

# Die Transformation der Distributed-Ledger-Technologie

Es wird erwartet, dass dieser technologische Wandel zu Innovationen führt, die heutige Geschäftspraktiken unterbrechen und Branchen in einem Ausmaß revolutionieren wird, wie es seit der Entwicklung des Internets nicht mehr der Fall war.

Elementum Metals: 24/03/2021

24/03/2021



**D**ie Distributed-Ledger-Technologie, wie z. B. Blockchain, verspricht, sowohl Unternehmen als auch das Privatleben der Menschen zu verändern: nicht nur durch die Revolutionierung der Buchführung und Transaktionsaufzeichnung, sondern auch durch die Ermöglichung der Übertragung von Werten durch digitale Vermögen und Smart Contracts.

## Distributed Ledger Technologie

Die anonyme Person mit dem Pseudonym Satoshi Nakamoto erfand Blockchain im Jahr 2008 als Ermöglichungsmechanismus für Bitcoin.<sup>1</sup> Eine der Herausforderungen bei der Entwicklung von Systemen, die eine Wertaufbewahrung ermöglichen, besteht darin, dass das wichtigste Designziel von Computern die schnelle und genaue Replikation von Aktivitäten und Daten ist; infolgedessen ist Knappheit und Einzigartigkeit schwer zu erreichen. Mit Blockchain hat Satoshi Nakamoto jedoch einen Mechanismus entwickelt, der einzigartige Transaktionen und Datensätze ermöglicht, zusammen mit der Möglichkeit, die Duplizierung eben dieser Datensätze zu kontrollieren.

Blockchain ist im Wesentlichen eine gemeinsam genutzte Datenbank, die sich an mehreren Standorten über verschiedene Regionen und Organisationen hinweg befindet. Alle Teilnehmer kontrollieren ihre eigene Kopie des Ledgers und verfügen über digitale Schlüssel und Signaturen, die es ihnen ermöglichen, auf ihr Ledger zuzugreifen und es gemäß den Regeln des Systems zu aktualisieren, sobald die Verifizierungsprotokolle erfüllt wurden.

Eine Blockchain ist eine Liste von Transaktionen, von denen jede mit der vorhergehenden Transaktion verknüpft ist, wobei ein Kennzeichnungssystem verwendet wird, das sich direkt auf die vorherige Transaktion bezieht. Blockchain-Algorithmen ermöglichen es, Transaktionen in "Blöcken" zusammenzufassen, indem eine neue Transaktion mit Hilfe einer kryptografischen Signatur an die vorhergehende Transaktion angehängt wird. Die

Sicherheit und Datenintegrität verteilter Ledger wird durch das Vorhandensein mehrerer Versionen derselben Datenbank an verschiedenen Orten gewährleistet; eine unbefugte Änderung der Datenbank müsste gleichzeitige Änderungen in allen Datenbanken nach sich ziehen - etwas, das außerordentlich schwer zu erreichen ist, besonders wenn die Zahl der Benutzer wächst.

Im Gefolge von Satoshi Nakamotos Spezifikation der Blockchain wurden eine Reihe anderer Distributed-Ledger-Systeme entwickelt. Dazu gehören Direct Acyclic Graph (DAG), das versucht, die Einschränkungen der Blockchain in Bezug auf Skalierbarkeit und Transaktionen pro Sekunde durch unabhängige Datenstrukturen zu überwinden; Hashgraph, das "virtuelle Abstimmungsprotokolle" ("Gossip") verwendet, um Transaktionen durch einen Konsens zu validieren; und Holochain, das versucht, Datenstaus zu reduzieren, indem es die Daten über eine Reihe von Knotenpunkten verteilt.<sup>2</sup>

