Goldschürfen im Crypto Valley

Erik Brühlmann

Hinter den seltsam zusammengesetzten Begriffen Blockchain und Bitcoin verbergen sich hochtechnologische Entwicklungen, die für Laien nur schwer zu fassen sind. Trotzdem deutet manches darauf hin, dass Blockchain und Bitcoin alltagsverändernde Technologien sein könnten – zumindest für die Geschäftswelt. Zwar stecken sie noch in den Kinderschuhen und haben noch einige Kinderkrankheiten. Ihr Potenzial wird jedoch bereits jetzt deutlich, und zwar überall dort, wo es um Werte, Transaktionen und Sicherheit geht.

Die Schweiz gilt global als eine Vorreiterin bezüglich Blockchain und den Entwicklungen um Kryptowährungen. Mancher spricht schon von einem veritablen Goldrausch im Crypto Valley, dem europäischen Blockchain-Cluster, dessen Zentrum sich im Kanton Zug befindet. So gut ist der digitale Ruf der Schweiz mittlerweile, dass die amerikanische Firma Crypto Explorers sogar Kurztrips ins Schweizer Crypto Valley anbietet.

BLOCKCHAIN

Technologisch gesehen handelt es sich bei einer Blockchain um eine kontinuierlich erweiterbare Liste von Datensätzen oder «Blöcken», die mittels kryptografischer Verfahren miteinander verkettet sind. Der Technologie-Experte Jamie Skella verwendet eine allgemein verständliche Analogie: Eine Blockchain ist wie ein Kassenbuch. Tausende identische Kopien dieses Kassenbuchs befinden sich auf Computern auf der ganzen Welt. Wenn zwischen einem Absender und einem Empfänger eine Transaktion stattfindet, wird diese im Kassenbuch eingetragen. Erst wenn der neue Eintrag von allen Kassenbuchkopien verifiziert wird, ist die Transaktion gültig. Aufgrund dieses Systems gilt eine Blockchain als so gut wie fälschungssicher, denn eine Fälschung eines Eintrages müsste auf allen Kopien vorgenommen werden.

Die Analogie ist jedoch mit Bedacht gewählt. Denn obwohl das Blockchain-System theoretisch auf jede beliebige Wertetransaktion angewendet werden kann, sind der Bitcoin und seine Ableger eine der ersten und sicherlich die bisher bekannteste Blockchain-Anwendung.

KRYPTO-WÄHRUNG

Kryptowährungen sind digitale Zahlungsmittel und gehören zu den ersten Anwendungen der Blockchain-Technologie. Bitcoin gilt dabei als Pionier. Sie bestehen nur aus einem Binärcode, haben also lediglich einen Wert, weil eine bestimmte Community sie als Zahlungsmittel anerkennt. Die verfügbare Menge einer bestimmten Kryptowährung wie Bitcoin ist in der Regel begrenzt. Für Experten ist der Begriff «Währung» jedoch irreführend, da viele der Kryptowährungen als symbolische Wertmarken konzipiert sind – ein «Token» dafür, dass man in eine Technologie, ein Start-up oder eine Community investiert hat.

In einem solchen Initial Coin Offering (ICO) wird ein Teil neu generierter Krypto-Tokens an Investoren verkauft. Das Start-up erhält so Kapital im Rahmen eines Crowdfundings, die Investoren mit den Tokens eine Art Faustpfand, das in Zukunft eingelöst werden kann. So gesehen funktionieren viele Krypto-Tokens ähnlich wie Cumulus-Punkte. Krypto-Tokens existieren jedoch nicht in einem rechtsfreien Raum. Bestehendes Recht kann auf die Tokens angewendet werden – und wird es auch.

ANZAHL KRYPTO-WÄHRUNGEN

Da Kryptowährungen nicht physisch gedruckt werden müssen und nicht von irgendwelchen Banken oder Regierungen abhängig sind, kann im Prinzip jeder seine eigene Kryptowährung erfinden. So erklärt es sich, dass es weltweit nur gerade 162 offizielle «physische» Währungen gibt, aber 2034 aktive Kryptowährungen.

TOTE KRYPTO-WÄHRUNGEN

Auch wenn Bitcoin nach einem gigantischen Höhenflug zuletzt wieder an Boden verloren hat, scheinen Kryptowährungen doch eine einzige, nie enden wollende Erfolgsgeschichte zu sein. Weit gefehlt! Die Website Deadcoins.com listet alle Kryptowährungen und damit Projekte auf, die entweder vom Projektteam aufgegeben oder als Betrug entlarvt wurden – von Secretcoin über Kreita bis Bitmillion. Alles in allem zählt die Website derzeit 929 gescheiterte Kryptowährungen.

