

Der Blockchain Hype

Die Kryptowährung Bitcoin ist weltweit bekannt. Die darunterliegenden Konzepte und Technologien sind aber vielen Leuten unbekannt. Der Begriff Blockchain hingegen sagt meist nur technisch interessierten Personen etwas. Die Blockchain ist die Technologie, welche Kryptowährungen wie Bitcoin überhaupt erst ermöglicht. Kryptowährungen und vor allem Blockchains durchlaufen gerade eine Hype-Phase und immer mehr Projekte werden gestartet, die mit Blockchains zu tun haben. In diesem Artikel beschreiben wir, was es mit dem ganzen Hype auf sich hat, wie die tragende Technologie dahinter funktioniert und was sich damit alles bewerkstelligen lässt.

Markus Knecht | markus.knecht@fhnw.ch

Die Idee von *Bitcoin* [1] und der *Blockchain* wurde 2008 von Satoshi Nakamoto in [2] publiziert. Satoshi Nakamoto ist ein Pseudonym und es ist unklar, welche reale Person, Gruppe oder Firma dahintersteckt [3]. Seit der Erfindung von Bitcoin hat sich vieles getan im Blockchain-Bereich: In den letzten Jahren sind sehr viele neue Kryptowährungen aufgekommen, wovon bereits mehr als 800 auf verschiedensten Handelsplätzen gehandelt werden [4]. Die meisten dieser Kryptowährungen bieten diverse Vorteile gegenüber Bitcoin. Eine Auswahl der Bekannteren ist in Abbildung 1 aufgeführt.

Mittlerweile hat auch die Industrie Interesse an Blockchains gefunden, aber weniger bezüglich der Möglichkeit, eigene Währungen zu erstellen, sondern vorrangig wegen der Eigenschaft, dass auf Blockchain basierte Applikationen ohne vertrauenswürdige Instanz auskommen können. Dies hat das enorme Potenzial, ganze Abteilungen oder Firmen aus bestimmten Prozessabläufen zu entfernen, ohne eine Einbusse der Vertrauenswürdigkeit zu erleiden.

Blockchains werden häufig als ultimative Technologie für dezentrale Applikationen ver-

marktet und Projekte, die auf Blockchains aufbauen, erhalten relativ leicht grosse Projektmittel. Einige Beispiele solcher Projekte sind in Tabelle 1 aufgelistet. Dazu verwenden sie oft eine neue Art von Crowdfunding, dem sogenannten *Initial Coin Offering* (ICO), welches eine auf Kryptowährungen basierte Art des Crowdfundings ist. Ein ICO hat zum Ziel, die Entwicklung eines Produkts zu finanzieren. Bei einem ICO werden Münzen einer neuen digitalen Währung verkauft. Meist kann nur mit anderen Kryptowährungen bezahlt werden, es gibt aber einige Drittfirmen wie zum Beispiel die Bitcoin Suisse AG [10], welche Investitionen in bestimmten Fiat-Währung¹ ermöglichen. Die in einem ICO erstellte neue Währung ist projektspezifisch und kann verwendet werden, um Services im Endprodukt zu beziehen. Einige ICO verfolgen einen klassischeren Ansatz und geben den Besitzern der Währung relativ zu ihrem Kapital Stimmrechte und/oder schütten Dividenden aus. Da die ICO Währung auch gehandelt werden kann, hängt ihr Wert stark von den Erwartungen in das entsprechende Projekt ab und verhält sich in diesem Aspekt ähnlich wie eine Aktie. Die Preisschwankungen sind jedoch oft sehr viel grösser als es bei Aktien der Fall ist.

