Technische Grundlagen & Entwicklungstendenzen der Blockchain-Technologie

Stefanie Rinderle-Ma, Wolfgang Klas

I Technische Grundlagen

Dieser Abschnitt führt zunächst die wichtigsten technologischen Bausteine von Blockchain ein und diskutiert anschließend die damit verbundenen Herausforderungen und beobachteten Defizite.

A Technologische Bausteine einer Blockchain

1 Hashing

Ein grundlegender Baustein bei der Realisierung von Blockchains sind Hashfunktionen aus der Klasse der kryptographischen Hashfunktionen[1], die neben grundsätzlichen Eigenschaften von Hashfunktionen (zB Gleichverteilung der Hashwerte, geringe Wahrscheinlichkeit von Kollisionen, Surjektivität und Deterministik der Funktion) noch besondere Eigenschaften aufweisen.

Eine derartige Hashfunktion *H* nimmt als Eingabewert ein Datum x beliebiger, aber endlicher Größe und berechnet einen sogenannten Hashwert *h* (kurz Hash *h*, oft auch digest genannt), wobei dieser immer eine vorbestimmte Länge aufweist.

Eine derartige Hashfunktion muss die folgenden besonderen Eigenschaften aufweisen:

---

[1] *Menezes*, Alfred J., Paul C. *van Oorschot*, and Scott A. *Vanstone*, Hash Functions and Data Integrity, in: Handbook of Applied Cryptography. Ed. by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. CRC Press 1996.

- Die Hashfunktion ist eine Einwegfunktion: Es ist praktisch unmöglich, innerhalb eines Zeitraums, in dem die Sicherheit von Eingabewerten grundsätzlich gewährleistet sein soll, zu einem gegebenen Hashwert h einen Eingabewert x zu bestimmen, den die Hashfunktion auf h abbildet, dh, $H(x) = h$.
  Die Hashfunktion weist eine schwache Kollisionsresistenz auf: Es ist praktisch unmöglich, für einen zuvor gegebenen Eingabewert x einen davon verschiedenen Eingabewert x^0 zu bestimmen, zu dem derselbe Hashwert berechnet wird: $h(x^0) = h(x)$ mit $x^0 6= x$.
  Die Hashfunktion weist auch eine starke Kollisionsresistenz auf: Es ist praktisch unmöglich, zwei frei wählbare, verschiedene Eingabewerte x und x^0 zu finden, die denselben Hashwert ergeben: $x^0 6= x^0$ und $H(x^0) = H(x)$.
- Effiziente, dh, einfache und schnelle Berechnung des Hashwerts $h = H(x)$ ohne großen Ressourcenbedarf, wobei h eine fixierte Länge aufweist.

Wie in Abb. 1 illustriert, werden also zwei Eingabewerte (in unserem Beispiel zwei Texte), die geringfügig im letzten Zeichen von einander abweichen, auf völlig unterschiedliche, 64 Zeichen lange Hashwerte abgebildet. Wählt man einen der beiden Texte aus dem Beispiel, dann ist es praktisch unmöglich, einen anderen Text zu bestimmen, zu dem derselbe 64 Zeichen lange Hashwert berechnet wird. Weiters ist es praktisch unmöglich, zwei beliebige Texte zu bestimmen, für die derselbe Hashwert berechnet wird.

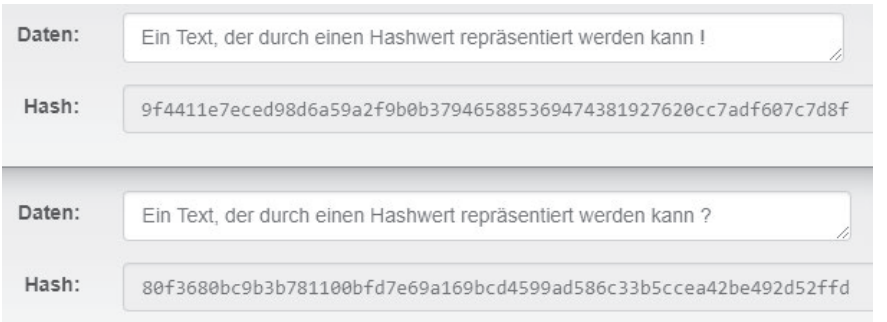

Abbildung 1: Hashwerte von unterschiedlichen Daten (Beispiel erzeugt mit https://anders.com/ blockchain/)

2 Block

2.1 Bestandteile eines Blocks

Ein Block besteht aus einigen strukturellen Elementen, im einfachen Fall aus zumindest einer Blocknummer (Block #), einem Datenelement (Daten), einem speziellen Element Nonce, und einem Hashwert (Hash). Abb. 2 illustriert einen einfach strukturierten Block.