CRYPTO VALLEY

Die USA haben das Silicon Valley, Europa hat das Crypto Valley – mit Zentrum in Zug. Nicht nur, weil dort viele international tätige Unternehmen ansässig sind, für die Blockchain und Bitcoin interessant sind. Auch die Crypto Valley Association hat sich dort niedergelassen und versucht, die Entwicklung auf diesen Gebieten voranzutreiben. Warum aber gerade in Zug? Wegen der «Pro-Business-Philosophie» der Behörden, den niedrigen Steuern und der Offenheit der Regierung für neue Technologien. Letzteres stimmt definitiv, denn man kann auf dem Einwohneramt kleinere Beträge mit Bitcoin bezahlen und sich auch eine Blockchain-basierte Identität zulegen. Das Crypto Valley breitet sich derweil immer weiter aus; mittlerweile gehören dazu die ganze Schweiz und das Fürstentum Liechtenstein. Im März dieses Jahres waren im Crypto Valley laut Cryptovalley.directory 320 Firmen mit rund 600 Mitarbeitenden ansässig. Jetzt sind es 539 Firmen mit über 3000 Mitarbeitenden.

MINING

Bitcoin-Mining ist mittlerweile ein Geschäft. Weltweit finden ständig Transaktionen statt, bei denen mit Bitcoins bezahlt wird. Alle in einem bestimmten Zeitraum stattfindenden Transaktionen werden in einer Liste – dem Block – zusammengefasst. Bitcoin-Mining bezeichnet das Aufspüren, Bestätigen und virtuelle Verbuchen aller Vorgänge innerhalb eines Blocks. Ein bestätigter Block wird in einen Hash – eine Reihe von Zahlen und Buchstaben – umgewandelt und endgültig in die Blockchain übertragen.

Als Belohnung für das Mining werden bei der Erstellung eines Hashs neue Bitcoins erzeugt, und der Miner erhält einen Teil der Transaktionsgebühren. Wie beim realen Goldschürfen ist es jedoch schwer, mit Mining reich zu werden. Jedesmal wenn jemand erfolgreich einen Hash erzeugt, erhält er derzeit lediglich 12,5 Bitcoins. Die Konkurrenz ist gross, und die nötige Technik zum effizienten Mining wird immer teurer.

WALLET

Wie beim richtigen Portemonnaie ist ein Bitcoin-Wallet dafür da, Bitcoins virtuell aufzubewahren. Jedes Wallet ist im Grunde eine einmalige Zeichenkette, in der das Guthaben gespeichert wird. Das Wallet ist anonym, persönliche Daten werden nicht hinterlegt. Zusätzlich ist das Wallet mit einem persönlichen Passwort geschützt. Wallets gibt es für Computer, Smartphones, Tablets, als Online-Wallets und in Form von USB-Sticks. Wie jede andere Software kann auch von einem Bitcoin-Wallet ein Backup zur Sicherheit erstellt werden.

ERSTE BITCOIN-TRANSAKTION

Die erste Bitcoin-Transaktion soll am 21. Mai 2010 stattgefunden haben. Der Programmierer Laszlo Hanyecz aus Florida schickte nach einem Aufruf in einem Forum 10 000 Bitcoins an einen Freiwilligen in England, der daraufhin eine Pizza für 19 Euro bestellte. Auf den heutigen Kurs umgerechnet, würde diese Pizza rund 61,5 Millionen Franken kosten.

ERSTE BLOCKCHAIN-ABSTIMMUNG

Bei der Umsetzung von Blockchain-Anwendungen ist vieles noch am Entstehen. Das Potenzial der Technologie wird aber bereits deutlich. Im Juni dieses Jahres führte die Stadt Zug zum Beispiel die erste Blockchain-Testabstimmung der Schweiz durch. Im Gegensatz zu anderen E-Voting-Systemen erfolgte der Abstimmungsprozess nicht über einen einzigen zentralen Server, sondern verteilt über eine Blockchain auf vielen Computern. Derzeit werden die technischen Details ausgewertet: Persönlichkeitsschutz, Abstimmungsgeheimnis, Unveränderbarkeit der Abstimmung sowie Prüf- und Nachvollziehbarkeit der Ergebnisse.

BLOCKCHAIN-FORSCHUNG

Die Blockchain-Technologie treibt Entwickler aller Branchen an. Dies vor allem, weil die Anwendungsmöglichkeiten zumindest in der Theorie schier endlos sind. Hochschulen könnten Diplome und Zertifikate unfälschbar ausstellen, und digitale Ausweise liessen Identitäten schnell und sicher verifizieren – eine Anwendung, die kürzlich in den Niederlanden vorgestellt wurde. Das Gesundheitswesen könnte elektronische Patientendossiers zusammenstellen, die überall auf der Welt im Notfall alle nötigen Patienteninformationen beinhalten – und das unter Einhaltung des Datenschutzes. Künstler könnten sich vor der Verbreitung von Raubkopien schützen. Südkorea denkt derzeit sogar darüber nach, Blockchain-Technologien zur Kontrolle und Verifizierung von Zolldokumenten einzusetzen.