Das momentane Investitionsverhalten für Blockchain-Projekte wird häufig mit dem Investitionsverhalten bei Internetprojekten während der Dotcom-Blase verglichen. Es wird in diesem Zusammenhang häufig vom Internet of Value [19] gesprochen. Die Erwartung ist, dass Blockchains einen Paradigmenwechsel einleiten wird in Bezug auf die Transferierung von Besitztümern, ähnlich dem Paradigmenwechsel, der durch das Internet in Bezug auf die Übertragung von Informationen stattgefunden hat. Bei der Frage ob sich der Kryptowährungsmarkt in einer Blase befindet oder nicht, gehen die Meinungen auseinander, da das



Abbildung 1: Auswahl grösserer Kryptowährungen gemessen am Marktwert: Bitcoin [1], Ethereum [5], Litecoin [6], Ripple [7], Dash [8], Monero [9]

¹ Währung ohne intrinsischen Wert, welche von einer Regierung herausgegeben wird

Projekt	Land	Volumen	Dauer
Tezos [11]	Schweiz	206	14 Tage
Bancor [12]	Schweiz	153	3 Stunden
Status [13]	Schweiz	95	17.2 Stunden
MobileGo [14]	USA	53	1 Monat
Basic Attention Token [15]	USA	35	30 Sekunden
Polybius [16]	Estland	31	6 Wochen
Aragon [17]	Estland	25	15 Minuten
Aeternity [18]	Lichtenstein	24	3 Wochen

Tabelle 1: Beispielhafte Auflistung abgeschlossener ICOs (Volumen in Millionen Dollars)

ökonomische Verhalten² von Kryptowährungen so unterschiedlich ist zu klassischen Märkten, dass eine Analyse schwerfällt.

Können Kryptowährungen bereits verwendet werden?

Die rapide Entwicklung von Kryptowährungen hat auch zur Folge, dass es ständig mehr Möglichkeiten gibt, um Kryptowährungen zu erwerben und damit Einkäufe zu machen. In Zug befindet sich das sogenannte *Crypto Valley* [20], begrifflich angelehnt am Silicon Valley, wodurch die Schweiz eine führende Rolle in der Entwicklung von Blockchain-Technologien einnimmt und viele namhafte Blockchain-Firmen und Stiftungen dort ihren Sitz haben. Dies hat die Gemeinde Zug motiviert, Bitcoins als Zahlungsmittel für Gemeindedienstleistungen bis zu 200 CHF anzunehmen [21]. In der Schweiz ist es sehr einfach Bitcoins zu erwerben, da jeder SBB-Automat diese zum Verkauf anbietet [22]. Auch sogenannte Bitcoin-Geldautomaten gibt es bereits einige über die ganze Schweiz verteilt. Die erworbenen Bitcoins können dann schnell, bequem und günstig über einen Krypto-Exchange, wie zum Beispiel den Schweizer Anbieter *Shapehift* [23], in andere Kryptowährungen getauscht werden. Möchte man seine Kryptowährungen einfach und bequem im Alltag verwenden können so kann man sich eine Krypto Kredit/Debit Karte anschaffen und dann überall bezahlen, wo mit herkömmlichen Karten wie *Visa* und *Master Card* bezahlt werden kann. Zu guter Letzt akzeptieren immer mehr Anbieter von Produkten und Services Kryptowährungen als Zahlungsmittel.

² Da es in Kryptowährungen im Gegensatz zu Fiat-Währungen keine zentrale Autorität (Zentralbank) gibt, welche neues Geld erschafft und Zinssätze festlegt, haben Kryptowährungen ein anderes, noch unerforschtes ökonomisches Verhalten. Zudem existieren noch praktisch keine Erfahrungswerte aus der Vergangenheit, an denen man sich orientieren könnte. Für den interessierten Leser bieten folgende Artikel Informationen aus ökonomischer Sicht zu diesem Thema:
<https://www.cryptocoinsnews.com/digital-currencies-bringing-reality-hayeks-free-market-money/>
<https://benbest.liberty.me/persuading-austrian-economists/>

Wieso dieser Hype, was bietet die Blockchain?