Die Blocknummer ist idR eine laufende Nummer, die einen Block eindeutig identifiziert.

Das Datenelement kann beliebige Daten, die aufgrund einer Transaktion in einer Anwendung entstehen, enthalten. Meist sind die Daten selbst noch weiter strukturiert. So könnte zB die Information ‚Eigentümer der 960.000,– EUR ist Organisation A' auch in einer weiter unterteilten Struktur (Eigentümer = Organisation A, Betrag = 960.000, Währung = EUR) in einem Datenelement gespeichert werden. Die Möglichkeiten der Strukturierung des Datenelements ist in Blockchain-Systemen unterschiedlich ausgeprägt. Manche Systeme unterstützen nur vorkongurierte Strukturen, manche Systeme erlauben die Adaption der Struktur des Datenelements exibel je nach Bedarf einer Anwendung.

Nonce ist ein speziell bestimmter Wert, in unserem Fall eine speziell errechnete ganze Zahl. Dieser Wert spielt eine besondere Rolle bei der rechnerischen Feststellung, wann ein Block als korrekt zu betrachten ist.

Hash ist der Hashwert, der sich aus den anderen Strukturelementen mittels eines Hashing-Verfahrens (siehe Kapitel I.A.1) berechnet.

2.2 Korrekte Blöcke

Blöcke können in einer Blockchain nur aufgenommen werden, wenn diese eine korrekte Ausprägung annehmen, dh, bestimmte Bedingungen eingehalten werden. Zum Beispiel wird für einen korrekten Block verlangt, dass der Hashwert und der Nonce-Wert zu diesem Block eine bestimmte Bedingung erfüllt: Für eine konkrete Blocknummer (zB Block # = 1) und konkrete Daten eines Blocks (zB ‚Eigentümer der 960.000,– EUR ist Organisation A' wird eine spezielle Wertbelegung für Nonce gesucht, und zwar derart, dass der dann aus Blocknummer, Daten, und Nonce-Wert berechnete Hashwert eine bestimmte, vorab festgelegte und gewünschte Struktur aufweist, zB eine vorgegebene Anzahl von führenden Nullen enthält. Im gewählten Beispiel ist die Vorgabe, dass ein Nonce-Wert verwendet werden muss, so dass der Hashwert vier führende Nullen enthält. Die Wahl dieser strukturellen Vorgabe hat unmittelbaren Einfluss darauf, wie schwierig die Bestimmung von passendem Hashwert und Nonce-Wert ist.

2 (a)

(b)

Abbildung 2: Elemente eines Blocks: (a) Block mit Verweis auf Organisation ‚A'; (b) Block mit Verweis auf Organisation ‚B'. Elemente Nonce und Hash unterscheiden sich daher in (a) und (b) (Beispiel erzeugt mit https://anders.com/blockchain/).

Der Prozess der Bestimmung von passendem Hashwert und Nonce-Wert wird als Mining (siehe Abschnitt I.A.5) bezeichnet.

In realen Blockchain Systemen ist die Struktur eines Blocks komplizierter und weist einen Block-Header und die Block-Datensätze auf. Der Block-Header umfasst typischerweise zusätzlich zu einer Blocknummer und einem Nonce-Wert auch Zeitstempel, Speicheradresse der Block-Datensätze (zB mit Hilfe eines Merkle-Tree organisiert), Angaben zur strukturellen Vorgabe für Hashwerte sowie weitere wichtige technisch administrative Informationen, die zur Konstruktion einer Blockchain benötigt werden. Typischerweise werden alle diese Informationen bei der Festlegung der Korrektheit eines Blocks berücksichtigt.

