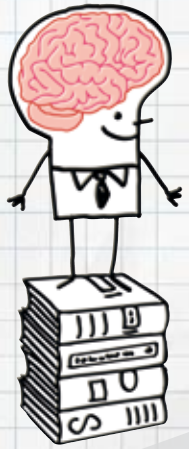
TechnoScope
by satw 4/21

Blockchain

Chancen und Risiken

www.satw.ch/technoscope

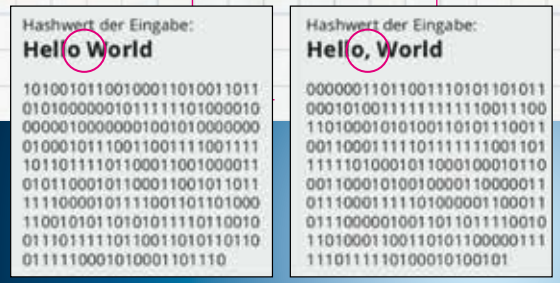
Wie sicher ist die Blockchain?



Die Blockchain gilt als unangreifbar, da sie über unzählige Computer verteilt ist. Zudem tragen verschiedene kryptographische Verfahren zur Sicherheit bei. Das Wort Kryptographie stammt aus dem Griechischen (kryptos: verborgen; graphein: schreiben) und bedeutet «Geheimschrift» oder Verschlüsselung. Bei der Blockchain spielt die Hashfunktion eine besondere Rolle. Sie besteht aus einem Algorithmus, der eine digitale Datei beliebiger Länge und verschiedenster Natur, also zum Beispiel einen Text, ein Video oder ein Audiofile, in eine Zeichenfolge mit fixer Länge komprimiert – den Hash (Prüfzahl). Bei SHA-256, dem in der Blockchain-Welt meistgenutzten Algorithmus, besteht der Hash immer aus 256 Zeichen. Jede kleinste Änderung der Eingabe erzeugt einen ganz anderen Output. Was passiert, wenn auch nur ein Komma hinzugefügt wird, zeigt das folgende Beispiel.

Und schliesslich benötigen alle, die an der Blockchain teilnehmen, eine Zugangssoftware. Diese besteht aus einem öffentlichen und einem privaten Schlüssel. Mit dem öffentlichen Schlüssel können alle auf einer Blockchain gespeicherten Dante eingesehen werden. Aber nur mit dem privaten Schlüssel können Transaktionen signiert werden. Der private Schlüssel ist eine geheime Zahlenfolge. Wer diese besitzt, hat Zugriff auf die mit diesem Schlüssel signierten Werte und kann sie zum Beispiel an andere übertragen.

Aufbewahrt wird das Schlüsselpaar in einem Wallet, einem «digitalen Portemonnaie»: online, mithilfe eines Softwareprogramms, oder offline, auf einer Festplatte oder als «Paper Wallet» ausgedruckt auf einem Stück Papier. Wallets können gefährliche Schwachstellen sein: Sie können gehackt werden, Passwörter und Festplatten können verloren gehen. Das ist der Supergau in der Bitcoin-Welt: Wer nicht mehr an seinen privaten Schlüssel kommt, kommt auch nie mehr an seine auf der Blockchain gespeicherten Werte heran. Zwischen drei bis fünf Millionen Bitcoins sollen so im Cyberraum blockiert sein.