Bei den Blockchains kann man zwischen öffentlichen und privaten Blockchains unterscheiden. Private Blockchains sind im Gegensatz zu öffentlichen nicht für jedermann zugänglich und werden entwickelt, um einen Dienst für einen geschlossenen Benutzerkreis bereitzustellen. Vergleicht man Blockchains mit der Internettechnologie, so sind die öffentlichen Blockchains mit dem Internet vergleichbar und die privaten mit einem Intranet. Viele Puristen betrachten private Blockchains oft nicht als reale Blockchains, da diese teilweise stark von der ursprünglichen Idee abweichen und in vielen Bereichen Kompromisse eingehen. Im Folgenden werden öffentliche Blockchains beschrieben, da diese besser vereinheitlicht werden können.

Eine Blockchain ist ein Protokoll, das einen Zustand verwaltet, welcher sich nur nach festgelegten Regeln verändern lässt. Eine Veränderung wird über deterministische Transaktionen von einem Teilnehmer ausgelöst. Dieser Zustand ist dezentral auf den Geräten der Nutzer der Blockchain abgelegt, wobei sich alle über den aktuellen Zustand einig sind und diesen nur anhand von vorgegebenen Regeln verändern können. Eine Blockchain hat diverse Eigenschaften und bietet Garantien, die Anwendungen ermöglichen, welche ohne diese Garantien nicht realisiert werden könnten.

In einer öffentliche Blockchain kann jeder mitmachen (*open*), egal wo er ist (*borderless*) und wie er mit der Blockchain interagiert (*censorship resistant*). Man muss keine persönlichen Daten preisgeben um teilzunehmen (*pseudonym*). Es gibt keine privilegierten Teilnehmer: für jeden gelten die gleichen Regeln, ob Mensch oder Kühlschrank (*neutral*). Die Regeln können nicht gebrochen werden (*uncorruptable*). Es muss keiner zentralen Instanz vertraut werden, um sich sicher zu sein, dass das System korrekt funktioniert (*trustless*). Die Blockchain kann nicht abgestellt werden, solange es Teilnehmer gibt, die sie weiterführen wollen (*unstoppable*). Eine bestätigte regelkonforme Änderung kann nicht mehr rückgängig gemacht werden (*immutable*) und ist für jeden für immer einsehbar (*transparent*).

Wie funktioniert eine Blockchain?

Damit alle Teilnehmer den selben Zustand verwenden ist es essentiell, dass jeder dieselben Transaktionen in derselben Reihenfolge verarbeitet. Dazu werden die Transaktionen in Blöcke zusammengefasst, wobei die Transaktionen in jedem Block eine klare Reihenfolge aufweisen. Neben den Transaktionen enthält jeder Block einen Verweis auf einen anderen bereits existierenden Block und bildet somit eine verkettete Liste (Abb. 2). Alle Transaktionen im Block auf den verwiesen wird, sind vor den Transaktionen im verweisen-

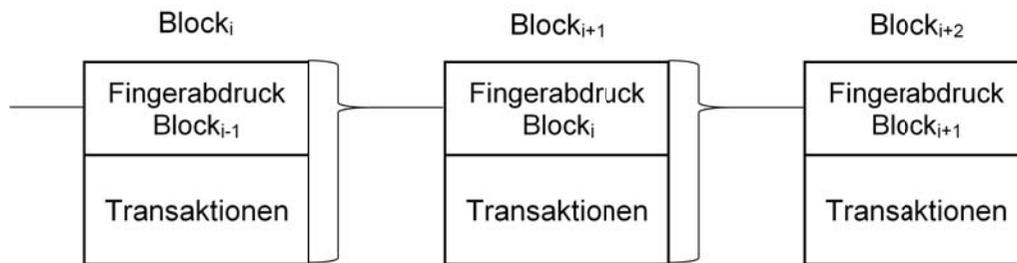


Abbildung 2: Grundlegende Struktur der Blockchain

den Block angeordnet. Der Verweis wird durch einen Fingerabdruck (*Hash-Wert*) des Inhaltes des Vorgängerblocks dargestellt, was mit ausreichend hoher Wahrscheinlichkeit sicherstellt, dass der Inhalt des Vorgängers nicht mehr geändert werden kann, ohne auch den Nachfolger zu ändern.