3 Verkettung von Blöcken

Unter einer Blockchain versteht man i.A. eine sequentielle Verkettung von Blöcken B_0, B_1, B_2, ..., B_n, die nach obigen Ü berlegungen eine korrekte Struktur aufweisen. Eine Blockchain entsteht ausschließlich durch das wiederholte Anhängen von korrekten Blöcken. Die Verkettung der Blöcke wird dadurch

erreicht, dass der Hashwert des Vorgänger-Blocks B_{i-1} als strukturelles Datenelement im Block-Header des Blocks B_i zusätzlich gespeichert wird. Jeder Block verweist mit Hilfe dieses zusätzlichen Hashwerts damit auf seinen Vorgängerblock. Diese Definition einer Blockchain erlaubt es, dass nach Anhängen eines korrekten Blocks alle zuvor in der Blockchain verketteten Blöcke mit Hilfe der Hashwerte auf Korrektheit überprüft werden können. Jede nachträgliche Manipulation eines Datenelements in einem Block B_{i-1} verändert den Hashwert des Blocks B_{i-1}, der dann nicht mehr mit dem im korrekten Nachfolgerblock B_i gespeicherte Hashwert von B_{i-1} übereinstimmt. Nach einer Manipulation eines Datenelements im Block B_{i-1} kann nur durch erneutes Mining des Blocks B_{i-1} und aller nachfolgenden Blöcke B_j, $j \geq i$, wieder eine verkettete Sequenz von korrekten Blöcken erzeugt werden, wobei alle betroffenen Blöcke B_{i-1}, B_i, B_{i+1}..., B_n veränderte Hashwerte (und Nonce-Werte)

aufweisen. Mit der unter https://anders.com/blockchain/ verfügbaren Demo kann die Verkettung von Blöcken beispielhaft sehr einfach illustriert werden.

Der erste Block B_0 in einer Blockchain wird meist Genesis-Block genannt und enthält wesentliche technische Informationen zur Konfiguration der Blockchain. Alle weiteren Blöcke B_i, $i \geq 1$ sind typischerweise Blöcke, die Daten aus der Anwendung speichern.

4 Verteilung der Daten

Die Verteilung der Blockchain über verschiedene Rechner erfolgt in einem Peer-to-peer (P2P) System. In einem derartig verteilten System sind die Peers im Prinzip gleichgestellte Teilnehmer, die ein sog P2P Netzwerk von Knoten bilden. Jeder Knoten hat eine vollständige Kopie der Blockchain verfügbar. Durch diese Replikation der Blockchain werden viele Risiken, die mit einer einzigen zentralen Stelle der Datenhaltung einhergehen, eliminiert. Allerdings ist eine stetige Kommunikation zwischen den Knoten innerhalb des P2P Netzwerks nötig. Die Daten aus Transaktionen einer Anwendung, die daraus geformten Blöcke sowie die korrekten Blöcke müssen im Netzwerk verteilt werden. Der insgesamt verbrauchte Speicherplatz aufgrund der Replikation der Blockchain ist selbstverständlich um ein Vielfaches höher als dies bei einer zentralen Datenhaltung der Fall wäre. Grundsätzlich kann jeder Teilnehmer die gleiche Funktionalität der Blockchain nutzen, allerdings ist denkbar, dass bestimmte Knoten nur bestimmte Aufgaben zum Betrieb des Blockchain-Systems wahrnehmen. Eine typische Rollenverteilung der Knoten ist die Teilnahme als Miner oder Client. Als Miner beteiligt sich der Knoten an der Berechnung von korrekten Blöcken und damit an der stetigen Erweiterung der Blockchain. Als Client beteiligt sich ein Knoten nur als Nutzer der Blockchain, dh, er liest oder schreibt Daten gemäß Anwendungstransaktionen auf der Blockchain.

Der Zugang zu den Daten in der Blockchain wird über kryptographische Public-Private-Key Lösungen abgesichert. Public Keys dienen als öffentlich verfügbare Adressen in der Blockchain, denen Daten in der Blockchain zugeordnet werden. Der einem Public Key zugeordnete Private Key ist vergleichbar einem Passwort, mit dem der Zugang zu den entsprechenden Daten ermöglicht wird. In analoger Form kann die Nutzung von Diensten und Funktionalität eines Blockchain-Systems durch Knoten im Netzwerk abgesichert und autorisiert werden.

Grundsätzlich stellt das stetige Wachsen von großen Blockchains eine Herausforderung dar und kann auch mit gewissen Risiken einer späteren Zentralisierung verbunden sein, da die Kosten für den stetig steigenden Ressourcenbedarf zur Verarbeitung einer großen Blockchain sich kontinuierlich erhöhen. So hat die Bitcoin zugrundeliegende Blockchain mit Stand Juli 2019 eine Größe von 266 GB, die Public Ethereum-Blockchain eine Größe von 269 GB erreicht.

