GENERATION BLOCKCHAIN

Master-Studiengang
Blockchain-Technologie & Kryptowährungen

www.generationblockchain.eu

2022-2024
OERS

Unter
Frankfurt School of Finance & Management

Co-funded by the European Union

01

MODUL 3

Kryptowährungen

Co-funded by the European Union

Finanziert von der Europäischen Union. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich die des Autors/der Autoren und spiegeln nicht unbedingt die der Europäischen Union oder der Nationalen Agentur wider. Weder die Europäische Union noch die Nationale Agentur können für sie verantwortlich gemacht werden.

Inhalt Modul 3

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODUL 3 Kryptowährungen

Kapitel Überblick

In diesem Modul stehen Bitcoin-Transaktionen und Bitcoins Mining-Mechanismus im Mittelpunkt. Zusätzlich werden Sie in die Grundlagen von Ethereum, Transaktionen auf Ethereum und Smart Contracts eingeführt. Schließlich werden wir die Prinzipien des dezentralen Finanzwesens (DeFi) behandeln, indem wir Vergleiche zum traditionellen Finanzsystem ziehen.

Lernziele

Nach dem zweiten Modul sollten Sie dazu in der Lage sein:

- Wiederholen Sie, wie eine Bitcoin-Transaktion funktioniert.
- Diskutieren Sie Probleme der Skalierbarkeit von Bitcoin.
- ein Verständnis für die Rentabilität des Bitcoin-Minings und der Hard- und Software haben
- Anforderungen für Bergleute.
- Verstehen Sie, was Ethereum ist und was die Unterschiede zwischen Ethereum und Bitcoin sind.
- Bewertung der Rolle der Ethereum-Gasgebühr bei Transaktionen.
- Wiederholen Sie, wie eine Ethereum-Transaktion funktioniert.
- Verstehen des Konzepts und der Anwendungsfälle von Smart Contracts.
- die verschiedenen Anwendungsebenen des dezentralen Finanzwesens zu verstehen.
- Nennen und analysieren Sie die Parallelen und Unterschiede zwischen dezentraler Finanzierung und traditioneller Finanzierung.
- Ermitteln Sie die derzeitigen Nachteile der dezentralen Finanzierung und der traditionellen Finanzierung.

01| BITCOIN TIEF EINTAUCHEN

1.1 Bitcoin-Transaktionen

Nachdem wir zuvor einen groben Überblick über Bitcoin-Transaktionen erhalten haben, werden wir uns nun Bitcoin-Transaktionen genauer ansehen.

Es gibt keine Bitcoins

Es ist wichtig zu wissen, dass es keine Bitcoins gibt, sondern nur Aufzeichnungen über Bitcoin-Transaktionen. Bitcoins existieren technisch gesehen nirgendwo, nicht einmal auf einer Festplatte. Wenn Sie nach einer bestimmten Bitcoin-Adresse suchen, werden Sie dort keine digitalen Bitcoins finden. Es gibt keinen physischen Gegenstand oder eine digitale Datei, die Bitcoin "ist". Stattdessen gibt es nur Aufzeichnungen von Transaktionen zwischen verschiedenen Adressen mit Guthaben, die sich entweder erhöht oder verringert haben. Jede Transaktion, die jemals durchgeführt wurde, wird in einem öffentlichen Hauptbuch (der Blockchain) gespeichert. Wenn Sie den Kontostand einer beliebigen Bitcoin-Adresse berechnen wollen, müssen Sie ihn anhand der Blockchain berechnen, da in der Adresse keine Informationen gespeichert sind.

Jeder Nutzer des Bitcoin-Netzwerks kann jede jemals getätigte Transaktion über die Bitcoin-Blockchain einsehen. Wie wir bereits wissen, sind Bitcoin-Transaktionen durch digitale Signaturen gesichert und werden zwischen Bitcoin-Wallets über deren Adressen hin- und hergeschickt.

Zeit der Transaktionsbestätigung

Die Transaktionsbestätigung kann Minuten, Stunden oder Tage dauern, weil eine Transaktion von Minern bestätigt werden muss. Abhängig von der Transaktionsgebühr, die Sie bezahlt haben, kann Ihre Transaktion für eine lange Zeit im Transaktionspool verbleiben, einfach weil der gebotene Anreiz (d.h. die Transaktionsgebühr) nicht hoch genug ist, damit Ihre Transaktion sofort in einen Block aufgenommen wird. Je nach Verkehr im Bitcoin-Netzwerk kann dies die Transaktion um Stunden oder Tage verzögern oder sogar zur Ablehnung der Transaktion führen.

