



## [401] Die Erfassung von Kryptowährungen im Schweizer Vermögensstrafrecht NOÉMIE SCHÄR<sup>\*</sup>/MONIKA SIMMLER<sup>\*\*</sup>

Schlagwörter: Kryptowährungen, virtuelle Währungen, Vermögensstrafrecht, Vermögensdelikte, Datendelikte

### A. Einleitung

Der Handel mit Kryptowährungen wie Bitcoin, Ripple oder Ethereum hat seit geraumer Zeit viel Aufmerksamkeit erhalten und insbesondere die Finanzbranche in Unruhe versetzt. Mit steigender Bedeutung dieser «virtuellen Währungen» wachsen allerdings gleichsam die damit verbundenen Risiken. Kryptowährungen bieten sich aufgrund ihrer spezifischen Charakteristiken für verschiedene kriminelle Handlungen besonders an. Die Popularität der virtuellen Zahlungsmittel im *Darknet*,<sup>1</sup> aber auch zunehmende Schlagzeilen über Fälle von «Diebstählen», Hackerangriffen und anderen Vermögensdelikten haben die Schattenseiten von Kryptowährungen längst offenbart.

Das in der Medienmitteilung der Kantonspolizei Zürich Anfang 2018 Geschilderte dürfte keine Ausnahme darstellen. Ihr zufolge haben sich mit dem «Boom» von Kryptowährungen Betrugsfälle und Diebstähle, die für die Opfer üblicherweise mit einem Totalverlust einhergehen, gehäuft.<sup>2</sup> Als Beispiel wird angeführt, in zwei Fällen seien IOTA – eine Kryptowährung –, mit einem Gegenwert von rund einer Million Franken «gestohlen» worden. Im Medienbericht wird dabei in allgemeiner Weise von Betrug und Diebstahl gesprochen. Ungeklärt ist jedoch, wie sich die vermögensstrafrechtliche Qualifikation und [402] Erfassung solcher «Betrugs- und Diebstahlshandlungen» in Bezug auf Kryptowährungen gestaltet. Angesichts der zunehmenden strafrechtlichen Praxisrelevanz dieser neuen Art von «Vermögenswerten» ist es das Ziel dieser Abhandlung, einen Beitrag zur Klärung ihres vermögensstrafrechtlichen Schutzes zu liefern und allfällige Lücken im Rechtsschutz herauszuarbeiten. Dabei steht die Frage im Zentrum, ob und inwiefern der Einzelne beim Gebrauch und Besitz von Kryptowährungen durch die **Art. 137 ff. StGB** ausreichenden Schutz geniesst, wenn ein Dritter diese gegen seinen Willen entwendet.

Dieser Forschungsfrage entsprechend umreisst dieser Beitrag zunächst die zentralen technischen Eigenheiten von Kryptowährungen (B.) und die weiteren Grundlagen, welche für die darauf aufbauende rechtliche Analyse wesentlich sind (C.). So wird zunächst nach der allgemeinen Qualifikation von virtuellen Währungen gefragt. Nur wenn klar ist, ob es sich dabei um Vermögenswerte, Daten oder Sachen handelt, kann der vermögensstrafrechtliche Schutz beurteilt werden. Ebenso wird in diesem Abschnitt eingeführt, welche Fallkonstellationen von hoher Praxisrelevanz sind und einer eingehenden Prüfung bedürfen. Im zweiten Teil nimmt sich dieser Beitrag sodann den als relevant eruierten Strafbestimmungen an, um diese auf ihre Anwendbarkeit

hin zu überprüfen. Dabei wird zunächst auf die Tatbestände der «traditionellen» Vermögensdelikte eingegangen (D.), bevor vermögensbezogene Computerdelikte genauer betrachtet werden (E.). Dabei werden Schwachstellen in Bezug auf den Schutz virtueller Vermögenswerte identifiziert und mögliche Lösungsansätze diskutiert. Im Rahmen einer Synthese wird im Anschluss die Strafbarkeit der häufigsten Fallvarianten zusammengefasst (F.). Die Untersuchung bietet entsprechend einen umfassenden Überblick über die Strafbarkeit von «Diebstahls- und Betrugshandlungen» im Zusammenhang mit Kryptowährungen.

## B. Technische Grundlagen

### I. Was sind Kryptowährungen?

Als virtuelle Währung wird ein digitaler, wertverkörpernder Code verstanden, welcher an Börsen gehandelt und zur Bezahlung realer Güter und Dienstleistungen verwendet werden kann.<sup>3</sup> Virtuelle Währungen werden als Kryptowährungen bezeichnet,<sup>4</sup> weil der für die Informationsverschlüsselung zuständige Algorithmus auf Prinzipien der Kryptographie beruht.<sup>5</sup> Nachfolgend werden diese zwei Begriffe synonym verwendet.

[403] Als zentrales Charakteristikum von Kryptowährungen gilt, dass sie dezentral organisiert sind.<sup>6</sup> Es existiert keine zentrale Instanz, welche die Währung emittiert, das System betreibt oder die Echtheit bzw. den tatsächlichen Wert gehandelter Währungseinheiten garantiert.<sup>7</sup> Vielmehr funktionieren virtuelle Währungen über ein *Peer-to-Peer*-Netzwerk.<sup>8</sup> Als *Peer-to-Peer* wird dieses bezeichnet, da die gleichgestellten Teilnehmer direkt miteinander kommunizieren, ohne dass sie auf einen zentralen Verwalter oder einen Finanzintermediär zurückgreifen müssen.<sup>9</sup> Virtuelle Währungen existieren des Weiteren lediglich in digitaler Form.<sup>10</sup> Es wird kein «materialisiertes Gegenstück» ausgegeben.<sup>11</sup> Vielmehr treten an deren Stelle kryptographische Schlüssel, welche den Zugang zur Werteinheit und damit den Tauschwert verkörpern.<sup>12</sup>

Kryptowährungen ist gemein, dass sie auf der *Blockchain*-Technologie basieren. Eine *Blockchain* stellt eine Art «digitales Grundbuch» dar, in welchem alle Transaktionen öffentlich vermerkt und theoretisch endlos zurückverfolgt werden können. Bei einem «Block» handelt es sich um eine verschlüsselte Liste von Transaktionen, die im Grundbuch – dem sog. *Distributed Public Ledger* – registriert werden.<sup>13</sup> Bei jeder Transaktion werden also Daten in einem Block gespeichert. Der sequentielle Aufbau der Blöcke ergibt eine Kette, weshalb von einer *Blockchain* gesprochen wird.<sup>14</sup>

### II. Private Key und Pseudononymität

Kryptowährungen und die ihnen zugrundeliegenden Netzwerke zeichnen sich durch Pseudoanonymität aus,<sup>15</sup> was virtuelle Währungen für verschiedene Kriminalitätsformen besonders attraktiv macht. Auch wenn die *Blockchain* öffentlich ist, erlauben sowohl deren Funktionsweise als auch die Abwesenheit einer [404] Kontrollinstanz eine erhöhte Anonymität.<sup>16</sup> Schliesslich finden Transaktionen nicht zwischen Individuen direkt, sondern zwischen «Adressen» statt.<sup>17</sup> Bei den meisten Kryptowährungen wie *Bitcoin* ersetzen kryptographische Schlüsselpaare, welche aus einem öffentlichen und einem privaten Schlüssel bestehen, die Funktion herkömmlicher Bankkonten.<sup>18</sup> Der öffentliche Schlüssel – der *Public Key* – ist mit einer Kontonummer vergleichbar, welche öffentlich zugänglich ist.<sup>19</sup> Jeder Teilnehmer kann mehrere derartige Adressen besitzen.<sup>20</sup> Dieser *Public Key* wird zu einer Art «Pseudonym», da er zwar einsehbar ist, jedoch – ohne besondere Vorkehrungen – nicht mit der Identität des Besitzers verknüpft werden kann. Das erschwert die Identifizierung von Inhabern und Ermittlungen deutlich,<sup>21</sup> was kriminellen Aktivitäten Vorschub leistet.

Der private Schlüssel – der *Private Key* – ist mit einem Passwort oder einer Unterschrift vergleichbar und dient der Signierung von Transaktionen.<sup>23</sup> Dabei handelt es sich um einen nur dem jeweiligen Nutzer bekannten Code, der aus Zahlen und Buchstaben besteht. Er dient als Nachweis, dass die mit der öffentlichen Adresse verknüpften virtuellen Währungen einer bestimmten Person gehören und sie diesbezüglich verfügungsberechtigt ist.<sup>24</sup> Ist der *Private Key* anderen Personen als dem rechtmässigen Eigentümer bekannt, kann daher jeder mit Wissen um den Schlüssel Währungseinheiten zum Nachteil des Berechtigten verschieben.<sup>25</sup> Eine Möglichkeit des Rückgängigmachens besteht nicht. Neben der Pseudoanonymität ist es gerade diese Eigenheit, welche Kryptowährungen für Vermögensdelikte interessant und für Strafverfolgungsbehörden zu einer Herausforderung macht.

### [405] III. Wallets und Aufbewahrungsmöglichkeiten

Kryptowährungen werden in sog. *Wallets*, zu Deutsch Geldbörsen, aufbewahrt, die sowohl der Aufbewahrung als auch dem Empfangen und Versenden von Währungseinheiten dienen.<sup>26</sup> In Bezug auf die verschiedenen Speichermethoden kann im Allgemeinen zwischen *Web*-, *Hardware*- und *Paper-Wallets* unterschieden werden.

*Web-Wallets* speichern sowohl den öffentlichen als auch den privaten Schlüssel auf dem Server des Anbieters.<sup>27</sup> Zugriff erlangt man über einen Computer oder eine Applikation auf dem Smartphone.<sup>28</sup> Die Anmeldung erfolgt dabei mittels eines Benutzernamens und Passworts oder durch das Abspeichern einer Internetadresse.<sup>29</sup> Bei *Hardware-Wallets* wird der private Schlüssel auf einem kleinen Gerät und nicht auf einem Server gespeichert.<sup>30</sup> Dieses Gerät wird dann zur Signierung von Überweisungen benötigt und ist durch ein Passwort selbst vor unbefugten Zugriffen geschützt.<sup>31</sup> Da lediglich die *Wallet*-Funktionen über eine Website abgewickelt werden, sind *Hardware-Wallets* grundsätzlich eine sichere Methode, um Kryptowährungen aufzubewahren.<sup>32</sup> Bei *Paper-Wallets* handelt es sich um Ausdrucke des Schlüssels auf Papier. Deren Vorteil besteht darin, dass sie vollständig offline sind und Hacking-Angriffe deshalb verunmöglicht werden.<sup>33</sup> Entsprechend ist dies einer der sichersten – wenn auch umständlichsten – Wege, um Kryptowährungen zu verwahren.<sup>34</sup>

## C. Vermögensstrafrechtlicher Schutz de lege lata

### I. Geschütztes Rechtsgut und Vermögensbegriff

Die Vermögensstraftatbestände bilden einen «Eckpfeiler des strafrechtlichen Schutzes der gesellschaftlichen Eigentums- und Wirtschaftsordnung».<sup>35</sup> Fraglich ist, inwieweit neuartige «Vermögensformen» wie Kryptowährungen durch diese traditionellen Normen geschützt sind. In erster Linie ist zu eruieren, ob [406] virtuelle Währungen unter die bestehenden Begrifflichkeiten subsumiert werden können und ausreichenden Schutz geniessen, waren dem Gesetzgeber zu Zeiten der Schaffung dieser Tatbestände doch keine digitalen Währungen bekannt. Nachfolgend bedürfen deshalb sowohl die begriffliche Subsumtion als auch die strafrechtliche Erfassung der mit Kryptowährungen einhergehenden Deliktssituationen einer eingehenden Prüfung.

Trotz der Schwierigkeiten, ein einheitliches Rechtsgut zu bestimmen,<sup>36</sup> sieht der überwiegende Teil der Lehre das *Vermögen* als geschütztes Rechtsgut der Art. 137 ff. StGB an.<sup>37</sup> Damit stellt sich unweigerlich die Frage, was alles unter den Vermögensbegriff fällt. Die h. L.<sup>38</sup> und das Bundesgericht<sup>39</sup> folgen mittlerweile einer juristisch-wirtschaftlichen Vermögenskonzeption. Danach umfasst das Vermögen «die Summe der rechtlich geschützten oder der rechtlich nicht missbilligten wirtschaftlichen Werte».<sup>40</sup> Auf den ersten Blick scheint es angesichts der «vermögenswerten»

Funktion von Kryptowährungen plausibel, dass sie unter diesen Vermögensbegriff fallen und das von **Art. 137 ff. StGB** geschützte Rechtsgut im Zusammenhang mit virtuellen Währungen tangiert sein kann. Allerdings ist eine detaillierte Auslegung der Begrifflichkeiten vorzunehmen, um beurteilen zu können, ob und inwiefern Kryptowährungen tatsächlich unter die Tatbestände dieses Titels subsumiert werden können. Dafür ist es weitergehend Voraussetzung, dass sie als «Sachen», «Daten» oder «Vermögenswerte» erfasst werden können und damit taugliche Tatobjekte i. S. d. Bestimmungen darstellen.

## **[407] II. Eignung von Kryptowährungen als Sachen, Daten oder Vermögenswerte**

### **1. Qualifikation von Kryptowährungen als Sachen?**

Als Sache gilt ein körperlicher Gegenstand i. S. v. **Art. 713 ZGB**.<sup>41</sup> Ebenfalls unter den Sachbegriff fallen Rechte und Forderungen, sofern sie in einem Wertpapier verkörpert sind.<sup>42</sup> Bei einem derartigen Wertpapier genießt allerdings nicht das darin verbriefte Recht, sondern die Verfügungsmacht über eine körperliche Sache Schutz.<sup>43</sup> Nicht als Sachen gelten unkörperliche Daten, fraglos aber Datenträger, d. h. körperliche Gegenstände, auf denen Daten gespeichert sind.<sup>44</sup>

Kryptowährungen existieren als Eintrag in der *Blockchain*, welcher in elektronischer Form gespeichert ist.<sup>45</sup> Damit stellen der *Private Key* und die damit einhergehende Verfügungsgewalt grundsätzlich ein immaterielles Gut dar, welches zunächst ohne physische Verkörperung bleibt.<sup>46</sup> Eine Qualifikation als Sache ist daher vorerst ausgeschlossen. Neben der Möglichkeit, Kryptowährungen virtuell zu übertragen, ist allerdings, wie bereits ausgeführt, ein Hinterlegen des Zugangsschlüssels auf einem verkörperten Datenträger oder auf Papier gebräuchlich. Selbst wenn solche materiellen Surrogate als körperliche Gegenstände qualifiziert werden können, lässt sich diese rechtliche Einordnung nicht auf darauf gespeicherte virtuelle Währungseinheiten ausdehnen.<sup>47</sup> Dafür spricht im Besonderen, dass bei Verlust des Datenträgers nicht sein Wert, sondern die Menge vorhandener Einheiten das zentrale Bemessungskriterium ist.<sup>48</sup> Dies lässt den Bezug zur Sacheigenschaft missen.

