2. Begriffserläuterung

Worte werden grundsätzlich erst durch deren Interpretation und Auslegung für andere Menschen zugänglich, wobei stets das Risiko besteht, dass Sprache unterschiedlich wahrgenommen wird.

Je neuer, unerforschter und damit weniger bekannt ein Thema ist, desto höher ist die Gefahr, dass unter bestimmten Begrifflichkeiten etwas anderes verstanden wird, da es noch kein allgemein gefestigtes Verständnis der jeweiligen Termini gibt. Jüngst kritisierte erst *Gassebner,* dass es im Bereich der Blockchain-Technologie an einer einheitlichen Terminologie fehlt, wodurch es zu unterschiedlichen Auslegungen des anwendbaren Rechts käme und immense Rechtsunsicherheiten entstehen würden.[23]

ME ist es – wie *Gassebner* [24] im Ergebnis völlig richtig ausführt – für die eingehende juristische Auseinandersetzung mit einem Thema unabdingbar, dass den jeweiligen Begriffen dasselbe (Grund-)Verständnis beigemessen wird. Daher werden nachfolgend für die vorliegende Arbeit wichtige Begriffe aufgegriffen und erklärt sowie – soweit notwendig – voneinander abgegrenzt.

Dieses Kapitel soll daher ergänzend zum Glossar, welches als Nachschlagewerk dienen soll, besonders wichtige Begrifflichkeiten der vorliegenden Arbeit herausstreichen und genau(er) darlegen.

2.1. Blockchain

Als Ursprung der Blockchain-Technologie wird allgemein die Kryptowährung Bitcoin durch *Satoshi Nakamoto* (Pseudonym)[25] betrachtet. Die Bitcoin-Blockchain wurde von Nakamoto als Lösung des Problems der Mehrfachausgabe (*Double Spending*[26]) in einem dezentralen Netz gesehen, wodurch eine zentrale Stelle überflüssig würde. Die (notwendige) Kontrolle könnte durch die Blockchain dezentral erfolgen.[27]

Im allgemeinen Sprachgebrauch wird stets von „der Blockchain" oder „der Blockchain-Technologie" gesprochen[28], wobei es „*die* [eine] *Blockchain*" nicht gibt. Tatsächlich ist es so, dass etliche Blockchains in unterschiedlichen Ausprägungen existieren, die – abhängig

23 *Gassebner*, ecolex 2018, 801.
24 Im Ergebnis wohl *Gassebner* in seinen einleitenden Ausführungen zu *Gassebner*, ecolex 2018, 801.
25 Es ist unklar, ob Satoshi Nakamoto eine Person ist oder eine Gruppe von Personen. In der vorliegenden Arbeit wird derart verfahren, dass jeweils von Satoshi Nakamoto als einer natürlichen Person ausgegangen wird.
26 Siehe dazu unter Punkt 2.7.
27 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2.
28 ZB sprechen folgende Artikel in den Medien lediglich von „der Blockchain": *diePresse*, Blockchain könnte Anleihegeschäft revolutionieren; *diePresse*, Credit Suisse springt auf den Blockchain-Zug der UBS auf; *Blockchain Austria*, Blockchain.

von dem zugrundeliegenden Programmcode – den Nutzern der jeweiligen Blockchain unterschiedliche Anwendungsgebiete eröffnen.[29] Dennoch ist es mE nicht (völlig) unberechtigt, vereinfachend von „der Blockchain" oder „der Blockchain-Technologie" zu sprechen, da die charakteristischen Eigenschaften der derzeit dominierenden Blockchains[30] vergleichbar[31] sind.[32] Es wird daher für die vorliegende Arbeit ebenfalls vereinfacht stets von „*der Blockchain*" oder „*der Blockchain-Technologie*" gesprochen, wohlwissend, dass es nicht „*die Blockchain*" gibt.[33]

> Eine Blockchain besteht aus einer Vielzahl an miteinander verknüpften, validierten Blöcken, die auf der Blockchain durchgeführte und bestätigte Transaktionen enthalten. Es gibt keinen zentralen Speicherort der Blockchain, sondern es sind Kopien der Blockchain auf viele verschiedene, dezentrale Rechner aufgeteilt (dezentrale Datenbank). Die einzelnen, validierten Blöcke der Blockchain sind, bis zu dem ersten Block der jeweiligen Blockchain zurück, stets mit dem vorangegangenen Block verlinkt, wodurch eine [beinahe] unveränderliche Transaktionshistorie entsteht. Folglich sind die auf der Blockchain gespeicherten Datensätze gegen Manipulationen gesichert; jede Änderung eines Blocks wird transparent erfasst.[34]

29 So zB *Freitag*, CFOaktuell 2018, 59.

30 Unter dominierenden Blockchains werden in der vorliegenden Arbeit insbesondere die Bitcoin- und die Ethereum-Blockchain verstanden.

