

MAI 2017

## Newsletter

Autoren:  
Roland Mathys  
Samuel Klaus



ICT / NEW TECHNOLOGIES

## Blockchain - Mythen, Fakten und Rechtsfragen

**Blockchain** ist das *Buzzword* der Stunde. Nicht immer entsprechen die Mythen um Blockchain auch den Fakten. Dieser Newsletter klärt zentrale Begriffe und Aussagen und identifiziert die sich stellenden rechtlichen Probleme. Im Vordergrund stehen dabei weniger technische Details als vielmehr die offenen Fragen bei der Umsetzung und deren rechtliche Konsequenzen.

### 1 DIE BLOCKCHAIN-TECHNOLOGIE

#### 1.1 BLOCKCHAIN ALS GRUNDLAGENTECHNOLOGIE

Es gibt nicht "die Blockchain", genausowenig wie es "das Auto" gibt. Mit dem Begriff der Blockchain wird eine Grundlagentechnologie bezeichnet, die in verschiedenster Weise für ganz unterschiedliche Produkte genutzt werden kann. Genauso wie es Lieferwagen, Sportwagen, Family-Vans oder Offroadler gibt.

#### 1.2 FUNKTIONSWEISE UND CHARAKTER

Die Blockchain-Technologie bezeichnet eine Datenbank bzw. ein **Register (Ledger)**, in dem die Inhaber bestimmter Rechte verzeichnet sind, und das **dezentral (distributed)** verwaltet werden kann (aber nicht muss). In der Fachwelt ist deshalb eher die Rede von **Distributed Ledger Technology** ("DLT").

Blockchain-Anwendungen stellen somit im Grunde einfach **Register von Rechteinhabern** dar - ein vergleichbares Pendant aus der nicht-digitalen Welt wäre z.B. das Grundbuch. In einem solchen Register sind die Rechteinhaber (zumeist) nicht namentlich, sondern anonymisiert eingetragen (mittels Verschlüsselung). Der Ausweis über die Berechtigung erfolgt mit dem entsprechenden kryptographischen Schlüssel (sog. *Private Key*). Änderungen im Register (z.B. bei der Transaktion eines Rechtes) kann somit nur der Inhaber des *Private Key* auslösen (vergleichbar mit dem Grundeigentümer, der bei einem Grundbucheintrag seinen Ausweis vorlegen muss). Im Register (d.h. in der Blockchain) wird der gesamte Änderungsverlauf (d.h. die Transaktionshistorie) aufgezeichnet und ist jederzeit ersichtlich (wie sich auch im Grundbuch die früheren Handwechsel nachvollziehen lassen).

Der Vorteil eines auf einer Blockchain basierenden Registers ist deren Charakter als **effizientes und kostengünstiges Abwicklungsinstrument**. Während es z.B. bei einer Grundbuchtransaktion bis zum Eintrag mehrere Tage dauern kann, können Änderungen in einem Blockchain-Register innert weniger Sekunden erfolgen. Welche Rechte mittels einer Blockchain verwaltet werden, ist dabei zweitrangig (vgl. dazu Ziff. 1.3); relevant ist der **Vorteil der einfacheren Abwicklung** gegenüber herkömmlichen Registern (gleich wie jeder Inhalt eines Briefes auch per E-Mail versandt werden kann - einfach schneller und kostengünstiger).

**"Blockchain-/DLT-Anwendungen sind hocheffiziente und kostengünstige Abwicklungsinstrumente."**

Da die gesamte Abwicklung elektronisch erfolgt, müssen Blockchain-Register nicht mehr zwingend zentral (d.h. von einer zentralen Kontrollinstanz), sondern können **dezentral** geführt werden (sog. **Distributed Ledger**). Diesfalls werden identische Kopien des Registers (d.h. der Blockchain) gleichzeitig auf einer Vielzahl von Computern gespeichert, auf denen die entsprechende Anwendungs-Software läuft (sog. **Nodes**). Der Abgleich zwischen den **Nodes** erfolgt mittels eines in der Anwendungs-Software festgelegten Mechanismus, damit bei einer Änderung des Registers umgehend wieder auf allen **Nodes** die aktuellste Version vorliegt (vergleichbar mit einer Backup-Lösung, die gleichzeitig eine Vielzahl von Backups 'in der Cloud' erstellt).