Falls nun das Erstellen eines Blockes mit einem grossen Ressourcen-Aufwand verbunden wird, so wird die Fälschung eines existierenden Blockes umso aufwendiger, je weiter entfernt er vom neuesten Block in der Blockkette entfernt ist. Dieser Ressourcen-Aufwand wird in Bitcoin mit dem sogenannten *Proof of Work* (einem Consensus Algorithmus) erreicht. Andere Blockchains verwenden Alternativen wie zum Beispiel *Proof of Stake*.

Im Proof of Work versuchen sogenannte *Miner* ein rechenintensives Rätsel (ein sogenanntes Hash-Puzzle) zu lösen, welches abhängig ist vom Block, den er produzieren möchte. Die effizienteste Variante das Rätsel zu lösen erfolgt durch die Erzeugung von Zufallszahlen und der Überprüfung, ob diese eine Lösung darstellen. In Bitcoin wird die Schwierigkeit des Rätsels automatisch angepasst, so dass im Durchschnitt alle zehn Minuten jemand eine Lösung findet, sprich einen neuen Block produzieren kann. Für das Lösen des Rätsels und das Generieren eines Blocks gibt es eine Belohnung in Bitcoins, sofern der Block als Teil der Hauptkette angesehen wird. Zudem zahlt der Ersteller einer Transaktion eine Gebühr an denjenigen, der sie in einen Block integriert. Als Hauptkette wird diejenige Kette mit den meisten Blöcken angesehen, welche nur Transaktionen enthält, die eine gültige Zustandsveränderung herbeiführen und jede Transaktion nur einmal beinhaltet. Die Miner sind somit dem Anreiz ausgesetzt, die momentane Hauptkette zu erweitern und nur Blöcke mit gültigen Transaktionen und ohne Duplikate zu generieren, da sie sonst ohne Belohnung ausgehen.

Ein Block, der Teil der Hauptkette ist, kann nur dann aus der Hauptkette wegfallen und damit die darin enthaltenen Transaktionen nichtig machen, wenn jemand eine neue Kette erstellt, die vor diesem Block abzweigt und länger ist als die momentane Hauptkette. Dies erfordert jedoch, dass er mehr Rechenleistung zur Rätsellösung einsetzt als all diejenigen, die die Hauptkette erweitern, damit seine Kette irgendwann länger als die momentane Hauptkette wird. Da das Rätsellösen ei-

nen Glücksfaktor beinhaltet, können kurze Überholmanöver auch mit weniger Rechenleistung vorkommen, was zur Folge hat, dass neue Blöcke erst nach einer gewissen Zeit als final angesehen werden. In Bitcoin wartet man, bis fünf weitere Blöcke auf einem Block aufbauen, bis man diesen als final und somit quasi-unveränderbar ansieht.

Was kann mit einer Blockchain gemacht werden?

Im folgenden Abschnitt realisieren wir anhand der gegebenen Definitionen eine beispielhafte Kryptowährung. Die entsprechende Blockchain vermerkt als Zustand, welcher Teilnehmer wie viele der Kryptomünzen besitzt. Die Regeln um diesen Zustand zu verändern besagen, dass wenn sich jemand authentifizieren kann (mit Hilfe von Kryptographie), dass er seine Anzahl Münzen verringern kann und die eines anderen Teilnehmers um dieselbe Anzahl erhöhen kann, solange seine Anzahl dabei nicht negativ wird. Solche Regeln laufen immer als Ganzes (atomar) ab und im vorherigen Beispiel ist deshalb garantiert, dass Münzen nur transferiert, jedoch nicht dupliziert werden können, wodurch ihre Anzahl ständig konstant bleibt.