## Blockchain-Systeme

Während traditionelle Ledger zentralisiert arbeiten und alle Informationen an einem Ort gehalten werden, arbeiten Blockchain-Plattformen mit dezentralisierten Prinzipien. Bei permissionless-public ("erlaubnisfreien öffentlichen") Systemen gibt es keinen zentralen Eigentümer, der den Zugriff auf das Netzwerk kontrolliert. Bitcoin ist das bekannteste Beispiel, bei dem jeder einen Block zur bestehenden Kette hinzufügen kann, sobald er ein kryptografisches Rätsel gelöst hat, das als "Mining" (Bergbau) bezeichnet wird. Andere Beispiele sind Ethereum, das eine Reihe von Tools und Diensten anbietet, darunter dezentrale Anwendungen ("distributed applications", Dapps), und Monet, eine Open-Source-Blockchain, die für Ad-hoc-Peer-to-Peer-Zusammenarbeit gedacht ist.<sup>3</sup> In erlaubnisfreien Systemen wird die Integrität durch kryptografische und algorithmische Lösungen erreicht, die sicherstellen, dass anonyme Netzwerkteilnehmer einen Anreiz haben, die Genauigkeit des Ledgers ohne Regulierung und administrative Kontrolle durchzusetzen. Erlaubnisfreie-offene Netzwerke ("permissionless open networks") sind tendenziell leistungsfähiger als geschlossene Netzwerke; die Beteiligten haben ein Interesse daran, sich gemeinsam auf Standards für das Betriebsmodell zu einigen, einschließlich der Aufteilung von Vorteilen und Kosten und der Art und Weise, wie der Zugang gewährt und das Risiko verwaltet wird.

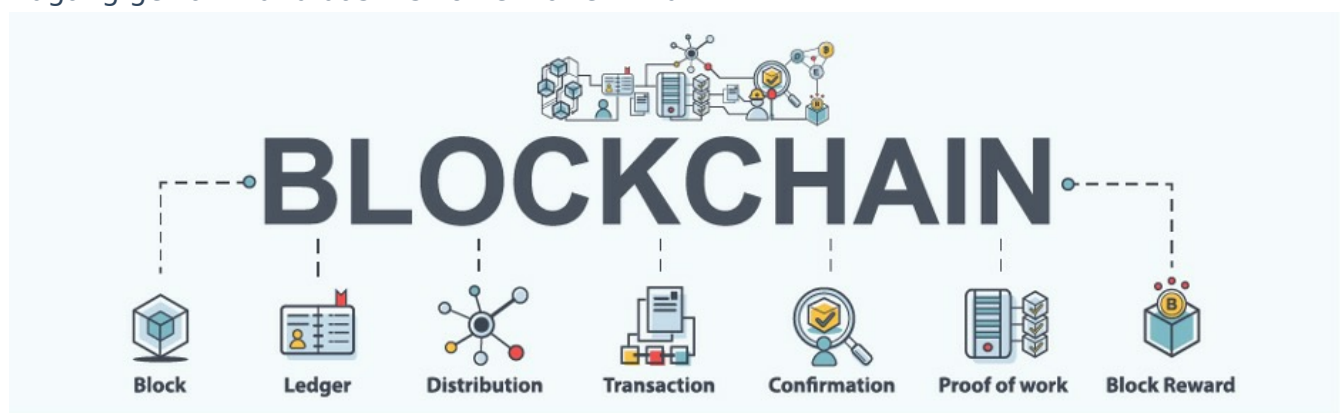


Bild aus <https://blockruption.com>

In genehmigten (permissioned) Blockchain-Systemen, die oft auf privater Basis arbeiten, werden die Mitglieder im Voraus ausgewählt, wobei ein Administrator den Zugang kontrolliert und Regeln durchsetzt. Durch die zentrale Verwaltung und Regulierung wird sichergestellt, dass die Identität und der Datenschutz bei permissioned Systemen besser geschützt sind. Ein weiteres attraktives Attribut dieses Modells ist, dass es sich leichter in

bestehende rechtliche und regulatorische Rahmenbedingungen einfügt und daher besser geeignet ist, traditionelle Aufzeichnungs- und Transaktionssysteme zu ersetzen. Hyper-Ledger Fabric ist ein Beispiel für ein erlaubnisfreies System, das private Transaktionen und Vereinbarungen unterstützt und von Organisationen wie Walmart, der Regierung von British Columbia und der Deutschen Börse genutzt wird.<sup>4</sup>

