

Bitcoins unter dem Hammer

- Folgt die Justiz dem
Krypto-Hype?



How to sell Bitcoin online 'fast' – Die Krypto-Auktionen der Justiz NRW

Ramon Schmitt und Ferdinand Wegener



Open Peer Review

Dieser Beitrag wurde lektoriert von: Louis Goral-Wood

Ramon studiert Jura an der Universität zu Köln mit dem Schwerpunkt Unternehmensrecht. Er arbeitet als wissenschaftlicher Mitarbeiter im Bereich Corporate | M&A. Deshalb verbindet er sein Interesse am Recht der Digitalisierung mit gesellschafts- und handelsrechtlichen Themen. Er ist Vorstandsmitglied im Legal Tech Lab Cologne.



Ferdinand ist Jurastudent an der Universität zu Köln und Head of CTRL im Legal Tech Lab Cologne. Neben dem Studium beschäftigt er sich insbesondere mit Technologien wie Blockchain, KI und IoT sowie ihren rechtlichen Implikationen.

Am 25.12.2021 tauchte auf der Webseite, welche die deutschen und österreichischen Justizbehörden für Versteigerungen nutzen,¹ zwischen den üblichen Inseraten von gebrauchten Bürostühlen und ausgedienten Office-PCs im Zehnerpack etwas Neues auf. Zwar war die Versteigerung ungewöhnlicher Objekte durch die Justiz, wie etwa einer 5-Meter-langen Motoryacht, fast Routine. Doch dieses Inserat versuchte, eine ganz neue *„Sache“* zu Geld zu machen. Die Justiz NRW versteigerte als Pionier unter den deutschen Justizbehörden erstmalig insgesamt 16.5-- (BTC), aufgeteilt in 15 Inserate. Dabei waren die Tranchen nicht gleich groß, sondern die Inserate variierten von 0.1, 0.5, 1.0 bis zu 10 BTC. Die Bitcoins stammen, wie man es aus dem Netflix-Hit *„How to sell drugs online fast“* kennt, vorwiegend aus dem illegalen Online-Handel mit Betäubungsmitteln. Als Vorteile aus den Taten wurden sie wohl nach § 73 StGB eingezogen.

¹ <https://www.justiz-auktion.de> (Stand: 20.12.2021)

1 Bitcoin

Gegenstand der Versteigerung ist 1 Bitcoin (1 BTC). Der Betrag ist gesichert auf einer behördlichen Paperwallet mit der Adresse bc1q94q983ux063vamk0mflp2fy4w4cffwa0uhnnl5.

Public Key: 

Die Übertragung erfolgt im Wege der persönlichen Übergabe der Paperwallet einschließlich des zur weiteren Verfügung notwendigen privaten Schlüssels am Dienstsitz der Staatsanwaltschaft Köln. Sollte statt der Übergabe eine elektronische Übertragung auf eine Adresse des Käufers gewünscht sein, erfolgt diese zu Lasten des Käufers zu den üblichen Transaktionsgebühren. Die Übergabe bzw. Übertragung erfolgt erst nach Buchung des Zahlungseingangs des Kaufpreises bei der Staatsanwaltschaft Köln. Der Buchungsprozess kann regelmäßig 2 Werktage in Anspruch nehmen.

Staatsanwaltschaft Köln
Zentral- und Ansprechstelle Cybercrime
Nordrhein-Westfalen - ZAC NRW

JUSTIZ AUKTION

1 Bitcoin

Auktion ID 147523

Startgebot: 42.400,00 €

Aktuelles Gebot: **52.641,50 €**

[Zum Bieten bitte einloggen](#)

[Seite ausdrucken](#)
[Gebote anschauen](#)

[Auktion beobachten](#)
[Auktion weiterempfehlen](#)

Höchstbietender	A**h**5
Anzahl Gebote	20
Anzahl Klicks	2771
Anzahl Beobachter	49

Abgebildet ist eines der 15 versteigerten Paper-Wallets. Dieses Inserat enthält eine Auktion mit einem Bitcoin.