31 Freilich könnte in diesem Zusammenhang argumentiert werden, dass bspw derzeit „aufstrebende" „**Blockchains" – wie IOTA – eine andere Technologie verfolgen** und die Ergebnisse einer juristischen Analyse, deren Basis die Bitcoin-/Ethereum-Blockchain ist, nicht auf diese „Blockchains" übertragbar sind. Einer solchen Argumentation wäre mE nur teilweise zuzustimmen. Vorweg kann festgehalten werden, dass die IOTA „Blockchain" derzeit mangels Bekanntheit und (ausreichend) kommerzieller Nutzung wohl ohnehin noch keine „dominierende" „Blockchain" ist, wobei sich das aufgrund des primär ins Auge gefassten Anwendungsgebiets der IOTA-„Blockchain", nämlich das viel umworbene „Internet of Things", schnell ändern könnte (vgl dazu zur Einsatzmöglichkeit von IOTA im Bereich des IoT zB *IOTA*, Industrial IoT; *Heumüller/Richter*, Mikrotransaktionen im IoT per IOTA). Fraglich ist, ob die IOTA-„Blockchain" überhaupt eine „Blockchain" in dem Sinne dieses Buches ist. Denn die IOTA-„Blockchain" verfügt über keine „Blöcke", in denen die Transaktionen gespeichert werden, sondern diese Funktion wird mit Hilfe der Technologie des „Tangle" erfüllt (vgl dazu zB *Popov*, The Tangle [„IOTA WHITEPAPER"] 1 ff). Folglich ist die IOTA-„Blockchain" wohl keine „Blockchain", sondern eine „Distributed Ledger Technology". Dem folgend kann IOTA bei strenger Wortinterpretation keine „dominierende Blockchain" iS der vorliegenden Arbeit sein. Es ist aber nicht Ziel dieses Buches, lediglich aufgrund solcher technischen Feinheiten Aussagen zu treffen, sondern es soll vielmehr eine grundlegende Einschätzung der neu aufstrebenden Blockchain-Technologie/Distributed Ledger Technology gegeben werden. Dem folgend ist IOTA, als ein (wohl) aufstrebender und wichtiger Teil der Distributed Ledger Technologies, jedenfalls auch Teil der „Blockchain-Technologie/Distributed Ledger Technology" (zur Relevanz von IOTA: es kooperieren bereits bekannte Gesellschaften mit der IOTA Foundation zB Bosch, Microsoft, Fujitsu, Accenture, Audi uvm; vgl dazu *IOTA,* Data Marketplace). Aufgrund der technischen Ausprägung der IOTA-Blockchain (Tangle vs Blocks), können die Ausführungen in diesem Buch, die speziell die Aneinanderreihung von verschiedenen Blöcken an den bereits vorhandenen Strang einer Blockchain thematisieren, nur bedingt auf eine Distributed Ledger Technology wie IOTA übertragen werden, hingegen hat die Klärung etlicher anderer grundlegender Fragen auch für weitere Distributed Ledger Technologies wie IOTA grundsätzlich Geltung. Dem folgend wäre mE eine Argumentation, dass die vorliegende juristische Analyse auf Distributed Ledger Technologies wie IOTA nicht anwendbar ist, nur bedingt richtig.

32 *Martini/Weinzierl,* NVwZ 2017, 1251.

33 Die Literatur verwendet den Begriff „Distributed Ledger Technology" tlw synonym für die Blockchain-Technologie. Im Rahmen dieses Buches wird weitgehend von der Blockchain oder der Blockchain-Technologie gesprochen. In Fällen, in denen eine Differenzierung zwischen den technischen Gegebenheiten der einzelnen Blockchains notwendig ist, wird gesondert darauf hingewiesen.

34 Eigene Definition in Anlehnung an *Creusen/Gall/Hackl*, Digital Leadership. Führung in Zeiten des digitalen Wandels (2017) 17; *Moring/Maiwald/Kewitz*, Bits and Bricks: Digitalisierung von Geschäftsmodellen in der Immobilienbranche (2018) 102; *Hosp*, Kryptowährungen (2017) 42; *Antonopoulos*, Bitcoin & Blockchain (2018) Glossar XXIV.