**[408]** Wie erwähnt, können auch Forderungen als Sachen gelten. Dafür muss die Forderung in einem Wertpapier verkörpert sein. Bei einem Wertpapier handelt es sich in Anlehnung an **Art. 965 OR** um eine Urkunde, die mit einem Recht derart verknüpft ist, dass es ohne die Urkunde weder geltend gemacht noch übertragen werden kann. Vergleichbar könnte auch bei Kryptowährungen angenommen werden, es handle sich beim *Private Key* um eine Forderung, die in der Speicherung des Schlüssels auf einem Datenträger ihre Verkörperung erfährt. Allerdings scheitert eine Einordnung als Wertpapier: Selbst wenn der private Schlüssel durch die Speicherung eine quasi «Verbriefung» erfährt, kann über die Werteinheiten nicht nur ausschliesslich mit diesem Datenträger verfügt werden.<sup>49</sup> Vielmehr ist es möglich, den Schlüssel zu vervielfältigen und es reicht die Kenntnis darüber aus, um das Schicksal der damit verknüpften Werteinheiten zu bestimmen. Eine derartige Analogie gelingt deshalb nicht. Der private Schlüssel verbrieft kein Recht.<sup>50</sup> Er dient lediglich dem Zugang zur Verfügungsmacht, wobei diese aufgrund der Reproduzierbarkeit des Schlüssels nicht abschliessend garantiert ist. Zusammengefasst ist vom Versuch, Kryptowährungen in irgendeiner Weise unter den Sachbegriff zu subsumieren, Abstand zu nehmen. Das zentrale Kriterium der Körperlichkeit ist nicht gegeben.<sup>51</sup>

### **2. Qualifikation von Kryptowährungen als Daten?**

Gewisse Delikte des Vermögensstrafrechts nennen ein weiteres Tatobjekt, nämlich Daten. Gemäss der Botschaft fallen darunter «alle Informationen über einen Sachverhalt in Form von Buchstaben,

Zahlen, Zeichen, Zeichnungen u. a., die zur weiteren Verwendung ermittelt, verarbeitet oder aufbewahrt werden».<sup>52</sup> Ob die Informationen einen wirtschaftlichen Wert oder einen Geheimnischarakter aufweisen, ist für ihre Einordnung als Daten irrelevant.<sup>53</sup> Dieses Begriffsverständnis ist relativ weit, wobei nur diejenigen Daten, die von einer Datenverarbeitungsanlage «verarbeitet, gespeichert und weitergegeben werden», strafrechtlich geschützt sind.<sup>54</sup> Kryptowährungen existieren als digitaler Code – einerseits als *Private Key*, andererseits als Eintrag in der *Blockchain*. [409] Sie lassen sich folglich unter den Datenbegriff subsumieren. Diese Qualifikation wird auch in der Literatur vorgenommen.<sup>55</sup>

### 3. Qualifikation von Kryptowährungen als Vermögenswerte?

Der Begriff der Vermögenswerte findet sich erst seit 1995 im StGB.<sup>56</sup> Als Vermögenswerte gelten im Allgemeinen spezifische Vermögensbestandteile<sup>57</sup> bzw. sämtliche «wirtschaftlichen Vorteile, die sich rechnerisch ermitteln lassen».<sup>58</sup> So stellen z. B. zweifelsfrei Forderungen Vermögenswerte dar.<sup>59</sup> Ob es sich bei Kryptowährungen um einen spezifischen Vermögensbestandteil handelt, ist hingegen nicht auf Anhieb zu beantworten. Entsprechend ist zu klären, ob sie unter den Forderungsbegriff oder anderweitig unter den Begriff der Vermögenswerte subsumiert werden können.

Eine Forderung stellt «ein Recht der Gläubigerin auf Leistung durch den Schuldner» dar.<sup>60</sup> Ist eine Qualifikation des verfügungsberechtigten Inhabers des *Private Key* als Forderungsinhaber grundsätzlich möglich, stellt sich die Frage nach dem Forderungsgegner. Hier gilt es, die dezentrale Struktur der zugrundeliegenden *Blockchain*-Technologie in Erinnerung zu rufen: Es gibt keine zentrale Instanz, die die virtuellen Währungseinheiten emittiert.<sup>61</sup> Folglich basiert deren Wert nicht auf einer Zweiparteien-Beziehung: Der eigentliche Schuldner fehlt.<sup>62</sup> Es ist jedoch zu bedenken, dass oftmals Drittpersonen – wie Betreiber von Handelsbörsen oder *Wallet*-Anbieter – involviert sind. In diesem Fall hätte der Berechtigte evtl. Forderungsrechte gegenüber derartigen Dienstleistern. In diesen Konstellationen wäre die vertragliche Abrede genauer zu untersuchen.<sup>63</sup> Dennoch bestünde dadurch keine Forderung gegenüber der *Blockchain* selbst. Kryptowährungen können demnach nicht unter den herkömmlichen Forderungsbegriff subsumiert werden.<sup>64</sup> Sie sind allerdings trotz mangelnder Forderungseigenschaft als Vermögenswerte zu klassifizieren, da es [410] sich bei ihnen um wirtschaftliche Werte i. S. d. juristisch-wirtschaftlichen Vermögensbegriffs handelt.

### 4. Kryptowährungen als Vermögenswert sui generis?

Bei Kryptowährungen handelt es sich dem Vorangegangenen folgend also um Daten mit Vermögenswert *sui generis*,<sup>65</sup> d. h. weder um herkömmliche elektronische Daten, denen bereits eigens ein Wert zukommt, noch um einen herkömmlichen Vermögenswert. Vielmehr sind Kryptowährungen Daten, denen aufgrund ihrer Schlüsselfunktion in Bezug auf die *Blockchain* ein Vermögenswert inhärent ist.<sup>66</sup> Diese Daten erhalten ihren Wert nicht durch Speicherung. Sie berechnen den Inhaber vielmehr, eine Transaktion zu tätigen.<sup>67</sup> Der Vermögenswert hängt entsprechend von der Verfügungsgewalt über die Daten ab, d. h. der Zugang zu diesem ist durch den (ausschliesslichen) Besitz des privaten Schlüssels und der Kenntnis über die relevanten Daten garantiert.<sup>68</sup>

Wie bereits festgestellt, fallen Kryptowährungen mangels Körperlichkeit nicht unter den Sachbegriff. Als Information handelt es sich bei ihnen um Daten, denen ein Vermögenswert zukommt.<sup>69</sup> Dieser Vermögenswert basiert mangels eines klar definierten Schuldners nicht auf einer Forderung. Vielmehr handelt es sich dabei um einen Vermögenswert eigener Art.<sup>70</sup> Entsprechend wird

nachfolgend davon ausgegangen, dass es sich bei Kryptowährungen sowohl um Daten als auch um Vermögenswerte i. S. d. vermögensstrafrechtlichen Terminologie handelt.

### [411] III. Überblick über Fallkonstellationen und zu untersuchende Delikte

Gegenstand der vorliegenden Abhandlung bilden «Entwendungen» von Kryptowährungen i. w. S. Entsprechend beschränkt sich die Untersuchung auf diejenigen Delikte, die sich bei derartigen «Betrugs- und Diebstahlshandlungen» als relevant erweisen. Dabei stehen nachfolgende vier Konstellationen einer Verschiebung des Vermögenswertes zum Nachteil des Berechtigten im Zentrum:

- «Diebstahl» von *Private Keys* (Fallvariante I): Ein Dritter erlangt den *Private Key* des eigentlich Berechtigten durch die Entwendung eines Datenträgers (z. B. *Hardware-* oder *Paper-Wallet*) und verfügt über die Kryptowährungen.
- «Betrügerische Entwendung» von *Private Keys* (Fallvariante II): Ein Dritter erlangt den *Private Key* des eigentlich Berechtigten durch eine Täuschung und verfügt über die Kryptowährungen.
- «Veruntreuung» anvertrauter *Private Keys* (Fallvariante III): Ein Dienstleistungsanbieter (z. B. *Wallet-Betreiber*) verfügt mittels des bei ihm hinterlegten *Private Key* unberechtigtweise über Kryptowährungen.
- «Hacking» von *Private Keys* (Fallvariante IV): Ein Dritter beschafft sich unbefugt Zugang zu einer Datenverarbeitungsanlage oder *Web-Wallet* und verfügt über damit erlangte Kryptowährungen.

Nachfolgend wird geprüft, inwiefern sich entsprechende Handlungen unter bestehende Straftatbestände subsumieren lassen und ob der Einzelne beim Gebrauch von Kryptowährungen ausreichend Schutz geniesst, wenn ein Dritter diese gegen seinen Willen entwendet.

## D. Kryptowährungen und traditionelle Vermögensdelikte

### I. Diebstahl

Tatobjekt des Diebstahls ist eine «fremde bewegliche Sache». <sup>71</sup> Da Kryptowährungen keine Sachen darstellen, <sup>72</sup> ist eine Anwendbarkeit dieses Tatbestands grundsätzlich ausgeschlossen. Anders muss betreffend das Schicksal des Datenträgers entschieden werden: Dieser ist ohne Weiteres taugliches Tatobjekt. Doch selbst wenn dieser entwendet wird, stellt der Gesetzgeber nicht die Verfügungsgewalt über die Daten, sondern ausschliesslich diejenige über die körperliche Sache als Diebstahl unter Strafe. Bei der Wegnahme eines Datenträgers ist folglich i. d. R. Diebstahl anzunehmen; die Strafbarkeit bezieht sich allerdings nur auf den Datenträger, nicht aber auf die darauf gespeicherten Daten. <sup>73</sup> Ein [412] eigentlicher «Diebstahl» von Kryptowährungen ist nicht möglich. Sie selbst erfahren durch Art. 139 StGB keinen Schutz.

### II. Betrug

#### 1. Kryptowährungen als Zielobjekt von Täuschungshandlungen

Beim Betrug wird kein spezifisches Tatobjekt, dafür aber explizit ein Vermögensschaden vorausgesetzt. <sup>74</sup> Erfasst wird die spezifische Beeinträchtigung des Vermögens mittels Täuschung. <sup>75</sup> Kryptowährungen lassen sich, wie bereits erläutert, unter den Vermögensbegriff subsumieren. <sup>76</sup> In Bezug auf die Täuschungshandlung, der vorausgesetzten Arglist und des täuschungsbedingten Irrtums ergeben sich keine Besonderheiten. Es spricht deshalb vorerst nichts dagegen, Art. 146

**StGB** auf virtuelle Währungen anzuwenden. Der Tatbestand verlangt ferner, dass der Getäuschte eine irrtumsbedingte Vermögensdisposition vornimmt, die sich vermögensmindernd auswirkt.<sup>77</sup> Als Erfolg ist entsprechend ein Vermögensschaden verlangt, der unmittelbar aus der Disposition resultiert.<sup>78</sup>

Kryptowährungen können auf verschiedene Arten Gegenstand von Betrugshandlungen sein. Einerseits ist denkbar, dass jemand durch eine arglistige Täuschung dazu verleitet wird, Kryptowährungen direkt zu transferieren. Durch den damit einhergehenden endgültigen Verlust des Vermögenswertes und den direkten Zusammenhang von Täuschung und schädigender Vermögensdisposition wird eine Subsumtion unter **Art. 146 Ziff. 1 StGB** in diesen Fällen regelmässig gelingen. Komplexer gestaltet es sich, wenn durch die Täuschung nicht bereits die Transaktion herbeigeführt wird, sondern diese nur dazu dient, den *Private Key* zu erlangen. Bringt der Täter sein Opfer dazu, ihm den Zugangsschlüssel auszuhändigen, ist nämlich noch nicht zwingend ein unmittelbarer Schaden eingetroffen.

## 2. Unmittelbarkeit der Vermögensminderung bei Verlust des Private Keys

Unmittelbarkeit ist gemäss Bundesgericht gegeben, wenn «das irrtumsbedingte Verhalten des Getäuschten zu der Vermögensminderung führt, ohne dass dafür noch zusätzliche deliktische Zwischenhandlungen des Täters erforderlich sind».<sup>79</sup> Insofern trifft keine Vermögensdisposition, wer dem Täter lediglich [413] die Möglichkeit zur Begehung anderer Vermögensdelikte einräumt oder deren Begehung erleichtert. Im Falle des Verlustes eines *Private Key* ist – vergleichbar mit einer Bankomatkarte, welche der Täter aufgrund einer Täuschung erlangt –<sup>80</sup> nicht automatisch eine Vermögensminderung gegeben. Ist er noch anderweitig vorhanden, kann ein Verlust allenfalls noch abgewendet werden.<sup>81</sup> Besteht diese Option allerdings nicht mehr, könnte es sich um eine Vermögensgefährdung handeln, die einem Vermögensschaden gleichzusetzen wäre. Ein Vermögensschaden liegt nämlich auch dann vor, wenn das Vermögen des Täuschungsofers in einem Masse gefährdet wird, dass es in seinem wirtschaftlichen Wert vermindert ist, d. h. dann, wenn «der Gefährdung im Rahmen einer sorgfältigen Bilanzierung durch Wertberichtigung oder Rückstellung Rechnung getragen werden muss».<sup>82</sup> Ist der *Private Key* unwiderruflich verloren gegangen und liegt keine andere Zugriffsmöglichkeit mehr vor, die eine Schadensabwendung ermöglicht, ist eine solche Verminderung der Aktiven anzunehmen.

Zusammenfassend lässt sich festhalten, dass Kryptowährungen ein taugliches Angriffsobjekt des Betrugs darstellen. Auch zeigt sich, dass keiner der Tatbestandselemente grundsätzlich gegen die Anwendung des Tatbestands auf virtuelle Währungen spricht. Dennoch gilt es zu berücksichtigen, dass bei einer täuschungsbedingten Herausgabe des privaten Schlüssels nicht automatisch auf eine Erfolgsverwirklichung geschlossen werden kann. Vielmehr ist im Einzelfall zu prüfen, ob daraus eine *unmittelbare* Vermögensverminderung resultierte.

## III. Veruntreuung

### 1. Wallet-Betreiber als mögliche Treuehmer

Beim Handel mit Kryptowährungen sind regelmässig Intermediäre wie Handelsbörsenbetreiber oder *Wallet*-Anbieter involviert. In der als Fallvariante III eingeführten Konstellation ist beim Verlust von Währungseinheiten durch eine unbefugte «Entwendung» oder «Unterschlagung» durch derartige Drittanbieter eine Vermögensveruntreuung nach **Art. 138 Ziff. 1 Abs. 2 StGB** zu prüfen.

Der Tatbestand der Vermögensveruntreuung erfüllt, wer ihm anvertraute Vermögenswerte unrechtmässig verwendet. Bei diesem echten Sonderdelikt<sup>83</sup> kann also nur Täter sein, wer ihm geschenktes Vertrauen missbraucht.<sup>84</sup> Taug [414] liche Tatobjekte sind Vermögenswerte, die in die Verfügungsmacht des Täters übergegangen sind, aber «wirtschaftlich zum Vermögen eines anderen gehören».<sup>85</sup> «Anvertraut» ist, «was jemand mit der Verpflichtung empfängt, es in bestimmter Weise im Interesse eines andern zu verwenden, insbesondere es zu verwahren, zu verwalten oder abzuliefern».<sup>86</sup> Für Vermögenswerte folgt daraus, dass die Verfügungsmacht dem Treuhänder übertragen worden sein muss.<sup>87</sup> Bezüglich Kryptowährungen stellt sich vor allem die Frage, inwiefern *Web-Wallet*-Anbieter oder anderweitige Online-Dienstleister (wie z. B. Börsenbetreiber), die *Private Keys* verwahren, mit dem wirtschaftlich Berechtigten ein derartiges Treuhandverhältnis eingehen. Dabei ist vor allem strittig, inwiefern eine solche Aufbewahrung eine ausreichende Auf- bzw. Übergabe der Verfügungsmacht darstellt.

## 2. Erfordernis der Ausschliesslichkeit der Verfügungsmacht über den Private Key

Im Allgemeinen genügt es z. B. bei Forderungen, wenn der Treugeber die Zugriffsberechtigung übergibt oder den Zugang zum Vermögenswert, etwa durch Übergabe einer Kontokarte, ermöglicht.<sup>88</sup> Unklar ist allerdings, ob der Treugeber seine Verfügungsmacht vollständig aufgeben muss, damit die Vermögenswerte als anvertraut gelten. Unbestritten ist, dass dies auf Sachen zutrifft, zeichnet sich der Vorgang dort gerade durch Begründung ausschliesslichen Gewahrsams aus.<sup>89</sup> Dass Gleiches bei Vermögenswerten gilt, verneint das Bundesgericht: Eine Forderung sei anvertraut, sobald der Bevollmächtigte «ohne Mitwirkung des Treugebers über die Werte verfügen kann».<sup>90</sup> Die blossе Verfügungsmöglichkeit des Treuhänders soll folglich ausreichen; auch dann, wenn der Treugeber ebenfalls verfügungsberechtigt bleibt.<sup>91</sup> Folgte man dieser Auslegung, wäre die Hinterlegung von *Private Keys* bei *Wallet*-Anbietern grundsätzlich als tatbestandsmässiges «Anvertrauen» eines Vermögenswertes zu qualifizieren. Schliesslich zeichnet sich eine *Web-Wallet* gerade dadurch aus, dass zwar der private Schlüssel des Berechtigten auf dem Server des Anbieters gespeichert wird, Ersterer aber weiterhin über die Kryptowährungen verfügen kann.