5 Konsensusverfahren – Mining

Liegen genügend viele Datensätze aus einer Anwendung vor, die in einem Block gespeichert werden sollen, werden diese Datensätze zusammengestellt, in eine Blockstruktur gebracht und anschließend das sog Mining des Blocks veranlasst. Dieser Mining-Schritt zur Erstellung eines korrekten Blocks kann in unterschiedlicher Form ausgestaltet sein. So kann dies zB – wie in Bitcoin der Fall – als frei zugänglicher Wettbewerb innerhalb des Peer-to-Peer Netzwerks, der jenen Teilnehmer belohnt, dem als erster die Berechnung des passenden Hashwerts und des Nonce-Wert gelingt, gestaltet sein. Oder die Feststellung der Korrektheit wird an autorisierte Teilnehmer im Netzwerk übertragen, die als Ergebnis die Korrektheit eines Blocks feststellen.

Unter Berücksichtigung von gewünschten Eigenschaften einer Blockchain wie zB Glaubwürdigkeit, öffentliche Nachvollziehbarkeit, Aspekten der Sicherheit gegenüber Attacken und Manipulation, Rechenaufwand für das Mining und Produzieren von korrekten Blöcken kann der Schwierigkeitsgrad für die Bestimmung des passenden Hashwerts und des Nonce-Wert, somit der Aufwand für das Mining, unterschiedlich ausgestaltet werden. In der von Bitcoin verwendeten Blockchain war zu Beginn gefordert, dass zumindest die ersten 32 von insgesamt 256 Bits des Hashwerts Null sein müssen. Da aber die für das Mining eingesetzte Hardware immer schnellere Berechnungen ermöglicht, Bitcoin aber das Ziel des Erstellens von ca. 6 Blöcken pro Stunde einhalten will, wurde diese Vorgabe im Januar 2019 dahingehend angehoben, dass die ersten 74 der insgesamt 256 Bits des Hashwerts Null sein müssen.

Wesentlich geringerer Aufwand für das Berechnen der korrekten Werte für Hash und Nonce entsteht durch das Delegieren der Feststellung der Korrektheit eines Blocks an eine oder mehrere (wenige) autorisierte Stelle(n). Diese können bei entsprechend geringen strukturellen Vorgaben an den Hashwert sehr schnell die Bestimmung des passenden Hashwerts und des Nonce-Wert vornehmen. Ein derartiges Modell würde möglicherweise sehr nahe dem Entscheidungsprozess in einem Verein durch Vorstand und Präsidium mit gewählten, autorisierten Funktionsträgern kommen.

Wenn Teilnehmer im Peer-to-Peer Netzwerk die Möglichkeit haben, im Wettbewerb parallel an der Berechnung von korrekten Blöcken teilzunehmen, dann können letztlich auch mehrere Varianten eines korrekten Blocks entstehen. Somit stellt sich die Frage, welcher der verschiedenen korrekten Blöcke wird letztlich in die Blockchain aufgenommen und welche Blöcke werden verworfen. Diese Entscheidung kann wiederum auf Zufallsprinzipien beruhen, oder auf Entscheidungen, die bestimmten Teilnehmern zugestanden werden. In Bitcoin wurde das Verfahren für diese Entscheidung adaptiert: Zu Beginn berücksichtigte die Referenzimplementierung den tatsächlich als erster eingelangte Block. Später wurde aus Sicherheitsgründen diese Entscheidung auf eine zufällige Entscheidung der am Mining-Prozess beteiligten Teilnehmer abgeändert. Letztlich setzt sich jener Block durch, der Teil der Kette ist, die den höchsten kumulativen Rechenaufwand aufweist – und damit auch die

längste Kette ist. Alle alternativen korrekten Blöcke bleiben in Folge unberücksichtigt (sog stale blocks).

Die Verfahren zur Bestimmung von korrekten Blöcken und damit indirekt die Entscheidung, welche Blöcke in einer Blockchain verkettet werden, beeinflussen maßgeblich die Eigenschaften einer Blockchain. Sie legen die Regeln fest, nach denen alle Teilnehmer in einem Blockchain System den Konsens über den korrekten Zustand einer Blockchain feststellen und akzeptieren. Diese Regeln müssen selbstverständlich sicher und robust gegenüber verschiedensten Risiken und Attacken sein. Das Verfahren bestimmt auch die sog, Block Time, die durchschnittliche Zeit die benötigt wird, um einen Block der Blockchain hinzuzufügen. Manche Blockchain-System ermöglichen das Erzeugen von neuen Blöcken ca. alle fünf Sekunden. Bei der EOS blockchain beträgt die Block Time derzeit ca. 500 ms, bei der Ethereum Public Blockchain liegt die Block Time bei derzeit ca. 15 Sekunden, bei der Monero Blockchain sind es ca 2 Minuten, bei der Bitcoin Blockchain liegt dieser Wert derzeit bei ca. 10 Minuten. Je kürzer die Block Time, desto schneller kann eine Transaktion aus Sicht einer Anwendung auf der Blockchain abgewickelt werden. Die Block Time hat wesentlichen Einfluss auf den Transaktionsdurchsatz eines Blockchain Systems.

