Blockchain – FAQ

Frequently Asked Questions

Blockchain ist ein weiterer, unsichtbarer Technologie-Gigant auf dem Weg in die digitale Zukunft. Weltweit wird an individuellen Lösungen rund um die Blockchain gearbeitet. Das Tempo ist dabei atemberaubend. Wer nicht aufpasst, dem droht hier schon bald die Digitale Demenz. Die nachfolgenden Zeilen können hier – recht Kompakt – ein wenig Licht ins Dunkel bringen.

Multiple Chancen einer revolutionären Basis-Technologie

Blockchain findet in der Wirtschaft zunehmend Anklang

Die Blockchain-Technologie wurde erstmals für Bitcoin, ein privates digitales Geldsystem entwickelt. Dabei übernimmt die Blockchain-Technologie die Funktion eines Registers, in dem Geldtransaktionen sicher gespeichert werden können. Diese Technologie ist weit über Bitcoin hinaus einsetzbar. Die Blockchain-Technologie wird seither weltweit von einer Vielzahl von Personen und Organisationen weiterentwickelt und für andere Einsatzgebiete erweitert. Die Möglichkeiten der Blockchain-Technologie sind dabei nicht nur auf einfache Geldüberweisungen zwischen Privatpersonen beschränkt. Sie bietet vielmehr die Möglichkeit für eine große Palette an wirtschaftlichen Dienstleistungen.

IT und Finanzbranche

Basisinnovationen durch gesteigerte Rechenleistung

Die Entwicklung der Informationstechnologie hat die Finanzbranche seit jeher stark beeinflusst. Parallel zur Leistungssteigerung der Computer hat sich auch seine Einsatzbreite in den Finanzdienstleistungen entwickelt und die Effizienz und die Leistungsfähigkeit des Finanzwesens sukzessive gesteigert. Neben dem exponentiellen Wachstum der Rechenleistung hat die Computertechnik einige weitere Basisinnovationen ermöglicht, welche das Privatleben und die Wirtschaft stark beeinflussen.

Internet und Smartphone

Digitale Revolution

Zu diesen Basisinnovationen gehören die Erfindung des Internets und des Smartphones, die es ermöglichen, von überall her auf Informationen zuzugreifen und

diese auszutauschen. Dazu kommen Angebote wie die günstige und skalierbare Verfügbarkeit von Hochleistungsrechnern und Datenspeichern sowie große Fortschritte im Bereich der Künstlichen Intelligenz, welche mit der Leistungssteigerung der Rechner einhergehen. Mit diesen Entwicklungen, die üblicherweise als digitale Revolution oder Digitalisierung zusammengefasst werden, sind grundlegend neue Geschäftsmodelle möglich geworden.

Fin-Techs und Kryptogeld

„Fin-Tech" steht für „Financial Technology", also „Finanztechnologie" als Sammelbegriff für technologisch weiterentwickelte Finanzdienstleistungen.

Im Finanzbereich fasst man diese Unternehmen unter dem Begriff „Fin-Techs" zusammen. Die Fin-Techs haben seit Ende der Neunziger Jahre immer weitere Prozesse der Finanzbranche adaptiert oder unterstützt: Während der Fokus am Anfang mehr auf Zahlungsdienstleistungen (z.B. Paypal) lag, sind später die Kreditversorgung von Privatpersonen und Kleinunternehmen und die Finanzierung von Start-ups und Unternehmen dazugekommen (Crowd-Lending, Crowd-Investing). Diese Typen von Fin-Techs verwenden jedoch meistens noch die klassische Finanzmarktinfrastruktur (Bankkonti, Zahlungsinfrastruktur etc.). Die Entwicklung vom Kryptogeld hingegen führt vom klassischen Transaktionssystem weg. Kryptogeld (wie z.B. Bitcoin) ist ein digitales Zahlungsmittel, das mit den Prinzipien der Kryptographie erstellt wird. Das Konzept und die Umsetzung von Bitcoin im Jahr 2008 hat eine Entwicklung in Gang gesetzt, deren Auswirkungen heute kaum vollständig abschätzbar sind.