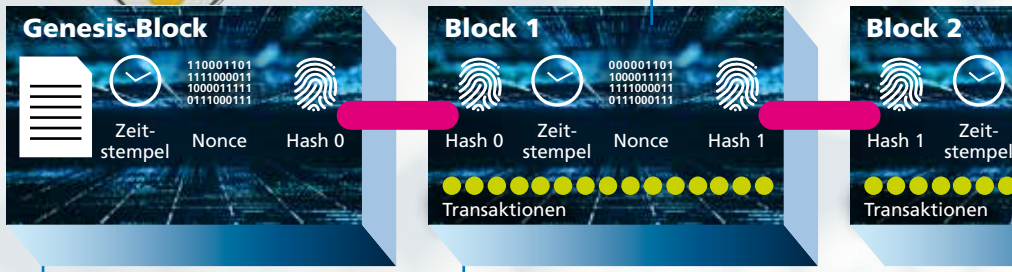
BLOCKCHAIN

Digitales Vertrauen

Die Blockchain ist nichts anderes als eine Datenbank in Form einer Kette von aneinandergereihten Datenblöcken. In jedem Block sind Informationen verschlüsselt hinterlegt. Jeder neue Block nimmt auf den vorhergehenden Bezug. So kann jeder Block nur mit genau zwei anderen Blöcken verbunden sein: dem, der ihm in der Kette vorangeht und dem, der ihm nachfolgt. Damit wird es unmöglich, Blöcke nachträglich zu verändern zu manipulieren oder gehackt zu werden.

Die Blockchain wird als unbestechliches, digitales Kontenbuch bezeichnet. Es gibt unzählige identische Kopien davon, die miteinander verknüpft sind. Wird in einem der Bücher ein Eintrag geändert, dann wird diese Änderung automatisch in allen anderen verbucht. Die Blockchain-Technologie wird deshalb auch Verteilte-Kontenbuch-Technologie oder Distributed-Ledger-Technologie (DLT) genannt.

Zentrale Kontrollinstanzen braucht es in dieser Kette keine. Umwege über vermittelnde Instanzen, wie Banken oder Versicherungen, werden mit der Blockchain überflüssig. Durch ihre Unveränderbarkeit schafft die Blockchain Vertrauen. Das sehen die einen als grosses Versprechen. Und die anderen als Bedrohung altbewährter Verfahren und Kontrollmechanismen. Welche Seite recht hat, ist bisher noch nicht ganz klar. Daher kommt der Hype rund um die Blockchain.

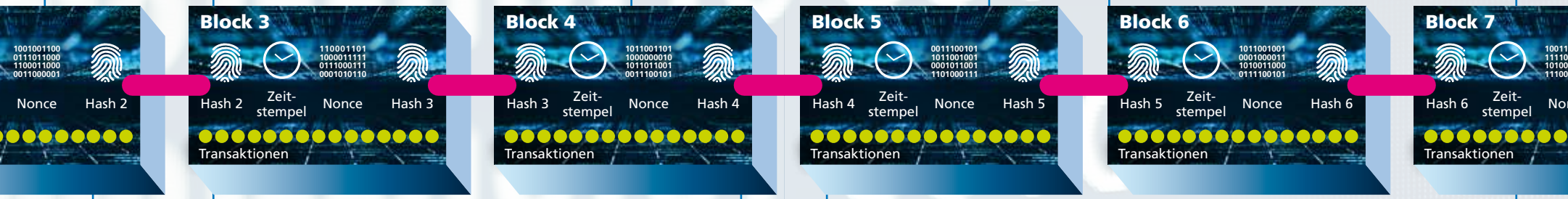


Schöpfer-Block: Im ersten Block einer Blockchain ist das Konsensprotokoll hinterlegt. Dieses wird von allen an der Blockchain-Beteiligten ausgehandelt und bestimmt, wie oft ein neuer Block in die Kette eingeschrieben wird, wie gross er sein kann, d.h. wie viele Transaktionen darin gespeichert werden dürfen. Und es legt fest, wer neue Blöcke überprüfen darf und welche Aufgabe dafür zu erfüllen ist.

Block 1, 2, 3....: Der Inhalt jedes Blocks besteht aus dem Hash-Wert (Prüfzahl oder digitaler Fingerabdruck, Details siehe: AHA!) aller im Block gespeicherten Informationen. Dazu kommen ein Zeitstempel und eine Zufallszahl (Nonce), die zur Validierung des Blocks benötigt wird. Und schliesslich der Hash-Wert des vorhergehenden Blocks.
Aus all diesen Elementen wird der Hash des neuen Blocks berechnet. Dieser ist sozusagen seine digitale Identitätskarte: Sie garantiert, dass es ihn nur einmal gibt (dass zum Beispiel darin enthaltene Geldwerte nicht mehrmals verrechnet werden können).