Neben Kryptowährungen gibt es viele andere Anwendungen die mithilfe von Blockchains realisiert werden können:

- *Lunyr*: Dezentrale Wissensdatenbank, ähnlich zu Wikipedia aber mit einem finanziellen Anreizsystem, um die Qualität der Artikel mithilfe von *Peer Reviews* ständig zu verbessern [28].
- *BitGive*: Eine dezentrale Hilfsorganisation, die das Spenden erleichtert und es erlaubt transparent nachzuverfolgen, dass die Spende auch wirklich für den angedachten Zweck eingesetzt wird [29].
- *uPort*: Digitale Identitätsplattform, welche die Kontrolle der Identität zurück an das Individuum gibt [30]. Die Gemeinde Zug arbeitet mit *uPort* zusammen, um für seine Bürger eine digitale Identität zur Verfügung zu stellen [31].
- *Arcade City*: Dezentralisierte Plattform zum Etablieren einer *Sharing Economy*, beginnend mit einem dezentralisierten Service vergleichbar mit Uber [32].
- *Slock.it*: Smart Lock Projekt um Schlösser sowie Öffnungsberechtigungen dynamisch auf der Blockchain zu verwalten, um Eigentums-transfers und Ausleihen zu digitalisieren [25].

- *Everledger*: Dezentralisierte Verfolgung von Diamanten, um Betrug und andere Risiken zu reduzieren «Schlüsselwort Blutdiamanten» [33].

Smart Contracts

Einige Blockchains, wie zum Beispiel *Ethereum* [5], machen ihre Blockchain durch sogenannte *Smart Contracts* programmierbar, was erlaubt, Subsysteme einzuführen, die ihren eigenen Zustand und Regeln haben. Die Struktur des Zustands und die Regeln, um diesen zu verändern, werden mithilfe einer Programmiersprache beschrieben. Listing 1 zeigt, wie eine neue Kryptowährung mit minimalem Funktionsumfang als Smart Contract auf Ethereum als Subsystem implementiert werden kann. Ethereum verwendet als Programmiersprache *Solidity* [24]. Jeder kann eine Instanz dieses Smart Contracts erstellen, um seine eigene Kryptowährung zu generieren, wobei dann jede Instanz eine unterschiedliche und eigenständige Währung repräsentieren würde.

Blockchains sind jedoch nicht auf Kryptowährungen beschränkt, sondern können auch dazu verwendet werden, um alle möglichen Arten von Besitz zu verfolgen, wie zum Beispiel ein Haus. Hat das Haus sogar noch ein *Smart Lock* [25], das mit der Blockchain verbunden ist, könnte es seinen momentanen Besitzer kennen und nur diesem (und von ihm autorisierte Personen) Zutritt zum Haus gewähren. Sobald der Besitz digital repräsentiert werden kann, eröffnen sich neue Möglichkeiten, wie zum Beispiel eine dezentrale *AirBnB*-Variante [26]. Um dies zu bewerkstelligen, würde ein Smart Contract eine Zutrittserteilung für einen bestimmten Zeitraum ausstellen, falls ein entsprechender Auftrag existiert und die dazugehörige Zahlung eingegangen ist. Das Smart Lock kann bei einer Öffnungsanfrage nun überprüfen, ob die entsprechende Person die Erlaub-

nis besitzt um einzutreten. Das Interessante an einer solchen Lösung ist, dass eine Institution wie AirBnB als zentrale und verwaltende Instanz überflüssig gemacht werden kann, was das System robuster gegen Angriffe und Einflüssen von Drittparteien macht. Zudem kann die Kosteneffizienz verbessert werden.