Abhängig von dem potentiellen Teilnehmerkreis einer Blockchain, wird grundsätzlich zwischen einer *öffentlichen* (Public Blockchain) und *privaten* Blockchain (Private Blockchain) unterschieden. Teile der Blockchain-Community sowie Teile der Lehre nehmen darüber hinaus weitere Unterteilungen der Blockchain vor, zB die *Konsortium-Blockchain*. Obwohl diese Blockchains in ihrer technischen Grundfunktion idR ähnlich[35] sind,[36] hat die (mögliche) Zugangsbeschränkung einer öffentlichen und privaten Blockchain weitreichende Konsequenzen für Teilaspekte des anwendbaren Rechts. In der vorliegenden Arbeit wird dabei stets an passender Stelle auf etwaige Unterschiede zwischen einer Public und einer Private Blockchain eingegangen. Neben der Einteilung in Public und Private Blockchains, abhängig von dem potentiellen Teilnehmerkreis, hat eine weitere Unterteilung anhand der erlaubten Schreibrechte der User zu erfolgen; sowohl eine Public als auch eine Private Blockchain kann dabei grundsätzlich „Permissionless" oder „Permissioned" sein (siehe dazu unten ausführlich).[37]

2.1.1. Öffentliche Blockchain („Public Blockchain")

Eine Public Blockchain ist jene Ausprägung der Blockchain-Technologie, die durch Kryptowährungen wie Bitcoin & Co allgemeine Bekanntheit erlangt hat, wobei häufig in den Medien lediglich von der Kryptowährung und nicht der dahinterstehenden Blockchain-Technologie gesprochen wird.

Einer öffentlichen Blockchain („**Public Blockchain**") kann jeder beitreten. Somit kann jeder – wenn die technischen Voraussetzungen erfüllt sind – die jeweilige öffentliche Blockchain auf seinen Computer laden und daran teilnehmen. Die initiale Teilnahme erfolgt durch Installation des passenden Client[38] auf dem gewünschten Rechner und der anschließenden Aufnahme der Kommunikation mit anderen Teilnehmern des Blockchain-Netzwerkes.[39]

Im Fall einer Public Blockchain erfolgt keine Authentifikation der Blockchain-Teilnehmer gegenüber einer zentralen Stelle oder einem/mehrerer Teilnehmer der speziellen Blockchain.[40] Es können beliebig viele Rechner an einer öffentlichen Blockchain teilnehmen und miteinander nach den dieser Blockchain zugrundeliegenden Regeln interagieren.[41]

35 Die größten Unterschiede bestehen wohl in der Konsensfindung innerhalb der Blockchain. Im Rahmen von privaten Blockchains kann auf aufwändige Konsensfindungsmechanismen verzichtet werden, da es – je nach Ausprägung der privaten Blockchain – uU bereits zu einer Prüfung der Zuverlässigkeit der Nodes vor Zulassung zur Blockchain gekommen ist (vgl dazu zB *Sixt*, Bitcoins und andere dezentrale Transaktionssysteme (2017); *Martini/Weinzierl*, NVwZ 2017, 1252).

36 *Kienzler* in *Burgwinkel*, Blockchain Technology (2016) 112.

37 *Wüst/Gervais* in 2018 Crypto Valley Conference on Blockchain Technology (2018) 45 ff.

38 Im Falle der Bitcoin Blockchain ist der am häufigsten verwendete Client „Bitcoin Core", der unter https://bitcoin.org./en/download jederzeit auf den eigenen Rechner geladen werden kann. Damit kann eine Teilnahme jederzeit gestartet werden. Im Fall der Ethereum-Blockchain sind die – derzeit – beliebtesten Clients Geth und Parity (*Javor*, An introduction to Geth and running ethereum Nodes).

39 Eine erste Kontaktaufnahme wird dabei meist mit den „umliegenden" „Nodes" erfolgen, um die soeben auf den eigenen Rechner geladene Blockchain warten und aktuell halten zu können.

40 *Kienzler* in *Burgwinkel*, Blockchain Technology (2016) 112.

41 *Welzel/Eckert/Kirstein/Jacumeit,* Mythos Blockchain (2017) 15; *Berentsen/Schär*, Bitcoin, Blockchain und Kryptoassets (2017) 98.

> Eine Public Blockchain ist „eine Blockchain, der jeder jederzeit durch Download des öffentlich zur Verfügung stehenden Client beitreten kann, sofern die technischen Voraussetzungen zur Teilnahme erfüllt sind. Es kommt idR weder zu einer Prüfung von Voraussetzungen durch eine zentrale Stelle, noch zu einer Authentifikation der einzelnen Teilnehmer der Blockchain."[42]