### 1.3 ANWENDUNGSBEREICHE

DLT-Anwendungen sind **in allen Bereichen denkbar, in denen Transaktionen hinsichtlich irgendwelcher Rechte schnell, kostengünstig und möglichst beweissicher** ausgeführt werden sollen. Dabei kann es sich um digitale Versionen bereits existierender Papier-Register handeln (wie z.B. eine Blockchain-Version des Grundbuchs oder eines Aktienbuchs) oder auch um neue Register, deren Umsetzung bisher an den Kosten oder der Komplexität der Umsetzung gescheitert wäre (wie z.B. ein Register von Bildern, Diamanten oder Ersatzteilen, um deren Herkunft zu belegen und damit Raubkunst, 'Blood Diamonds' oder Fälschungen einzudämmen). Die Mehrzahl heutiger Blockchain-Anwendungen findet sich im Bereich der **Kryptowährungen** (wie z.B. Bitcoin).

## 2 MYTHEN UND FAKTEN

Blockchain und DLT-basierte Anwendungen generell werden oftmals damit beworben, dass Blockchain **sicher** sei, die Einträge in einer Blockchain **unveränderbar** seien, und dass bei einer Blockchain-Anwendung **kein Vertrauen in eine zentrale Instanz** mehr nötig sei, da eine solche Anwendung **vollständig dezentral** funktioniere. Ganz so weit halten diese Mythen den Fakten jedoch nicht stand.

### 2.1 SICHER?

Wohl sind die im Rahmen einer DLT-basierten Anwendung eingesetzten **kryptographischen Verfahren grundsätzlich sicher** (bei richtiger Implementierung). Dies betrifft jedoch nur die DLT als Grundlage einer darauf basierenden Anwendung. **Nur weil eine Anwendung auf Blockchain basiert, ist sie aber nicht einfach als Ganzes sicher**. Um auf das Beispiel des Autos zurückzugreifen: Nur weil die beim Verbrennungsmotor eingesetzte Technologie mittler-

weile als "sicher" gilt, lässt sich nicht folgern, dass jedes Auto mit Verbrennungsmotor automatisch "ein sicheres Auto" sei.

### 2.2 UNVERÄNDERBAR?

Auch die Aussage, die **Blockchain sei unveränderbar**, entspricht in dieser Allgemeinheit nicht den Fakten. Tatsächlich hängt die Integrität einer Blockchain von verschiedenen Faktoren ab, die je nach Implementierung der DLT-Technologie **Möglichkeiten zu (nachträglichen) Änderungen eröffnen**.

Weitreichende Eingriffsmöglichkeiten bietet zum einen die **Anwendungs-Software** der **Nodes** zur Verwaltung einer dezentral geführten DLT-Anwendung. Dies wurde eindrücklich vorgeführt im Sommer 2016, als die Anwendungs-Software des DLT-basierten Investment-Vehikels 'The DAO' geändert wurde, um unliebsame Transaktionen im Wert von damals USD 50 Mio. gegen den Willen des Betroffenen rückgängig zu machen (Stichwort: *Ethereum Hard Fork*).

Aber auch sonst kann Einfluss auf eine Blockchain genommen werden, je nachdem wie der **Mechanismus zum Abgleich unter den verschiedenen Nodes** implementiert wurde. Zählt hier z.B. in erster Linie die Rechenleistung der Nodes (wie bei gewissen Kryptowährungen), so eröffnet dies ebenfalls Möglichkeiten zur Manipulation, wie etwa im Sommer 2014 im Rahmen der Bitcoin-Blockchain (Stichwort: *GHash.io 51% attack*).

### 2.3 KEIN VERTRAUEN NÖTIG?

Die DLT wurde zwar u.a. mit dem Ziel entwickelt, ein Transfersystem zu schaffen, das nicht unter Kontrolle einer Zentralinstanz (wie z.B. einer Bank als zentralem Zahlungsvermittler) steht und somit **kein Vertrauen in eine solche Instanz** voraussetzt. Jedoch ist auch bei DLT-Anwendungen **weiterhin ein gehöriges Mass an Vertrauen nötig - einfach in eine andere Instanz**: Traditionelle Systeme setzen Vertrauen in die Abwicklungsinstanz voraus, DLT-Anwendungen einerseits in die Entwickler der Anwendungs-Software (gewollte Änderungen (vgl. Ziff. 2.2 [*Ethereum*]), fehlerhafte Implementierung, schadhafter Code, etc.). Andererseits verlangt ein vollständig dezentrales DLT-System auch Vertrauen in die (zumeist anonymen) Betreiber der **Nodes**, da eine Mehrheit derselben durch koordiniertes Handeln eine Blockchain beeinflussen kann (vgl. Ziff. 2.2 [*GHash.io*]).