Es existieren verschiedene Konsensusverfahren zur Auflösung von Konflikten. Bekannte Vertreter, die auch am häufigsten in Blockchain-Systemen zur Realisierung von digitalen Währungen verwendet werden, sind Proof-of-Work (PoW), Proof-of-Stake (PoS), und Practical-Byzantine-Fault-Tolerance (PBFT). Weitere interessante Verfahren sind ua Delegated-Proof-of-Stake (DPoS), Proof-of-Importance (PoI), Delegated-Byzantine-Fault-Tolerance (dBFT), und Proof-of-Authority (PoA).

In manchen dieser Konsensusverfahren wird in der Literatur in Abhängigkeit des algorithmischen Aufwands für die Berechnung eines korrekten Blocks anstatt des bisher verwendeten Begriffs Miner die Bezeichnung Validator verwendet. Letzterer wird tendenziell meist dann verwendet, wenn die Festlegung, dass ein Block korrekt ist, nicht mit einem hohen Rechenaufwand (mining) verbunden ist, sondern auf die Entscheidung von einzelnen autorisierten Instanzen (Validators) beruht.

6 Kryptowährungen

Im Kontext von Blockchain-Systemen wird meist auch das Konzept einer virtuellen, digitalen Währung (Kryptowährung) genutzt. Dabei müssen die unterschiedlichen Rollen, die eine virtuelle Währung im Rahmen eines Blockchain-Systems spielen kann, unterschieden werden:

(i) Digitale Währung als Zahlungsmittel für Anwender, realisiert auf Basis eines Blockchain-Systems wie zB die Kryptowährung Bitcoin. Dabei dient Blockchain-Technologie zur technischen Realisierung des Zahlungsmittels.

(ii) Digitale Währung als internes Instrumentarium für die Ausgestaltung von Funktionalität in einem Blockchain-System um Anreize für bestimmte Aktivitäten, die für den Betrieb einer Blockchain nötig sind, zu realisieren. Diese Rolle einer digitalen Währung ist meist ein wesentlicher Baustein zur Realisierung von Blockchain-Systemen.

Die beiden Rollen können logischerweise auch verknüpft werden. Ein prominentes Beispiel für diese Verknüpfung ist das Blockchain-System für Bitcoin. Bitcoin dient zum einen als Krypto-Zahlungsmittel für Anwender, verfügbar als digitale Währung, und ist gleichzeitig die Verrechnungseinheit für systeminterne Anreize wie die Vergütung für das Mining von Blöcken. Ein anderes Beispiel ist das Ethereum Blockchain System, das für die interne Verrechnung von Leistungen sog Gas-Einheiten verwendet, die wiederum mit Hilfe der eigenen digitalen Kryptowährung Ether, welches als Zahlungsmittel für Anwender verfügbar ist, bezahlt werden muss. Damit erfolgt eine Entkopplung der digitalen Währung Ether von der Rolle des systeminternen Instrumentariums Gas für die Ausgestaltung von Funktionalität in Ethereum.

Anreizsysteme in Blockchain-Systemen werden meist unter Nutzung einer (idR eigenen) Kryptowährung realisiert. Um zB Teilnehmer zu motivieren, ihre Hardware- und Computing-Ressourcen für den möglicherweise sehr aufwendigen Mining-Prozess zur Verfügung zu stellen, können Teilnehmern Beträge in einer virtuellen Währung als Gegenleistung zugeordnet werden, die dann entweder wieder innerhalb des Systems für die Nutzung von Blockchain-Systemressourcen eingesetzt werden können oder – im Kontext eines Zahlungssystems einer virtuellen Währung – für die Bezahlung von Leistungen und Gütern eingesetzt werden.

