

Ein Blockchain-Siegel schützt edlen Wein vor Fälschern

Ein Zürcher Startup vernetzt Produzenten und Konsumenten mit digital-analogen Siegeln. Etikettenschwindel wird damit massiv erschwert. VON RUTH FILTERER (TEXT) UND JONAS OESCH (ILLUSTRATION)

Wein, Parfum, Pestizide und Medikamente haben einiges gemeinsam. Erstens kann Qualität teuer sein. Zweitens: Der Laie erkennt Qualität leichter an der Verpackung als am Inhalt. Das führt zu einer dritten Gemeinsamkeit: All diese Waren sind ein leichtes Ziel für Fälscher, die sie strecken oder den Inhalt ganz austauschen.

Durch Etikettenschwindel und Panscherei bei Weinen und Spirituosen entsteht laut der EU-Behörde für geistiges Eigentum jährlich ein Schaden von 2,3 Milliarden Euro, das würde grob gerechnet bedeuten, dass jede 21. Flasche gefälscht ist. Laut dem Umweltprogramm der Vereinten Nationen erfüllt jedes dritte Pestizid, das in Entwicklungsländern verkauft wird, nicht die Qualitätsstandards. Und die WHO schätzt, dass jedes Jahr Zehntausende Menschen an gefälschten Medikamenten sterben.

Als die Blockchain-Technologie bekannter und zum Synonym für Transparenz und Sicherheit wurde, kamen gleich mehrere Geschäftsleute auf die Idee, damit globale Lieferketten nachzuvollziehen. Konsumenten sollten einfach feststellen können, ob ein Produkt durch vertrauenswürdige Hände ging.

Der Chip auf der Flasche

Einer dieser Geschäftsleute ist der in Zürich ansässige Italiener Matteo Panzavolta. Die Lösung seines Startups Authena sieht in Aktion ganz simpel aus. Es klebt als Siegel am Korken einer Weinflasche, dort wo sonst Behörden oder Zertifizierer ihr Etikett hinterlassen. Doch das Authena-Siegel ist mehr als ein Stück Plastik: Als Panzavolta sein Smartphone näher heranholt, öffnet sich auf diesem ein Fenster. Dort steht, welchen Wein wir vor uns haben. Es handelt sich um einen 2015er Etna Rosso vom Weingut Marchese delle Saline aus Sizilien. Dabei steht noch eine Beschreibung des Weins und: «Die Flasche ist verschlossen.»

Diese Informationen schickt das Siegel durch dieselbe Technik ans Smartphone, die auch kontaktloses Bezahlen möglich macht. Die Nahfeldkommunikation (englisch: Near-Field-Communication, kurz NFC). Im Siegel steckt ein kleiner Chip. Wenn ein Lesegerät, in diesem Fall das Handy, dem Chip auf wenige Zentimeter nahekommt, wird sein elektromagnetisches Feld aktiviert und eine kleine Menge Informationen übertragen – in diesem Fall eine einzigartige Identifikationsnummer und die Information darüber, ob das Siegel noch intakt ist. Durch das Öffnen der Flasche wird ein Schaltkreis unterbrochen. Das «spürt» der Chip. Er stellt auf den Zustand «geöffnet» um, physisch und digital, und zwar unumkehrbar.

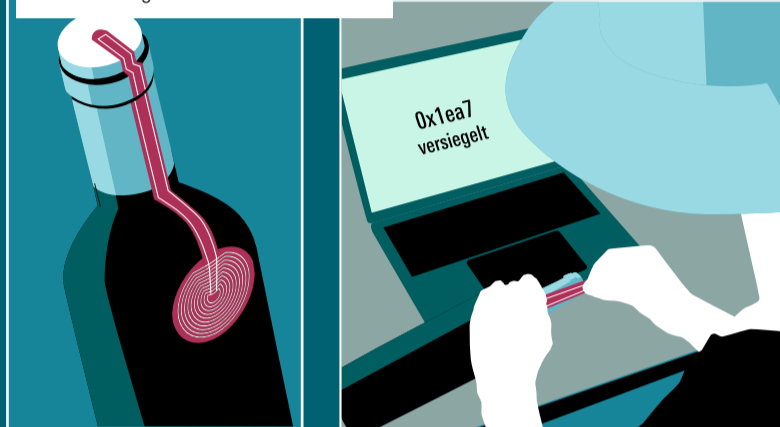
Der sizilianische Wein kostet etwa 50 Franken. Das könnte Anreiz genug sein, zu versuchen, das Siegel abzuziehen, um die Flasche mit etwas anderem zu befüllen. Doch wenn man versucht, die Folie vom Glas zu zupfen, bleibt etwas vom Metall am Flaschenhals kleben. Der Chip ist zerstört und kann nicht mehr gelesen werden. Für Konsumenten wäre das ein Zeichen, dass etwas nicht stimmt.