2.1.2. Private Blockchain („Private Blockchain")

Im Gegensatz zu einer öffentlichen Blockchain, an der jeder teilnehmen kann, ist eine private Blockchain („**Private Blockchain**") an einen bestimmten Nutzerkreis gerichtet. Dieser Adressatenkreis wird idR zuvor vom Blockchain-Initiator festgelegt.[43] Bei einer Private Blockchain ist es daher nicht ausreichend, dass ein Rechner, der an der Private Blockchain teilnehmen möchte, die technischen Voraussetzungen erfüllt; vielmehr müssen darüber hinaus auch weitere Zulassungskriterien geprüft werden. Diese werden in der Regel von einer zentralen Stelle, einem sogenannten „Gatekeeper", geprüft.[44] Neben dieser objektiven Überprüfungsmethode ist es bei einer privaten Blockchain möglich, eine Teilnahme an der Blockchain lediglich von der Zustimmung des Gatekeepers abhängig zu machen. Es ist insbesondere nicht erforderlich, dass diese Entscheidung auf objektiv nachvollziehbaren Kriterien beruht.[45] Im Rahmen einer Private Blockchain kommt es zu einer Authentifikation diverser (oder aller) Teilnehmer gegenüber allen (oder bestimmten) Teilnehmern der Blockchain. Ob die Kontrolle der Zutrittsvoraussetzungen von einer zentralen Stelle ausgeübt wird, von bestimmten oder allen übrigen Blockchain-Teilnehmern, ist abhängig von der jeweiligen Blockchain.[46]

> Eine Private Blockchain ist „eine Blockchain, an der lediglich bestimmte Personen teilnehmen können. IdR erfolgt vor Teilnahme an der Blockchain eine Prüfung der jeweiligen (persönlichen) Voraussetzungen durch den Gatekeeper. Im Rahmen der Prüfung der Zulassungsvoraussetzungen erfolgt regelmäßig eine Authentifikation der Nutzer, oder werden zumindest ausreichend Daten über die Teilnehmer bekannt, sodass dem Gatekeeper eine Identifikation der Blockchain-Teilnehmer möglich wäre. Die Zulassung zur jeweiligen Blockchain kann entweder an objektiv nachvollziehbare Kriterien gebunden sein, oder im alleinigen Ermessen des Gatekeepers stehen."[47]

2.1.3. Konsortium-Blockchain

Neben den bekannten Ausprägungen der privaten und öffentlichen Blockchains argumentieren Teile der Lehre und der Blockchain-Community, dass es noch eine weitere Unterteilung der Blockchain gibt. Sie führen dabei regelmäßig die „Konsortium-Blockchain" an. Eine Konsortium-Blockchain liegt hinsichtlich ihrer Eigenschaften zwischen

42 Definition in Anlehnung an *Welzel/Eckert/Kirstein/Jacumeit,* Mythos Blockchain (2017) 15; *Berentsen/Schär*, Bitcoin, Blockchain und Kryptoassets (2017) 98; *Kienzler* in *Burgwinkel*, Blockchain Technology (2016) 112; *Gorzala/Hanzl*, RdW 2018, 487.

43 *Sixt*, Bitcoins und andere dezentrale Transaktionssysteme (2017); *Martini/Weinzierl,* NVwZ 2017, 1252; *Gorzala/Hanzl*, RdW 2018, 487.

44 *Martini/Weinzierl*, NvWZ 2017, 1253; *Gorzala/Hanzl*, RdW 2018, 487.

45 *Chamber of Digital Commerce*, Smart Contracts: 12 Use Cases for Business & Beyond, 11.

46 *Kienzler* in *Burgwinkel*, Blockchain Technology (2016) 112.

47 Definition in Anlehnung an *Kienzler* in *Burgwinkel*, Blockchain Technology (2016) 112; *Chamber of Digital Commerce*, Smart Contracts: 12 Use Cases for Business & Beyond, 11; *Martini/Weinzierl*, NvWZ 2017, 1253; *Gorzala/Hanzl*, RdW 2018, 487.

einer Public und einer Private Blockchain, wobei sie – abhängig von der jeweiligen Ausgestaltung – eher der einen oder der anderen ähnelt.[48] Grundsätzlich ist bei einer Konsortium-Blockchain die Teilnahme – wie auch bei einer Private Blockchain – lediglich auf Einladung bzw nach Prüfung gewisser Zulassungskriterien möglich. Der klassische Anwendungsfall einer Konsortium-Blockchain ist der Zusammenschluss führender Unternehmen[49], die sich die Eigenschaften einer Blockchain zu Nutze machen wollen.[50] Eine Konsortium-Blockchain ist daher „*eine Blockchain, die je nach ihrer konkreten Ausgestaltung eher einer öffentlichen oder einer privaten Blockchain ähnelt, wobei sie nie jedermann offen steht.*"[51]

2.1.4. Permissionless oder Permissioned Blockchain?

Wie bereits oben dargelegt, ist bei Public und Private Blockchains (und wohl auch bei Konsortium-Blockchains, sofern eine solche weitere Unterteilung vorgenommen wird) stets anhand der den Blockchain-Teilnehmern zukommenden Schreibrechte zwischen „Permissioned" und „Permissionless" Blockchains zu unterscheiden. Folglich gibt es – geht man lediglich von den zwei Hauptkategorien der Public und Private Blockchain aus – die (i) Public Permissionless Blockchain, die (ii) Public Permissioned Blockchain, die (iii) Private Permissionless Blockchain sowie die (iv) Private Permissioned Blockchain.[52] In der Praxis wird häufig lediglich von der „Public Blockchain" bzw der „Private Blockchain" gesprochen, wobei damit idR die Public Permissionless Blockchain bzw die Private Permissioned Blockchain gemeint ist.