Ursprünglich wurden erlaubnisfreie offene Netzwerke vor allem für Krypto-Assets verwendet, die von der Öffentlichkeit gehalten wurden, während unternehmensbasierte Systeme erlaubt waren und privat betrieben wurden. Seit 2019 gibt es jedoch einen Trend weg von zentralisierten Systemen hin zu dezentralen erlaubnisfreien Systemen, angetrieben durch branchenübergreifende Zusammenarbeit und eine erhöhte Bereitschaft, mit öffentlichen Plattformen zu experimentieren.<sup>5</sup>

## Blockchain in der Praxis

Die bekannteste Anwendung für Blockchain ist Bitcoin, die größte der vielen digitalen Währungen. Es gibt jedoch viele andere Anwendungen, quer durch alle Branchen, wie z. B. die Transaktionsabwicklung bei Finanzdienstleistungen, die Verwaltung von Versicherungsansprüchen, Urheberrechtsaufzeichnungen in den Medien und Patientenakten im Gesundheitswesen.

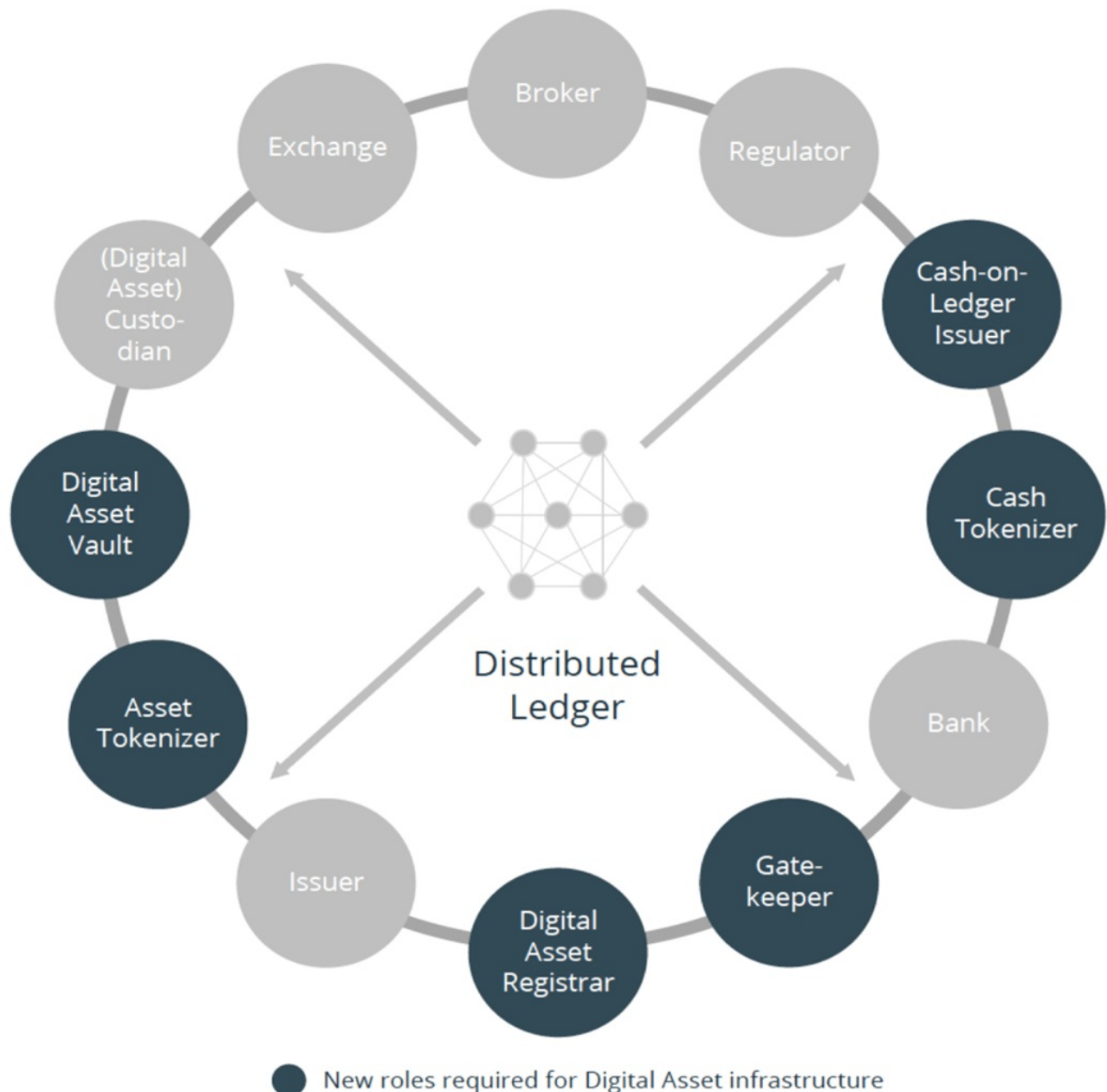
Anwendungen konzentrieren sich in der Regel auf die Senkung von Verwaltungskosten und die Steigerung der Effizienz, wie z. B. im Gesundheitswesen, wo es ein erhebliches Potenzial für die Rationalisierung bestehender Prozesse gibt, wie z. B. den Austausch von Patientenakten zwischen Gesundheitsdienstleistern, Versicherern und Patienten.