Hersteller weiss von jedem Scan

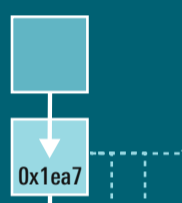
Praktisch jedes Smartphone kann NFC lesen, dazu ist keine eigene App nötig. Authena stellt aber auch eine App bereit, auf der Weinhersteller noch mehr Informationen zu dem jeweiligen Produkt hinterlegen können, etwa passende Rezepte. Käufer können den Wein dort bewerten – und sie können mit einem Link zur Blockchain prüfen, ob dort tatsächlich der Nachweis über die Flasche gespeichert ist, und zwar schon vor dem Kauf.

Wie das Blockchain-Siegel funktioniert

Eine Weinflasche mit einem NFC-Siegel. NFC steht für Nahfeldkommunikation. Dieselbe Technologie, die kontaktloses Bezahlen möglich macht.



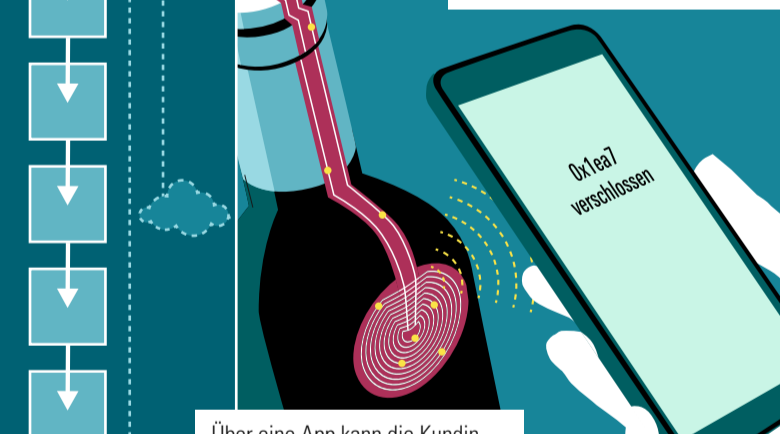
Die Blockchain



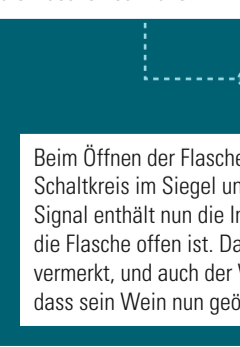
Ein Weinbauer auf dem Weingut Marchese delle Saline in Sizilien versiegelt die Flasche und trägt deren Code via Cloud in die Blockchain ein. Der Eintrag lässt sich danach nicht mehr verändern.



... es fliesst Strom, und das Siegel sendet ein Signal zurück. Darin steht einerseits der Code und andererseits die Information, dass die Flasche noch verschlossen ist.



Unabhängig davon erfährt der Weinbauer, dass das Siegel gescannt wurde und die Flasche noch zu ist.



Beim Öffnen der Flasche wird ein Schaltkreis im Siegel unterbrochen. Das Signal enthält nun die Information, dass die Flasche offen ist. Das wird auch digital vermerkt, und auch der Weinbauer erfährt, dass sein Wein nun geöffnet wurde.

Im Hintergrund bekommen es die Produzenten mit, wenn das Siegel eines ihrer Produkte ausgelesen wird. Zeit und Ort des Scans und die Information, ob das Produkt geöffnet wurde, werden über das Smartphone des Nutzers automatisch an die Cloud übermittelt. Sogar wenn in dem Moment kein Netz da ist, werden die Informationen auf dem Handy der Nutzer zwischengespeichert.

Als Beispiel führt Panzavolta Bauern in Lateinamerika an. Authena hat seine Siegel für den Chemiekonzern Lonza wegen des Vertriebs einer Fungizidlinie in Brasilien getestet. «Das Pilotprojekt ist noch nicht ganz abgeschlossen. Aber bereits jetzt ist klar, dass unser Siegel auch auf andere Produkte soll.» Das Siegel soll den Bauern Sicherheit geben, dass der Flascheninhalt nicht gestreckt oder ganz ausgetauscht wurde. Lonza erfährt andererseits Details darüber, was mit seinen Produkten nach dem Verkauf passiert.

Für viele Branchen attraktiv

Die Hoffnung auf eine Waffe gegen Fälscher, das Tracken von Produkten und die direkte Kommunikation mit dem Endabnehmer: All das ist für Hersteller von ganz verschiedenen Produk-

«Betrug soll jeweils so aufwendig gemacht werden, dass er sich nicht mehr rentiert.»