2.1.4.1. Permissionless Blockchain

Bei einer Permissionless Blockchain gibt es keine Restriktionen der Schreib- und Prüfrechte auf der Blockchain. Jeder, der an der Blockchain teilnehmen kann, darf der Blockchain selbst neue Transaktionen hinzufügen und auch andere Transaktionen überprüfen, solange die Voraussetzungen zur Teilnahme an der Blockchain gegeben sind (zB die technischen Mindestanforderungen erfüllt sind).[53] Sowohl eine Public als auch eine Private Blockchain kann eine „Permissionless Blockchain" sein. Eine Blockchain ist „permissionless" (zulassungsfrei), wenn jeder, der an der Blockchain teilnehmen darf, auch grundsätzlich selbst Transaktionen der Blockchain hinzufügen und auch andere auf der Blockchain stattfindende Transaktionen überprüfen darf.[54]

48 *Zimmermann/Hoppe*, Chancen und Risiken der Blockchain für die Energiewende, Germanwatch (2018) 30.

49 Eines der bekanntesten Projekte im Bereich der Konsortium-Blockchain, das mE wohl insbesondere Züge einer Private Blockchain aufweist, ist das R3 Bankenkonsortium. Zielsetzung des R3 Bankenkonsortiums ist es, basierend auf der Blockchain-Technologie, die Plattform Corda, eine private Blockchain, zu entwickeln, wobei diese insb für Anwendungen der Finanzindustrie gedacht ist (vgl anstatt vieler *Gorzala/Hanzl*, RdW 2018, 487).

50 *Voshmgir*, Blockchains, Smart Contracts und das Dezentrale Web, Technologiestiftung Berlin 12.

51 *Wüst/Gervais* in 2018 Crypto Valley Conference on Blockchain Technology (2018) 45 ff; *Parsons*, Blockchain Types Explained: It's More Than Public vs Private.

52 *Wüst/Gervais* in 2018 Crypto Valley Conference on Blockchain Technology (2018) 45 ff; *Parsons*, Blockchain Types Explained: It's More Than Public vs Private.

53 *Parsons*, Blockchain Types Explained: It's More Than Public vs Private.

54 In Anlehnung an *Blockchainhub*, Blockchains & Distributed Ledger Technologies; *Parsons*, Blockchain Types Explained: It's More Than Public vs Private.

2.1.4.2. Permissioned Blockchain

Im Gegensatz zu einer Permissionless Blockchain gibt es bei einer Permissioned Blockchain gewisse Restriktionen iZm der Überprüfung der Transaktionen. Im Rahmen der Permissioned Blockchain ist es lediglich ausgewählten Blockchain-Teilnehmern möglich, der Blockchain neue Transaktionen hinzuzufügen sowie andere auf der Blockchain stattfindende Transaktionen zu überprüfen.[55] Sowohl eine Public als auch eine Private Blockchain kann eine Permissioned Blockchain sein. Eine Blockchain ist „Permissioned" (beschränkt), wenn die Rechte gewisser Blockchain-Teilnehmer beschränkt sind. Es können lediglich ausgewählte Blockchain-Teilnehmer der Blockchain neue Transaktionen hinzufügen und andere auf der Blockchain stattfindende Transaktionen validieren.[56]

2.1.5. Die vier Hauptspielarten von Blockchains in a nutshell

Wie bereits dargelegt, sind die zwei Grundsatzausprägungen der Blockchain-Technologie die Private und die Public Blockchain, wobei diese jeweils anhand der Schreibrechte der Blockchain-Teilnehmer in „Permissioned" und „Permissionless" unterteilt werden können. Freilich kann – wie auch zuvor in diesem Unterkapitel – noch eine weitere Unterteilung der Blockchains zB in eine Konsortium-Blockchain erfolgen. Im Folgenden sollen die wichtigsten Charakteristika der jeweiligen Ausprägung der Blockchain zusammengefasst und anhand eines Beispiels nach *Saive* veranschaulicht werden.