Dabei hat den Tätern auch das Mantra der Krypto-Szene „**Not your keys – not your coins**“ nicht viel genützt: Sie haben ihre Private Keys, die Zugang zu ihren Bitcoin-Wallets gewähren, nicht gut genug vor dem Zugriff der Justizbehörden geschützt. Die Keys konnten bei der Festnahme der Täter – entweder unverschlüsselt in digitaler Form oder physisch – sichergestellt werden, sodass die Justiz Zugang zu den Wallets erhielt. Diese Nachlässigkeit ermöglichte es der Justiz, nachdem die Urteile gegen die Täter rechtskräftig geworden waren, die Bitcoins zugunsten der Staatskasse zu liquidieren.

Dies erfolgte aber, anders als bei einem regulären Krypto-Nutzer, nicht einfach direkt über eine Krypto-Börse, sondern verlangte ein komplizierteres Vorgehen. Die Bitcoins wurden auf der Plattform der Justiz in mehreren Auktionen angeboten. Die Behörde entschied sich für diesen Weg aufgrund von rechtlichen Gesichtspunkten: Wären die eingezogenen Tokens auf einer externen Krypto-Börse versteigert worden, hätte es sich nicht mehr um eine öffentliche Versteigerung² gehandelt, sondern es wäre ein freihändiger Verkauf gewesen. Ein solcher freihändiger Verkauf unterliegt nach § 64 StVollstrO besonderen Voraussetzungen. So darf gemäß § 64 VI StVollstrO beispielsweise kein Verkauf an Angehörige der Justiz erfolgen und nach § 64 V StVollstrO darf auch nicht an die Täter und Teilnehmer selbst verkauft werden. Bei dem Verkauf über reguläre Krypto-Börsen, wenn auch schneller und mit mehr liquiden Käufern, kann aufgrund der Pseudonymität der Nutzer die Erfüllung dieser Voraussetzung nicht ohne hohen Aufwand sichergestellt werden.³

A. Was haben wir von der ersten Krypto-Auktion der deutschen Justiz erwartet?

Als erster solcher Verkauf durch die deutsche Justiz stellten wir uns deshalb die Frage, wie die Resonanz der Öffentlichkeit – insbesondere der potenziellen Käufer – sein würde und wie sich diese auf den erzielten Verkaufspreis auswirken würde.

² Eine Legaldefinition findet sich in § 383 III S. 1 BGB. Näheres zu den Voraussetzungen einer öffentlichen Versteigerung: *Ulrici*, in: *BeckOGK, BGB*, Stand: 01.05.2021, § 383 Rn. 69 – 73; sowie zum Anwendungsbereich der zivilrechtlichen Definition: *ebd.* Rn. 11.

³ Näheres zu Bitcoin im Strafverfahren, insbesondere auch zur Sicherstellung und Notveräußerung: *Goger*, *MMR* 2016, 431 ff.

Dieser Beitrag wurde mithilfe einer Presseanfrage bei der Zentral- und Ansprechstelle für Cybercrime (kurz ZAC NRW) erstellt. Die ZAC NRW ist eine Hauptabteilung der Staatsanwaltschaft Köln, die auf die Bekämpfung von Kriminalität unter Nutzung von und gegen IT-Systeme spezialisiert ist. Dies umfasst kriminelle Aktivitäten von Betrug unter Nutzung des Internets, Cybercrime im engeren Sinne wie Datenhehlerei § 202d StGB oder Computerbetrug § 263a StGB, über Hasspostings auf Social Media bis zur Verbreitung kinderpornografischer Inhalte. Die ZAC NRW stellt dabei die bundesweit größte solche Einheit dar. Wir danken der ZAC NRW, insbesondere ihrem Pressesprecher Dr. Christoph Hebbecke, ganz herzlich für die schnelle und vollumfängliche Beantwortung unserer Fragen.

