

# Des Kaisers neue Kleider

Keine Gazette, die etwas auf sich hält, konnte sich in den vergangenen Monaten eines Beitrags zum Thema Blockchain enthalten. „Disruptiv“, ja, „revolutionär“ sei diese Technologie, kann man da lesen. Sie stelle ganze Wirtschaftszweige in Frage und ermögliche neue Geschäftsmodelle, werde in vielen Bereichen zentrale Systeme (wie Banken) überflüssig machen und neue Transparenz in undurchsichtige Märkte bringen.

Ein solches Wunderding mag man nicht unbeachtet vorbeiziehen lassen – und so stürzen sich allerorten große und größere Unternehmen darauf: Wer lässt sich schon gerne abschaffen? Also werden Kooperationen ausgerufen und Konzeptideen in die Welt gesetzt – und die Blockchain mutiert zum „Must have“: Wer jetzt noch nicht dabei ist, hat die Zukunft verspielt.

Unglücklicherweise ist das Blockchain-Konzept nicht so einfach zu verstehen. Selbst Kryptologen ringen mit den Sicherheitsannahmen, die dem Verfahren zu Grunde liegen (siehe z. B. Achenbach, Baumgart, Rill in DuD 11/2017 oder das Schwerpunktheft 8/2017). Und so darf nicht verwundern, dass viele Beiträge und Nutzungsszenarien nebulös bleiben – denn es hat wohl auch der eine oder andere, der gerade neue Blockchain-Geschäftsideen herbeiträumt, nicht genau verstanden, wie das alles funktioniert. Details ja werden ohnehin überbewertet.

Darum stieg das Vertrauen in die „Kryptowährung“ Bitcoin ins Unglaubliche – und machte das Konzept zur *self fulfilling prophecy*: Wenn alle vertrauen, dann ist das Verfahren sicherlich vertrauenswürdig...

So faszinierend die Ideen hinter der Blockchain, so schwer lassen sich Anwendungen jenseits von Bitcoin (oder einer ähnlichen „virtuellen Währung“) vorstellen, für die eine dezentrale, komplett transparente und aufwändig zu verifizierende Blockchain die richtige technische Umsetzung ist. Schließlich muss die Prüfung aller „Kettenglieder“ der Blockchain honoriert werden (sie kostet Aufwand und Rechenleistung) und darf Datenschutz keine zu große Rolle spielen (denn in der Blockchain können alle Einträge eingesehen werden und die Nutzer sind lediglich pseudonym). In vielen der diskutierten Anwendungsfälle, in denen die Nutzung einer Blockchain ins Spiel gebracht wird, sind denn auch vertrauenswürdige Dritte wie „Notare“, die allgemein überprüfbare Bestätigungen für die Richtigkeit einer Transaktion ausstellen, oft eine bessere und elegantere Lösung.

Selbst für ein Zahlungssystem ist Bitcoin nur eingeschränkt geeignet: Transaktionen dauern lange, die Verifikation ist aufwändig und die dezentral zu speichernde Transaktionskette wird mit jeder Transaktion länger. Will man die Verifikation seiner Transaktion beschleunigen, kann das zudem kostspielig werden, weil man den „Minern“ eine zusätzliche Gebühr anbieten muss, um die rechenaufwändige Prüfung attraktiv zu machen. Schließlich darf man seinen geheimen Schlüssel zu seiner „digitalen Geldbörse“ nicht verlieren, sonst ist das Vermögen futsch.

Für die Bitcoin- und Blockchain-Investoren bleibt daher zu hoffen, dass so schnell niemand „Der König ist ja nackt!“ ruft.

Mit herzlichen Grüßen, Ihr



Dirk Fox