

## Stichwortverzeichnis zu technischen Begriffen

|                                   |  |
|-----------------------------------|--|
| Access-Blocking                   | – bezeichnet eine Zugangsbeschränkung von einzelnen Inhalten im Internet, die technisch in verschiedener Weise umgesetzt werden kann und in der juristischen Literatur häufig auch als „Sperrmaßnahme“ bezeichnet wird.                            |
| Bloom-Filter-Attack               | – Verknüpfung einer IP-Adresse zu einer oder mehreren Bitcoin-Adressen durch Abfrage bei dem von SPV-Clients verwendeten Bloom-Filtern, die einen schnellen Abgleich ermöglichen, ob ein bestimmter Datensatz in einer Datenstruktur enthalten ist |
| Candidate-block                   | – Datenblock, der von einem <i>miner</i> erstellt wurde, aber noch nicht vom Netzwerk als Teil der Blockchain bestätigt wurde  |
| Classifier                        | – Algorithmus, der typischen Eigenschaften von bestimmtem Transaktionsverhalten ermittelt  |
| Clustering                        | – Auswertung von großen Datensätzen, um Ähnlichkeiten und Unterschiede aufzudecken   |
| Denial-of-Service (kurz: DoS)     | – Nichtverfügbarkeit eines Netzwerks; regelmäßig auf Grund von Überlastung durch zu viele Anfragen   |
| Distributed-Ledger (-Technologie) | – „verteiltes Kontobuch“ (öffentlich), dezentral geführtes Register  |
| DNS-Blockade                      | – Sperrmaßnahme, die am <i>Domain Name System</i> ansetzt. Bei bestimmten Domain-Namen findet keine Weiterleitung mehr an die jeweilige IP-Adresse mehr statt  |
| Domain Name System                | – Zentraler Server, der für die Kommunikation im Internet bestimmte Domain-Namen einzelnen IP-Adressen zuordnet  |
| Double Spending                   | – Doppelte Ausgabe der gleichen Werteinheit  |
| Entität                           | – Person oder Organisation, die über eine oder mehrere Bitcoin-Adressen verfügen kann  |
| Ethereum                          | – Weiterentwicklung der Bitcoin-Blockchain<br>– Erlaubt Nutzern, eigene Anwendungen – insbesondere <i>Smart Contracts</i> – auf ihr abzulegen und ist entwicklungs-<br>offen   |
| Exit-Relay                        | – Server im Tor-Netzwerk, über den auf das tatsächliche Kommunikationsziel zugegriffen wird  |

|                                   |   |
|-----------------------------------|---|
| Guard-Relay                       | – Server im Tor-Netzwerk, mit dem sich der Tor-Nutzer zuerst verbindet  |
| Hashfunktion                      | – Rechnerische Funktion, durch die eine Zeilenfolge beliebiger Länge in eine Zeichenfolge mit einheitlicher Länge dargestellt wird  |
| Hashwert                          | – Ergebnis einer <i>Hashfunktion</i>  |
| IMSI-Catcher                      | – Ermittlungsinstrument, mit dem eine virtuelle Funkzelle simuliert werden kann und so die IMSI oder IMEI eines bestimmten Gerätes erhoben werden kann  |
| Input                             | – Absendeadresse einer Bitcoin-Transaktion  |
| Internet-of-Things<br>(kurz: IoT) | – Sammelbegriff für Technologien, die es ermöglichen, dass Gegenstände miteinander kommunizieren  |
| IP-Adressen-Sperre                | – Weiterleitung von Telekommunikation wird dadurch verhindert, dass bestimmte IP-Adressen aus den Routing-Tabellen, die zur Weiterleitung von Kommunikation eingesetzt werden, gelöscht werden                            |
| Labelling                         | – Kategorisierung einer Bitcoin-Entität   |
| Memory-pool                       | – Pool der Transaktionsnachrichten, die noch nicht in die Blockchain aufgenommen wurden   |
| Middle-Relay                      | – Server im Tor-Netzwerk, der zwischen den Beginn und das Ende der Kommunikation geschaltet wird (siehe Guard- und Exit-Relay)  |
| Miner                             | – <i>Node</i> , der die Blockchain fortschreibt   |
| Node                              | – Knotenpunkt von Kommunikationsnetzen<br>– In dezentralen Kommunikationsnetzen läuft die Kommunikation darüber, dass die <i>nodes</i> die Kommunikation an die anderen <i>nodes</i> verteilen                            |
| Output                            | – Empfangsadresse einer Bitcoin-Transaktion   |
| Peer-to-Peer-<br>Netzwerk         | – Dezentrales Kommunikationsnetzwerk über das Internet, in dem die Kommunikation nicht über zentrale Knoten läuft, sondern zwischen den Teilnehmern direkt erfolgt  |
| Private und<br>Public key         | – Asymmetrisches Schlüsselpaar mit dem Bitcoin-Nutzer im Netzwerk aktiv werden<br>– <i>Public key</i> dient zum Empfang von Transaktionen<br>– <i>Private key</i> dient zur Authentifizierung von Transaktionsnachrichten |
| Route                             | – Ablauf der Netzwerkverbindung, über die die Kommunikation im Tor-Netzwerk abläuft   |

|  |   |
|--|---|
| Simplified Payment Verification<br>(kurz: SPV) | – Vereinfachte Transaktionsbestätigung zur Datenreduzierung   |
| Smart Contract                                 | – Software, die rechtlich relevante Handlungen in Abhängigkeit von digital überprüfbaren Ereignissen steuert, kontrolliert und/oder dokumentiert <sup>1963</sup>  |
| Token  | – Ausschließlicher, einzigartiger und nicht vervielfältigbarer Eintrag in einer Datenbank <sup>1964</sup><br>– Kann Forderungen und Rechte abbilden   |
| Tor-Netzwerk/<br>-Browser                      | – Verschleierung von IP-Adressen durch mehrfache Weiterleitung der Kommunikation  |
| Unspent transaction output                     | – Nicht weitergeleitete Transaktionen   |
| URL-Sperre                                     | – Sperrmaßnahme, bei der Anfragen von bestimmten URLs nicht weitergeleitet werden   |
| Vehicular Ad Hoc Network<br>(kurz: VANET)      | – Kommunikationssystem für KfZ, um andere Verkehrsteilnehmer über Verkehrsverhältnisse zu informieren   |
| Wallets  | – Digitale Brieftasche, in der die <i>public</i> und <i>private keys</i> eines Nutzers gespeichert werden<br>– Häufig von Nutzern verwendet, da sie häufig mehr als nur einen <i>public key</i> verwenden |
| Web-Crawler                                    | – Algorithmus, der das Internet oder bestimmte Internetseiten automatisch nach vorher festgelegten Daten durchsucht   |
| Webtracker                                     | – Analyseprogramm, das das Nutzungsverhalten von Internetnutzern auswertet  |

---

1963 Kaulartz/Heckmann, CR 2016, 618 (618).

1964 Kaulartz/Matzke, NJW 2018, 3278 (3278).