Unternehmen, die Blockchain für das Lieferkettenmanagement einsetzen, verwenden in der Regel private-permissioned Systeme, die es dem Management des Sponsors ermöglichen, Mitgliedschaft, Zugriff und Rechte zu kontrollieren. Everledger hat zum Beispiel eine Reihe von Blockchain-basierten Plattformen zur Unterstützung von Fachunternehmen aufgebaut, darunter ein Distributed-Ledger, das Diamanten aufzeichnet. Für jeden Diamanten wird ein digitaler "Pass" erstellt, in dem seine Herkunft, seine Bewegung, seine Schleifarbeiten, der Austausch von Eigentumsrechten und andere relevante Informationen aufgezeichnet werden. Das System soll unter anderem die Fälschung von Dokumenten und Betrug reduzieren, einen effektiven Versicherungsschutz ermöglichen und Informationen über die Herkunft von Edelsteinen liefern, um deren Nachhaltigkeitsstatus zu belegen. Akteure auf dem Diamantenmarkt nutzen das System, um zu vermeiden, Teil der Kette zu sein, die mit Geldwäsche, Terrorismusfinanzierung und der Beschaffung aus Konfliktgebieten in Verbindung gebracht wird.<sup>6</sup>

In der Metallindustrie nutzen Unternehmen Blockchain, um Transaktionen in der Lieferkette von Metallen wie Zinn, Wolfram, Tantal und Gold aufzuzeichnen, bei denen die Gefahr besteht, dass sie aus Minen stammen, die mit Konflikten oder Menschenrechtsverletzungen in Verbindung gebracht werden. So hat Sustain Block, unterstützt von der European Partnership for Responsible Metals, 2019 ein System zur Nachverfolgung von Lieferketten für Metalle aus Ruanda eingerichtet. iPoint hat ein System zur Nachverfolgung von Metallen von der Mine bis zum Laden entwickelt, um die Bemühungen von Verbrauchermarken zu unterstützen, ihren Kunden ihre hohen Standards in Bezug auf Nachhaltigkeit und soziale Verantwortung nachzuweisen,<sup>7</sup> während Minespider ein weiteres System zur Nachverfolgung von Metallen von den Minen über die Schmelzwerke bis hin zu den Fabriken ist.<sup>8</sup>