Allerdings wird diese Rechtsprechung vom überwiegenden Teil der Lehre abgelehnt.<sup>92</sup> Es wird argumentiert, die strukturelle Gleichheit zwischen der Ver [415] untreuung von Sachen und derjenigen von Vermögenswerten<sup>93</sup> erfordere, dass der Treuneher *ausschliessliche* Verfügungsgewalt erlangt. Nur dann handle es sich um ein Anvertrauen. Reichte eine blossе Zugriffsberechtigung aus, würde die ungetreue Geschäftsbesorgung unterlaufen bzw. ihrem Anwendungsbereich massgeblich beraubt.<sup>94</sup> Daraus folgt, dass sich eine Anwendbarkeit der Vermögensveruntreuung auf Fälle von Missbräuchen durch *Wallet*-Betreiber oder anderen Verwahrern von Kryptowährungen daran entscheidet, ob der Position des Bundesgerichts oder derjenigen der Lehre gefolgt wird.

Nach hier vertretener Auffassung schränkt die Auffassung der h. L. den Anwendungsbereich der Vermögensveruntreuung bei virtuellen Währungen unzweckmässig ein. Der Unrechtsgehalt dieses Tatbestands besteht im Missbrauch von Vertrauen hinsichtlich der Verfügungsgewalt konkreter Vermögenswerte. Wird der Lehre gefolgt, wäre der Tatbestand nur dann erfüllt, wenn der *Wallet*-Betreiber ausschliessliche Verfügungsgewalt erlangt hat. Das wird in der Praxis kaum je der Fall sein. Gerade die Erfassung eines solchen Missbrauchs der Verfügungsgewalt über deponierte Kryptowährungen entspräche aber der *ratio legis* von Art. 138 Ziff. 1 Abs. 2 StGB. Eine Veruntreuung durch *Wallet*-Betreiber übersteigt den Schutzbereich der unbefugten Datenbeschaffung oder des Computerbetrugs und enthält eine zusätzliche Unrechtskomponente – diejenige des Treubruchs. Dieser Treubruch bezüglich anvertrauter digitaler Vermögenswerte zu

pönalisieren, scheint unabhängig der Ausschliesslichkeit der Verfügungsgewalt angebracht. Der Anwendungsbereich der ungetreuen Geschäftsbesorgung wird damit nicht unterlaufen, da sich **Art. 158 StGB** in seinem Anwendungsbereich auf den spezifischen Treubruch von Vermögensverwaltern bezieht. Der Auslegung des Bundesgerichts ist deshalb zu folgen, womit eine Anwendbarkeit der Vermögensveruntreuung auf die hier diskutierte Konstellation möglich ist. Eine eindeutige Klärung dieser Streitfrage wäre jedoch wünschenswert.

#### [416] IV. Ungetreue Geschäftsbesorgung

Eine missbräuchliche Verwendung von Kryptowährungen durch einen *Wallet*-Anbieter könnte auch eine ungetreue Geschäftsbesorgung darstellen. Auf Anhieb erscheint es indes fraglich, ob der Anbieter von Online-Applikationen zur Verwaltung von Kryptowährungen Schutzgarant für fremde Vermögensinteressen und damit tauglicher Täter ist.<sup>95</sup> Als Täter kommen gemäss **Art. 158 Abs. 1 StGB** Vermögensverwalter und Personen, die eine Vermögensverwaltung beaufsichtigen, infrage.<sup>96</sup> Vermögensverwalter ist, wer zur selbständigen Verfügung über einen wesentlichen Vermögenskomplex befugt ist.<sup>97</sup> *Wallet*-Betreiber sind gerade nicht zur selbständigen Vermögensverwaltung berechtigt. Ebenso scheidet die zweite Kategorie aus. Die Subsumtion unter **Art. 158 Abs. 1 StGB** scheitert also am Element des tauglichen Täters. Im Einzelfall wäre jedoch zu prüfen, ob die Vermögensverwaltung bei der Vereinbarung mit dem *Wallet*-Betreiber den wesentlichen Vertragsinhalt bildet.

### E. Kryptowährungen und vermögensbezogene Computerdelikte

#### I. Unbefugte Datenbeschaffung

##### 1. Kryptowährungen als taugliches Angriffsobjekt

Es wurde bereits dargelegt, dass sich Kryptowährungen unter den Datenbegriff subsumieren lassen.<sup>98</sup> Entsprechend ist bei ihrer «Entwendung» eine Strafbarkeit wegen unbefugter Datenbeschaffung nach **Art. 143 Abs. 1 StGB** naheliegend. Dieser sog. Datendiebstahl verlangt eine Bestrafung desjenigen, der mit Bereicherungsabsicht elektronisch oder in vergleichbarer Weise gespeicherte und nicht für ihn bestimmte Daten beschafft, die gegen seinen unbefugten Zugriff besonders gesichert sind. Die Norm erfasst also Fälle, bei denen sich ein Täter Daten behündigt, aber mangels Körperlichkeit derselben nicht für Diebstahl nach **Art. 139 StGB** bestraft werden kann.<sup>99</sup>

Kryptowährungen sind elektronisch gespeichert. Dadurch alleine stellen sie indes kein taugliches Angriffsobjekt dar. Der Tatbestand verlangt ferner, dass diese Daten nicht für den Täter bestimmt und gegen seinen unbefugten Zugriff [417] besonders gesichert sind.<sup>100</sup> Nicht für den Täter bestimmt sind Daten, für die ihm die Zugriffsberechtigung fehlt,<sup>101</sup> bei denen er also weder Datenberechtigter noch Datenherr ist.<sup>102</sup> Für eine unbefugte Beschaffung von Kryptowährungen darf dem Täter also keine Zugriffsberechtigung zukommen, was i. d. R. jedoch keine besonderen Probleme verursachen sollte.

##### 2. Wallets und Private Keys als besondere Sicherung

Ein Datendiebstahl setzt voraus, dass Daten gegen den Zugriff des Täters besonders gesichert sind, womit eine Parallele zum Gewahrsam beim Diebstahlstatbestand hergestellt wird.<sup>103</sup> Hinsichtlich der konkreten Voraussetzungen des Zugriffsschutzes schweigt das Gesetz. Als elektronische Zugangsschranken dienen z. B. *Firewalls*, Zugangscodes und Passwörter, die Verschlüsselung von Daten oder auch biometrische Schlüssel. Als physische kommt etwa das

Verschliessen des Computerraumes oder das Einschliessen des Datenträgers infrage.<sup>104</sup> In Bezug auf die Anforderungen an die Sicherung kann jedenfalls festgehalten werden, dass es sich dann um eine solche handelt, wenn «Personen in der Rolle des konkreten Täters üblicherweise» der Zugang verunmöglicht wird. Darunter fallen sowohl der gänzliche Ausschluss als auch bereits eine erhebliche Erschwerung.<sup>105</sup>

Hinsichtlich der Entwendung von Kryptowährungen ist folglich die Frage der besonderen Sicherung des *Private Key* zu betrachten. Virtuelle Währungen erfahren gerade durch diesen Schlüssel eine Sicherung. Da diesem Zugangscode selbst ebenfalls Datenqualität zukommt, kann bereits die Wegnahme dieses Codes einen Eingriff in besonders gesicherte Daten darstellen. Ist der *Private Key* z. B. in einem *Hardware-Wallet* gespeichert, d. h. auf einem USB-Stick, und wird dieser entwendet, ist zu untersuchen, ob dieser als gegen den unbefugten Zugriff besonders gesichert zu gelten hat. Dies ist zu bejahen, sofern eine elektronische Sicherung, etwa in Form eines Passworts besteht. Da in der Praxis die meisten *Wallets* – seien sie verkörpert oder virtuell – passwortgeschützt sind, wird diese Variante den Regelfall darstellen. Sollte der Schlüssel jedoch ungeschützt gespeichert oder auf Papier notiert sein, dürfte die spezielle physische Verwahrung (z. B. in einem verschlossenen Raum oder Behälter) als ausreichende Sicherung gelten. Dieses Tatbestandsmerkmal wird bei der Erlangung von *Private Keys* deshalb nur in denjenigen Fällen nicht erfüllt sein, in denen das Opfer diesen völlig ungeschützt und für jedermann zugänglich aufbewahrt. Aber gar in diesem Fall wird eine allfällig später erfolgte Transaktion des Vermögenswerts (d. h. eine Veränderung der *Blockchain*) eine Umgehung einer besonderen Zugriffssicherung darstellen. Der Zugriff auf diesen Vermögenswert ist nämlich bereits deshalb tatbestandsmässig, da – wie angedeutet – bereits der *Private Key* als Sicherung i. S. d. Tatbestands zu klassifizieren ist.

Die Tathandlung besteht in der Beschaffung der Daten, was wiederum dem Gewahrsamsbruch beim Diebstahl nachgebildet ist.<sup>106</sup> Beschaffen bedeutet, dass der Täter die Hindernisse überwunden hat, die ihm den Zugriff verwehren sollten, und er die Daten nutzen kann.<sup>107</sup> Der Täter muss die Daten in der Folge nicht tatsächlich für seine Zwecke einsetzen, um das Delikt zu vollenden.<sup>108</sup> In Bezug auf Kryptowährungen bedeutet diese Auslegung, dass nicht erst die Nutzung des privaten Schlüssels zwecks Veränderung der *Blockchain*, sondern bereits der Zugriff auf den *Private Key* eine Datenbeschaffung darstellt. Verschafft sich ein Täter also Zugang zu solchen privaten Schlüsseln, wird – sofern darüber hinaus die subjektiv geforderte Bereicherungsabsicht vorliegt – der Tatbestand des Datendiebstahls erfüllt sein. Eine tatsächliche Verfügung über die Vermögenswerte ist nicht erforderlich.

### 3. Relevanz von Art. 172<sup>ter</sup> StGB für den Diebstahl von Daten mit Vermögenswert

Eine spezielle Frage stellt sich in diesen Fällen hinsichtlich Art. 172<sup>ter</sup> Abs. 1 StGB. Diese Bestimmung sieht bei Vermögensdelikten eine generelle Privilegierung vor, wenn es sich beim Angriffsobjekt um einen geringfügigen Vermögenswert handelt. Geringfügigkeit ist gemäss Bundesgericht bis zu einem Wert von CHF 300 anzunehmen.<sup>109</sup> Die unbefugte Datenbeschaffung ist als Verletzungsdelikt ausgestaltet. Ob Art. 143 StGB indes einen Vermögensvorteil erfordert, ist diskutabel. Gemäss *Weissenberger* müsse das Verfügungsrecht des Datenberechtigten stets berührt sein, Ungleiches gelte jedoch für seine Vermögensinteressen.<sup>110</sup> Anderer Meinung ist *Schmid*, der die unbefugte Datenbeschaffung primär als Vermögensdelikt versteht.<sup>111</sup> Ginge man mit Letzterem davon aus, dass die Datenbeschaffung einen Vermögensvorteil mit sich bringen muss, wäre Art. 172<sup>ter</sup> StGB ohne Weiteres anwendbar, was sich mit Blick auf die hier diskutierten Fälle als problematisch erwiese.

Es ist zweifelhaft, dass ein privater Schlüssel, welcher erst in Verbindung mit der *Blockchain* werthaltig wird, eigens die Grenze der Geringwertigkeit jemals überschreiten wird, sofern man nicht bereits den potenziellen Vermögenswert bei der Benutzung des Schlüssels miteinbezieht. Es stellt sich hier die Frage, ob eine Gesamtbetrachtung erlaubt, die Bagatellklausel bei nur scheinbar wertlosen Daten auszuschliessen, auch wenn die unmittelbare unrechtmässige Bereicherung eine zusätzliche strafbare Handlung erfordert. Gemäss *Stratenwerth*, *Jenny* und *Bommer* schliesse der Umstand, dass «der Täter etwa mit Hilfe eines entwendeten Schlüssels oder einer Codekarte usw., die als solche geringwertig sind, den Zugang zu weiteren Vermögenswerten verschaffen will», die Anwendung von Art. 172<sup>ter</sup> StGB nicht aus.<sup>112</sup> Diese Auslegung ist bei der Entwendung von Kryptowährungen gerade deshalb kritisch, als dass bei einer solchen Nichtberücksichtigung des optionalen Vermögenswerts der Daten immer eine Privilegierung anzunehmen wäre. Ferner ist auch bei gegenläufiger Positionierung die Tatsache, dass es Delinquenten einfach möglich ist, mehrfach Einheiten unter der relevanten Schwelle abzuziehen, in Anbetracht der Abwesenheit eines Qualifikationstatbestands der Gewerbsmässigkeit mit Blick auf den Rechtsgüterschutz unbefriedigend. Deshalb sollen diese beiden Schwachstellen nachfolgend genauer erörtert und allfällige Lösungen eruiert werden.

#### 4. Berücksichtigung des «Datenwertes» beim Datendiebstahl de lege ferenda

Es ist fraglich, ob Daten mit einer «Schlüsselfunktion» in Bezug auf einen konkreten Vermögenswert – d. h. eben «Daten mit Vermögenswert *sui generis*» – anders zu behandeln sind als «gewöhnliche» Daten. Ein Teil der Lehre hat mit Blick auf die verwandte Frage bei der Aneignung von herkömmlichen (Haus-)Schlüsseln immerhin erkannt, dass nicht nur der wirtschaftliche Wert der Sache selbst, sondern ebenso der darin verkörperte Wert massgeblich sein müsse.<sup>113</sup> Es sei die Gesamtheit der Vermögenswerte oder Schäden zu berücksichtigen, die der Täter erlangen oder herbeiführen wollte.<sup>114</sup> Hinsichtlich des Datendiebstahls fehlen bis anhin vergleichbare Konzepte. Es ist deshalb *Gless*, *Kugler* [420] und *Stagno* zuzustimmen, dass diesbezüglich neue Ansätze gefunden werden müssten, wie dies bereits bei der Einführung anderer Zahlungsmethoden der Fall war.<sup>115</sup> Zu denken sei insbesondere an die Sachwerttheorie, wonach nicht die Substanz der Sache, sondern der darin verkörperte Wert als Objekt der Zueignung entscheidend ist.<sup>116</sup> Es ist in der Tat naheliegend, dass in Analogie zum Diebstahl an Sachen bei demjenigen an Daten die Anwendbarkeit von Art. 172<sup>ter</sup> StGB auf der Grundlage einer «Datenwerttheorie» verneint würde. So käme die Bagatellklausel nur dann infrage, wenn auch der mit den Daten zugängliche Vermögenswert die Bagatellschwelle nicht überschreitet.

#### 5. Gewerbsmässigkeit als qualifizierendes Element beim Datendiebstahl de lege ferenda

Neben der Frage, wie sich der Wert bei *Private Keys* genau bemisst, besteht aufgrund der Klausel in Art. 172<sup>ter</sup> StGB ferner die Gefahr, dass Täter die Geringfügigkeitsgrenze bewusst niemals überschreiten. Das Anvisieren von Konten bzw. *Wallets* unterhalb der relevanten Schwelle könnte eine von Datendieben bewusst verfolgte Strategie sein. Wie bereits erwähnt, wäre das mit Blick auf den Rechtsgüterschutz deshalb von Tragweite, da Art. 143 StGB keine Qualifikation der gewerbsmässigen Verwirklichung vorsieht.<sup>117</sup> Konkret wird deshalb vorliegend empfohlen, die gewerbsmässige Tatbegehung als Qualifikationstatbestand aufzunehmen und mit einer höheren Strafe zu bedrohen. So wäre der Tatbestand dem Diebstahl von Sachen diesbezüglich gleichgestellt. Sodann wäre die Anwendbarkeit von Art. 172<sup>ter</sup> StGB verunmöglicht, da Gewerbsmässigkeit diese Privilegierung generell ausschliesst.<sup>118</sup> Planvoll vorgehende

Mehrfachdiebe könnten bei einer derartigen Ergänzung also auch in Bezug auf Kryptowährungen angemessen verfolgt werden und eine Herabsetzung zum Antragsdelikt bzw. eine verminderte Strafandrohung i. S. v. Art. 172<sup>ter</sup> StGB wäre stets ausgeschlossen.

In der Summe ergab die Prüfung der Anwendbarkeit des Art. 143 StGB auf Entwendungen von *Private Keys*, dass diese Verhaltensweisen generell erfasst sind und den entsprechenden vermögensstrafrechtlichen Schutz geniessen. Dennoch wurden Schwachstellen offenbart, denen sowohl mit einfachen Ergänzungen der Gesetzgebung als auch mit Verfeinerungen der Lehre begegnet werden könnte.