4 (Haupt-)arten von Blockchains[57]

- **Public Permissionless Blockchain:** Grundsätzlich steht diese Blockchain jedem offen, der den jeweiligen Client der Blockchain herunterlädt; alle Blockchain-Teilnehmer haben überdies dieselben Schreibrechte, dh jeder kann Transaktionen auf die Blockchain schreiben.
- **Public Permissioned Blockchain:** Grundsätzlich ist die Blockchain allen zugänglich, wobei nur gewissen (idR durch eine zentrale Stelle ausgewählten) Personen Schreibrechte zukommen.
- **Private Permissionless Blockchain:** Diese Art der Blockchain steht nur einem – nach bestimmten Kriterien ausgewählten – Kreis offen; wobei allen zugelassenen Blockchain-Teilnehmern dieselben Rechte zukommen.
- **Private Permissioned Blockchain:** Es darf lediglich ein nach bestimmten Kriterien ausgewählter Kreis an der Blockchain teilnehmen, wobei wiederum lediglich gewisse Blockchain-Teilnehmer auch tatsächlich auf die Blockchain schreiben dürfen.

Anwendungsbeispiel der 4 Arten von Blockckchains in Anlehnung eines Beispiels nach Saive[58]

Ziel: Es soll durch eine Blockchain der Aufenthaltsort eines bestimmten Geräts dokumentiert werden.

Vorgehensweise: Bei der Verwendung/Übergabe des bestimmten Geräts von einer Person an die nächste Person wird dies jeweils durch eine entsprechende Transaktion in der Blockchain dokumentiert.

55 *Parsons*, Blockchain Types Explained: It's More Than Public vs Private.
56 In Anlehnung an: Blockchainhub, Blockchains & Distributed Ledger Technologies; Parsons, Blockchain Types Explained: It's More Than Public vs Private.
57 *Saive*, CR 2018, 187.
58 *Saive*, CR 2018, 187.

Wahl der Blockchain? Fraglich ist in diesem Zusammenhang, welche der genannten Ausprägungen von Blockchains zur Erreichung des Ziels zweckdienlich ist. Diese Frage kann nicht pauschal beantwortet werden. Das oben definierte Ziel kann grundsätzlich von allen vier Arten der Blockchain erreicht werden. Abhängig von der Wahl der Blockchain kann jedoch ein unterschiedlicher Personenkreis auf die Daten zugreifen bzw die Blockchain sogar beschreiben. Im Ergebnis ist es daher grundsätzlich eine Management-Entscheidung, welche der Spielarten der Blockchain gewählt wird.

Anhand dieser Ausgangssituation können die grundlegenden Unterschiede der Arten der Blockchain-Technologie gezeigt werden:

Public Permissionless Blockchain: Jede Person der Welt könnte die Blockchain downloaden und Transaktionen darauf schreiben. Folglich würde das bedeuten, dass jede Person der Welt stets den Standort des zu bestimmenden Geräts wüsste und selbst eine Standortveränderung auf der Blockchain niederschreiben könnte.

Public Permissioned Blockchain: Es könnte zwar jede Person der Welt den Standort des bestimmten Geräts einsehen, doch nur bestimmte ausgewählte Blockchain-Teilnehmer könnten diesen Standort auf der Blockchain niederschreiben.

Private Permissionless Blockchain: Es könnte bereits der Teilnehmerkreis lediglich auf bestimmte Personen eingeschränkt werden, die auch tatsächlich mit dem bestimmten Gerät in Berührung stehen bzw dieses zB benützen. All jene Personen, die von der zentralen Stelle ausgewählt wurden an der Blockchain teilzunehmen, da sie – potentiell – mit dem Gerät in Berührung stehen, können den Standort dieses Geräts auf der Blockchain niederschreiben.

Private Permissioned Blockchain: Es werden sowohl der Teilnehmerkreis der Blockchain als auch die Schreibrechte der Teilnehmenden beschränkt. Es können lediglich ausgewählte Blockchain-Teilnehmer auf die Blockchain schreiben. Auf das Beispiel umgemünzt würde das bedeuten, dass alle Personen, in deren (mittelbaren) Einflussbereich das bestimmte Gerät steht, den Standort des Geräts kennen dürfen, aber lediglich die Personen, die auch befugt sind, das Gerät zu bewegen, über die notwendigen Schreibrechte verfügen, um auf der Blockchain eine Standortveränderung des bestimmten Geräts einzutragen.

Es zeigt sich daher, dass grundsätzlich das Ziel der „Dokumentation des Aufenthaltsortes des jeweiligen Geräts" von allen Ausprägungen der Blockchain-Arten erfüllt werden kann. Die Entscheidung für die jeweilige Ausprägung der Blockchain sollte daher von den Rechten, die den jeweiligen Blockchain-Teilnehmern zukommen sollen, abhängig gemacht werden. Letztlich wird die Entscheidung, (i) ob bzw (ii) welche Art der Blockchain gewählt wird, davon abhängen, welche Rechte den Blockchain-Teilnehmern bzw auch Nicht-Blockchain-Teilnehmern zukommen sollen (zB ob ggf auch Nicht-Blockchain-Teilnehmern die Möglichkeit gewährt werden soll, den Standort des Gerätes ausfindig zu machen).