Dazu hatten wir vor dem Auslaufen der Auktion mehrere Hypothesen aufgestellt, welche sich an unterschiedlichen Szenarien orientierten:

I. Hypothese: Der Verkaufspreis wird deutlich unter dem aktuellen Marktwert liegen.

Zunächst haben wir erwartet, dass der Preis deutlich hinter dem Marktwert im Zeitpunkt des Auktionsschlusses zurückbleiben wird. Dafür sprach, dass die verwendete Auktionsplattform durch das Anbieten der Bitcoins wie eine Krypto-Börse funktioniert, allerdings ohne den etablierten Kundenstamm und ohne die Bekanntheit. Im Hinblick auf die Zahl der angebotenen Bitcoins – 16.5 BTC mit einem Marktwert bei Auktionsbeginn von ca. 890.850 € – schien fraglich, ob die begrenzte Anzahl an Kunden dieses Angebot mit einer angemessenen Nachfrage und der dazugehörigen Liquidität decken könnten. Extrem potenziert wird dieses Missverhältnis durch das Inserat in Höhe von 10 BTC, was nicht nur ganze 60 % vom Gesamtvolumen der Inserate ausmachte, sondern auch eine verschwindend kleine Gruppe potenzieller Kunden ansprach. Der Käufer müsste über einen Kontostand von etwa

539.910 € frei verfügen können und würde durch sein erfolgreiches Gebot direkt zum stolzen Inhaber eines der 0,33 % reichsten Bitcoin-Wallets werden;⁴ hätte es also in den 1 %-Club geschafft.

II. Hypothese: Der Preis wird praktisch dem Marktwert entsprechen.

Das Problem der ersten Hypothese ist, dass Bitcoin über einen hoch liquiden Markt verfügt und jederzeit nach dem Kauf bei der Justiz-Auktion auf einer regulären Krypto-Börse verkauft werden kann. Solange es mindestens zwei liquide Bieter gibt, würden somit beide weiter Gebote abgeben, bis der aktuelle Marktwert erreicht ist. So böten sich nur wenige Chancen für Arbitrage⁵.

Gegen die erste Hypothese sprach auch, dass die Inserate von der Justiz mit Mindeststartgebots versehen waren, die bereits 80 % des aktuellen Marktwerts bei Erstellung der Auktion entsprachen. Dies stieß bei einigen Kaufinteressenten auf Verwunderung und hätte bei den üblichen hohen Schwankungen im Tageskurs schnell zu einem sehr unattraktiven Inserat führen können. Die Justiz hatte aber Glück: Der Bitcoin-Preis blieb über die Laufzeit der Auktion von 48 Stunden relativ stabil.

Üblicherweise laufen Auktionen auf der Website deutlich länger, meist mehrere Wochen. Nach Justiz-Angaben rechnete man bei den Bitcoin-Auktionen aber aufgrund der Preisvolatilität damit, dass erst kurz vor Auktionsende die Gebote eingehen werden. Vergleichbar erscheint die Auktion der Justiz zunächst mit Auktionen auf der Online-Plattform **eBay**. Dort gibt der Ersteller der Auktion in Einklang mit den AGB schon bei Einstellen des Inserats ein verbindliches Angebot im Sinne von § 145 BGB ab. Dieses richtet sich an denjenigen Bieter, der innerhalb der Auk-

tionslaufzeit, als Annahmefrist im Sinne von § 148 BGB, das Höchstgebot abgibt.⁶ Das Gebot des potenziellen Käufers ist dabei selbst eine rechtsverbindliche Willenserklärung im Sinne der §§ 145, 147 BGB, meist unter der aufschiebenden Bedingung nach § 158 I BGB bei Fristablauf das Höchstgebot zu sein.

Die Justiz-Auktionen sind aufgrund ihrer AGB ähnlich gelagert: Nach Nummer 4 lit. e) der Allgemeine Versteigerungsbedingungen der Justiz-Auktion⁷ ist der Bieter an sein Gebot gebunden, bis es durch ein höheres Gebot erlischt. Damit trägt der Bietende ab der Abgabe des Gebots das Risiko für abrupte Bitcoin-Preisabstürze, sodass er die Zeit zwischen Abgabe des Gebots und dem Zeitablauf der Auktion möglichst gering halten möchte. Daher müsste sein Gebot nah am Marktwert liegen.