### 2.4 DEZENTRAL?

Theoretisch sind **weitgehend dezentrale DLT-Anwendungen denkbar** (wie z.B. Bitcoin). Selbst hier aber liegt eine gewisse Zentralisierung (im Sinne einer Kontroll-/Einflussmöglichkeit) durch den Einfluss auf die Anwendungs-Software vor, oder sie erfolgt über marktbedingte Konzentrationseffekte, z.B. wenn sich **Nodes** zu sog. *Mining-Pools* zusammenschliessen, um durch Kombination ihrer Rechenleistung Skaleneffekte zu erzielen (zu den Folgen vgl. Ziff. 2.2 [*GHash.io*]).

Im Gegensatz zum Credo der vollständigen Dezentralisierung kann eine **Kontrolle durch eine zentrale Instanz** gerade dazu dienen, durch Vertrauen in diese Instanz auch **Vertrauen in das Abwicklungssystem** zu generieren (vgl. Ziff. 2.3), falls entsprechende rechtliche Rahmenbedingungen vorgesehen werden (vgl. Ziff. 3.2). Eine zentrale Kontrollinstanz ermöglicht zudem DLT-Anwendungen in Branchen, wo aufgrund **regulatorischer Vorgaben** keine

vollständig dezentralisierten Systeme ohne Kontrollmöglichkeit zulässig sind (z.B. Bankenbereich, Wertschriftenhandel, etc.).

### 3 KONSEQUENZEN UND RECHTSFRAGEN

Welche Konsequenzen ergeben sich nun aus den vorstehenden Betrachtungen in tatsächlicher und rechtlicher Hinsicht?

#### 3.1 UMSETZUNG AUSSCHLAGGEBEND

DLT stellt eine Grundlagentechnologie dar – und nicht ein bestimmtes Produkt. Die Eigenschaften und Qualitäten eines auf einer Blockchain basierenden Produktes ergeben sich aus der konkreten Implementierung. **Ausschlaggebend ist immer die technische und rechtliche Umsetzung.**

"DLT als solche ist nicht alleiniger Erfolgsgarant - ausschlaggebend ist die technische und rechtliche Umsetzung."

Die Bedeutung der **technischen Umsetzung** lässt sich mit dem Erfolg der Elektroautos illustrieren: Autos mit elektrischem Antrieb gibt es schon lange und in vielen Formen, aber erst die technisch hochstehende und eine breite Masse ansprechende Umsetzung führte zum Durchbruch. Blockchain-basierte Anwendungen gibt es viele, aber **DLT als solche ist nicht alleiniger Erfolgsgarant – ausschlaggebend ist deren konkrete Umsetzung.**

Auch wenn DLT-Anwendungen rein elektronisch, quasi 'virtuell' funktionieren, agieren sie nie losgelöst von der realen Wirtschaft – zumindest dann nicht, wenn sie für wirtschaftlich interessante Anwendungen eingesetzt werden sollen. Dann nämlich sind **Schnittstellen zur realen Wirtschaft** nötig, und spätestens in diesem Zeitpunkt wird die **rechtliche Ausgestaltung einer DLT-Anwendung relevant**. Diese ist ausschlaggebend für das Vertrauen, das dem System entgegengebracht wird, für den Umgang mit Fehlern (z.B. in der Implementierung), Problemen (z.B. in der technischen Abwicklung) und Unklarheiten (z.B. bei Streitfragen, insb. über die Zulässigkeit gewisser Aktionen, vgl. Ziff. 2.2 [Ethereum]).

#### 3.2 RECHTSFRAGEN

Im Rahmen der rechtlichen Ausgestaltung stellen sich aus vertragsrechtlicher Sicht insbesondere Fragen zu den folgenden Punkten (zu den regulatorischen Aspekten vgl. den Newsletter von April 2017):

Von grundlegender Bedeutung ist die Frage nach den **Rechtsverhältnissen**, d.h. die Klärung, **wer im Rahmen einer DLT-Anwendung mit wem kontrahiert** (und dabei welche **Leistungspflichten** und welche **Haftung** übernimmt). Je nach Art der DLT-Anwendung können Nutzer direkt mit anderen Nutzern in einer vertraglichen Beziehung stehen oder aber - z.B. bei DLT-Anwendungen mit Kontrollinstanz (vgl. Ziff. 2.4) - in erster Linie mit einem Systembetreiber bzw. der Kontrollinstanz. Ebenfalls hierunter fällt die Frage der Qualifikation der sogenannten **Smart Contracts**. Dieser Begriff bezeichnet bedingte Transaktionsanweisungen mit automatisierter Abwicklung im Rahmen einer DLT-Anwendung. Die Bezeichnung als