Bitcoin und Blockchain

Bitcoin (digitale Münze) ist eine digitale Währung mit der Blockchain als Transaktionsprotokoll

Der Erfinder von Bitcoin wollte ein Geld- und Zahlungssystem schaffen, das komplett ohne staatliche Währungen, Zentralbanken und staatlich kontrollierte Banken auskommt. Dabei hatte er mehrere Probleme zu lösen. Einerseits musste die Geldwertstabilität gewährleistet werden. Er löste dies durch die Festlegung der Maximalgrenze der geschaffenen Geldmenge und klare Regeln, wie neues Geld geschöpft wird. Ein weiterer Themenkomplex war die sichere Zuordnung des Geldes zu einer Person, die sichere Übertragung von Geld im Rahmen eines Zahlungsvorgangs sowie - damit verbunden – die Vermeidung der Kopie des Geldes (double spending problem).

Dafür hat er die sogenannte Blockchain geschaffen, ein Transaktionsprotokoll, das mit Hilfe von Verschlüsselungstechnik (Kryptographie) ohne zentralen Zwischenhändler (Zentralbank oder Bank) eine gleichwertige oder bessere Sicherheit gewährleisten soll. Dabei ist wesentlich, dass die Integrität des Transaktionsprotokolls rein durch Technologie gewährleistet wird, während im Bankensystem ein Zwischenhändler (Finanzintermediär) für diese Integrität sorgen muss. Die Protokollierung, Verschlüsselung und Speicherung der Transaktionen finden nur über das Internet statt.

Im Gegensatz zum heutigen Zahlungssystem, in dem jeder Teilnehmer (z.B. eine Bank) ein eigenes Hauptbuch führt und dies zu einem definierten Zeitpunkt mit seinen Schnittstellen (z.B. Korrespondenzbanken) abgleichen muss, hat die Blockchain nur ein einziges Hauptbuch, das aber auf allen teilnehmenden Rechnern als Kopie dezentral gespeichert ist. Man spricht deshalb auch von der Technologie der dezentralen Hauptbücher („Decentralized Ledger Technology" bzw. „Distributed Ledger Technology" oder kurz „DLT").

Krypto-Assets und Blockchain-Systeme

Anfangsprobleme von Blockchain durch neuere Generationen bereits teilweise gelöst

Bitcoin hat sich seit dem Start im Jahr 2008 stark verbreitet und entwickelt. Aufgrund der hohen Wertsteigerung in den letzten Jahren wird es von spezialisierten Anlegern immer mehr als Anlageobjekt (Krypto-Asset) verwendet. Aufgrund der Tatsache, dass bei Bitcoin der Inhaber des Geldes nicht bekannt ist, steht Bitcoin auch immer wieder in der Kritik, für kriminelle Zwecke verwendet zu werden (z.B. Geldwäsche, Lösegeldforderungen).

Die erste Generation der Blockchain, die für Bitcoin entwickelt wurde, weist darüber hinaus einige Problemstellungen auf, die den Einsatz für die breite Wirtschaft erschweren, wie z.B. den hohen Energieverbrauch oder eine relativ geringe Transaktionskapazität. Diese Probleme sind teilweise von den neueren Generationen von Blockchain-Systemen heute bereits intelligent gelöst. Angesichts der weltweit für die Weiterentwicklung der Blockchain eingesetzten Innovationskraft ist davon auszugehen, dass die zukünftigen Generationen der Blockchain die noch offenen Probleme zeitnah lösen werden.

Blockchain und Tauschgeschäfte

Blockchain für die effiziente Abwicklung von Transaktionen

Bei der Blockchain geht es um eine neue Software-Technologie auf der Basis mathematischer Modelle, um Transaktionen effizient abzuwickeln. Tauschgeschäfte bilden seit jeher die Grundlage der Wirtschaft – die einfachste Form ist der privatwirtschaftliche Tausch eines Gutes gegen Geld durch persönlichen Kontakt und Vertrag. Um Güter über die Distanz zwischen zwei Parteien, die sich nicht direkt kennen, tauschen zu können, hat man spezialisierte Handelssysteme aufgebaut. Beispiele dafür sind Zahlungsverkehrssysteme und Wertpapierhandelssysteme.