Gegen die Hypothese, dass die Bitcoins zum Marktpreis versteigert werden, sprechen aber die Modalitäten der Auktion: Nach Ende der Auktion dauert es nach Justiz-Angaben bis zu 48 Stunden bis der Höchstbietende Zugriff auf die Bitcoins erhält – wahlweise durch Videoidentifizierung und digitalem Transfer der Bitcoins oder Abholung des Paper-Wallets⁸ bei der Behörde vor Ort. In diesem Zeitraum trägt der Käufer das gesamte Risiko für Preisschwankungen, ohne Vorteile daraus zu ziehen: Hätte der Käufer auf einer regulären Krypto-Börse gekauft, würden ihm seine Bitcoins direkt zur Verfügung stehen. Steigt der Preis zwischen Auktionsende und Abholung, ändert sich für unseren Käufer nichts, außer dass er nicht in der Lage ist, seinen Gewinn durch den Verkauf der ersteigerten Bitcoin vor Abholung zu sichern. Sinkt der Preis allerdings, so kann er auf einer Krypto-Börse verkaufen, um seine Verluste zu minimieren, während ihm bei der Auktion nichts anderes übrig bleibt, als die Abholung abzuwarten.

Daher müsste eigentlich damit gerechnet werden, dass dieses zusätzliche Preisrisiko für den Käufer zu Abschlägen bei den erzielten Verkaufspreisen führen würde.

⁴ Vergleiche hierzu *Bitcoin Distribution Chart*, abrufbar [hier](#) (Stand: 20.12.21).

⁵ Arbitrage ist die gewinnorientierte Nutzung von Kursdifferenzen bei demselben Asset zwischen unterschiedlichen Handelsplattformen, indem der Marktteilnehmer das Asset auf der Plattform mit dem niedrigeren Kaufpreis einkauft und sofort mit Gewinn auf der Plattform mit dem höheren Preis verkauft. Die Differenzen im Marktpreis ergeben sich aus den leicht verschiedenen Gegebenheiten von Angebot und Nachfrage zwischen den jeweiligen Plattformen.

⁶ BGH NJW 2017, 468 ff; BGH NJW 2005, 53 ff.

⁷ Allgemeine Versteigerungsbedingungen der Justiz-Auktion (DE), abrufbar [hier](#) (Stand: 31.12.2021).

⁸ Paper-Wallets sind physische Dokumente, etwa Stücke von Papier, welche jeweils den Private Key und die Wallet-Adresse enthalten. In Abbildung 3 ist der öffentliche Teil eines der Paper-Wallets, also die Wallet-Adresse, abgebildet, welches die Justiz für die Auktion verwendete. Die zugehörigen Private Keys erhielten die Käufer durch Abholung. Jedes Inserat erhielt ein eigenes Paper-Wallet.

WalletExplorer.com: smart Bitcoin block explorer

Search address/txid/wallet id/firstbits

Wallet [338bee3dde] ([show wallet addresses](#))

Displaying wallet [338bee3dde], of which part is address bc1qugj09uc4aj757dhf95urzgt4z69sx3z9gz6r2u. [Show only address bc1qugj09uc4aj757dhf95urzgt4z69sx3z9gz6r2u](#)

Page 1 / 1 (total transactions: 1) [Download as CSV](#)

date	received/sent	balance	transaction
2021-08-05 14:06:31	[3d3b3aa211] +0.1	0.1	0b8f78ef94e9f4ae6b3c...

Page 1 / 1 (total transactions: 1) [Download as CSV](#)

Updated to block 714689 (2021-12-18 18:59:05). All times are in UTC and taken from block time.
[FAQ: What is on this site?](#) | [Privacy Notice](#)
Want to trace bitcoins with even better tool? Check [Chainalysis.com](#). It has even better detection of wallets, more wallet names, address metadata, graphic visualization of links between wallets and so on. Author of [WalletExplorer.com](#) now works there as analyst and programmer :-)

Abgebildet ist die Wallet-Adresse eines der verkauften Inserate mit 0.1 BTC. Hier ist zu erkennen, dass sich die 0.1 BTC weiterhin auf dem Wallet befinden und noch nicht vom Erwerber auf ein anderes Wallet transferiert wurden.

B. Was ist wirklich passiert und warum?

Als am Mittag des 27.10.2021 die Auktionen ausliefen, konnte sich das Ergebnis für den staatlichen Haushalt sehen lassen: In vierzehn von fünfzehn Fällen stand am Ende ein Auktionsergebnis über dem Marktwert fest. Dieses Ergebnis verwunderte uns und widersprach unseren Hypothesen.

Das höchste Gebot für eine Tranche von 0.1 BTC lag sogar 33 % über dem aktuellen Marktpreis. Was könnten die Gründe dafür sein?