## [421] II. Computerbetrug

### 1. Unrichtige und unbefugte Verwendung von Daten

Nach Art. 147 Abs. 1 StGB macht sich schuldig, wer mit Bereicherungsabsicht durch unbefugte Verwendung von Daten auf einen Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt. Art. 147 StGB ist dem Betrug nachgebildet und kommt nur subsidiär zur Anwendung.<sup>119</sup> Im Gegensatz zum herkömmlichen Betrug steht bei Art. 147 StGB nicht die Täuschung eines Menschen, sondern diejenige eines Computers im Vordergrund.<sup>120</sup>

Die Tathandlung setzt sich aus mehreren Merkmalen zusammen: Zum einen ist verlangt, dass der Täter die Daten in einer unrichtigen, unbefugten, unvollständigen oder vergleichbaren Weise verwendet. Zum anderen muss der Täter durch diese Verwendung auf einen Datenverarbeitungsvorgang einwirken. Ferner gilt als ungeschriebenes Tatbestandsmerkmal, dass diese Einwirkung ein inhaltlich unrichtiges Ergebnis herbeizuführen braucht.<sup>121</sup> Sowohl in Bezug auf die Entwendung von *Private Keys* zum Zwecke der Verschiebung von Kryptowährungen als auch hinsichtlich einer missbräuchlichen Verwendung von virtuellen Vermögenswerten durch Dienstleistungsanbieter stellt sich also die Frage, ob es sich dabei um ein tatbestandsmässiges Einwirken auf einen Datenverarbeitungsvorgang handelt, das zum erforderlichen unrichtigen Ergebnis führt.

Unrichtigkeit kann angenommen werden, wenn der Eingriff zu einem anderen Ergebnis führt, als dies «gemäss gegebener Sach- und Rechtslage» der Fall gewesen wäre,<sup>122</sup> d. h. wenn die «computermässig erfassten (vermögensrelevanten) Vorgänge und Beziehungen» unzutreffend gezeichnet werden.<sup>123</sup> Die unbefugte Verwendung nimmt Fälle ins Visier, bei denen «Unberechtigte durch die an sich «richtige» Verwendung von Daten in die Datenverarbeitung eingreifen»,<sup>124</sup> wobei auch hier auf die Herbeiführung eines unzutreffenden Ergebnisses abzustellen ist.<sup>125</sup> Als typischer Anwendungsfall gilt die Verwendung einer Bankomatkarte durch einen Nichtberechtigten.<sup>126</sup> Der Generalklausel «in vergleichbarer Weise» kommt aufgrund ihrer Unbestimmtheit kaum eigenständige Bedeutung zu.<sup>127</sup>

### [422] 2. Entwendung von Kryptowährungen als Einwirken auf einen Datenverarbeitungsvorgang

Da es sich bei Kryptowährungen um Daten handelt, steht einer Anwendbarkeit der Bestimmung diesbezüglich nichts entgegen. Die Daten müssen von einer Datenverarbeitungsanlage «verarbeitet, gespeichert und weitergegeben werden».<sup>128</sup> Als Datenverarbeitungsanlage gelten typischerweise Computer, aber auch Smartphones und jede andere Form eines automatisierten Datenvorganges.<sup>129</sup> Bei Kryptowährungen handelt es sich um derartige

Datenverarbeitungsvorgänge, da diese lediglich als Eintrag in einer Datenbank (der *Blockchain*) existieren und Transaktionen eine Aktualisierung derselben verlangen.<sup>130</sup> Dazu kommt, dass ein Computer oder ein Smartphone benötigt wird, um auf die Werteinheiten zuzugreifen, was ebenfalls für einen Datenverarbeitungsvorgang spricht.

Verschiebt ein Täter Währungseinheiten, ohne dazu berechtigt zu sein, führt er damit ein Ergebnis herbei, das nicht der betreffend diese Vermögenswerte geltenden Rechtslage entspricht. Der Unberechtigte greift mittels Verwendung von Daten (des *Private Key*) in den Datenverarbeitungsprozess (Veränderung der *Blockchain*) ein. Dieses tatbestandsmässige Verhalten kommt dem Musterfall nahe, bei welchem ein Dritter mit richtigem Code, aber mit gestohlener Karte an einem Automaten Geld bezieht. Die unbefugte Verwendung eines privaten Schlüssels ist i. d. S. tatbestandsmässig.

### 3. Veränderung der Blockchain als Taterfolg

Als Taterfolg sieht Art. 147 StGB eine Vermögensverschiebung zum Nachteil eines anderen vor oder das Verdecken einer solchen «unmittelbar darnach». In der Grundvariante entspricht der Erfolg *mutatis mutandis* demjenigen des Betrugs.<sup>131</sup> Um den Eintritt einer unmittelbaren Schädigung zu bejahen, muss der Täter in «ein der automatisierten Datenverarbeitung oder -übermittlung unterliegendes Vermögen» eingreifen.<sup>132</sup> Der Taterfolg wird in den hier diskutierten Fallkonstellationen immer dann gegeben sein, wenn der Zugriff auf den *Private Key* tatsächlich zu einer Transaktion der Währungseinheiten geführt hat, was i. d. R. der Fall sein wird. Entsprechend ergeben sich hier keine besonderen Probleme. Ist der Schlüssel hingegen nur entwendet, aber nicht genutzt worden, bleibt der Taterfolg aus. In diesen Fällen greift jedoch, wie bereits dargetan, Art. 143 StGB. Ebenso könnte es sich dann – je nach Tatumständen – um einen Versuch handeln. Beide Tatbestände sind natürlich nur dann anwendbar, wenn [423] eine Bereicherungsabsicht vorliegt. Ist keine solche erkennbar, ist weder Art. 143 StGB noch Art. 147 StGB einschlägig.

Zusammenfassend lässt sich festhalten, dass der Computerbetrug die unbefugte Entwendung von Kryptowährungen («Diebstahlshandlungen» i. w. S.) zu erfassen vermag. Die eingangs eingeführten Fallvarianten dürften im Regelfall unter diesen relativ weiten Tatbestand zu subsumieren und folglich nicht straflos sein. Art. 147 StGB schliesst damit diejenigen Lücken, welche sich in gewissen Fällen aufgrund der Nichtanwendbarkeit der traditionellen Vermögensdelikte ergeben können.

## III. Übrige vermögensbezogene Computerdelikte

### 1. Hacking

Art. 143<sup>bis</sup> StGB ist bei den Fällen von Interesse, bei denen *Private Keys* mittels eines unbefugten Eindringens in eine Datenverarbeitungsanlage zugänglich gemacht werden. Gemäss Botschaft verfolgt der Hacking-Tatbestand den Zweck, «bereits das Eindringen» und eine «Verletzung des Datenverfügungsrechts» zu erfassen.<sup>133</sup> Das kann dann bedeutsam werden, wenn eine Person unberechtigt in eine *Wallet* eindringt, ohne sich den Vermögenswerten tatsächlich zu bedienen. Daneben ist auch denkbar, dass sich jemand Zugang zu einem Computersystem verschafft, um zwecks *Mining* die Rechnerleistung zu nutzen.<sup>134</sup> Ebenso ist an die zahlreichen Krypto-Börsen zu denken, die in den letzten Jahren «gehackt» wurden.<sup>135</sup> Dieser Tatbestand wird jedoch in den hier diskutierten Fällen im Normalfall hinter Art. 143 StGB und Art. 147 StGB zurücktreten.

### 2. Datenbeschädigung

In Bezug auf die Datenbeschädigung nach **Art. 144<sup>bis</sup> Ziff. 1 StGB** stellt sich die Frage, ob durch die unbefugte Verwendung des privaten Schlüssels Daten i. S. dieser Bestimmung beschädigt werden. Verwendet ein Unberechtigter den *Private Key*, werden die sich vormals in der *Wallet* befindlichen Wertseinheiten insofern unbrauchbar, als dass sie vom Berechtigten nicht mehr gehandelt werden können.<sup>136</sup> Auch wenn eine Anwendbarkeit also nicht ausgeschlossen ist, tritt die Bestimmung in den hier bedeutsamen Fällen allerdings aufgrund unechter Konkurrenz hinter **Art. 143 StGB** und **Art. 147 StGB** zurück.

## [424] F. Synthese

### I. Strafbarkeit des «Diebstahls» von Kryptowährungen

Zurückkommend auf die vier präsentierten Fallvarianten, erlaubt die vorausgegangene Untersuchung eine differenzierte Einschätzung. In Bezug auf «Diebstahlshandlungen» hat sich gezeigt, dass ein eigentlicher Diebstahl aufgrund mangelnder Sacheigenschaft nicht möglich ist.<sup>137</sup> Es handelt sich um einen Datendiebstahl, bei dem sich der Täter fremde Daten beschafft, die gegen seinen Zugriff besonders gesichert sind. Diese Voraussetzung muss im Einzelfall geprüft werden, ist aber i. d. R. gegeben – aufgrund spezieller Passwörter oder bereits aufgrund des Vorhandenseins des *Private Key* selbst. Eine Subsumtion unter **Art. 147 StGB** gelingt ebenfalls, sofern die Entwendung des privaten Schlüssels zu einer tatsächlichen Disposition der Währungseinheiten führt. Bei einem «Diebstahl» von Kryptowährungen handelt es sich folglich sowohl um Datendiebstahl als auch um Computerbetrug. Führt der Verlust des privaten Schlüssels nicht zu einer Transaktion, handelt es sich nur um einen Datendiebstahl und ggf. um einen versuchten Computerbetrug. Wenn die Entwendung zu einer Transaktion führt, überschneiden sich **Art. 143 StGB** und **Art. 147 StGB**. Aufgrund der unterschiedlichen Schutzrichtungen ist jedoch echte Konkurrenz anzunehmen, und zwar auch dann, wenn die Datenbeschaffung (des *Private Keys*) dem Computerbetrug (dem Eintrag in der *Blockchain*) dient.

### II. Strafbarkeit der «betrügerischen Entwendung» von Kryptowährungen

Erlangt ein Unberechtigter aufgrund einer Täuschung Kenntnis über den *Private Key*, stellen Kryptowährungen ein taugliches Angriffsobjekt des Betrugstatbestands dar. Bei der Beurteilung der Strafbarkeit nach **Art. 146 StGB** ist jedoch danach zu differenzieren, ob die täuschungsbedingte Herausgabe des Schlüssels auch tatsächlich zu einer Vermögensminderung führt. Ebenso kommt in dieser Fallvariante eine Subsumtion unter den Computerbetrug infrage, wird doch bei Benutzung des Schlüssels erfolgreich und in unbefugter Weise auf einen Datenverarbeitungsprozess eingewirkt. Hinsichtlich der Konkurrenz ist festzustellen, dass **Art. 147 StGB** hier zurücktritt. Wenn die Vermögensdisposition sowohl auf die Täuschung des Menschen als auf den Eingriff in die Datenverarbeitungsanlage zurückzuführen ist, geht **Art. 146 StGB** vor.<sup>138</sup> Der Computerbetrug als subsidiäre Regelung wäre in diesem Falle mitbestrafte [425] *Nachtat*. Diese Lösung überzeugt, da die getrennte Betrachtung von Datenbeschaffung und -verwendung in Fällen, bei denen das Erlangen der Daten einzig dem Zwecke der späteren Vermögensdisposition dient, zu einer doppelten Pönalisierung der gleichen Rechtsgutsverletzung führen würde.<sup>139</sup>

### III. Strafbarkeit des «Hackings» von Kryptowährungen

Werden Kryptowährungen durch einen Eingriff in die Datenhoheit entwendet, ist dies als unbefugte Datenbeschaffung nach **Art. 143 StGB** zu klassifizieren, wobei bereits der Zugriff auf den *Private Key* tatbestandsmässig ist. Da der Tatbestand keinen Vermögensschaden erfordert, ist die Beschaffung

selbst für eine Strafbarkeit ausreichend, sofern sie mit Bereicherungsabsicht erfolgt. Ebenfalls handelt es sich in diesen Fällen um einen Computerbetrug, falls mittels des erlangten Schlüssels auch tatsächlich über die Einheiten disponiert wird. Nicht minder kann diese Verhaltensweise unter den Hacking-Tatbestand subsumiert werden, wobei dieser aufgrund der Subsidiarität von **Art. 143<sup>bis</sup> StGB** hinter **Art. 143 StGB** und **Art. 147 StGB** zurücktritt.

#### IV. Strafbarkeit der «Veruntreuung» von Kryptowährungen

Bei der als «Veruntreuung» anvertrauter Kryptowährungen eingeführten Fallvariante, bei der ein Betreiber seine Verfügungsberechtigung missbraucht, greift i. d. R. der Vermögensveruntreuungstatbestand nach **Art. 138 Ziff. 1 Abs. 2 StGB**. Die Subsumtion gelingt jedoch nur, wenn der Kritik der h. L. an der bundesgerichtlichen Rechtsprechung in Bezug auf die Ausschliesslichkeit der Verfügungsgewalt des Trenehmers nicht gefolgt wird. Wird hingegen, wie hier, die Auffassung vertreten, dass es für das Anvertrautsein ausreicht, wenn der Treuehmer ohne Mitwirkung des Treugebers über die Währungen verfügen kann, ist eine Anwendbarkeit von **Art. 138 StGB** generell möglich. Damit wird dem Unrechtsgehalt dieser Deliktssituation, der nicht nur im Verlust der Kryptowährungen, sondern gerade im Treubruch besteht, Rechnung getragen. Eine Subsumtion unter die ungetreue Geschäftsbesorgung scheitert indes an der Tauglichkeit des Täters. Hingegen kann auch hier von Computerbetrug ausgegangen werden, da der *Wallet*-Betreiber bei einer unautorisierten Verwendung der Vermögenswerte einen Datenverarbeitungsvorgang missbräuchlich und damit unbefugt beeinflusst. Da der Unrechtsgehalt der Veruntreuung bereits die Vermögensschädigung enthält und der unbefugte Einsatz des Schlüssels als Tathandlung dieser Bestimmung aufzufassen ist, ist in den hier diskutierten Fällen von unechter Konkurrenz auszugehen. **Art. 147 StGB** tritt folglich zurück.

#### [426] G. Schlussfolgerung

Die in diesem Beitrag vorgenommene Analyse hat erkennen lassen, dass der vermögensstrafrechtliche Schutz von Kryptowährungen *de lege lata* grundsätzlich gewahrt ist. Mit Blick auf die Rechtsnatur von Kryptowährungen wurde herausgearbeitet, dass es sich bei diesen sowohl um Daten als auch um Vermögenswerte handelt. Eine Qualifikation als Sache scheidet mangels Körperlichkeit aus. Als Daten und als Vermögenswerte *sui generis* sind virtuelle Währungen im Allgemeinen dem vermögensstrafrechtlichen Schutz unterstellt.

Die skizzierten Standardkonstellationen von «Entwendungen» von Kryptowährungen sind alle mindestens von einem Straftatbestand erfasst und bleiben damit nicht straflos. So lassen sich allen voran die Computerdelikte, insb. die unbefugte Datenbeschaffung nach **Art. 143 StGB** und der Computerbetrug nach **Art. 147 StGB**, auf Fälle von «Diebstählen» von Kryptowährungen anwenden. Aber auch traditionelle Vermögensdelikte, wie der Betrug nach **Art. 146 StGB** oder die Vermögensveruntreuung nach **Art. 138 Ziff. 1 Abs. 2 StGB**, bieten je nach Tatkonstellation Schutz. Da keine der diskutierten Fallvarianten straflos bliebe, kann nicht von einer eigentlichen Rechtslücke i. e. S. gesprochen werden. Obwohl Kryptowährungen bei der Schaffung dieser Tatbestände unbekannt waren, decken die Bestimmungen des dritten Teils des StGB die relevantesten – eingangs als «Diebstahls- und Betrugshandlungen» bezeichneten – deliktischen Verhaltensweisen im Zusammenhang mit Kryptowährungen ab.

Es lässt sich konstatieren, dass der vermögensstrafrechtliche Schutz grundsätzlich gewahrt ist. Dennoch weist das schweizerische Strafrecht *de lege lata* Schwachstellen auf, die hinsichtlich virtueller Währungen Praxisrelevanz erlangen. Einerseits hat sich der Lehrstreit hinsichtlich der Voraussetzung der Verfügungsgewalt bei der Vermögensveruntreuung bzw. hinsichtlich der Frage,

ob diese ausschliesslich vorliegen muss, als problematisch erwiesen. Eine baldige Klärung wäre begrüssenswert. Andererseits zeigt sich, dass die Anwendbarkeit der Bagatellklausel von Art. 172<sup>ter</sup> StGB beim Datendiebstahl von Kryptowährungen zu inadäquaten Ergebnissen führen könnte. Diesem Umstand wäre mit einer der Sachwerttheorie vergleichbaren «Datenwerttheorie» zu begegnen. Ebenso könnte die Einführung eines Qualifikationstatbestands der Gewerbsmässigkeit bei Art. 143 StGB – in Anlehnung an Art. 139 StGB – beim gezielten Missbrauch der Bagatellklausel Abhilfe schaffen. In der Summe unterliegen Kryptowährungen als Vermögenswerte eigener Art im schweizerischen Strafrecht dennoch einem angemessenen Vermögensschutz.