Durch das geschickte Zusammenspiel von IoT-Geräten mit einer Blockchain eröffnen sich neue, futuristische und bisher undenkbar Anwendungen: Ein mit einer Blockchain verbundenes, selbstfahrendes, elektrisches Auto könnte einen Service ähnlich zu *Uber* [27] anbieten. Das autonome Auto nimmt über das Internet Aufträge entgegen und holt dann selbständig die Kunden ab, welche während der Fahrt kontinuierlich für jede Minute und/oder Kilometer über eine Kryptowährung direkt das Auto bezahlen. Mit den Einnahmen bezahlt das selbstfahrende Auto seine Auslagen, wie zum Beispiel Reinigungen, Reparaturen, Serviceüberprüfung und das Aufladen der Batterie. Nebenbei zahlt es von den Einnahmen noch die Schulden für ein Darlehen ab, mit dem seine Produktion finanziert worden ist. Damit ein solches Szenario seitens der Blockchain möglich wird, müssen zuerst einige Veränderungen in Bezug auf die Akzeptanz von Kryptowährungen zur Bezahlung von diversen Ressourcen, Gütern und Dienstleistungen (z.B. Reparaturen und Reinigungen) erfolgen.

Eignung für alle dezentralen Applikationen?

Blockchains haben auch diverse Nachteile, zu denen haben sie momentan noch einen geringen Transaktionsdurchsatz. Bitcoin kann zum Beispiel nur etwa sieben Transaktionen pro Sekunde verarbeiten, weit entfernt von den mehreren tausend die Visa aktuell pro Sekunde abwickeln kann. In diesem Bereich werden jedoch ständig Fortschritte gemacht und neuere Blockchains sind

```
// Example Smart contract
contract FokusReportToken {
    // adds overflow safe arithmetic operations to unsigned integers
    using SafeMath for uint;

    // balances, tracks who (address) owns how many (uint) coins
    mapping(address => uint) balances;

    // constructor
    function FokusReportToken() {
        // creator of contract (msg.sender) gets all the initial tokens
        balances[msg.sender] = 10*1000*1000;
    }

    // transfers some coins (value) from authenticated sender (msg.sender) to somebody else (to)
    function transfer(address to, uint value) {
        balances[msg.sender] = balances[msg.sender].sub(value);
        balances[to] = balances[to].add(value);
    }
}
```

Listing 1: minimale funktionsfähige Kryptowährung in Solidity

performanter. Viele Projekte versprechen momentan eine Performance, die mit der Transaktionsmenge der Grössenordnung von Visa oder sogar noch grösser klarkommen könnte. Diese Projekte sind aber erst in der frühen Entwicklungsphase oder sehr spezialisiert, wie zum Beispiel nur für Bezahlvorgänge aber nicht für Smart Contracts verwendbar.

Ein weiterer Nachteil ist, dass der Speicherbedarf der Blockchain ständig wächst und droht, mit der Zeit zu gross zu werden für herkömmliche Endnutzengeräte. Die Bitcoin Blockchain braucht momentan etwas mehr als 130 GByte an Speicherplatz und diese Zahl wächst linear mit der Zeit. Solange *Moore's Law* anhält, welches voraussagt, dass sich die Speicherkapazität von Speichermedien alle 18 Monate verdoppelt bei gleichem Preis, ist die linear wachsende Blockchain für Nicht-Endnutzengeräte unproblematisch. Zudem werden auch in diesem Bereich der Blockchain ständig Fortschritte gemacht: *Light Clients* und *Sharding*-Ansätze [34] ermöglichen es, dass ein Teilnehmer nur einen kleinen Teil der Blockchain speichern muss, ohne Sicherheitseinbussen in Kauf nehmen zu müssen.