Der hohe Preis zeigt klar, dass hier das Kaufinteresse über den wirtschaftlichen Nutzen hinausgehen muss. Wirtschaftlich erhält man mit der Justiz zwar eine seriöse Schuldnerin, von der man die gekauften Bitcoins auch mit Sicherheit erhält. Dies mag in der Anfangszeit von Bitcoin mit Börsen wie **Mt. Gox** noch ein valides Argument gewesen sein, doch mit einer ausgeprägten Landschaft an etablierten Krypto-Börsen gehört dieses Schuldnerisiko der Vergangenheit an.

Als Motivation bleibt nur noch der Status der versteigerten Bitcoin als ‚**Novelty Items**‘. Es handelt sich schließlich um die erste Krypto-Versteigerung durch die Justiz in Deutschland und damit um ein historisches Ereignis. Dafür spricht insbesondere, dass bei den 15 Inseraten nur zwei Käufer den bequemen Weg der digitalen Übertragung mittels Videoidentifizierung für die Abholung ihrer Bitcoins wählten. Die übrigen 13 Käufer machten sich auf die beschwerliche Reise quer durch Deutschland bis zur Behörde in NRW, um dort ihre Bitcoins auf dem physisch ausgedruck-

ten Paper-Wallet der Justiz entgegen zu nehmen. Das zeigt, dass die Käufer keine Mühen scheuten, um ein gegenständliches Andenken an ihren virtuellen Einkauf zu erhalten. Die ausgestellten Paper-Wallets der Justiz haben sicherlich in Krypto-Kreisen einen Sammlerwert, wenn nicht sogar einen eigenständigen Wiederverkaufswert – eine Art ‚**Reverse-NFT**‘.

Für den Status der Paper-Wallets als Sammlerstück spricht auch, dass für die geringeren Mengen von Bitcoins prozentual mehr über dem Marktpreis bezahlt wurde, wobei die extremsten Abweichungen vom Marktwert immer bei den kleins-

ten Tranchen von 0.1 BTC auftraten. Außerdem befinden sich hier die erworbenen Bitcoins teilweise noch in den ursprünglichen Paper-Wallets, während diese bei den größeren Mengen an Bitcoins oftmals aus Sicherheitsgründen oder zum Weiterverkauf auf andere Wallets transferiert wurden. Gegen die weitere Aufbewahrung auf dem Paper-Wallet spricht insbesondere, dass dieses durch die Behörden erstellt wurde und so mutmaßlich mindestens ein Mitarbeiter der Justiz jederzeit vollen Zugriff auf den Inhalt des Wallets mittels des Private Key hat, der dann später dem Käufer übergeben wird. Andere Gründe als ein ‚*Novelty-Bonus*‘ der verkauften Bitcoins sind nicht erkennbar. Insbesondere stellt die Behörde, wie eine normale Krypto-Börse, die Identität der Käufer mittels eines *KYC*-Verfahrens (*Know-Your-Customer*) fest. So werden auch keine Geldwäscherichtlinien durch den Auktionskauf umgangen, die beim Kauf eines Paper-Wallets etwa über *eBay* – vorbehaltlich dessen, dass sie dort überhaupt anwendbar wären – auf der Strecke bleiben könnten. Anderes war bei einer Auktion der Justiz auch nicht zu erwarten.

C. Ein Blick in die Zukunft der Krypto-Auktionen der Justiz

Unsere Prognose für zukünftige Versteigerungen durch die Justiz orientiert sich trotzdem an unseren aufgestellten Hypothesen. Der ersten Krypto-Versteigerung kommt noch ein starkes Öffentlichkeits- und Medieninteresse und somit ein ‚*Novelty-Faktor*‘ zugute. In Zukunft wird dieser Effekt jedoch merklich abflauen. Dies wird dazu führen, dass der Preis bei den Auktionen deutlich hinter dem Marktwert zurückbleibt, solange der Kundenstamm durch die Plattform begrenzt ist und das Preisrisiko durch – für die schnelllebige Krypto-Szene erstaunlich lange – Abholzeiten beim Käufer liegt.

