

Was man mit Blockchain nicht machen kann

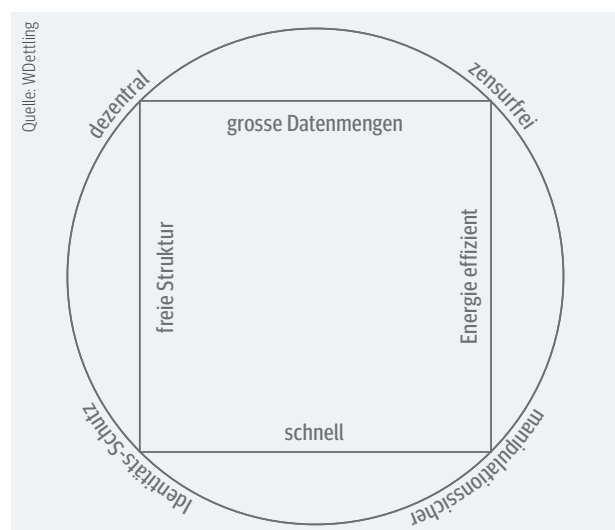
Nach der ersten Begeisterung über Kryptowährungen und Blockchain ist eine gewisse Ernüchterung eingetreten. Kryptowährungen wie Bitcoin halten sich zwar tapfer, aber bei den übrigen Blockchain-Anwendungen ist noch keine «Killerapplikation» in Sicht. Woran könnte das liegen?

Nachdem Bitcoin und generell die Kryptowährungen in den letzten beiden Jahren zuerst rasante Kurssteigerungen mit anschliessenden heftigen Einbrüchen verzeichnet haben, hat sich die Situation bei den «Kryptos» vorerst beruhigt. Der Handelswert der meisten Tokens ist gegen null gesunken und die Zahl der relevanten Kryptowährungen ist auf wenige Duzend geschrumpft. Unangefochten ist Bitcoin immer noch der Primus unter den Kryptowährungen.

Wie sieht die Situation bei Blockchain-Anwendungen ohne die Kryptowährungen aus?

Wir stellen fest, dass es in diesem Bereich viele Start-ups gibt, die davon träumen, mit ihren Blockchain-Anwendungen die Welt zu erobern. Genauso zahlreich sind Projekte von gestandenen Unternehmen, die mit einer Blockchain-Anwendung die Zukunft ihres Unternehmens gestalten wollen. Auch die grossen Technologieunternehmen wie IBM, SAP oder Microsoft investieren viel in die Blockchain-Entwicklung. Wie kommt es, dass trotz grosser und mittlerweile jahrelanger Anstrengungen bisher noch keine Blockchain-Anwendung den Markt überzeugen konnte?

In der Regel sind es meistens verschiedene Ursachen, die den Erfolg einer Idee verhindern oder verzögern. Folgende Überlegung könnte einen Anhaltspunkt geben, warum Blockchain noch nicht den grossen Durchbruch geschafft hat.



Die Quadratur des Blockchainkreises: Man kann Daten nicht gleichzeitig dezentral und schnell fälschungssicher online verfügbar machen.

Wofür die Blockchain-Architektur geeignet ist

Der Prototyp für die Blockchain-Architektur ist und bleibt Bitcoin. Die mehr als zehnjährige Geschichte von Bitcoin belegt, dass Architektur und Idee zusammenpassen, auch wenn die Konstruktion gewisse Mängel aufweist. Im Kern löst Bitcoin folgende Aufgabe: die fälschungssichere Veröffentlichung von digitalen Informationen ohne zentrale Kontrolle. Diese Aufgabe hört sich einfach an, war aber vor Bitcoin mit den verfügbaren digitalen Instrumenten nicht lösbar. Auch Bitcoin löst diese Aufgabe nicht allein mit technischen und kryptografischen Methoden, sondern mit der Kombination von Technologie, Kryptografie, wirtschaftlichen Anreizen und dem Öffentlichkeitsprinzip. Und genau die Tatsache, dass die dezentrale Speicherung von Daten nicht allein mit technischen Mitteln sicher gemacht werden kann, ist die Ursache für den grössten Schwachpunkt von Bitcoin: die begrenzte Skalierbarkeit. Es ist nicht möglich, tausende oder Millionen Transaktionen innerhalb von Sekunden mit den oben genannten Eigenschaften auszustatten. Alle Versuche, die Skalierung bei Blockchains deutlich zu verbessern, führten bisher zum Wegfall oder einer massiven Einschränkung der Dezentralisierung.

Wofür die Blockchain-Architektur nicht geeignet ist

Es liegt nahe, den Vergleich mit der Quadratur des Kreises zu machen, die nachweislich nicht möglich ist. Übersetzt auf die Blockchain lautet das unlösbare Problem: Man kann Daten nicht gleichzeitig dezentral und schnell fälschungssicher online verfügbar machen. Daran scheitern bisher alle Blockchain-Anwendungen. Sie setzen voraus, dass man bestehende Geschäftsprozesse in gewohnter Weise digital abbildet. Damit erzeugen sie Datenstrukturen und -mengen, die keine Blockchain genügend schnell verarbeiten kann.

Fazit

Bei der Suche nach geeigneten Blockchain-Anwendungen muss man sich von der gewohnten Anwendungs- und Datenstruktur befreien. Die Anwendungsdaten, die heute praktisch beliebig gross sein können, gehören nicht in die Blockchain. Man muss sich darauf beschränken, diejenigen Signaturen in einer Blockchain zu speichern, mit denen Zugriffsrechte, Integrität sowie Eigentums- und Herkunftsinformationen gesichert werden sollen.