Der Handel und die Handelsfinanzierung sind ein weiterer Bereich, der sich stark entwickelt

hat. Marco Polo und Contour sind Beispiele für Handelsfinanzierungsnetzwerke, die zur Unterstützung von Banktransaktionen eingerichtet wurden.<sup>9</sup> TradeLens, eine Blockchain-basierte digitale Lieferkette, die gemeinsam von Maersk und IBM entwickelt wurde, soll die Komplexität der Nachverfolgung des internationalen Handels durch papierbasierte Systeme reduzieren.<sup>10</sup> 2018 führten HSBC und ING die erste Handelsfinanzierungstransaktion über Blockchain für eine Lieferung von Sojabohnen von Argentinien nach Malaysia durch, wobei eine einzige gemeinsame Plattform verwendet wurde, um Transaktionen innerhalb von 24 Stunden abzuwickeln, verglichen mit den 5 bis 10 Tagen, die herkömmliche Methoden normalerweise benötigen.<sup>11</sup>



## Treiber der Akzeptanz

Unternehmen wenden viel Zeit und Ressourcen für den Abgleich ihrer Datensätze mit externen Quellen auf, um deren Integrität zu prüfen und Inkonsistenzen mit den Datensätzen von Partnern zu erkennen. Auch organisationsinterne Abstimmungen sind üblich, da die meisten Unternehmen mehrere Systeme für die Verwaltung verschiedener Prozesse, die Aufzeichnung von Transaktionen und Vermögenswerte verwenden. Blockchain-Systeme automatisieren diese teure und fehleranfällige manuelle Tätigkeit durch fortlaufende automatisierte Verifizierungsprozesse, die die Genauigkeit und

Konsistenz der Daten über die Knoten des Netzwerks hinweg überprüfen.

Blockchain ermöglicht eine Abkehr von der traditionellen sequentiellen Kommunikation und der damit verbundenen Verarbeitung durch die Parteien in einer Transaktionskette, um eine gleichzeitige gemeinsame Kommunikation und Aktivitäten zu ermöglichen, die durch netzwerkbasierte Kommunikation ermöglicht werden. Einer der Anwendungsbereiche ist die Wertpapierabwicklung; der Paxos Settlement Service, der die Blockchain-Technologie für die Abwicklung von börsennotierten US-Aktiengeschäften einsetzt, erzielt Effizienzgewinne durch die Kombination von Asset-Register und Abwicklungsregistern, wodurch die Verarbeitungsgeschwindigkeit erhöht und der Bedarf an Cross-Ledger-Abstimmungen reduziert wird.<sup>12</sup>

Vorteile wie Automatisierung, Transparenz, verbesserte Kontrollierbarkeit und Programmierbarkeit tragen zu Effizienzsteigerungen und Kostensenkungen bei, obwohl es in vielen Branchen Herausforderungen bei der Implementierung gibt, da die rechtlichen und regulatorischen Rahmenbedingungen für diese neuen und sich entwickelnden Geschäftsmodelle und -beziehungen noch nicht vollständig etabliert sind.

## Digitale Token

Digitale Token sind Datensätze innerhalb eines Blockchain-Systems, die das Eigentum aufzeichnen. Digitale Token können nativ digital sein, wie z. B. das Eigentum an einer Kryptowährung oder an digitalen Anleihen, wie sie z. B. von der Weltbank ausgegeben werden, oder sie können verwendet werden, um das Eigentum an einem physischen Vermögenswert aufzuzeichnen. Vermögenswerte können fungibel sein, was sich auf nicht einzigartige Vermögenswerte wie Soft Commodities bezieht, oder nicht fungibel, die einzigartig sind, wie Kunstwerke, was Sammlern ermöglicht, seltene und wertvolle Gegenstände leicht zu identifizieren, zu verfolgen und zu handeln.