*Smart 'Contract'* ist irreführend, da es sich gerade **nicht um Verträge im Rechtssinn handelt**, sondern um Mechanismen zur automatisierten Abwicklung vorbestimmter Transaktionsanweisungen. Sind diese einmal implementiert, bieten sie - je nach Umsetzung - kaum Möglichkeiten zur nachträglichen Beeinflussung und können zu unvorhergesehenen Resultaten führen. **Smart Contracts setzen deshalb nicht weniger, sondern eher mehr rechtliche Regelung voraus.**

Eine Möglichkeit zur Klärung der Rechtsfragen, insbesondere bei DLT-Anwendungen mit einer zentralen Kontrollinstanz, können Bedingungen für die Teilnahme am betreffenden DLT-System sein - eigentliche **"Blockchain-AGB"**. Je nach Umsetzung und Ausgestaltung der jeweiligen DLT-Anwendung (Zweck, Art der verwalteten Rechte, Anonymität, Koordinationsmechanismus, etc.) sind in solchen Bedingungen ganz unterschiedliche Punkte zu regeln.

Wird eine DLT-Anwendung nicht von einer zentralen Instanz betrieben, sondern durch ein **selbstorganisierendes System**, erfolgt die Koordination durch in der DLT-Anwendung implementierte Koordinations- und Entscheidungsmechanismen, z.B. Abstimmungsverfahren mit Stimmrechten. Hier sind nebst vertrags- auch **gesellschaftsrechtliche Fragen** zu klären, insbesondere bei Nutzern, *Node*-Betreibern oder 'Gesellschaftern', die verschiedenen Rechtsordnungen unterstehen.

Auch wenn sich die Prinzipien der DLT theoretisch verlässlich umsetzen lassen, so werden sich in der Praxis doch immer wieder Fehler, Unklarheiten oder Widersprüche ergeben. Besonderes Augenmerk ist deshalb auf die **Anspruchsdurchsetzung** und die **Streitschlichtung** im Zusammenhang mit DLT-Anwendungen zu legen. Einer unserer nächsten Newsletter wird sich spezifisch diesem Thema widmen.

### 4 FAZIT

Einige der vielgehörten Aussagen zu Blockchains stammen eher aus dem Bereich 'Mythen und Marketing'. Dennoch sprechen die Fakten für sich: **DLT ist eine vielversprechende Grundlagentechnologie zur effizienten Kommunikations- und Transaktionsabwicklung**. Deren Umsetzung wird die Digitalisierung in bisher davon wenig betroffenen Bereichen vorantreiben.

Die stark von technischen "Unfehlbarkeits-Vorstellungen" geprägte Terminologie jedoch **weckt zum Teil falsche Erwartungen und blendet tatsächliche Probleme aus**. Eine erfolgreiche Implementierung von DLT-Anwendungen setzt deshalb nicht nur deren technisch korrekte Umsetzung voraus, sondern auch eine **angemessene rechtliche Regelung** der besonderen Fragen, die sich bei auf Blockchain basierenden Systemen und Produkten stellen.

"Die Implementierung von DLT-Anwendungen setzt nicht nur deren technisch korrekte Umsetzung, sondern auch eine angemessene rechtliche Regelung voraus."

## Kontakte

Der Inhalt dieses Newsletter stellt keine Rechts- oder Steuerauskunft dar und darf nicht als solche verwendet werden. Sollten Sie eine auf Ihre persönlichen Umstände bezogene Beratung wünschen, wenden Sie sich bitte an Ihre Kontaktperson bei Schellenberg Wittmer oder an eine der folgenden Personen:

In Zürich:



**Roland Mathys**

Partner  
roland.mathys@swlegal.ch

In Genf:



**Olivier Hari**

Of Counsel  
olivier.hari@swlegal.ch



**Samuel Klaus**

Rechtsanwalt  
samuel.klaus@swlegal.ch



**Louis Burrus**

Partner  
louis.burrus@swlegal.ch



**SHELLENBERG WITTMER AG / Rechtsanwälte**

**ZÜRICH** / Löwenstrasse 19 / Postfach 2201 / 8021 Zürich / Schweiz / T+41 44 215 5252

**GENÈVE** / 15bis, rue des Alpes / Postfach 2088 / 1211 Genève 1 / Schweiz / T+41 22 707 8000

**SINGAPUR** / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapur 049909 / [www.swlegal.sg](http://www.swlegal.sg)

[www.swlegal.ch](http://www.swlegal.ch)

Dieser Newsletter ist auf unserer Website [www.swlegal.ch](http://www.swlegal.ch) auf Deutsch, Englisch und Französisch verfügbar.