The screenshot shows the interface of WalletExplorer.com. At the top, it says "WalletExplorer.com: smart Bitcoin block explorer". There is a search bar with the placeholder text "Search address/txid/wallet id/firstbits". Below that, it displays "Wallet [5951365f84] (show transactions)". Underneath, it says "Page 1 / 1 (total addresses: 1)". A table follows with the following data:

address	balance	incoming txs	last used in block
bc1qs484tw29e739tekxc6ldhghr0gn3e856vdgmr2	102.1482168	1	694320

Below the table, it says "Page 1 / 1 (total addresses: 1)".

Dies ist das mutmaßliche Behörden-Wallet, welches [hier](#) (Stand: 31.12.2021) abrufbar ist.

Diese Nachteile wurden bereits bei dem Inserat mit 10 BTC evident: Die 10 BTC waren die einzige Tranche, die leicht unter Marktwert verkauft wurde. Hier trifft ein kleiner potenzieller Kundenkreis auf ein vielfach erhöhtes Preisrisiko, da negative Preisschwankungen bei Bitcoin bis zur Abholung für den Käufer gleich in 10-facher Höhe spürbar werden, wenn man dies mit einer Tranche von 1 BTC vergleicht.

Verfolgt man die Spur der Transaktionen von den Paper-Wallets zurück an ihren Ursprung,⁹ stößt man auf ein Wallet, das aller Wahrscheinlichkeit nach den Behörden zugeordnet werden kann und auf welchem – seit dem Verkauf der 16.5 BTC – noch ‚*etwa*‘ 102.1482168 BTC verbleiben.

Diese wurden sehr wahrscheinlich ebenfalls im Zusammenhang mit Straftaten sichergestellt. Dementsprechend ist damit zu rechnen, dass es noch weitere Auktionen geben wird. Sobald die jeweiligen Urteile zulasten der mutmaßlichen Täter rechtskräftig geworden sind, werden die Bitcoins wohl in gleicher Weise versteigert.




⁹ Aufgrund der Transparenz der Bitcoin-Blockchain können Wallets auf ihren Inhalt und ein- und ausgehende Transaktionen überprüft werden. Bei den Inseraten der Justiz war der Public Key der Paper-Wallets, also die Wallet-Adresse, erkennbar.

WalletExplorer.com: smart Bitcoin block explorer

Search address/txid/wallet id/firstbits

Wallet [860a6e61be] [\(show wallet addresses\)](#)

Page 1 / 1 (total transactions: 2) [Download as CSV](#)

date	received/sent	balance	transaction
2021-08-05 12:30:44	-117.648261  [b81559dafb] -1.  [6e787c66d0] <i>(-0.00000329) fee</i>	0.	00a1c19ed27444ab6429...
2021-08-03 10:39:05	 [7808a640ba] +118.64826429	118.64826429	c763fad6c8c4bcd86516...

Page 1 / 1 (total transactions: 2) [Download as CSV](#)

Hier ist die Erstellung eines Paper-Wallets durch die Behörde erkennbar. Hierfür wurden auf dieses Wallet ca. 118.6 BTC transferiert. Daraufhin wurde 1 BTC auf eine neue Adresse gebucht, woraus dann ein Paper-Wallet entstanden ist. Die übrigen ca. 117.6 BTC wurden dann auf eine neue Adresse transferiert. Verfolgt man die Wallet-Adresse, die hier die 118.6 BTC überwiesen hat, zurück, so kommt man schnell zu einem Wallet, das viele kleine Zahlungsein- und -ausgänge verbucht. Hierbei dürfte es sich um das Wallet eines Täters handeln, der im Internet mehrfach Betäubungsmittel verkaufte.

Das mutmaßliche Behörden-Wallet findet sich [hier](#) (Stand: 30.12.2021).

Die Transparenz der Bitcoin-Blockchain ist hier mehr Fluch als Segen für die Justizbehörden: Aus den auf der Blockchain verzeichneten Daten können Informationen abgeleitet werden, welche die Behörden wohl eher nicht der Öffentlichkeit preisgeben wollen. Insbesondere sollte die Wallet-Adresse der inserierten Paper-Wallets nicht für alle Auktionsteilnehmern einsehbar gemacht werden, sondern zusammen mit dem Private Key nur dem letztendlichen Käufer mitgeteilt werden. Zwar können Kaufinteressierte mittels der Wallet-Adresse verifizieren, dass das Wallet tatsächlich die von der Justiz angegebene Menge an Bitcoins enthält. Allerdings scheint das Risiko betrügerischer Aktivitäten durch die Justiz doch eher gering.