#### [427] Zusammenfassung

Der Beitrag adressiert die vermögensstrafrechtliche Qualifikation und Erfassung von Kryptowährungen. Es wird festgestellt, dass es sich bei diesen um Daten und Vermögenswerte handelt, nicht jedoch um Sachen. Als Vermögenswerte *sui generis* unterstehen sie dem Rechtsgutsschutz der Art. 137 ff. StGB. Eine Prüfung der vier als zentral bewerteten Fallkonstellationen von «Entwendungen» von Kryptowährungen, d. h. von eigentlichen «Betrugs- und Diebstahlshandlungen» derartiger Vermögenswerte, ergab, dass alle von mindestens einem Tatbestand erfasst sind und nicht straflos bleiben. Sowohl Computerdelikte, insb. die unbefugte Datenbeschaffung und der Computerbetrug, als auch traditionelle Vermögensdelikte wie der Betrug oder die Vermögensveruntreuung finden Anwendung. Dennoch zeigt der Beitrag gewisse Schwächen der bestehenden Rechtslage auf und diskutiert Mittel zu deren Behebung. So erweist es sich für einen adäquaten Vermögensschutz als zielführend, bei der Vermögensveruntreuung keine ausschliessliche Verfügungsgewalt über Kryptowährungen zu verlangen. Ebenso zeigen sich mit Blick auf die Bagatellklausel von Art. 172<sup>ter</sup> StGB die Entwicklung einer «Datenwerttheorie» und die Einführung eines Qualifikationstatbestands der Gewerbsmässigkeit bei Art. 143 StGB als notwendig sinnvoll. In der Summe wird dennoch festgestellt, dass Kryptowährungen im Schweizer Strafrecht einem angemessenen Vermögensschutz unterliegen.

#### Résumé

La présente contribution traite de la qualification pénale des cryptomonnaies. Il est établi qu'il s'agit de données et de valeur patrimoniales, mais non des choses mobilières. Appréhendées en tant que valeurs patrimoniales *sui generis*, elles sont soumises à la protection du patrimoine consacrée aux art. 137 ss du code pénal suisse (CP). L'examen des quatre cas principaux de «soustraction» de cryptomonnaies, à savoir des actes de vol ou d'escroquerie de telles valeurs patrimoniales, a permis de constater que chacune de ces variantes remplissent les éléments constitutifs d'au moins une norme pénale et, partant, s'avèrent punissables. Tant les infractions informatiques, en particulier la soustraction de données et l'utilisation frauduleuse d'un ordinateur, que les infractions traditionnelles contre le patrimoine telles que la fraude ou l'abus de confiance sont concernées. Dans cette perspective, cette contribution identifie certaines faiblesses dans la situation juridique actuelle et examine les moyens d'y remédier. Ainsi, dans l'optique d'une protection adéquate des valeurs patrimoniales, il s'avère opportun de ne pas exiger un pouvoir de disposition exclusif des cryptomonnaies en cas d'abus de confiance. En outre, s'agissant [428] de l'art. 172<sup>ter</sup> CP relatif aux infractions d'importance mineure, le développement d'une «théorie de la valeur des données» ainsi que l'introduction d'une circonstance aggravante d'activité par métier au libellé de l'art. 143 CP semblent nécessaires. En définitive, le présent article constate que les monnaies cryptomonnaies font l'objet d'une protection du patrimoine appropriée en droit pénal suisse.

#### Fussnoten:

- 1 So war Bitcoin z. B. die «currency of choice» auf der Schwarzmarktplattform *Silk Road*; siehe dazu z. B. HANNA HALABURDA/MIKLOS SARVARY, *Beyond Bitcoin. The Economics of Digital Currencies*, Houndmills 2016, S. 99.
- \* M.A. HSG in Law, LL.M. (Santa Clara), Junior Associate bei der Homburger AG.
- \*\* Dr. iur., Postdoctoral Fellow für Strafrecht, Strafprozessrecht und Kriminologie an der Universität St. Gallen.
- 1 So war Bitcoin z. B. die «currency of choice» auf der Schwarzmarktplattform *Silk Road*; siehe dazu z. B. HANNA HALABURDA/MIKLOS SARVARY, *Beyond Bitcoin. The Economics of Digital Currencies*, Houndmills 2016, S. 99.
- 1 So war Bitcoin z. B. die «currency of choice» auf der Schwarzmarktplattform *Silk Road*; siehe dazu z. B. HANNA HALABURDA/MIKLOS SARVARY, *Beyond Bitcoin. The Economics of Digital Currencies*, Houndmills 2016, S. 99.
- 2 Kantonspolizei Zürich, Vorsicht im Umgang mit Kryptowährungen, 2018, <[https://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2018\\_01/1801311j.html](https://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2018_01/1801311j.html)> (zuletzt abgerufen am 30.09.2018).
- 3 Bundesrat, Bericht zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, S. 7 f.; TIANA LAURENCE, *Blockchain for dummies*, Weinheim 2018, S. 24.
- 4 DANIEL DRESCHER, *Blockchain Grundlagen*, Frechen 2017, S. 201.
- 5 Siehe z. B. Bundesrat (Fn. 3), S. 8.
- 15 DANIEL BURGWINKEL, *Blockchaintechnologie und deren Funktionsweise verstehen*, in: Burgwinkel (Hrsg.): *Blockchain Technology. Einführung für Business- und IT Manager*, Berlin u. a. 2016, S. 3 ff., S. 23; HERLIN (Fn. 13), S. 84; KERSCHER (Fn. 6), S. 55.
- 16 Dazu bereits MONIKA SIMMLER/SINE SELMAN/DANIEL BURGERMEISTER, *Beschlagnahme von Kryptowährungen im Strafverfahren*, *AJP* 8/2018, S. 963 ff., S. 966.
- 17 SANDER DUIVESTEIN ET AL., *Blockchain: Cryptoplattform for a Frictionless Economy, Design to Disrupt*, 2015, S. 9.
- 18 HERLIN (Fn. 13), S. 76; GEORG KAES *Bitcoin. Technische Einleitung*, in: Helgo Eberwein /Anna-Zoe Steiner (Hrsg.): *Bitcoin*, Wien 2014, S. 1 ff., S. 3; SCHNECK/BUCHBINDER (Fn. 10), S. 216.
- 19 HERLIN (Fn. 13), S. 76; JUDMAYER ET AL. (Fn. 14), S. 25; KERSCHER (Fn. 6), S. 22.
- 20 KAES (Fn. 18), S. 4.
- 21 Vgl. SABINE GLESS/PETER KUGLER/DARIO STAGNO, *Was ist Geld? Und warum schützt man es?*, in: *recht* 2015, S. 82 ff., 87.
- 22 ANDY EXTANCE, *The future of cryptocurrencies: Bitcoin and beyond*, in: *Nature*, Vol. 526 (7571), S. 21–23, S. 22 f.; CHRISTOPH SAFFERLING/CHRISTIAN RÜCKERT, *Telekommunikationsüberwachung bei Bitcoins*, *MMR* 2015, S. 788 ff., S. 791.
- 26 KOENIG (Fn. 23), S. 71; BURGWINKEL (Fn. 15), S. 48.
- 3 Bundesrat, Bericht zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, S. 7 f.; TIANA LAURENCE, *Blockchain for dummies*, Weinheim 2018, S. 24.
- 4 DANIEL DRESCHER, *Blockchain Grundlagen*, Frechen 2017, S. 201.
- 5 Siehe z. B. Bundesrat (Fn. 3), S. 8.
- 3 Bundesrat, Bericht zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, S. 7 f.; TIANA LAURENCE, *Blockchain for dummies*, Weinheim 2018, S. 24.

- 4 DANIEL DRESCHER, Blockchain Grundlagen, Frechen 2017, S. 201.
- 5 Siehe z. B. Bundesrat (Fn. 3), S. 8.
- 6 Anstatt vieler DANIEL KERSCHER, Bitcoin. Funktionsweise, Risiken und Chancen der digitalen Währung, 2. Aufl., Dingolfing 2014, S. 12; JOERG PLATZER, Bitcoin kurz & gut. Banking ohne Banken, Köln 2014, S. 17.
- 7 ALEKSANDER BERENTSEN/FABIAN SCHÄR, Bitcoin, Blockchain und Kryptoassets. Eine umfassende Einführung, Norderstedt 2017, S. 10; HALABURDA/SARVARY (Fn. 1), S. 2.
- 8 HALABURDA/SARVARY (Fn. 1), S. 2; KERSCHER (Fn. 6), S. 11; DON TAPSCOTT/ALEX TAPSCOTT, Die Blockchain Revolution, 2. Aufl., Kulmbach 2016, S. 22.
- 9 BERENTSEN/SCHÄR (Fn. 7), S. 95; PLATZER (Fn. 6), S. 17.
- 10 OTTMAR SCHNECK/FELIX BUCHBINDER, Eine Welt ohne Geld. Alternativen zum bisherigen Geldsystem, Konstanz/München 2015, S. 212.
- 11 Bundesrat (Fn. 3), S. 8.
- 12 SCHNECK/BUCHBINDER (Fn. 10), S. 212.
- 13 PHILIPPE HERLIN, La fin des banques? Comment la technologie va changer votre argent, Paris 2015, S. 77 f.; LAURENCE (Fn. 3), S. 26.
- 14 ALJOSHA JUDMAYER/NICHOLAS STIFTER/KATHARINA KROMBHOLZ/EDGAR WEIPPL, Blocks and Chains, San Rafael 2017, S. 7 und 19; PLATZER (Fn. 6), S. 21; TAPSCOTT /TAPSCOTT (Fn. 8), S. 24.
- 15 DANIEL BURGWINKEL, Blockchaintechnologie und deren Funktionsweise verstehen, in: Burgwinkel (Hrsg.): Blockchain Technology. Einführung für Business- und IT Manager, Berlin u. a. 2016, S. 3 ff., S. 23; HERLIN (Fn. 13), S. 84; KERSCHER (Fn. 6), S. 55.
- 16 Dazu bereits MONIKA SIMMLER/SINE SELMAN/DANIEL BURGERMEISTER, Beschlagnahme von Kryptowährungen im Strafverfahren, [AJP 8/2018, S. 963 ff.](#), S. 966.
- 17 SANDER DUIVESTEIN ET AL., Blockchain: Cryptoplatform for a Frictionless Economy, Design to Disrupt, 2015, S. 9.
- 18 HERLIN (Fn. 13), S. 76; GEORG KAES Bitcoin. Technische Einleitung, in: Helgo Eberwein /Anna-Zoe Steiner (Hrsg.): Bitcoin, Wien 2014, S. 1 ff., S. 3; SCHNECK/BUCHBINDER (Fn. 10), S. 216.
- 19 HERLIN (Fn. 13), S. 76; JUDMAYER ET AL. (Fn. 14), S. 25; KERSCHER (Fn. 6), S. 22.
- 20 KAES (Fn. 18), S. 4.
- 21 Vgl. SABINE GLESS/PETER KUGLER/DARIO STAGNO, Was ist Geld? Und warum schützt man es?, in: recht 2015, S. 82 ff., 87.
- 22 ANDY EXTANCE, The future of cryptocurrencies: Bitcoin and beyond, in: Nature, Vol. 526 (7571), S. 21–23, S. 22 f.; CHRISTOPH SAFFERLING/CHRISTIAN RÜCKERT, Telekommunikationsüberwachung bei Bitcoins, MMR 2015, S. 788 ff., S. 791.
- 15 DANIEL BURGWINKEL, Blockchaintechnologie und deren Funktionsweise verstehen, in: Burgwinkel (Hrsg.): Blockchain Technology. Einführung für Business- und IT Manager, Berlin u. a. 2016, S. 3 ff., S. 23; HERLIN (Fn. 13), S. 84; KERSCHER (Fn. 6), S. 55.
- 16 Dazu bereits MONIKA SIMMLER/SINE SELMAN/DANIEL BURGERMEISTER, Beschlagnahme von Kryptowährungen im Strafverfahren, [AJP 8/2018, S. 963 ff.](#), S. 966.
- 17 SANDER DUIVESTEIN ET AL., Blockchain: Cryptoplatform for a Frictionless Economy, Design to Disrupt, 2015, S. 9.
- 18 HERLIN (Fn. 13), S. 76; GEORG KAES Bitcoin. Technische Einleitung, in: Helgo Eberwein /Anna-Zoe Steiner (Hrsg.): Bitcoin, Wien 2014, S. 1 ff., S. 3; SCHNECK/BUCHBINDER (Fn. 10), S. 216.

- 19 HERLIN (Fn. 13), S. 76; JUDMAYER ET AL. (Fn. 14), S. 25; KERSCHER (Fn. 6), S. 22.
- 20 KAES (Fn. 18), S. 4.
- 21 Vgl. SABINE GLESS/PETER KUGLER/DARIO STAGNO, Was ist Geld? Und warum schützt man es?, in: recht 2015, S. 82 ff., 87.
- 22 ANDY EXTANCE, The future of cryptocurrencies: Bitcoin and beyond, in: Nature, Vol. 526 (7571), S. 21–23, S. 22 f.; CHRISTOPH SAFFERLING/CHRISTIAN RÜCKERT, Telekommunikationsüberwachung bei Bitcoins, MMR 2015, S. 788 ff., S. 791.
- 23 AARON KOENIG, Bitcoin – Geld ohne Staat, 3. Aufl., München 2018, S. 114; JUDMAYER ET AL. (Fn. 14), S. 25; HERLIN (Fn. 13), S. 77; LAURENCE (Fn. 3), S. 193;
- 24 NICOLAS JACQUEMART/STEPHAN D. MEYER, Der Bitcoin-/Bitcoin-Cash-Hardfork, GesKR 4, 2017, S. 469 ff., S. 475.
- 25 ANDREAS M. ANTONOPOULOS, Mastering bitcoin. Programming the open blockchain, 2. Aufl., Sebastopol 2017, S. 58; HALABURDA/SARVARY (Fn. 1), S. 105 und S. 109 f.
- 26 KOENIG (Fn. 23), S. 71; BURGWINKEL (Fn. 15), S. 48.
- 26 KOENIG (Fn. 23), S. 71; BURGWINKEL (Fn. 15), S. 48.
- 27 ANTONOPOULOS (Fn. 25), S. 7; KOENIG (Fn. 23), S. 71.
- 28 ARVIND NARAYANAN/JOSEPH BONNEAU/EDWARD FELTEN/ANDREW MILLER /STEVEN GOLDFEDER, Bitcoin and Cryptocurrency Technologies, Princeton/Oxford 2016, S. 88.
- 29 KOENIG (Fn. 23), S. 71.
- 30 ANTONOPOULOS (Fn. 25), S. 7; KOENIG (Fn. 23), S. 114.
- 31 KOENIG (Fn. 23), S. 114.
- 32 ANTONOPOULOS (Fn. 25), S. 7; KOENIG (Fn. 23), S. 114 f.
- 33 LAURENCE (Fn. 3), S. 61.
- 34 FELIX MAGO/TOBIAS GILLEN, Das Bitcoin-Handbuch, 3. Aufl., Hannover 2017, S. 72; ANTONOPOULOS (Fn. 25), S. 7; KOENIG (Fn. 23), S. 95; LAURENCE (Fn. 3), S. 61.
- 35 HANS VEST, Allgemeine Vermögensdelikte, in: Jürg-Beat Ackermann/Günter Heine (Hrsg.): Wirtschaftsstrafrecht der Schweiz, Bern 2013, S. 261 ff., § 13 N 10.
- 41 ANDREAS DONATSCH, in: Donatsch et al. (Hrsg.): StGB/JStG. Orell Füssli Kommentar, 20. Aufl., Zürich 2018, Art. 137 N 1; NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 33; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 13 N 5.
- 42 **BGE 81 IV 156** E. 1 S. 158; **99 IV 140** E. 2b S. 143 f.; **100 IV 31** f.; **103 IV 87** E. 1 S. 89; STEFAN TRECHSEL/DEAN CRAMERI, in: PK (Fn. 38), Vorb. Art. 137 N 2
- 43 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 38.
- 44 ANNINA BALTISSER, Datenbeschädigung und Malware im Schweizer Strafrecht. Der Tatbestand des **Art. 144<sup>bis</sup> StGB** im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, ZStr Bd. 69, Diss. Zürich, Zürich u. a. 2013, S. 68; BERNARD CORBOZ, Les infractions en droit suisse. Volume I, 3. Aufl., Bern 2010, S. 225 N 4; DONATSCH (Fn. 41), Art. 137 N 1.
- 52 Botschaft 1991, S. 986.
- 53 MICHEL DUPUIS/LAURENT MOREILLON/CHRISTOPHE PIGUET/SÉVERINE BERGER /MIRIAM MAZOU/VIRGINE RODIGARI (Hrsg.), Petit Commentaire. Code Pénal, 2. Aufl., Basel 2017, Art. 143 N 9; NIKLAUS SCHMID, Computer- sowie Check- und Kreditkarten-Kriminalität. Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994, § 2 N 24.