7 Konfigurationen von Blockchains und deren Eigenschaften

Die Konfiguration von Blockchain-Systemen umfassen meist sehr viele technische Parameter, die von einer Anwendung kaum oder nur selten direkt bestimmt werden. Die heute verfügbaren verschiedenen Plattformen für Blockchain-Systeme sind entweder auf bestimmte Anwendungsbereiche zugeschnitten oder zielen auf eine generische Nutzung ab. Im letzteren Fall ist es möglich und teils auch nötig, konzeptionelle Varianten bzw Konfigurationen des Blockchain-Systems je nach Erfordernissen einer Anwendung zu bestimmen.

Ein fast immer zu treffende Entscheidung ist die Konfiguration der Blockchain als Public Blockchain oder Private Blockchain, was unmittelbar eine wesentliche Eigenschaft einer Blockchain definiert. Diese Unterscheidung betrifft die Methodik, wie Konsens zum Zustand einer Blockchain herbeigeführt bzw festgestellt wird. Es können zwei Klassen von Blockchains unterschieden werden:

- Permissionless/Public Blockchain Systeme erfüllen die Eigenschaft, dass die Knoten, die den Konsens über den Zustand der Blockchain feststellen,

nicht bekannt sind. Diese Art von Blockchain wird meist auch als Public Blockchain, oft sogar einfach als Proof-of-Work-Blockchain bezeichnet.
- Permissioned/Private Blockchain Systeme erfüllen die Eigenschaft dass die Knoten, die den Konsens über den Zustand der Blockchain feststellen, bekannt sind. Eine weitergehende Unterscheidung in Permissioned und Private Blockchain Systeme ergibt sich aus der Selektion und der Komposition der Knoten, die zur Herbeiführung des Konsensus über den Zustand der Blockchain autorisiert sind. Solche Blockchain Systeme wenden nicht Proof-of-Work als Konsensusverfahren an, sondern zB Proof-of-Authority.

Blockchain-Systeme sind idR meist mit einem bestimmten Konsensusverfahren vorab konfiguriert. Manche unterstützen jedoch auch eine eingeschränkte Konfiguration des anzuwendenden Konsensusverfahrens. Im Fall von Ethereum kann zB die Blockchain als Private/Permissioned Blockchain mit PoA (anstatt mit PoW) konfiguriert werden, je nach Bedarf der Anwendung.

Public Blockchains weisen zudem keinerlei Zugangsrestriktionen auf. Jede/r der Zugang zum Internet hat, hat damit technisch als Knoten im Peer-to-Peer Netzwerk auch die Möglichkeit, sich der Funktionalität der Public Blockchain zu bedienen, sowohl als Anwendungsnutzer, der Transaktionen auf der Blockchain ausführen kann, als auch in der Rolle eines Miners, der über seine Beteiligung am Konsensusverfahren auch das stetige Wachstum der Blockchain mitgestaltet. In der Regel bieten Public Blockchains ökonomische Anreizsysteme, die eine Beteiligung in der Rolle als Miner fördern. Public Blockchains sind immer dann von besonderem Interesse, wenn eine umfassende öffentliche Kontrolle der Blockchain und der darin gespeicherten Information und das Vermeiden einer zentralen Kontrollinstanz erforderlich ist. Meist wird damit auch der höchst erzielbare Grad an Vertrauen in eine Blockchain assoziiert.

Private Blockchains hingegen weisen spezielle Zugangsrestriktionen auf. Teilnehmen kann man nur nach expliziter Aufforderung und Genehmigung durch den Administrator der Blockchain. Dies gilt sowohl in der Rolle als Anwendungsnutzer als auch in der Rolle des Miners, die spezielle Privilegien erfordert. Private Blockchains sind daher von besonderem Interesse für Organisationen, die die Vorteile von Blockchain-Systemen allgemein nutzen wollen, jedoch kein Interesse oder Bedarf für eine Kontrolle der Blockchain und all ihrer Inhalte auf Basis einer völligen Öffentlichkeit haben. Blockchain-Systeme werden dann sehr oft in die Buchhaltungs- und Dokumentationsverfahren für industrielle Prozesse integriert, ohne dabei die Autonomie der Organisationen zu opfern und ohne Risiko, dass sensitive Geschäftsdaten im Internet publik werden. Dies ist typischerweise in Industrieanwendungen der Fall, kann aber zB auch schon bei der IT-technischen Nachbildung von Geschäftsordnungen und -abläufen von Vereinen oder Verbänden mit hoher verteilter Organisationsstruktur eine sinnvolle Lösung darstellen.

Hybride Blockchains sind eine Kombination der Eigenschaften von Public/