Dementsprechend können eine ganze Reihe an Rückschlüssen aus den veröffentlichten Wallet-Adressen gezogen werden: Zunächst kann das Behörden-Wallet gefunden werden, von dem die auktionierten Bitcoins ursprünglich stammen. Damit lässt sich zudem feststellen, über welche Menge an Bitcoins die Justiz verfügt. Aber auch die Wallets der Täter können auf diesem Weg ausfindig gemacht werden. Anhand des Datums der letzten Transaktionen auf diesen Wallets und des Datums des Transfers der Bitcoins auf das Behörden-Wallet kann außerdem abgeschätzt werden, wann ungefähr die Festnahme des Täters erfolgte und wann das Urteil gegen ihn rechtskräftig wurde. Verfolgt man die Blockchain noch weiter, lassen sich auch Informationen über die Kunden der Drogendealer gewinnen, etwa Kauffrequenz und Umsatzhöhe. Durch die Nutzung von Applikationen wie **Chainalysis**, die Daten aus der Blockchain und anderen Quellen, etwa **KYC**-Verfahren, kombinieren, können noch weit mehr Informationen erschlossen werden.¹⁰ Die Justiz sollte daher die Wallet-Adressen nur Käufern preisgeben oder – noch besser – die Bitcoins vor der Erstellung der Paper-Wallets durch einen Bitcoin-Mixer laufen lassen, um ihren Ursprung zu verschleiern. Bitcoin-Mixer bündeln eine Reihe von Transaktionen mit unterschiedlichen Quell-Wallets auf einem oder mehreren Zwischen-Wallets und versenden sie erst von dort an die geplanten Zieladressen. So kann ein Dritter nicht mehr nachvollziehen, welches der Wallets der Ausgangspunkt der Bitcoins war.

¹⁰ Dies sind Applikationen wie *Chainalysis*, das unter anderem vom *United Nations Office on Drugs and Crime* zur Informationsgewinnung genutzt wird, abrufbar [hier](#). Der Programmierer des hier verwendeten Blockchain-Explorer-Tools *WalletExplorer.com* arbeitet nun auch für *Chainalysis* und verweist auf die vielen Möglichkeiten zur Nutzung von Metadaten, siehe Abbildung 4.

Die Justiz sollte für künftige Auktionen möglichst viele Inserate mit möglichst niedrigen Bitcoin-Beträgen erstellen. Die Höhe eines sinnvollen Mindestbetrags bemisst sich dabei neben dem aktuellen Marktpreis auch nach der Höhe der Transaktionsgebühren zur Erstellung der Paper-Wallets. Dieser Betrag kann dennoch problemlos auch unter 0.1 BTC liegen. Tranchen von 1 BTC oder sogar 10 BTC sollten beim jetzigen Marktwert von Bitcoin auf jeden Fall vermieden werden. Die Angaben der Justiz, wonach die größeren Tranchen aufgrund des hohen Aufwands bei der Erstellung von vielen separaten Paper-Wallets gewählt wurden, sind jedenfalls technisch nicht nachvollziehbar und gehen bei niedrigeren Verkaufspreisen zulasten des Staatshaushalts und damit auch zulasten des Steuerzahlers.

Referendariat bei der ZAC NRW

Sollte der Beitrag dein Interesse an der Arbeit der ZAC NRW geweckt haben, so weisen wir gerne auf die Möglichkeit einer Referendariatsstelle hin. Ansprechpartner für die Referendariatsplätze ist Oberstaatsanwalt Elmar Köstner, welcher unter Elmar.Koestner@sta-koeln.nrw.de erreichbar ist.

Zurück zum dynamischen
Inhaltsverzeichnis?

Zum dynamischen
Inhaltsverzeichnis

CTRL

Cologne Technology & Law
Forum & Law
view



+

Hier geht es zur ganzen Ausgabe



Dort findest Du in 19 Beiträgen alles von Datenschutz bei Connected Cars über Krypto-Auktionen bis hin zum Artificial Intelligence Act und Legal Tech.