- 54 Botschaft 1991, S. 987.
- 55 Bundesrat, Bericht zu virtuellen Währungen, S. 7 f., 21, 26; Botschaft 1991, S. 986; SABINE GLESS, Strafrechtsschutz für virtuelles Geld?, in: Daniel Jositsch/Christian Schwarzenegger/Wolfgang Wohlers (Hrsg.): Festschrift für Andreas Donatsch, Zürich u. a. 2017, S. 41 ff., S. 50; GLESS/KUGLER/STAGNO (Fn. 21), S. 89 f.; SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 ff.
- 56 Botschaft 1991, S. 1000 ff.
- 57 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 62.
- 58 GÜNTER STRATENWERTH/WOLFGANG WOHLERS: Schweizerisches Strafgesetzbuch. Stämpflis Handkommentar, 3. Aufl., Bern 2013, Art. 70 N 2 m. w. H.
- 59 Anstatt vieler NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 66; VEST (Fn. 35), § 13 N 269 f.
- 65 Dazu bereits SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 969.
- 66 SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 f.
- 67 Vgl. PLATZER (Fn. 6), S. 23.
- 68 CHRISTIAN RÜCKERT, Vermögensabschöpfung und Sicherstellung bei Bitcoins – Neue juristische Herausforderungen durch die ungeklärte Rechtsnatur von virtuellen Währungseinheiten, MMR 5, 2016, S. 295, S. 296; SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 969.
- 35 HANS VEST, Allgemeine Vermögensdelikte, in: Jürg-Beat Ackermann/Günter Heine (Hrsg.): Wirtschaftsstrafrecht der Schweiz, Bern 2013, S. 261 ff., § 13 N 10.
- 35 HANS VEST, Allgemeine Vermögensdelikte, in: Jürg-Beat Ackermann/Günter Heine (Hrsg.): Wirtschaftsstrafrecht der Schweiz, Bern 2013, S. 261 ff., § 13 N 10.
- 36 Dazu z. B. MARCEL A. NIGGLI/CHRISTOF RIEDO, in: Marcel A. Niggli/Hans Wiprächtiger (Hrsg.): **Basler Kommentar, Strafrecht II**, Art. 11–392 StGB, 3. Aufl., Basel 2013, **Vorb. Art. 137 N 19**; JOSÉ HURTADO POZO, Droit pénal general, 2. Aufl., Genf u. a. 2013, § 17 N 738.
- 37 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 20; VEST (Fn. 35), § 13 N 8; vgl. auch GUNTHER ARZT, in: **BSK-II** (Fn. 36), **Art. 146 N 16**.
- 38 ANDREAS DONATSCH, Strafrecht III, 10. Aufl., Zürich u. a. 2013, S. 96; JEAN-RICHARD-DIT-BRESSEL, Strafrecht, Zürich/St. Gallen 2015, S. 130; ALEXANDRE PAPAUX in: Alain Macaluso/Laurent Moreillon/Nicolas Queloz (Hrsg.): Commentaire Romand. Code pénal II, Basel 2017, Art. 137 N 13; MARK PIETH, Strafrecht. Besonderer Teil, 2. Aufl., Basel 2018, S. 174; GÜNTER STRATENWERTH/GUIDO JENNY/FELIX BOMMER, Schweizerisches Strafrecht. Besonderer Teil I, 7. Aufl., Bern 2010, § 15 N 47; STEFAN TRECHSEL in: Stefan Trechsel/Mark Pieth (Hrsg.): Schweizerisches Strafgesetzbuch. Praxiskommentar, 3. Aufl., Zürich/St. Gallen 2018, Art. 146 N 21.
- 39 **BGE 117 IV 139** E. 3d/aa S. 148; **122 IV 179** E. 3d S. 184; **126 IV 165** E. 3b S. 174.
- 40 STRATENWERTH/JENNY/BOMMER (Fn. 38), § 15 N 47; ebenso FELIX BOMMER, Grenzen des strafrechtlichen Vermögensschutzes bei rechts- und sittenwidrigen Geschäften, Diss. Bern, Bern 1996, S. 55, S. 64 ff.
- 41 ANDREAS DONATSCH, in: Donatsch et al. (Hrsg.): StGB/JStG. Orell Füssli Kommentar, 20. Aufl., Zürich 2018, Art. 137 N 1; NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 33; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 13 N 5.
- 42 **BGE 81 IV 156** E. 1 S. 158; **99 IV 140** E. 2b S. 143 f.; **100 IV 31** f.; **103 IV 87** E. 1 S. 89; STEFAN TRECHSEL/DEAN CRAMERI, in: PK (Fn. 38), Vorb. Art. 137 N 2
- 43 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 38.
- 44

ANNINA BALTISSER, Datenbeschädigung und Malware im Schweizer Strafrecht. Der Tatbestand des Art. 144<sup>bis</sup> StGB im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, ZStr Bd. 69, Diss. Zürich, Zürich u. a. 2013, S. 68; BERNARD CORBOZ, Les infractions en droit suisse. Volume I, 3. Aufl., Bern 2010, S. 225 N 4; DONATSCH (Fn. 41), Art. 137 N 1.

52 Botschaft 1991, S. 986.

53 MICHEL DUPUIS/LAURENT MOREILLON/CHRISTOPHE PIGUET/SÉVERINE BERGER /MIRIAM MAZOU/VIRGINE RODIGARI (Hrsg.), Petit Commentaire. Code Pénal, 2. Aufl., Basel 2017, Art. 143 N 9; NIKLAUS SCHMID, Computer- sowie Check- und Kreditkarten-Kriminalität. Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994, § 2 N 24.

54 Botschaft 1991, S. 987.

55 Bundesrat, Bericht zu virtuellen Währungen, S. 7 f., 21, 26; Botschaft 1991, S. 986; SABINE GLESS, Strafrechtsschutz für virtuelles Geld?, in: Daniel Jositsch/Christian Schwarzenegger /Wolfgang Wohlers (Hrsg.): Festschrift für Andreas Donatsch, Zürich u. a. 2017, S. 41 ff., S. 50; GLESS/KUGLER/STAGNO (Fn. 21), S. 89 f.; SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 ff.

56 Botschaft 1991, S. 1000 ff.

57 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 62.

58 GÜNTER STRATENWERTH/WOLFGANG WOHLERS: Schweizerisches Strafgesetzbuch. Stämpflis Handkommentar, 3. Aufl., Bern 2013, Art. 70 N 2 m. w. H.

59 Anstatt vieler NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 66; VEST (Fn. 35), § 13 N 269 f.

65 Dazu bereits SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 969.

66 SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 f.

67 Vgl. PLATZER (Fn. 6), S. 23.

68 CHRISTIAN RÜCKERT, Vermögensabschöpfung und Sicherstellung bei Bitcoins – Neue juristische Herausforderungen durch die ungeklärte Rechtsnatur von virtuellen Währungseinheiten, MMR 5, 2016, S. 295, S. 296; SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 969.

41 ANDREAS DONATSCH, in: Donatsch et al. (Hrsg.): StGB/JStG. Orell Füssli Kommentar, 20. Aufl., Zürich 2018, Art. 137 N 1; NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 33; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 13 N 5.

42 BGE 81 IV 156 E. 1 S. 158; 99 IV 140 E. 2b S. 143 f.; 100 IV 31 f.; 103 IV 87 E. 1 S. 89; STEFAN TRECHSEL/DEAN CRAMERI, in: PK (Fn. 38), Vorb. Art. 137 N 2

43 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 38.

44 ANNINA BALTISSER, Datenbeschädigung und Malware im Schweizer Strafrecht. Der Tatbestand des Art. 144<sup>bis</sup> StGB im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, ZStr Bd. 69, Diss. Zürich, Zürich u. a. 2013, S. 68; BERNARD CORBOZ, Les infractions en droit suisse. Volume I, 3. Aufl., Bern 2010, S. 225 N 4; DONATSCH (Fn. 41), Art. 137 N 1.

41 ANDREAS DONATSCH, in: Donatsch et al. (Hrsg.): StGB/JStG. Orell Füssli Kommentar, 20. Aufl., Zürich 2018, Art. 137 N 1; NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 33; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 13 N 5.

42 BGE 81 IV 156 E. 1 S. 158; 99 IV 140 E. 2b S. 143 f.; 100 IV 31 f.; 103 IV 87 E. 1 S. 89; STEFAN TRECHSEL/DEAN CRAMERI, in: PK (Fn. 38), Vorb. Art. 137 N 2

43 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 38.

- 44 ANNINA BALTISSER, Datenbeschädigung und Malware im Schweizer Strafrecht. Der Tatbestand des Art. 144<sup>bis</sup> StGB im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, ZStr Bd. 69, Diss. Zürich, Zürich u. a. 2013, S. 68; BERNARD CORBOZ, Les infractions en droit suisse. Volume I, 3. Aufl., Bern 2010, S. 225 N 4; DONATSCH (Fn. 41), Art. 137 N 1.
- 45 NICO KUHLMANN, Funktionsweise und rechtliche Einordnung der digitalen Währung, CR 10, 2014, S. 691 ff., S. 691; MERIH ERDEM KÜTÜK-MARKENDORF, Rechtliche Einordnung von Internetwährungen im deutschen Rechtssystem am Beispiel von Bitcoin, Schriften zum Wirtschafts- und Medienrecht, Urheberrecht und Immaterialgüterrecht Bd. 57, Diss. Erlangen-Nürnberg, Frankfurt a. M. 2016, S. 49.
- 46 So auch FRANZISKA BOEHM/PAULINA PESCH, Rechtliche Herausforderungen einer virtuellen Währung, MMR 2, 2014, 75 ff., S. 77.
- 47 Vgl. KÜTÜK-MARKENDORF (Fn. 45), S. 80; vgl. dazu auch HARALD BÄRTSCHI /CHRISTIAN MEISSER, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Rolf H. Weber/Florent Thouvenin (Hrsg.): Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich u. a. 2015, S. 113 ff., S. 141.
- 48 WEBER (Fn. 47), S. 30.
- 49 Vgl. auch die bundesgerichtliche Rechtsprechung zu «WIR-Checks»: BGE 95 II 176 E. 4 S. 181; dazu auch TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 138 N 10; a.M. z. B. MARCEL LAUTNER, Der «WIR»-Verrechnungsverkehr, Diss. Zürich, Zürich 1964, S. 182 f., S. 192 f.
- 50 So bereits BÄRTSCHI/MEISSER (Fn. 47), S. 149.
- 51 Ebenso bereits SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 und 971; für das Zivilrecht z. B. FRANÇOIS PILLER, Virtuelle Währungen – Reale Rechtsprobleme?, AJP 12, 2017, S. 1426 ff., 1429.
- 52 Botschaft 1991, S. 986.
- 53 MICHEL DUPUIS/LAURENT MOREILLON/CHRISTOPHE PIGUET/SÉVERINE BERGER /MIRIAM MAZOU/VIRGINE RODIGARI (Hrsg.), Petit Commentaire. Code Pénal, 2. Aufl., Basel 2017, Art. 143 N 9; NIKLAUS SCHMID, Computer- sowie Check- und Kreditkarten-Kriminalität. Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994, § 2 N 24.
- 54 Botschaft 1991, S. 987.
- 55 Bundesrat, Bericht zu virtuellen Währungen, S. 7 f., 21, 26; Botschaft 1991, S. 986; SABINE GLESS, Strafrechtsschutz für virtuelles Geld?, in: Daniel Jositsch/Christian Schwarzenegger /Wolfgang Wohlers (Hrsg.): Festschrift für Andreas Donatsch, Zürich u. a. 2017, S. 41 ff., S. 50; GLESS/KUGLER/STAGNO (Fn. 21), S. 89 f.; SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 ff.
- 52 Botschaft 1991, S. 986.
- 53 MICHEL DUPUIS/LAURENT MOREILLON/CHRISTOPHE PIGUET/SÉVERINE BERGER /MIRIAM MAZOU/VIRGINE RODIGARI (Hrsg.), Petit Commentaire. Code Pénal, 2. Aufl., Basel 2017, Art. 143 N 9; NIKLAUS SCHMID, Computer- sowie Check- und Kreditkarten-Kriminalität. Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994, § 2 N 24.
- 54 Botschaft 1991, S. 987.
- 55 Bundesrat, Bericht zu virtuellen Währungen, S. 7 f., 21, 26; Botschaft 1991, S. 986; SABINE GLESS, Strafrechtsschutz für virtuelles Geld?, in: Daniel Jositsch/Christian Schwarzenegger /Wolfgang Wohlers (Hrsg.): Festschrift für Andreas Donatsch, Zürich u. a. 2017, S. 41 ff., S.

50; GLESS/KUGLER/STAGNO (Fn. 21), S. 89 f.; SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 ff.

56 Botschaft 1991, S. 1000 ff.

57 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 62.

58 GÜNTER STRATENWERTH/WOLFGANG WOHLERS: Schweizerisches Strafgesetzbuch. Stämpflis Handkommentar, 3. Aufl., Bern 2013, Art. 70 N 2 m. w. H.

59 Anstatt vieler NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 66; VEST (Fn. 35), § 13 N 269 f.

56 Botschaft 1991, S. 1000 ff.

57 NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 62.

58 GÜNTER STRATENWERTH/WOLFGANG WOHLERS: Schweizerisches Strafgesetzbuch. Stämpflis Handkommentar, 3. Aufl., Bern 2013, Art. 70 N 2 m. w. H.

59 Anstatt vieler NIGGLI/RIEDO (Fn. 36), Vorb. Art. 137 N 66; VEST (Fn. 35), § 13 N 269 f.

60 BÄRTSCHI/MEISSER (Fn. 47), S. 141.

61 Vgl. vorne, **Kap. B.**

62 Vgl. BÄRTSCHI/MEISSER (Fn. 47), S. 142; KUHLMANN (Fn. 45), S. 694.

63 KÜTÜK-MARKENDORF (Fn. 45), S. 54; vgl. auch BÄRTSCHI/MEISSER (Fn. 47), S. 141 f.

64 So auch PILLER (Fn. 51), S. 1428; vgl. auch BOEHM/PESCH (Fn. 46), S. 78; GLESS (Fn. 55), S. 48; Auch *Ronc* und *Schuppli* kommen zum Schluss, dass eine Kategorie fehle, um diese «Vermögenspositionen juristisch adäquat zu erfassen». Gleichwohl seien Kryptowährungen als Vermögen zu qualifizieren; siehe PASCAL RONC/BENEDIKT SCHUPPLI, Kryptowährungen im Lichte der schweizerischen Geldwäschereigesetzgebung, *forumpenale* 6/2018, S. 529 ff., S. 532.

65 Dazu bereits SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 969.

66 SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 f.

67 Vgl. PLATZER (Fn. 6), S. 23.

68 CHRISTIAN RÜCKERT, Vermögensabschöpfung und Sicherstellung bei Bitcoins – Neue juristische Herausforderungen durch die ungeklärte Rechtsnatur von virtuellen Währungseinheiten, *MMR* 5, 2016, S. 295, S. 296; SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 969.

65 Dazu bereits SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 969.

66 SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 968 f.

67 Vgl. PLATZER (Fn. 6), S. 23.

68 CHRISTIAN RÜCKERT, Vermögensabschöpfung und Sicherstellung bei Bitcoins – Neue juristische Herausforderungen durch die ungeklärte Rechtsnatur von virtuellen Währungseinheiten, *MMR* 5, 2016, S. 295, S. 296; SIMMLER/SELMAN/BURGERMEISTER (Fn. 16), S. 969.