Minenarbeiter: Bevor ein neuer Block in die Kette eingereiht wird, kommen die Miner (Schürfer) ins Spiel. Sie sind die Buchhalter der Blockchain, prüfen die Gültigkeit der neuen Transaktionen, bündeln sie und versiegeln sie kryptographisch. Der Verfizierungsprozess (Proof of work) besteht aus der Lösung eines Krypto-Puzzles. Jeder Miner versucht im Wettstreit mit anderen, ein komplexes mathematisches Rätsel zu lösen. Wer die Aufgabe als Erstes löst, darf den Block an die Kette hängen und bekommt dafür eine Belohnung. Bei Bitcoin erhalten die Miner neue Bitcoins. Bei anderen Blockchains werden andere Formen von digitalen Werten (Token) geschaffen. Der Vorgang wird deshalb mit dem Schürfen von Gold verglichen.

Zutritt nur für Berechtigte: Bei privaten Blockchains ist die Zahl der Teilnehmenden begrenzt. Wer mitmachen darf, wer welche Zugriffsrechte hat und welche Validierungsprozesse gelten, bestimmt eine zentrale Instanz. Private Blockchains sind deshalb weniger transparent als öffentliche. Ihr Zweck ist aber meist auch ein anderer: Sie nutzen die Technologie, um sensible Daten fälschungssicher zu speichern. Private Blockchains kommen vor allem bei Unternehmen und öffentlichen Behörden zum Einsatz.



Öffentliches Gut: Bei öffentlichen Blockchains genügt es, das Open-Source-Protokoll herunterzuladen. Ein Identitätsnachweis ist nicht nötig. Alle Teilnehmenden haben die gleichen Rechte. Sie können alle Transaktionen einsehen und sich am Verifizierungsprozess beteiligen. Eine öffentliche Blockchain ist für alle Beteiligten völlig transparent.

Nodes (Knoten): Jeder Computer, der an der Blockchain teilnimmt, ist ein Knoten. Jeder Knoten speichert und verwaltet eine vollständige und fortwährend aktualisierte Kopie der Blockchain. Die mehrfache Abspeicherung der Daten macht das Netzwerk stabil und vertrauenswürdig. Es kann den Ausfall eines oder auch mehrerer Knoten ohne Weiteres verkraften.

Chancen der Blockchain:

- Weil sämtliche Informationen verschlüsselt gespeichert werden und die Blockchain auf viele Rechner verteilt ist, kann sie nicht manipuliert werden.
- Die Blockchain ist völlig transparent. Sie schafft Vertrauen zwischen Vertragspartnern, die sich nicht oder kaum kennen.
- Transaktionen werden direkt zwischen den Beteiligten abgewickelt. Das Ausschalten von Mittelmännern macht sie schneller, günstiger und weniger fehleranfällig.
- In Ländern mit wenig Rechtssicherheit hilft die Blockchain, Besitzrechte zu garantieren.

Pseudonymität: In einer öffentlichen Blockchain ist jede Transaktion einer öffentlichen Adresse zugeordnet, die keine Rückschlüsse auf die Person dahinter zulässt. Weil aber nicht auszuschliessen ist, dass jemand anhand der aufgezeichneten Transaktionen ihre Identität erraten könnte, ist die Blockchain genau genommen nicht anonym, sondern pseudonym. Aus diesem Grund eignet sie sich auch nicht besonders für krumme Geschäfte – auch wenn ihr dieser Ruf noch immer anhaftet.