Viele der zuvor erwähnten Eigenschaften (*open*, *borderless*, etc.) sind leider zusammenhängend und können nicht individuell ab oder angeschaltet werden. Möchte man zum Beispiel auf *transparent* verzichten und stattdessen mehr *privacy* haben, weil ein Pseudonym nicht ausreichend ist, so ist das nicht ohne weiteres möglich. Hat man die Anforderung, dass man auf Anfrage bestimmte Inhalte entfernen können muss, dann werden *copyright resistant* und *immutable* sowie *pseudonym* plötzlich zu einem Hindernis. Braucht eine Applikation nicht alle Eigenschaften, sollte man sich gut überlegen, ob die Blockchain die richtige Lösung ist oder ob man die Applikation nicht doch besser mit einer anderen Technologie realisiert. Sobald ein Teilnehmer einem Dienstleister vollständig vertrauen muss, wird die Blockchain in den meisten Fällen unnötig, da der Vertrauenspartner all die anderen benötigten Eigenschaften mithilfe einer auf einem vertrauenswürdigen Server laufenden Applikation sicherstellen kann. Ihr volles Potenzial entfaltet eine Blockchain-Applikation somit erst, wenn sie eine Dienstleistung zur Verfügung stellt, die ohne zusätzlich involvierte juristische Person funktionsfähig sein soll. Bitcoin und andere Kryptowährungen sind Paradebeispiele, da sie die Dienstleistung des Geldtransfers anbieten, ohne dass eine Bank oder ein anderes Institut involviert werden muss.

Private Blockchains versuchen momentan Lösungen zu finden, die Kompromisse eingehen, um bestimmte Eigenschaften wie *privacy* und *governance*, sowie *permissioning* zur Verfügung zu stellen, so dass Blockchains auch in Firmen eingesetzt werden können, wo Regulatoren verlangen,

dass die Applikation bestimmte Eigenschaften hat, welche eine öffentliche Blockchain nicht zur Verfügung stellen kann.

Referenzen

- [1] Bitcoin: <http://www.bitcoin.org>
- [2] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <http://www.bitcoin.org/bitcoin.pdf>, 2008.
- [3] Wer ist Satoshi Nakamoto: Die moderne Jagd nach Mr.X: <https://www.krypto-magazin.de/wer-ist-satoshi-nakamoto-die-moderne-jagd-nach-mr-x/>
- [4] Coinmarketcap: <https://coinmarketcap.com/>
- [5] Ethereum: <https://www.ethereum.org/>
- [6] Litecoin: <https://litecoin.com/>
- [7] Ripple: <https://ripple.com/>
- [8] Dash: <https://www.dash.org/>
- [9] Monero: <https://getmonero.org/>
- [10] Bitcoinsuisse: <https://www.bitcoinsuisse.ch/>
- [11] Tezos: <https://www.tezos.com/>
- [12] Bancor: <https://www.bancor.network/>
- [13] Status: <https://status.im/>
- [14] Mobile Go: <https://mobilego.io/>
- [15] BAT: <https://basicattentiontoken.org/>
- [16] Polybius: <https://polybius.io/>
- [17] Aragon: <https://aragon.one/>
- [18] Aethernity: <https://www.aethernity.com/>
- [19] Internet of Value: <https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/>
- [20] Crypto Valley: <https://cryptovalley.swiss>
- [21] Von Bitcoin zu Blockchain-Anwendungen: http://www.stadtzug.ch/de/ueberzug/ueberzugrubrik/aktuelles/aktuellesinformationen/welcome.php?action=showinfo&info_id=351680
- [22] Mit Bitcoin bequem und einfach Einkaufen: <https://www.sbb.ch/de/bahnhof-services/dienstleistungen/weitere-dienstleistungen/bitcoin.html>
- [23] Shapeshift: <https://shapeshift.io>
- [24] Solidity: <http://solidity.readthedocs.io/en/develop/index.html>
- [25] Slock.it: <https://slock.it>
- [26] AirBnB: <https://www.airbnb.ch>
- [27] Uber: <https://www.uber.com>
- [28] Lunyr: <https://lunyr.com>
- [29] Bitgive: <https://www.bitgivefoundation.org/>
- [30] Uport: <https://www.uport.me>
- [31] Blockchain-Identität für alle Einwohner: http://www.stadtzug.ch/de/ueberzug/ueberzugrubrik/aktuelles/aktuellesinformationen/?action=showinfo&info_id=383355
- [32] Arcade City: <https://arcade.city>
- [33] Everledger: <https://www.everledger.io>
- [34] What is Sharding? <https://themerke.com/what-is-sharding/>