69 Gemäss verbreiteter Ansicht kann Daten im Allgemeinen ein Vermögenswert zukommen siehe dazu z. B. DOMINIC RYSER, «Computer Forensics», eine neue Herausforderung für das Strafprozessrecht, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.): *Internet-Recht und Strafrecht. 4. Tagungsband*, Bern 2005, S. 553 ff., S. 560; FELIX BOMMER, Löschung als Einziehung von Daten, in: Christian Schwarzenegger/Oliver Arter /Florian S. Jörg (Hrsg.): *Internet-Recht und Strafrecht. 4. Tagungsband*, Bern 2005, S. 171 ff., S. 174; DANIEL STOLL, Le bitcoin et les aspects pénaux des monnaies virtuelles, *forumpenale* 2, 2015, S. 99 ff., S. 106.

70 Dies steht auch im Einklang mit der privatrechtlichen Einordnung. So wird Kryptowährungen u. a. die Sacheinlagefähigkeit zugesprochen, da sie nach **Art. 959 Abs. 2 OR** als

Vermögenswerte aktivierungspflichtig seien; dazu LUKAS MÜLLER/THOMAS STOLTZ /TOBIAS A. KALLENBACH, Liberierung des Aktienkapitals mittels Kryptowährung, **AJP 2017, S. 1318 ff.**, S. 1323 f.; Der Bundesrat bestätigt diese Position in seinem jüngsten Bericht; siehe Bundesrat, Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz vom 14. Dezember 2018, S. 54.

71 **Art. 139 Ziff. 1 StGB.**

72 Siehe vorne, **Kap. C.II.1.**

73 Vgl. **BGE 111 IV 74; 128 IV 11**; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 31; WEISSENBERGER, in **BSK-II**: (Fn. 36), **Art. 143 N 25**.

74 **Art. 146 Ziff. 1 StGB**; dazu z. B. STEFAN MAEDER, Gefährdung – Schaden – Vermögen, Grundlegendes Recht Bd. 26, Diss. Freiburg i. Üe., Basel 2017, S. 13 f.

75 MAEDER (Fn. 74), S. 14; PIETH, Strafrecht BT (Fn. 38), S. 168.

76 Siehe **Kap. C.II.3.**

77 **BGE 126 IV 113 E. 3a S. 117.**

78 MAEDER (Fn. 74), S. 111; STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 146 N 10.

79 **BGE 126 IV 113 E. 3a S. 117**; vgl. auch **BGE 128 IV 255 E. 2e S. 257**; DONATSCH (Fn. 41), Art. 146 N 17; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 15 N 33; verkannt von **BGE 105 IV 102**.

80 Die Übergabe der Karte stellt keine vermögensmindernde Verfügung dar. Art. 146 ist erst vollendet, wenn der Täter die Karte benutzt. Erlangung und Verwendung sind folglich zu unterscheiden; DONATSCH, Strafrecht III (Fn. 38), S. 227 m. w. H.; vgl. dazu **BGE 127 IV 68 E. 2c S. 74 ff.**; vgl. auch STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 146 N 8.

81 In diesen Fällen wird es sich allerdings regelmässig um einen strafbaren Versuch handeln.  
82 BGer **6B\_25/2017** (15. 11. 2017) E. 5.2.; **BGE 129 IV 124, 126; 122 IV 279 E. 2; 123 IV 17 E. 3**; ANDREAS DONATSCH, Aspekte der ungetreuen Geschäftsbesorgung nach **Art. 158 StGB**, ZStrR 114, 1996, S. 202 f.

88 NIGGLI/RIEDO (Fn. 36), Art. 138 N 89; vgl. auch DONATSCH, Strafrecht III (Fn. 38), S. 147.

89 NIGGLI/RIEDO (Fn. 36), Art. 138 N 82 f.

90 **BGE 109 IV 27 E. 3 S. 32; 117 IV 429 E. 3b/aa S. 434**; vgl. **BGE 133 IV 21 E. 6.2 S. 27**.

91 NIGGLI/RIEDO (Fn. 36), Art. 138 N 96.

95 Beachte TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 158 N 7, wonach «einfache Dienstleistungen wie Aufbewahren, Überbringen u. Ä.» nicht erfasst seien; ebenso STRATENWERTH/JENNY/BOMMER (Fn. 38), § 19 N 7.

96 Bei **Art. 158 StGB** handelt es sich folglich um ein Sonderdelikt; vgl. hierzu BGer **6B\_1020 /2015** (18. 11. 2015) E. 1.2.2.

97 **BGE 105 IV 307 E. 2a S. 311; 142 IV 346 E. 3.2 S. 350**; DONATSCH (Fn. 41), Art. 158 N 2.

71 **Art. 139 Ziff. 1 StGB.**

72 Siehe vorne, **Kap. C.II.1.**

73 Vgl. **BGE 111 IV 74; 128 IV 11**; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 31; WEISSENBERGER, in **BSK-II**: (Fn. 36), **Art. 143 N 25**.

71 **Art. 139 Ziff. 1 StGB.**

72 Siehe vorne, **Kap. C.II.1.**

73 Vgl. **BGE 111 IV 74; 128 IV 11**; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 31; WEISSENBERGER, in **BSK-II**: (Fn. 36), **Art. 143 N 25**.

74

Art. 146 Ziff. 1 StGB; dazu z. B. STEFAN MAEDER, Gefährdung – Schaden – Vermögen, Grundlegendes Recht Bd. 26, Diss. Freiburg i. Üe., Basel 2017, S. 13 f.

MAEDER (Fn. 74), S. 14; PIETH, Strafrecht BT (Fn. 38), S. 168.

Siehe Kap. C.II.3.

BGE 126 IV 113 E. 3a S. 117.

MAEDER (Fn. 74), S. 111; STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 146 N 10.

BGE 126 IV 113 E. 3a S. 117; vgl. auch BGE 128 IV 255 E. 2e S. 257; DONATSCH (Fn. 41), Art. 146 N 17; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 15 N 33; verkannt von BGE 105 IV 102.

Die Übergabe der Karte stellt keine vermögensmindernde Verfügung dar. Art. 146 ist erst vollendet, wenn der Täter die Karte benutzt. Erlangung und Verwendung sind folglich zu unterscheiden; DONATSCH, Strafrecht III (Fn. 38), S. 227 m. w. H.; vgl. dazu BGE 127 IV 68 E. 2c S. 74 ff.; vgl. auch STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 146 N 8.

In diesen Fällen wird es sich allerdings regelmässig um einen strafbaren Versuch handeln. BGer 6B\_25/2017 (15. 11. 2017) E. 5.2.; BGE 129 IV 124, 126; 122 IV 279 E. 2; 123 IV 17 E. 3; ANDREAS DONATSCH, Aspekte der ungetreuen Geschäftsbesorgung nach Art. 158 StGB, ZStrR 114, 1996, S. 202 f.

Art. 146 Ziff. 1 StGB; dazu z. B. STEFAN MAEDER, Gefährdung – Schaden – Vermögen, Grundlegendes Recht Bd. 26, Diss. Freiburg i. Üe., Basel 2017, S. 13 f.

MAEDER (Fn. 74), S. 14; PIETH, Strafrecht BT (Fn. 38), S. 168.

Siehe Kap. C.II.3.

BGE 126 IV 113 E. 3a S. 117.

MAEDER (Fn. 74), S. 111; STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 146 N 10.

Art. 146 Ziff. 1 StGB; dazu z. B. STEFAN MAEDER, Gefährdung – Schaden – Vermögen, Grundlegendes Recht Bd. 26, Diss. Freiburg i. Üe., Basel 2017, S. 13 f.

MAEDER (Fn. 74), S. 14; PIETH, Strafrecht BT (Fn. 38), S. 168.

Siehe Kap. C.II.3.

BGE 126 IV 113 E. 3a S. 117.

MAEDER (Fn. 74), S. 111; STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 146 N 10.

BGE 126 IV 113 E. 3a S. 117; vgl. auch BGE 128 IV 255 E. 2e S. 257; DONATSCH (Fn. 41), Art. 146 N 17; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 15 N 33; verkannt von BGE 105 IV 102.

Die Übergabe der Karte stellt keine vermögensmindernde Verfügung dar. Art. 146 ist erst vollendet, wenn der Täter die Karte benutzt. Erlangung und Verwendung sind folglich zu unterscheiden; DONATSCH, Strafrecht III (Fn. 38), S. 227 m. w. H.; vgl. dazu BGE 127 IV 68 E. 2c S. 74 ff.; vgl. auch STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 146 N 8.

In diesen Fällen wird es sich allerdings regelmässig um einen strafbaren Versuch handeln. BGer 6B\_25/2017 (15. 11. 2017) E. 5.2.; BGE 129 IV 124, 126; 122 IV 279 E. 2; 123 IV 17 E. 3; ANDREAS DONATSCH, Aspekte der ungetreuen Geschäftsbesorgung nach Art. 158 StGB, ZStrR 114, 1996, S. 202 f.

BGE 126 IV 113 E. 3a S. 117; vgl. auch BGE 128 IV 255 E. 2e S. 257; DONATSCH (Fn. 41), Art. 146 N 17; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 15 N 33; verkannt von BGE 105 IV 102.

Die Übergabe der Karte stellt keine vermögensmindernde Verfügung dar. Art. 146 ist erst vollendet, wenn der Täter die Karte benutzt. Erlangung und Verwendung sind folglich zu

unterscheiden; DONATSCH, Strafrecht III (Fn. 38), S. 227 m. w. H.; vgl. dazu **BGE 127 IV 68** E. 2c S. 74 ff.; vgl. auch STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 146 N 8.

- 81 In diesen Fällen wird es sich allerdings regelmässig um einen strafbaren Versuch handeln.
- 82 BGer **6B\_25/2017** (15.11.2017) E. 5.2.; **BGE 129 IV 124**, 126; **122 IV 279** E. 2; **123 IV 17** E. 3; ANDREAS DONATSCH, Aspekte der ungetreuen Geschäftsbesorgung nach **Art. 158 StGB**, ZStrR 114, 1996, S. 202 f.
- 88 NIGGLI/RIEDO (Fn. 36), Art. 138 N 89; vgl. auch DONATSCH, Strafrecht III (Fn. 38), S. 147.
- 89 NIGGLI/RIEDO (Fn. 36), Art. 138 N 82 f.
- 90 **BGE 109 IV 27** E. 3 S. 32; **117 IV 429** E. 3b/aa S. 434; vgl. **BGE 133 IV 21** E. 6.2 S. 27.
- 91 NIGGLI/RIEDO (Fn. 36), Art. 138 N 96.
- 83 BGer **6S.321/2005** (16.12.2005) E. 2.2; DUPUIS ET AL. (Fn. 53), Art. 138 N 23.
- 84 **BGE 98 IV 147** E. 4 S. 150; NIGGLI/RIEDO (Fn. 36), Art. 138 N 9.
- 85 **BGE 99 IV 206** E. 1 S. 206 f.; DONATSCH (Fn. 41), Art. 138 N 12.
- 86 **BGE 120 IV 117** E. 2b S. 119; ebenso **BGE 80 IV 53** S. 55; **80 IV 151** E. 2 S. 153; **88 IV 15** E. 5 S. 18.
- 87 BGer **6B\_596/2009** (27.05.2010) E. 4.2.2; DUPUIS ET AL. (Fn. 53), Art. 138 N 30.
- 88 NIGGLI/RIEDO (Fn. 36), Art. 138 N 89; vgl. auch DONATSCH, Strafrecht III (Fn. 38), S. 147.
- 89 NIGGLI/RIEDO (Fn. 36), Art. 138 N 82 f.
- 90 **BGE 109 IV 27** E. 3 S. 32; **117 IV 429** E. 3b/aa S. 434; vgl. **BGE 133 IV 21** E. 6.2 S. 27.
- 91 NIGGLI/RIEDO (Fn. 36), Art. 138 N 96.
- 88 NIGGLI/RIEDO (Fn. 36), Art. 138 N 89; vgl. auch DONATSCH, Strafrecht III (Fn. 38), S. 147.
- 89 NIGGLI/RIEDO (Fn. 36), Art. 138 N 82 f.
- 90 **BGE 109 IV 27** E. 3 S. 32; **117 IV 429** E. 3b/aa S. 434; vgl. **BGE 133 IV 21** E. 6.2 S. 27.
- 91 NIGGLI/RIEDO (Fn. 36), Art. 138 N 96.
- 92 ARZT (Fn. 37), S. 137; DONATSCH (Fn. 41), S. 25; HURTADO POZO, Strafrecht BT (Fn. 36), § 29 N 871; BERNHARD ISENRING, Die Strafbarkeit des direkten bürgerlichen Stellvertreters nach **Art. 158 Ziff. 2 StGB**, Diss. Zürich, Zürich u. a. 2007, S. 242 f.; GUIDO JENNY, Aktuelle Fragen des Vermögens- und Urkundenstrafrechts, ZBJV 124, 1988, S. 393 ff., S. 405; KARL-LUDWIG KUNZ, Grundstrukturen des neuen Vermögens- und Urkundenstrafrechts, ZBJV 132, 1996, S. 189 ff. S. 193; MAEDER (Fn. 74), S. 291; NIGGLI/RIEDO (Fn. 36), Art. 138 N 97; HANS SCHULTZ, Darlehen als anvertraute Vermögenswerte?, in: Niklaus Schmid/Martin Killias (Hrsg.): Le droit pénal es ses liens avec autres branches du droit. Mélanges en l'honneur du Professeur Jean Gauthier, Bern 1996, S. 81 ff., S. 84 f.; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 13 N 57; TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 138 N 11; VEST (Fn. 35), § 13 N 289; **a. M.** aber PASCAL DE PREUX/LYUSKA HULLIGER, in: Alain Macaluso/Laurent Moreillon/Nicolas Queloz (Hrsg.): Commentaire Romand. Code pénal II, Basel 2017, Art. 138 N 35.
- 93 «Abs. 2 soll nur jenes Unrecht erfassen, das mit dem in Abs. 1 umschriebenen strukturell gleichwertig ist»: so BGer **6B\_362/2013** (10.12.13) E. 1.3.1; ebenso **BGE 120 IV 117** E. 2e S. 121 m. w. H.; **133 IV 21** E. 6.2 S. 27.
- 94 NIGGLI/RIEDO (Fn. 36), Art. 138 N 97.
- 95 Beachte TRECHSEL/CRAMERI. in: PK (Fn. 38), Art. 158 N 7, wonach «einfache Dienstleistungen wie Aufbewahren, Überbringen u. Ä.» nicht erfasst seien; ebenso STRATENWERTH/JENNY/BOMMER (Fn. 38), § 19 N 7.
- 96

Bei Art. 158 StGB handelt es sich folglich um ein Sonderdelikt; vgl. hierzu BGer 6B\_1020 /2015 (18.11.2015) E. 1.2.2.