Bei diesen klassischen Handelssystemen wird die Verbindung zwischen Käufer und Verkäufer über einen oder mehrere Intermediäre hergestellt und die Transaktion rechtssicher abgewickelt. Dafür braucht es aber ein hohes Maß an Standardisierung und hohe Anforderungen an die Qualität der Intermediäre. Zur Qualitätssicherung und zur Schaffung von Vertrauen sind diese staatlich beaufsichtigt. Jeder Intermediär führt für sich ein Hauptbuch, um die Transaktionen sicher zu verbuchen und die Zuordnung zu den Kunden zu gewährleisten.

Die Abstimmung dieser verschiedenen Hauptbücher, die internen Prozesse und die staatliche Aufsicht sind aufwendig, weshalb sich diese Handelssysteme nur für bestimmte Vermögenswerte lohnen.

Blockchain – Basis-Technologie

Blockchain als Basis-Technologie ähnlich wie das TCP/IP-Protokoll für das Internet

Die Blockchain hingegen bietet ein Transaktionssystem, das ohne die Qualitätssicherung von Intermediären (Zwischenhändler) und ohne staatliche Aufsicht auskommt. Die Qualität wird über eine Kombination von Verschlüsselungstechnologien, den Möglichkeiten des Internets und software-basierten Regeln zur Missbrauchsvermeidung gesichert. Technologie und klare Regeln schaffen in einer Blockchain also das nötige Vertrauen, um sichere Transaktionen auszuführen.

Die heute erkennbaren Generationen von Blockchain basieren mehrheitlich auf dem Prinzip des dezentralen Hauptbuchs (DLT), bei dem alle Teilnehmer des Transaktionssystems eine Kopie desselben Hauptbuchs, in dem alle Transaktionen abgebildet sind, speichern und zur Qualitätssicherung verwenden. Dies muss jedoch nicht für alle zukünftigen Generationen entscheidend sein. Allen gemeinsam wird die Abwesenheit eines zentralen Intermediärs zur Qualitätssicherung des Hauptbuchs sein. In einem Blockchain-System fehlt also der klassische Aufsichtsansatz (z.B. Finanzmarktaufsicht).

Dieses Hauptmerkmal stellt Blockchain-Systeme als Basis-Technologie in die Nähe der Internet-Protokolle (z.B. TCP/IP), welche die Grundlage des heutigen Internets und ebenfalls die Grundlage für Geschäftsmodelle darstellen, aber selbst von keinem Intermediär direkt betrieben werden.

Digitalisierung von Geld, Vermögenswerten und Geistigem Eigentum

Wallet = Digitale Brieftasche
Token = Digitale Wertmarke

Da der klassische Ansatz für ein Handelssystem aufwendig und teuer ist, werden heute nur eingeschränkte Vermögenswerte auf diesen Systemen gehandelt. Mit der Blockchain-Technologie werden die Zugangskosten stark absinken. Es ist deshalb davon auszugehen, dass ein viel breiteres Spektrum an Vermögenswerten auf einer solchen Infrastruktur gehandelt wird und als Basis für Wirtschaftsprozesse und damit verbundene Dienstleistungen verwendet werden kann.

Die Blockchain übernimmt dann zusammen mit den Benutzerschnittstellen (z.B. Wallet-App auf einem Smartphone) die Funktion eines Zahlungssystems. Diese Information nennt man auf bestimmten Systemen „Token“, in Anlehnung an den englischen Begriff für eine private Prägemünze oder „Wertmarke“. Es gibt Blockchain-Systeme wie z.B. Bitcoin, in denen diese Information technisch nicht als Token ausgestaltet ist, doch der Begriff versinnbildlicht die Eigenständigkeit und Übertragbarkeit dieser Information.

Die Technologie der Blockchain-Systeme stellt dabei sicher, dass diese Information eindeutig ist. Es ist technisch deshalb nicht möglich, Kopien zu erstellen. Dadurch erfüllt die Blockchain Technologie die idealen Voraussetzungen für die Digitalisierung von Geld, Vermögenswerten und Geistigem Eigentum.

Quelle: AIF AG, Liechtenstein / Ministerium für Präsidiales und Finanzen, Liechtenstein