Abhängig von der schlussendlich gewählten Art der Blockchain muss sichergestellt werden, dass die (datenschutz-)rechtlichen Anforderungen eingehalten werden.

2.2. Node | Miner

Die Teilnehmer der Blockchain werden regelmäßig unter dem Begriff „Nodes" zusammengefasst (meist übersetzt als Knoten oder Netzwerkknoten), die abhängig von dem Ausmaß ihrer Beteiligung an der Blockchain und den ihnen zustehenden Kompetenzen in unterschiedliche Kategorien eingeteilt werden können.[59]

59 *Berentsen/Schär*, Bitcoin, Blockchain und Kryptoassets (2017) 97; *Hanzl/Rubey,* GesRZ 2018, 103; ebenso *Antonopoulos*, Bitcoin & Blockchain (2018) 174.

Laut *Berentsen/Schär* gibt es Knoten mit der (i) Verifizierungsfunktion, der (ii) „Wallet-Funktion" und der (iii) „Mining-Funktion".[60] *Antonopoulos* unterteilt die Aufgaben von Knoten in (i) die Wallet-Funktion, (ii) die Miner-Funktion, (iii) die vollständige Blockchain-Funktion und (iv) die Routing-Funktion.[61] Die Routing-Funktion ist für *Antonopoulos* die notwendige Voraussetzung um an der Blockchain teilnehmen zu können, die von jedem Node erfüllt werden muss; alle darüber hinausgehenden Funktionen sind optional und müssen nicht von jedem Node erbracht werden.[62] Im Ergebnis gehen *Berentsen/Schär* und *Antonopoulos* von denselben Funktionen aus, wobei deren Terminologie leicht abweichend ist. Die vierte – von *Antonopoulos* angeführte – Routing-Funktion, die eine notwendige Voraussetzung zur Teilnahme an der Blockchain ist, wird von *Berentsen/Schär* mE wohl vorausgesetzt und daher nicht explizit aufgezählt.[63]

In Fällen, in denen eine Differenzierung zwischen den einzelnen Gruppen von Knoten nicht notwendig ist, werden diese im Rahmen der vorliegenden Arbeit als „**Blockchain-Teilnehmer**", „**Nodes**" oder „**Knoten**" bezeichnet.

2.2.1. Full Nodes

Jene Knoten, die die Verifizierungsfunktion ausüben – das heißt Aktivitäten setzen, die zur selbstständigen Netzwerkteilnahme und dezentralen, unabhängigen Kontrolle notwendig sind – werden als „Full Nodes" bezeichnet.[64] Full Nodes speichern die gesamte Blockchain auf ihrem Rechner dezentral, verifizieren Transaktionen und leiten diese an umliegende Knoten weiter, um so sicherzustellen, dass auch die restlichen Nodes die auf ihrem Rechner dezentral gespeicherte Blockchain up to date halten können.[65] Full Nodes sind „*dezentrale Stellen, welche die gesamte Blockchain auf ihrem Rechner gespeichert haben und selbstständig up-to-date halten. Darüber hinaus erhalten full Nodes die Transaktionen, überprüfen diese und leiten die überprüften Transaktionen an andere Nodes weiter*".[66]

2.2.2. Light Nodes

Im Gegensatz zu Full Nodes speichern „Light Nodes" nicht die gesamte Blockchain auf ihrem Rechner, sondern verfügen lediglich über eine Wallet-Funktion. Diese Funktion erlaubt die sichere Verwahrung von privaten Schlüsseln sowie die Überwachung und Verwaltung des eigenen Guthabens.[67] Light Nodes sind „*Endnutzer, die selbst weder die Blockchain dezentral auf ihrem Rechner gespeichert haben, noch die Blockchain ‚aktiv warten oder up to date halten', sondern lediglich Anwendungen der Blockchain nutzen*".[68]