Matteo Panzavolta
Gründer und CEO
des Startup-Unternehmens Authena

ten attraktiv. Blockchain-Absicherungen gibt es auch für Handtaschen und Uhren, die bekanntesten Projekte in dem Bereich heissen Aura und Ariance. Der Technologiekonzern IBM hat sich eine Lösung für die Nahrungsmittelindustrie ausgedacht, IBM Food Trust. Unter den Abnehmern sind Nestlé, Dole und Walmart. Die Boston Consulting Group und der WWF finanzieren das Startup OpenSC, das den Konsumenten zeigen soll, woher genau ihr Essen kommt.

Auch der illegale Handel mit Medikamenten ist ein interessanter Anwendungsfall. Weil deren Preise staatlich reguliert sind, kommt es etwa vor, dass kriminelle Banden ein Krebsmedikament in der Türkei günstig einkaufen und in Dubai teurer weiterverkaufen, weil dort der staatlich festgesetzte Preis höher ist.

Blockchain ist nicht Blockchain

All diese Probleme soll die Blockchain lösen. Kunden denken dabei an Transparenz und Sicherheit, deshalb verwenden Firmen den Ausdruck inflationär. Doch es gibt grosse Unterschiede in der

Gestaltung. Bekannt ist die Blockchain durch die Kryptowährung Bitcoin geworden. Neben Bitcoin ist Ethereum die zweitbekannteste Blockchain. Sie ist die Grundlage für die Währung Ether, aber auch für Anwendungen wie die Lieferketten-Lösungen.

Diese Blockchains sind öffentlich. Das heisst, dass jede Transaktion für die ganze Welt offen einsehbar ist – auch wenn die Teilnehmer mit Pseudonymen, nicht mit Firmen- oder Klarnamen auftreten. Wichtig ist auch, dass alle Informationen über Überweisungen und Verträge bei unzähligen, anonymen Parteien zugleich gespeichert sind und dass diese Parteien anonym und unabhängig voneinander für deren Korrektheit einstehen. Durch diese Dezentralität ist eine öffentliche Blockchain trotz Anonymität gegen Manipulation gefeit, und deshalb wird die Technologie als revolutionär gefeiert. Der Preis dafür ist, zumindest im Moment, ein unglaublicher Energieverbrauch. Im Fall von Authena wird das Problem dadurch verkleinert, dass nur die allerwichtigsten Informationen direkt auf der Blockchain gespeichert werden.

Andere Anbieter betreiben nur lose an öffentliche Blockchains angeknüpfte oder ganz eigene Systeme. Diese nennt man private oder semiprivat Blockchains. Sie kosten manchmal weniger Energie und Geld, haben aber auch Nachteile. Etwa müssen die Teilnehmer bekannt und autorisiert sein. Es ist also kein öffentliches, dezentrales System mehr, sondern eine Art Klub von Leuten, denen man vertraut. Das können andere Firmen aus der Branche sein oder externe Autoritäten wie Notare.

Solche Lösungen sind nicht das, woran die meisten Menschen denken, wenn sie Blockchain hören. Sie liegen ein Stück näher bei jenen herkömmlichen Datenbanken, die eine einzige Person manipulieren kann.

Der Fälschungsaufwand steigt

Auch der sicherste Datenspeicherort nützt wenig, wenn die Verbindung zur realen Welt nicht fälschungssicher ist. Streifen- und QR-Codes beispielsweise können Betrüger recht leicht kopieren. Man könnte sich vorstellen, dass sie eine Verpackung mit falschem Inhalt befüllen und einfach einen neuen Kleber mit demselben Code anheften. NFC-Chips legen die Latte um einiges höher.

Panzavolta kritisiert Anwendungen, die private Blockchains oder QR-Codes nutzen: «Sie erzeugen eine Illusion von Vertrauenswürdigkeit.» Seiner Meinung nach steigt durch halbwegs sichere Lösungen der Anreiz, ein Produkt zu fälschen. Schliesslich seien Konsumenten bereit, für ein vermeintliches Premium-Produkt einen Aufpreis zu bezahlen. Die Hürden für Fälscher blieben im Vergleich relativ gering. Hundert Prozent Sicherheit kann keiner bieten. «Betrug soll jeweils so aufwendig gemacht werden, dass er sich nicht mehr rentiert», beschreibt Panzavolta das Ziel seiner Firma.

Noch einen Schritt weiter gehen dabei sogenannte «aktive» Siegel. Diese führen einen kleinen Akku mit und sind nicht davon abhängig, von einem Gerät gescannt zu werden. Sie überwachen selbständig Geodaten, Temperatur oder Feuchtigkeit und übermitteln diese Informationen, zum Beispiel über das Mobilfunknetz. Damit hat der Produzent eine nahezu ununterbrochene Kontrolle über den Weg seiner Produkte, von der Fabrik bis zum Verwender.

Solche Lösungen gehen allerdings ins Geld. Ob sich der Aufwand auszahlt, hängt davon ab, wie wertvoll das Produkt ist, das sie sichern sollen.