BLOCKCHAIN-GESETZ

Da auch in Liechtenstein an Blockchain-Anwendungen getüftelt wird, möchte die Regierung per Gesetz festlegen, welche Anforderungen für Blockchain-Transaktionen gelten. Das «Gesetz über auf vertrauenswürdigen Technologien beruhende Transaktionssysteme» soll einerseits dem Konsumentenschutz Rechnung tragen, andererseits auch etwaigen Reputationsverlusten des Fürstentums vorbeugen. Die Rechtssicherheit im Umgang mit solch neuen Technologien müsse mit Blick auf künftige Entwicklungen gewährleistet sein.

«Der Laie muss Blockchain nicht verstehen, aber nutzen können»

Blockchain-Expertin Isabella Brom, Board Member der Bitcoin Association Switzerland, über Potenziale und Erwartungen

Bitcoin und Blockchain – Revolution oder «Rattengift»?
Einen disruptiven und allenfalls revolutionären Charakter hat diese Technologie sicher. Bezüglich Blockchain und Bitcoin muss man aber differenzieren. Ob Bitcoin sich als Währung durchsetzt, wird sich weisen. Die darunter liegende Technologie, die Blockchain, wird jedoch vieles im Businessbereich grundlegend verändern.

Was genau ist denn an Blockchain so innovativ?
Das Internet ermöglichte den Transfer von und den Zugang zu Informationen. Blockchain ermöglicht den weltweiten Transfer von Werten. Wir sprechen deshalb jetzt schon vom Internet of Information – dem World Wide Web – und vom Internet of Value, der Blockchain. Künftig können Werte aller Art auf der Blockchain registriert werden, ohne Drittparteien, ohne Verzögerungen und ohne Möglichkeit, die Werte und Transaktionen zu manipulieren.

Ist diese neue Technologie wirklich so sicher?
Blockchain hat zwei markante Sicherheitsaspekte: Erstens sind die Daten und damit auch die «Kontostände» dezentral verwaltet, sie können nicht einfach zentral verändert werden. Man kann also nicht auf einer Kopie allein Werte verändern. Zweitens sind die Blöcke kryptografisch mit den «chained hashes» verbunden. Eine Veränderung würde einen Aufwand bedeuten, der sich kaum lohnt. Man müsste alle bereits existierenden Blocks der Chain ebenfalls verändern. Immer noch angreifbar ist und bleibt aber die User-Ebene. Passwörter wie 1234 sind auch bei der Interaktion mit Blockchain-Wallets ungenügend.

Muss sich der Laie überhaupt eingehend mit der Blockchain-Thematik beschäftigen?
Nein. Es ist wie beim TCP/IP-Protokoll: Kaum ein Laie kann erklären, wie es funktioniert, aber jeder kann das Internet nutzen. Es ist aber wichtig, dass Unternehmen jeglicher Branchen verstehen, was Blockchain ist und kann, und wofür man sie nutzen soll.

Alle möglichen Unternehmen beschäftigen sich schon mit Blockchain – auch des PR-Effekts wegen?
Natürlich hat das Thema vor allem 2017 für viel Aufregung gesorgt, aber es ist nicht nur ein PR-Gag. Die Technologie kann durchaus wertbringend sein. Allerdings ist klar, dass nicht jede Blockchain-Anwendung, an der heute getüftelt wird, zwingend mit Blockchain umgesetzt werden müsste. Die Innovationen um die Technologie, auch mit gescheiterten Versuchen, sind aber nötig, um die Technologie, die heute noch ganz am Anfang steht, voranzutreiben. Schliesslich wird kaum ein Unternehmen sagen: Morgen stellen wir den gesamten Laden auf Blockchain um und hoffen das Beste!

Und wann werden wir unseren Kaffee mit Bitcoin bezahlen können?
In hoch entwickelten Industrienationen mit funktionierenden Regierungs-, Bank- und Rechtssystemen vielleicht gar nie. Kreditkarten funktionieren – der Druck des Endkonsumenten wird also vielleicht nie gross genug. Als eigentliche Währung interessant ist Bitcoin aber in Ländern mit hoher Inflation und Korruption. Dort kann ein Zahlungssystem, das nicht von politischen Entwicklungen abhängig und eingriffsresistent ist, einen grossen Stellenwert bekommen.

Ist der ganze Hype um Blockchain und Bitcoin nicht zu gross?
Die mediale Aufmerksamkeit bringt natürlich das Thema voran und fördert auch das Wissen darüber. Sie schürt aber auch Erwartungen, welche die Technologie zurzeit – da muss man ehrlich sein – noch nicht erfüllen kann. Die Technologie entspricht noch nicht in sämtlichen Bereichen von Sicherheit, Skalierung und Nutzerfreundlichkeit allen Anforderungen.

Erik Brühlmann