60 *Berentsen/Schär,* Bitcoin, Blockchain und Kryptoassets (2017) 97.
61 *Antonopoulos*, Bitcoin & Blockchain (2018) 174.
62 *Antonopoulos*, Bitcoin & Blockchain (2018) 174.
63 In Anlehnung an die Ausführungen von *Antonopoulos*, Bitcoin & Blockchain (2018) 174; *Berentsen/Schär,* Bitcoin, Blockchain und Kryptoassets (2017) 97.
64 *Berentsen/Schär,* Bitcoin, Blockchain und Kryptoassets (2017) 97; ebenso *Antonopoulos*, Bitcoin & Blockchain (2018) 174.
65 *Hanzl/Rubey,* GesRZ 2018, 103; *Berentsen/Schär*, Bitcoin, Blockchain und Kryptoassets (2017) 97.
66 Definition in Anlehnung an *Hanzl/Rubey,* GesRZ 2018, 103; *Berentsen/Schär,* Bitcoin, Blockchain und Kryptoassets (2017) 97 f.
67 *Berentsen/Schär,* Bitcoin, Blockchain und Kryptoassets (2017) 98.
68 Definition in Anlehnung an *Berentsen/Schär,* Bitcoin, Blockchain und Kryptoassets (2017) 98.

2.2.3. Miner

Im Gegensatz zu den zuvor genannten Knoten überprüfen Miner nicht nur getätigte Transaktionen, sondern beteiligen sich aktiv an der Erstellung neuer Blöcke. Sie stellen den initialen Konsensus abhängig von dem der jeweiligen Blockchain zugrunde liegenden Konsensprotokoll her.[69] Im Rahmen des derzeitig vorherrschenden Proof-of-Work-Systems arbeiten Miner parallel stets an der Erstellung eines neuen Blocks. In den neu zu erstellenden Blocks können Miner aus dem Pool an *unconfirmed* (nicht bestätigten) Transaktionen bestimmte Transaktionen auswählen, die sie in ihren Block aufnehmen. Währenddessen müssen die Miner auch eine gewisse „Arbeit" erbringen (den sog *Proof of Work*), wobei dieser in dem Reverse Engineering eines kryptographischen Algorithmus besteht. Dieser Algorithmus kann lediglich durch das wiederholte Einsetzen von unterschiedlichen Inputvariablen gelöst werden.[70]

> Miner tragen damit aktiv zur Erweiterung des Blockchain-Registers bei und sind „die Blockchain-Teilnehmer, die unbestätigte Transaktionen in zu erstellende Blöcke aufnehmen und währenddessen einen kryptographischen Algorithmus lösen. Der Miner, der als erste die Lösung zu dem kryptographischen Algorithmus gefunden hat, kann seinen erstellten Block samt der Lösung des Algorithmus an das übrige Blockchain-Netzwerk verteilen. Wird die von dem Miner gefundene Lösung von den übrigen Nodes als valide anerkannt, fügt der jeweilige Node den Block an die bei ihm dezentral gespeicherte Blockchain und leitet den neuen Block an die um ihn liegenden Nodes weiter. Dadurch wird ein neuer und valider Block an die Blockchain gekettet.[71]

2.3. „Schlüssel" oder Adressen auf einer Blockchain

Auch im Rahmen von Blockchain-Systemen soll sichergestellt werden, dass lediglich dazu berechtigte Personen Transaktionen durchführen (zB einen bestimmten Betrag einer Kryptowährung übersenden).[72] Dies stellt sohin kein Unterscheidungsmerkmal zu den derzeit dominierenden Systemen (zB ggü einer Banküberweisung) dar, da es auch in diesen zentralistisch ausgestalteten Systemen einen Authentifikationsprozess gibt (zB ein Passwort). Analog zu „klassischen" Authentifizierungsmöglichkeiten, welche die Identität des Disponierenden sicherstellen sollen (zB Passwörter oder das Transaktionscode-Verfahren [„**TAC**"-Verfahren]), verwendet die Blockchain-Technologie ein System, das aus einer öffentlichen Adresse („**Public Key**") und einer privaten Adresse („**Private Key**") besteht. Eine valide Transaktion bedarf eines Zusammenspiels beider Adressen bzw „Schlüssel".

Der Private Key übernimmt die Funktion eines „Passwortes"/des TAC-Verfahrens und stellt sicher, dass signierte Überweisungen tatsächlich von der jeweiligen Person stammen, während der Public Key die aus dem Private Key generierte öffentliche Adresse ist und im Ergebnis die Funktion einer Kontonummer übernimmt (siehe dazu ausführlich unter Punkt 3.3.4.).[73]

69 *Hosp*, Kryptowährungen (2017) 55.
70 *Hosp*, Kryptowährungen (2017) 61 f.
71 *Berentsen/Schär,* Bitcoin, Blockchain und Kryptoassets (2017) 98; *Hosp*, Kryptowährungen (2017) 55 und 61 ff; *Antonopoulos*, Bitcoin & Blockchain (2018) Glossar XXVII.
72 *Wagner/Groß*, White Paper. Blockchain und Smart Contracts (2018) 13.
73 *Antonopoulos*, Bitcoin & Blockchain (2018) 59 ff.