Risiken der Blockchain:

- Die Blockchain basiert auf der enormen Rechenleistung einer Vielzahl von vernetzten Computern. Damit verbraucht sie Unmengen an Energie.
- Dass Nutzerinnen und Nutzer an öffentlichen Blockchains mit einem Pseudonym teilnehmen, kann für kriminelle Zwecke missbraucht werden.
- Wird die Person hinter einem Pseudonym bekannt, dann lassen sich sämtliche Transaktionen zurückverfolgen, die sie jemals auf der Blockchain ausgeführt hat. Das widerspricht dem vom Datenschutz vorgesehenen Recht auf Vergessen.
- Die Blockchain verspricht mehr Transparenz. Gleichzeitig ist sie so komplex, dass sie für die meisten Menschen völlig undurchsichtig und rätselhaft bleibt.

Wer hat's erfunden? 2008, mitten in der Bankenkrise, publizierte eine unbekannte Person oder Gruppe unter dem Pseudonym Satoshi Nakamoto einen wissenschaftlichen Aufsatz. Es ging darin um ein neues elektronisches System, mit Namen Bitcoin. Es sollte im Stande sein, Geldwerte ohne zentrale Kontrollinstanz anonym und fälschungssicher zu übermitteln. Bis heute weiss niemand, wer Satoshi Nakamoto ist oder ob es ihn – oder sie – überhaupt gibt. Aber noch immer ist seine Idee für viele revolutionär: Ein freies, offenes, von der digitalen Gesellschaft selbstverwaltetes Zahlungssystem. Als Alternative zum oft undurchsichtigen und krisenanfälligen Finanzsystem.

WAS KANN DIE BLOCKCHAIN NOCH?

Bitcoin und andere Kryptowährungen – es gibt inzwischen mehr als 6000 davon – sind nur eine Anwendung der Blockchain. Das unbestechliche digitale Registerbuch kann im Prinzip überall dort zum Einsatz kommen, wo Besitzverhältnisse transparent, öffentlich und fälschungssicher dokumentiert werden sollen: Ausweise, Diplome, Grundbucheinträge, Testamente. Ein konkretes Beispiel: Die Schweizer Uhrenfirma Breitling verkauft seit knapp einem Jahr alle neuen Modelle mit einem digitalen, blockchainbasierten Pass. Dieser dokumentiert alle wichtigen Informationen (Modell, Fabrikationsdatum, Seriennummer, Kaufdatum, Garantie, Reparaturen usw.) sicher und unveränderbar und garantiert die Echtheit der Uhr.

Besonders effizient werden Blockchainlösungen in Verbindung mit smarten Verträgen (Smart Contracts). Das sind in der Blockchain gespeicherte Wenn-Dann-Programmcodes, die vereinbarte Handlungen automatisch auslösen, sobald bestimmte Bedingungen erfüllt sind. So bleibt zum Beispiel das smarte Schloss der Ferienwohnung am Ankunftstag solange gesperrt, bis der Mieter die Kaution hinterlegt hat.

Kryptowährungen sind wie Pokemonkarten

Interview mit dem Blockchain-Experten Bernd Lapp

Mit Bitcoins zahlen

Im Schweizer Alltag ist Bezahlen mit Kryptowährung eher noch eine Rarität. Ausnahmen sind einzelne Cafés und Onlineshops oder Versicherungen. In der Stadt Zug kann man seit 2016 die Steuern mit Bitcoin bezahlen und in Zermatt akzeptiert die Gemeindeverwaltung seit Anfang Jahr Bitcoin für Schaltergeschäfte – mit wenig Echo. Eine Brücke zwischen der Welt des digitalen Geldes und der Franken-Welt ist eine Bitcoin-Kreditkarte: Damit zahlt es sich genau wie mit jeder anderen aufladbaren Pre-Paid-Karte.

Technoscope: Bitte erklären Sie uns die Blockchain so einfach wie möglich.