- 97 BGE 105 IV 307 E. 2a S. 311; 142 IV 346 E. 3.2 S. 350; DONATSCH (Fn. 41), Art. 158 N 2.
- 95 Beachte TRECHSEL/CRAMERI. in: PK (Fn. 38), Art. 158 N 7, wonach «einfache Dienstleistungen wie Aufbewahren, Überbringen u. Ä.» nicht erfasst seien; ebenso STRATENWERTH/JENNY/BOMMER (Fn. 38), § 19 N 7.
- 96 Bei Art. 158 StGB handelt es sich folglich um ein Sonderdelikt; vgl. hierzu BGer 6B\_1020 /2015 (18.11.2015) E. 1.2.2.
- 97 BGE 105 IV 307 E. 2a S. 311; 142 IV 346 E. 3.2 S. 350; DONATSCH (Fn. 41), Art. 158 N 2.
- 98 Kap. C.II.2.
- 99 Botschaft 1991, S. 983, 1009; DONATSCH, Strafrecht III (Fn. 38), S. 195; MARK PIETH, Wirtschaftsstrafrecht, Basel 2016, S. 137; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 23.
- 103 PIETH, Wirtschaftsstrafrecht (Fn. 99), S. 137; TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 143 N 6.
- 104 Botschaft 1991, S. 1011; HURTADO POZO, Strafrecht BT (Fn. 36), § 35 N 1045; SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 32 ff.; WEISSENBERGER, in: BSK-II (Fn. 36), Art. 143 N 20.
- 105 So SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 30; WEISSENBERGER, in: BSK-II (Fn. 36), Art. 143 N 19.
- 109 BGE 121 IV 261 E. 2d S. 268; 123 IV 113 E. E. 3d S. 119.
- 110 WEISSENBERGER, in: BSK-II (Fn. 36), Art. 143 N 3.
- 111 So in SCHMID Computer-Kriminalität (Fn. 53), § 4 N 14 ff.
- 113 So führen STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10, illustrativ aus, dass der Diebstahl eines Schlüssels, der es erforderlich mache, sämtliche Schlösser zu wechseln, eine Gesamtbetrachtung verlange, infolge derer die Tat nicht mehr zwingend ein Bagatelldelikt darstelle.
- 114 Siehe STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10 m. w. H.
- 115 GLESS/KUGLER/STAGNO (Fn. 21), S. 94.
- 116 GLESS/KUGLER/STAGNO (Fn. 21), S. 94; für Ausführungen zur Substanz- bzw. Sachwerttheorie bei der «Aneignung» anstatt vieler z. B. NIGGLI/RIEDO (Fn. 36), Art. 137 N 19 ff.; TRECHSEL/CRAMERI, in: PK (Fn. 38), Vorb. Art. 137 N 9.
- 117 Auch Bandenmässigkeit ist nicht als Qualifikation vorgesehen, was mit Blick auf Kryptowährungen bedenkenswert ist, sind Cyberkriminelle doch oft organisiert. Eine solche Ausweitung müsste aber in Bezug auf alle Vermögensdelikte überprüft werden, was den Untersuchungsgegenstand dieser Abhandlung übersteigt.
- 118 WEISSENBERGER, in: BSK-II (Fn. 36), Art. 172<sup>ter</sup> N 11 und N 45.
- 119 CORBOZ (Fn. 44), S. 339 N 1 f.; DONATSCH, Strafrecht III (Fn. 38), S. 248.
- 120 Botschaft 1991, S. 1020; FIOLKA, in: BSK-II (Fn. 36), Art. 147 N 6.
- 128 So die Voraussetzung gemäss Botschaft 1991, S. 987.
- 129 Vgl. z. B. FIOLKA, in: BSK-II (Fn. 36), Art. 147 N 24.
- 130 PLATZER (Fn. 6), S. 23; dazu bereits vorne, Kap. C.II.2.
- 131 Vgl. anstatt vieler DONATSCH, Strafrecht III (Fn. 38), S. 251; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 16 N 11; zu den Voraussetzungen beim Betrug bereits vorne, Kap. D. II.

- 132 STRATENWERTH/JENNY/BOMMER (Fn. 38), § 16 N 11.  
 133 So Botschaft 1991, S. 1011.  
 134 Vgl. GLESS/KUGLER/STAGNO (Fn. 21), S. 93.  
 135 Man denke z. B. an die japanische Börse *Mt. Gox*; hierzu HALABURDA/SARVARY (Fn. 1), S. 7.  
 136 Vgl. GLESS/KUGLER/STAGNO (Fn. 21), S. 94.  
 98 **Kap. C.II.2.**  
 99 Botschaft 1991, S. 983, 1009; DONATSCH, Strafrecht III (Fn. 38), S. 195; MARK PIETH, Wirtschaftsstrafrecht, Basel 2016, S. 137; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 23.  
 103 PIETH, Wirtschaftsstrafrecht (Fn. 99), S. 137; TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 143 N 6.  
 104 Botschaft 1991, S. 1011; HURTADO POZO, Strafrecht BT (Fn. 36), § 35 N 1045; SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 32 ff.; WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 20.**  
 105 So SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 30; WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 19.**  
 109 **BGE 121 IV 261** E. 2d S. 268; **123 IV 113** E. E. 3d S. 119.  
 110 WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 3.**  
 111 So in SCHMID Computer-Kriminalität (Fn. 53), § 4 N 14 ff.  
 113 So führen STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10, illustrativ aus, dass der Diebstahl eines Schlüssels, der es erforderlich mache, sämtliche Schlösser zu wechseln, eine Gesamtbetrachtung verlange, infolge derer die Tat nicht mehr zwingend ein Bagatelldelikt darstelle.  
 114 Siehe STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10 m. w. H.  
 115 GLESS/KUGLER/STAGNO (Fn. 21), S. 94.  
 116 GLESS/KUGLER/STAGNO (Fn. 21), S. 94; für Ausführungen zur Substanz- bzw. Sachwerttheorie bei der «Aneignung» anstatt vieler z. B. NIGGLI/RIEDO (Fn. 36), Art. 137 N 19 ff.; TRECHSEL/CRAMERI, in: PK (Fn. 38), Vorb. Art. 137 N 9.  
 117 Auch Bandenmässigkeit ist nicht als Qualifikation vorgesehen, was mit Blick auf Kryptowährungen bedenkenswert ist, sind Cyberkriminelle doch oft organisiert. Eine solche Ausweitung müsste aber in Bezug auf alle Vermögensdelikte überprüft werden, was den Untersuchungsgegenstand dieser Abhandlung übersteigt.  
 118 WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 172<sup>ter</sup> N 11** und **N 45.**  
 98 **Kap. C.II.2.**  
 99 Botschaft 1991, S. 983, 1009; DONATSCH, Strafrecht III (Fn. 38), S. 195; MARK PIETH, Wirtschaftsstrafrecht, Basel 2016, S. 137; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 23.  
 98 **Kap. C.II.2.**  
 99 Botschaft 1991, S. 983, 1009; DONATSCH, Strafrecht III (Fn. 38), S. 195; MARK PIETH, Wirtschaftsstrafrecht, Basel 2016, S. 137; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 23.  
 100 Damit wird eine Analogie zur Fremdheit der Sache beim Diebstahl hergestellt; siehe PIETH, Strafrecht BT (Fn. 38), S. 166; SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 20 ff.; TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 143 N 5.

- 101 PIETH, Strafrecht BT (Fn. 38) S. 166; STRATENWERTH/WOHLERS, in: SHK (Fn. 58), Art. 143 N 2.
- 102 Botschaft 1991, S. 1012; DONATSCH, Strafrecht III (Fn. 38), S. 195 f.; SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 20 ff., 68; TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 143 N 4; WEISSENBERGER, in **BSK-II**: (Fn. 36), **Art. 143 N 15**.
- 103 PIETH, Wirtschaftsstrafrecht (Fn. 99), S. 137; TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 143 N 6.
- 104 Botschaft 1991, S. 1011; HURTADO POZO, Strafrecht BT (Fn. 36), § 35 N 1045; SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 32 ff.; WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 20**.
- 105 So SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 30; WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 19**.
- 103 PIETH, Wirtschaftsstrafrecht (Fn. 99), S. 137; TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 143 N 6.
- 104 Botschaft 1991, S. 1011; HURTADO POZO, Strafrecht BT (Fn. 36), § 35 N 1045; SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 32 ff.; WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 20**.
- 105 So SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 30; WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 19**.
- 106 PIETH, Strafrecht BT (Fn. 38), S. 166.
- 107 STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 31; TRECHSEL/CRAMERI, in: PK (Fn. 38), Art. 143 N 7.
- 108 SCHMID, Computer-Kriminalität (Fn. 53), § 4 N 41; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 14 N 31; WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 23**; wohl **a.M.** PIETH, Wirtschaftsstrafrecht (Fn. 99), S. 137, wonach Beschaffen «die Überwindung des Hindernisses und die Verwendung der Daten» meine.
- 109 **BGE 121 IV 261** E. 2d S. 268; **123 IV 113** E. E. 3d S. 119.
- 110 WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 3**.
- 111 So in SCHMID Computer-Kriminalität (Fn. 53), § 4 N 14 ff.
- 109 **BGE 121 IV 261** E. 2d S. 268; **123 IV 113** E. E. 3d S. 119.
- 110 WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 143 N 3**.
- 111 So in SCHMID Computer-Kriminalität (Fn. 53), § 4 N 14 ff.
- 112 STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10 Fn. 21.
- 113 So führen STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10, illustrativ aus, dass der Diebstahl eines Schlüssels, der es erforderlich mache, sämtliche Schlösser zu wechseln, eine Gesamtbetrachtung verlange, infolge derer die Tat nicht mehr zwingend ein Bagatelldelikt darstelle.
- 114 Siehe STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10 m. w. H.
- 115 GLESS/KUGLER/STAGNO (Fn. 21), S. 94.
- 116 GLESS/KUGLER/STAGNO (Fn. 21), S. 94; für Ausführungen zur Substanz- bzw. Sachwerttheorie bei der «Aneignung» anstatt vieler z. B. NIGGLI/RIEDO (Fn. 36), Art. 137 N 19 ff.; TRECHSEL/CRAMERI, in: PK (Fn. 38), Vorb. Art. 137 N 9.
- 113 So führen STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10, illustrativ aus, dass der Diebstahl eines Schlüssels, der es erforderlich mache, sämtliche Schlösser zu wechseln, eine Gesamtbetrachtung verlange, infolge derer die Tat nicht mehr zwingend ein Bagatelldelikt darstelle.

- 114 Siehe STRATENWERTH/JENNY/BOMMER (Fn. 38), § 25 N 10 m. w. H.
- 115 GLESS/KUGLER/STAGNO (Fn. 21), S. 94.
- 116 GLESS/KUGLER/STAGNO (Fn. 21), S. 94; für Ausführungen zur Substanz- bzw. Sachwerttheorie bei der «Aneignung» anstatt vieler z. B. NIGGLI/RIEDO (Fn. 36), Art. 137 N 19 ff.; TRECHSEL/CRAMERI, in: PK (Fn. 38), Vorb. Art. 137 N 9.
- 117 Auch Bandenmässigkeit ist nicht als Qualifikation vorgesehen, was mit Blick auf Kryptowährungen bedenkenswert ist, sind Cyberkriminelle doch oft organisiert. Eine solche Ausweitung müsste aber in Bezug auf alle Vermögensdelikte überprüft werden, was den Untersuchungsgegenstand dieser Abhandlung übersteigt.
- 118 WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 172<sup>ter</sup> N 11** und **N 45**.
- 117 Auch Bandenmässigkeit ist nicht als Qualifikation vorgesehen, was mit Blick auf Kryptowährungen bedenkenswert ist, sind Cyberkriminelle doch oft organisiert. Eine solche Ausweitung müsste aber in Bezug auf alle Vermögensdelikte überprüft werden, was den Untersuchungsgegenstand dieser Abhandlung übersteigt.
- 118 WEISSENBERGER, in: **BSK-II** (Fn. 36), **Art. 172<sup>ter</sup> N 11** und **N 45**.
- 119 CORBOZ (Fn. 44), S. 339 N 1 f.; DONATSCH, Strafrecht III (Fn. 38), S. 248.
- 120 Botschaft 1991, S. 1020; FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 6**.
- 128 So die Voraussetzung gemäss Botschaft 1991, S. 987.
- 129 Vgl. z. B. FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 24**.
- 130 PLATZER (Fn. 6), S. 23; dazu bereits vorne, **Kap. C.II.2**.
- 131 Vgl. anstatt vieler DONATSCH, Strafrecht III (Fn. 38), S. 251; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 16 N 11; zu den Voraussetzungen beim Betrug bereits vorne, **Kap. D. II**.
- 132 STRATENWERTH/JENNY/BOMMER (Fn. 38), § 16 N 11.
- 119 CORBOZ (Fn. 44), S. 339 N 1 f.; DONATSCH, Strafrecht III (Fn. 38), S. 248.
- 120 Botschaft 1991, S. 1020; FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 6**.
- 119 CORBOZ (Fn. 44), S. 339 N 1 f.; DONATSCH, Strafrecht III (Fn. 38), S. 248.
- 120 Botschaft 1991, S. 1020; FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 6**.
- 121 Vgl. Botschaft 1991, S. 1022; FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 36**.
- 122 Botschaft 1991, S. 1022; vgl. auch DONATSCH, Strafrecht III (Fn. 38), S. 251.
- 123 STRATENWERTH/JENNY/BOMMER (Fn. 38), § 16 N 6.
- 124 Botschaft 1991, S. 1021; vgl. auch BGer **6S.247/2001** (10.05.2001) E. 2a; FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 11**.
- 125 FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 12**; STRATENWERTH/JENNY/BOMMER (Fn. 38), § 16 N 7.
- 126 MATTHIAS AMMANN, Sind Phishing-Mails strafbar?, AJP 2, 2006, S. 195 ff., S. 200; BGer **6S.247/2001** (10.05.2001) E. 2a; FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 11**.
- 127 So bezeichnet sie z. B. FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 18** als reine «Angst- und Absicherungsklausel».
- 128 So die Voraussetzung gemäss Botschaft 1991, S. 987.
- 129 Vgl. z. B. FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 24**.
- 130 PLATZER (Fn. 6), S. 23; dazu bereits vorne, **Kap. C.II.2**.
- 128 So die Voraussetzung gemäss Botschaft 1991, S. 987.
- 129 Vgl. z. B. FIOKA, in: **BSK-II** (Fn. 36), **Art. 147 N 24**.
- 130 PLATZER (Fn. 6), S. 23; dazu bereits vorne, **Kap. C.II.2**.

- 131 Vgl. anstatt vieler DONATSCH, Strafrecht III (Fn. 38), S. 251; STRATENWERTH/JENNY /BOMMER (Fn. 38), § 16 N 11; zu den Voraussetzungen beim Betrug bereits vorne, **Kap. D. II.**
- 132 STRATENWERTH/JENNY/BOMMER (Fn. 38), § 16 N 11.
- 131 Vgl. anstatt vieler DONATSCH, Strafrecht III (Fn. 38), S. 251; STRATENWERTH/JENNY /BOMMER (Fn. 38), § 16 N 11; zu den Voraussetzungen beim Betrug bereits vorne, **Kap. D. II.**
- 132 STRATENWERTH/JENNY/BOMMER (Fn. 38), § 16 N 11.
- 133 So Botschaft 1991, S. 1011.
- 134 Vgl. GLESS/KUGLER/STAGNO (Fn. 21), S. 93.
- 135 Man denke z. B. an die japanische Börse *Mt. Gox*; hierzu HALABURDA/SARVARY (Fn. 1), S. 7.
- 136 Vgl. GLESS/KUGLER/STAGNO (Fn. 21), S. 94.
- 133 So Botschaft 1991, S. 1011.
- 134 Vgl. GLESS/KUGLER/STAGNO (Fn. 21), S. 93.
- 135 Man denke z. B. an die japanische Börse *Mt. Gox*; hierzu HALABURDA/SARVARY (Fn. 1), S. 7.
- 133 So Botschaft 1991, S. 1011.
- 134 Vgl. GLESS/KUGLER/STAGNO (Fn. 21), S. 93.
- 135 Man denke z. B. an die japanische Börse *Mt. Gox*; hierzu HALABURDA/SARVARY (Fn. 1), S. 7.
- 136 Vgl. GLESS/KUGLER/STAGNO (Fn. 21), S. 94.
- 136 Vgl. GLESS/KUGLER/STAGNO (Fn. 21), S. 94.
- 137 In diesen Fällen wäre allerdings echte Konkurrenz zwischen dem Diebstahl des Datenträgers und dem Datendiebstahl anzunehmen; zu dieser Frage bereits vorne, Fn. 103.
- 138 FIOLKA, in: **BSK-II** (Fn. 36), **Art. 147 N 53** mit Verweis auf **BGE 129 IV 22**, 32; anderes sei anzunehmen, sofern die Datenmanipulation der Täuschung zeitlich vorgehe und überhaupt erst ermögliche.
- 139 So FIOLKA, in: **BSK-II** (Fn. 36), **Art. 147 N 61**.
- 137 In diesen Fällen wäre allerdings echte Konkurrenz zwischen dem Diebstahl des Datenträgers und dem Datendiebstahl anzunehmen; zu dieser Frage bereits vorne, Fn. 103.
- 137 In diesen Fällen wäre allerdings echte Konkurrenz zwischen dem Diebstahl des Datenträgers und dem Datendiebstahl anzunehmen; zu dieser Frage bereits vorne, Fn. 103.
- 138 FIOLKA, in: **BSK-II** (Fn. 36), **Art. 147 N 53** mit Verweis auf **BGE 129 IV 22**, 32; anderes sei anzunehmen, sofern die Datenmanipulation der Täuschung zeitlich vorgehe und überhaupt erst ermögliche.
- 139 So FIOLKA, in: **BSK-II** (Fn. 36), **Art. 147 N 61**.
- 138 FIOLKA, in: **BSK-II** (Fn. 36), **Art. 147 N 53** mit Verweis auf **BGE 129 IV 22**, 32; anderes sei anzunehmen, sofern die Datenmanipulation der Täuschung zeitlich vorgehe und überhaupt erst ermögliche.
- 139 So FIOLKA, in: **BSK-II** (Fn. 36), **Art. 147 N 61**.