigt die technologischen Möglichkeiten in diesem Bereich. Auch wird die fehlende Untreuestrafbarkeit des Geschäftsführers einer Kryptobörse mit umfasst, da dieser zwingend die Schlüssel seiner Kunden, also Daten i. S. d. Tatbestands, benötigt, um sich zu bereichern.

Zusätzliche Absätze, welche besonders schwere Fälle und Qualifikationen sanktionieren, sind vor dem Hintergrund sinnvoll, dass ein Entziehen von Token meist technisch komplex ist und daher mehrere Täter die Begehung erleichtern. Das Unrecht steigt, wenn die Täuschung oder das sonstige Erlangen des privaten Schlüssels professionell von mehreren Tätern vorgenommen wird oder einen besonders hohen Schaden beim Opfer hervorruft. Aus demselben Grund wurde § 263 StGB um Strafzumessungsregeln in Abs. 3 ergänzt.[136] Da das geschützte Rechtsgut des Betrugs das Vermögen ist[137] und Kryptotoken ein Vermögenswert innewohnt, ist eine Orientierung an diesen Regelbeispielen sinnvoll.

Das Strafmaß des Grundtatbestands sollte im Vergleich zu denen des § 242 StGB und § 263 StGB, wie in beiden Entwürfen vorgeschlagen, bei einer Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe verbleiben.

Die Anordnung der zu konstruierenden Strafnorm nach dem § 248c StGB erscheint sinnvoller. So wurde der § 248c StGB durch das dritte Strafrechtsänderungsgesetz von 1953 um die Strafbarkeit des Entziehens elektrischer Energie eingeführt, welche mangels Körperlichkeit nicht unter den Tatbestand des § 242 StGB zu subsumieren war.[138] Da Kryptowährungen ebenso wenig unter den Sachbegriff fallen, scheint eine Anordnung nach § 248c StGB naheliegend. Aufgrund dieser Erwägungen könnte ein Straftatbestand wie folgt aussehen:

§ 248d StGB-Entwurf: Unberechtigtes Verschaffen vermögensrelevanter Daten

(1) Wer sich als Nichtberechtigter Daten verschafft, die zum unmittelbaren Zugriff auf Vermögenswerte geeignet und bestimmt sind, um sich oder einem Dritten diese Vermögenswerte zu verschaffen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Die §§ 247, 248a gelten entsprechend.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Tatbegehung verbunden hat oder

2. einen Vermögensverlust großen Ausmaßes herbeiführt.

In den Fällen des Absatzes 4 Satz 2 Nr. 1 gilt § 243 II entsprechend.

(5) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat als Mitglied einer Bande, die sich zur fortgesetzten Begehung verbunden hat, gewerbsmäßig begeht.

E. Fazit

Die Besonderheit des Kryptowährungssystems stellt sich in der Subsumtion de lege lata problematisch dar. Dies liegt vor allem daran, dass der Gesetzgeber neue Technologien und die Entwicklungen in der Technik bei Inkrafttreten von Rechtsnormen noch nicht vor Augen hatte. Im Strafrecht tritt der Grundsatz des Analogieverbots und der Wortlautgrenze hinzu, welcher eine Einordnung von Kryptowährungen in das geltende Strafrecht erschwert. Wie aufgezeigt, sind einzelne Tathandlungen in bestimmten Fallkonstellationen durchaus strafbar. Eine generelle Strafbarkeit des „Diebstahls“ von Kryptowährungen besteht jedoch nicht. Dies ist vor dem Hintergrund problematisch, dass die Nutzung von Kryptowährungen heutzutage immer weiter zunimmt. So zählt allein in Deutschland jeder Zwanzigste Kryptowährungen zu seinem Vermögen.[139] Aus Sicht potenzieller Täter wird eine Tatbegehung also immer lohnender und die Schwelle zu Vornahme einer kriminellen Handlung immer geringer. Bezüglich des unberechtigten Entwendens von Token ist es daher unerlässlich, dass der Gesetzgeber tätig wird. Bis dahin gilt weiterhin der Grundsatz „not your keys, not your coins“.

---

[135] Clickout Media: AI Coins – Die Zukunft der Kryptowährungen?, https://www.wallstreet-online.de/nachricht/17838329-ai-coins-zukunft-kryptowaehrungen [Stand: 8.2.2025].
[136] Sechstes Gesetz zur Reform des Strafrechts (6. StrRG) vom 26. Januar 1998, BGBl. I S. 164 (178).
[137] BGH Urt. v. 18.7.1961 - 1 StR 606/60 = NJW 1961, S. 1876 (1876); *Beukelmann* in: BeckOK-StGB (Fn. 21), § 263 Rn. 1; *Perron* in: Schönke/Schröder StGB (Fn. 21), § 263 Rn. 2.
[138] RG Urt. v. 20.10.1896 – 2609/96. S. 111 (111); RG Urt. v. 1.5.1899 – 739/99, S. 165 (166).
[139] *Brummer*, Jeder zwanzigste Deutsche setzt auf Kryptowährungen, https://extraetf.com/de/news/etf-news/jeder-zwanzigste-deutsche-setzt-auf-kryptowaehrungen [Stand: 8.2.2025].