Bernd Lapp: Die Blockchain ist wie ein Blatt Papier, das man beschreibt. Wenn es voll ist, muss man es in einem Buch abheften. Sobald die neue Seite abgeheftet ist, können sie alle lesen, die das Buch in die Hand bekommen. Und rund um die Welt finden alle, die das genau gleiche Buch haben, diese Seite nun ebenfalls in ihrem Exemplar.

Wie hängen die Blöcke in der Kette zusammen?

Alle Informationen auf einer Seite werden zusammengezählt. Das Ergebnis wird kryptographisch verschlüsselt und das Ergebnis, der Hash, wird zum ersten Eintrag auf der nächsten Seite. Kenne ich den Verschlüsselungsmechanismus, dann kann ich allein mit diesem Hash die jeweils vorhergehende Seite wiederherstellen und die ganze Kette bis zu ihrem Anfang zurückzuverfolgen. Diese Transparenz ist die grosse Stärke der Blockchain.

Weshalb?

Es gibt grosse Wirtschaftsprüfungsunternehmen, die davon leben, dass sie Banken und anderen Firmen in die Bücher schauen und kontrollieren, dass alle Werte korrekt verbucht wurden. Wenn ich denen erkläre, was die Blockchain ist, kommt irgendwann der Punkt, wo sie ganz still werden. Weil sie realisieren,

Wohin damit?

Wer Bitcoins besitzt, braucht ein digitales Portemonnaie oder Wallet. Ein solches zu eröffnen, war bis vor Kurzem ziemlich kompliziert. Inzwischen ist es dank diversen Apps ein Kinderspiel geworden.

Bitcoin sparen

Das Schweizer Start-up-Unternehmen relai.ch ist überzeugt, dass sich Bitcoin besonders gut als Sparbatzen eignen. Mit seiner App wird das ganz einfach.

Bitcoins kaufen

In der Eingangshalle des Parkhotels Beau Site Zermatt steht auch der erste Bitcoin-Automat der Schweizer Alpen. Denn wer mit Bitcoin bezahlen will oder sie als Geldanlage kaufen möchte, der muss zuerst welche erwerben. Das geht zum Beispiel an allen SBB-Billetautomaten. Laut SBB nutzen pro Monat 1500 Personen diesen Service. Und seit kurzem bieten Manor und Valora sowie verschiedene Tankstellenshops Bitcoin-Gutscheinkarten an, die man online von Franken in Bitcoin wechseln kann.

«Alle haben Einblick in die Bücher, niemand kann mehr tricksen oder etwas verdrehen.»

dass diese neue Technologie ihr Geschäftsmodell überflüssig macht. Was sie tun, können mit der Blockchain jetzt alle: Alle haben Einblick in die Bücher, niemand kann mehr tricksen oder etwas verdrehen. Das funktioniert einfach nicht. Sobald eine Seite verschlüsselt ist, ist sie so gut wie in Stein gemeisselt.

Was kann die Blockchain, das E-Banking nicht bereits konnte?

Beim Online-Banking bin ich bei einer Bank angemeldet und gebe ihr Zugriff auf mein Geld. Bei der Blockchain habe ich allein den Zugriff darauf und wenn ich jemandem einen Betrag in Bitcoin oder einer anderen Kryptowährung überweise, ist keine dritte Partei involviert. Damit sind auch die Gebühren geringer und der ganze Vorgang wird effizienter.

Werden sich Kryptowährungen durchsetzen?

Kryptowährungen sind wie Pokemonkarten. Manche sind mehr wert, weil eine besondere Figur drauf ist, die alle gerne möchten, manche weniger selten und deshalb nicht so begehrt. Mit den Kryptowährungen verhält es sich ähnlich. Immer mehr Menschen und sogar ganze Länder erkennen ihren Wert an: Finanztransaktionen werden mit ihnen einfacher und günstiger, brauchen weniger Technologie, weniger Zwischenschritte und Zwischenhändler. Deswegen werden Kryptowährungen immer häufiger akzeptiert. Vor Kurzem hat El Salvador als erstes Land Bitcoin als offizielles Zahlungsmittel anerkannt.