Die Sygnum Bank hat die Anpassung des Schweizer Bundesgesetzes an die Distributed-Ledger-Technologie genutzt, um in der Schweiz und in Singapur Plattformen einzuführen, die die Ausgabe von Token in Bankqualität und den Handel mit digitalen Assets ermöglichen. Im Rahmen eines Teils dieser Plattform hat sie in Partnerschaft mit Fine Wine Capital das erste tokenisierte Angebot an investierbarem Wein ausgegeben.<sup>13</sup>

## Smart Contracts

Ein Smart Contract ist ein Stück Code, das in einer Blockchain gespeichert ist und automatisch ausgeführt wird, wenn vorher festgelegte Bedingungen erfüllt sind. In unternehmensübergreifenden Kooperationen können Smart Contracts eingesetzt werden, wenn Unternehmen zustimmen, an Vereinbarungen gebunden zu sein, ohne dass externe Vermittler wie Anwälte involviert sind. Die Regeln von Smart Contracts sind vordefiniert und die Ergebnisse sind klar, schnell verfügbar und kostengünstig; dies steht im Gegensatz zu traditionellen juristischen Verträgen, die einen erheblichen manuellen Aufwand für die Auslegung, die Einigung zwischen den Parteien und die Durchsetzung erfordern.<sup>14</sup>

Intelligente Verträge können z. B. zur Überwachung, zum Nachweis und zur Auslösung von Zahlungen für im Rahmen von Dienstleistungsverträgen erbrachte Leistungen verwendet werden, wobei die Zahlung automatisch erfolgt, sobald die erforderlichen Aktivitäten ausgeführt wurden. Smart Contracts sind besonders effizient, wenn sie in Finanzsysteme mit vielen Routinetransaktionen integriert werden, wie z. B. an Finanzbörsen.

## Fazit

Während die Bekanntheit von Blockchain in erster Linie mit Kryptowährungen in Verbindung gebracht wird, erstreckt sich ihre Relevanz im öffentlichen und privaten Bereich weit in kollaborative Netzwerke, Aufzeichnungen, Transaktionen und den Austausch von Werten. Die meisten Branchen erkennen die signifikanten Vorteile, was zu einer schnell wachsenden Akzeptanz führt, die die Art und Weise, wie Unternehmen und Privatpersonen miteinander interagieren, grundlegend zu verändern beginnt.

## Fußnoten

1. Distributed Ledger Technology and Blockchain, World Bank.  
<http://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>
2. Blockchain and DLT – Transforming the Financial World, Tokentrust AG BrightTalk with NTree. <https://www.brighttalk.com/webcast/17849/468189>
3. <https://ethereum.org/en/> , <https://monet.network/>
4. <https://www.hyperledger.org/use/fabric>
5. Hyper real: An overview of global blockchain industry trends, Invesco.  
<https://www.invesco.com/emea/en/invesco-insights/insights/hyper-real-an-overview-of-global-blockchain-industry-trends.html>
6. <https://www.everledger.io/industry-solutions/diamonds/>
7. <https://www.sustainblock.org/>
8. Bloomberg, April 2019. <https://www.bloomberg.com/news/articles/2019-04-24/using-blockchain-to-help-fight-conflict-minerals>
9. <https://www.marcopolo.finance/> , <https://www.contour.network/>
10. <https://www.tradelens.com/>
11. Rebooting a Digital Solution in Trade Finance, Bain and HSBC.  
[https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwil1-D52\\_3uAhVKQEAHTwsAvAQFjAAegQIARAD&url=https%3A%2F%2Fwww.gbm.hsbc.com%2Fmedia%2Fgbm%2Finsights%2Fattachments%2Frebooting-digital-solution-digital.pdf&usg=AOvVaw12HyGoam1-Ut9MHho3Oy0W](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwil1-D52_3uAhVKQEAHTwsAvAQFjAAegQIARAD&url=https%3A%2F%2Fwww.gbm.hsbc.com%2Fmedia%2Fgbm%2Finsights%2Fattachments%2Frebooting-digital-solution-digital.pdf&usg=AOvVaw12HyGoam1-Ut9MHho3Oy0W)
12. Hyper real: An overview of global blockchain industry trends, Invesco.  
<https://www.invesco.com/emea/en/invesco-insights/insights/hyper-real-an-overview-of-global-blockchain-industry-trends.html>
13. <https://news.bitcoin.com/swiss-companies-issue-first-tokenized-asset-for-trading-under-new-national-blockchain-rules/>
14. Blockchain and contracts – a smart new world, Freshfields.  
<https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/fintech/blockchain-and-smart-contracts/>