Sie leben und arbeiten im Zuger Kryptovalley. Warum zieht die Schweiz so viele Blockchainunternehmen an?

Die Blockchain veträgt sich sehr gut mit dem dezentralen föderalistischen System und der Eigenständigkeit von Bürgerinnen und Bürger, die gewohnt sind, an Entscheidungsprozessen teilzunehmen. Das ist genau die Philosophie, die auch hinter der Blockchain steckt.

An: **Prisca Sieber**

Kopie:

Betreff: **Studien- und Berufswahl**

Liebe Frau Sieber
Die Blockchain-Technologie interessiert mich sehr und ich möchte mich in diesem Bereich spezialisieren. Was soll ich bei der Studienwahl bedenken?

Lieber Mauro
Zurzeit kannst du in der Schweiz weder im Bachelor- noch im Masterstudium Blockchain als solches studieren. Die Studienlandschaft ändert sich aber ständig und da es sich um ein sehr aktuelles Thema handelt, wird vielleicht in absehbarer Zeit ein entsprechender Studiengang angeboten. Halte dich auf dem Laufenden, damit du nichts verpasst.

Prisca Sieber, Berufs-, Studien- und Laufbahnberatung Kanton Graubünden

In der Schweiz konzentrieren sich die spezifischen Studienangebote in Blockchain aktuell auf die Nachdiplomstufe in Form eines Certificate oder Master of Advanced Studies (CAS oder MAS). Du musst dir also überlegen, welches Studium du wählst, um dich später in einem Nachdiplomstudium zu spezialisieren. Sehr gute Voraussetzungen bilden Studiengänge in den Bereichen Wirtschaft, Informatik und Wirtschaftsinformatik. Interdisziplinäre Grundlagen dieser Fächer sind wichtig, um das Potential und die Anwendungsbereiche der Blockchain zu verstehen. Weitere Studiengänge sind z.B. Data Science, Digital Business Management, Computational and Data Sciences, Computer Science etc., die sich mit ähnlichen Fragestellungen beschäftigen und bei denen die Blockchain-Technologie teilweise auch als Teil des Studiums behandelt wird.

Wenn du dich bereits im Grundstudium mit Blockchain befassen möchtest, kannst du einzelne Vorlesungen dazu besuchen oder dich in der Masterarbeit mit dieser Thematik auseinandersetzen. Informiere dich gut, welche Hochschulen über eigene Blockchain Center verfügen und entsprechende Angebote führen.

Zudem ist es hilfreich, wenn du dich in der Freizeit mit der Blockchain-Technologie beschäftigst. Meetup-Gruppen bieten dir dabei praktische Einblicke und Diskussionen. Ausserdem solltest du deine Englischkenntnisse auf ein hohes Niveau bringen, denn sie sind unabdingbar.

Infos & Links

Auf **www.berufsberatung.ch** findest du die Beschreibungen aller Bachelor- und Masterstudiengängen sowie die Angebote auf Nachdiplomstufe in der Schweiz.

Impressum
SATW Technoscope 04/21 | Dezember 2021 | www.satw.ch/technoscope
Konzept und Redaktion: Ester Elices | **Redaktionelle Mitarbeit:** Christine D'Anna-Huber | **Grafik:** Andy Braun | **Bilder:** Adobe Stock, Bernd Lapp | **Titelbild:** Adobe Stock | **Lektorat:** Ars Linguae | **Druck:** Egger AG

Gratisabonnement und Nachbestellungen
SATW | St. Annagasse 18 | CH-8001 Zürich | technoscope@satw.ch | Tel +41 44 226 50 11

Das nächste Technoscope erscheint im April 2022 zum Thema «Musik»

satw it's all about technology

Hast du Fragen oder Anregungen an das Technoscope-Team? Dann schreibe uns! **technoscope@satw.ch**