Das Bitcoin-Protokoll ist so eingestellt, dass jeder Block etwa zehn Minuten braucht, um abgebaut zu werden. Einige Händler lassen den Nutzer warten, bis der Block bestätigt ist. Auf der anderen Seite gibt es einige Händler, die nicht warten, bis die Transaktion bestätigt ist. Sie nehmen das Risiko auf sich und gehen davon aus, dass die Leute nicht versuchen werden, ihre Bitcoins für andere Dinge auszugeben, bevor die Transaktion bestätigt ist. Dies ist bei kleinen Transaktionen (Micropayments) üblich, bei denen das Betrugsrisiko nicht so hoch ist. Jeder Empfänger kann selbst entscheiden, wie viele Bestätigungen er benötigt. Das Prinzip ist, dass mehr Bestätigungen die Transaktion sicherer machen, sie aber auch verlangsamen.

Die Logik von Bitcoin-Transaktionen und Bitcoin, die in Ihrer Wallet gespeichert sind

Da Bitcoins nur als Aufzeichnungen von Transaktionen existieren, können viele verschiedene Transaktionen mit einer bestimmten Bitcoin-Adresse verbunden sein. Vielleicht hat Jane Alice zwei Bitcoins geschickt, Chris hat ihr einen Bitcoin geschickt, und Eve hat nur einen geschickt - alle als separate Transaktionen zu separaten Zeiten. Sie werden nicht automatisch in Alices Wallet zu sechs vorhandenen Bitcoins in einer Datei konvertiert, sondern existieren nur als unterschiedliche Transaktionsdatensätze. Wenn Alice Bob Bitcoins schicken will, wird ihre Brieftasche versuchen, Transaktionsdatensätze mit verschiedenen Beträgen zu verwenden, die sich zu der Menge an Bitcoins addieren, die sie Bob schicken will. Anders als auf Ihrem Bankkonto summieren sich die Bitcoin-Beträge in Ihrer Wallet technisch gesehen nicht zu einer Masse, sondern bleiben einzelne Einheiten.

Es besteht die Möglichkeit, dass die Brieftasche von Alice nicht genau den Betrag an addierbaren Transaktionsdatensätzen enthält, den sie an Bob senden möchte. Wenn Alice z. B. 1,5 BTC an Bob senden möchte und keine der Transaktionen in ihrer Brieftasche mit diesem Betrag übereinstimmt oder zu diesem Betrag hinzugefügt werden kann, dann geschieht Folgendes:

Alice sendet die beiden Bitcoins, die sie von Jane erhalten hat, an Bob. Jane ist die Eingabe und Bob ist die Ausgabe. Da Alice jedoch den Betrag von 1,5 BTC senden möchte, erstellt ihre Brieftasche automatisch zwei Ausgänge für ihre Transaktion: 1,5 BTC an Bob und 0,5 BTC an eine neue Adresse, die eingerichtet wurde, um das Wechselgeld von Bob für Alice zu speichern.

Bitcoin-Transaktionen sind teilbar. Ein Satoshi ist ein Hundertmillionstel eines Bitcoins. Es ist möglich, eine Bitcoin-Transaktion im Wert von 5.730 Satoshi zu senden.

Bitcoins (Un)fähigkeit zur Abwicklung von Transaktionen

Bitcoin soll ein elektronisches Geldsystem sein, bei dem sich die Teilnehmer untereinander direkt Geld schicken können. Ein Geldsystem, das nicht von einer zentralen Stelle kontrolliert wird, sondern auf einem Computerprotokoll basiert. Theoretisch sollte dieses Geldsystem für jeden auf der Welt zugänglich sein. Dies würde einen universellen Geldstandard schaffen, eine gemeinsame "Sprache" für die gesamte Menschheit.

Doch die Theorie lässt sich nicht so einfach in die Realität umsetzen. Auch wenn Bitcoin bereits ein elektronisches Geldsystem ohne kontrollierende Mittelsmänner ist, kann es nicht von jedem genutzt werden. Der Grund dafür ist die erforderliche Skalierbarkeit.

Das Problem wird deutlich, wenn man sich vorstellt, wie viele Transaktionen täglich in der Weltwirtschaft stattfinden. Während die Bitcoin-Technologie problemlos gigantische Summen transferieren kann, stößt sie bei einer hohen Transaktionsfrequenz an ihre Grenzen. Der Grund dafür ist technischer Natur: Die Blockchain, auf der alle Transaktionen aufgezeichnet werden, bietet nur begrenzten Platz für Transaktionen.

Man kann es sich ein bisschen wie einen Bus vorstellen. Dieser Bus hat eine begrenzte Anzahl von Plätzen. Wenn alle Plätze belegt sind, können keine weiteren Personen mehr mitfahren. Dies ist ein ähnlicher Mechanismus wie die Blöcke in der Bitcoin-Blockchain. Auch diese haben nur eine bestimmte Anzahl von "Plätzen" für Transaktionen. Wenn alle Plätze belegt sind, können keine weiteren Transaktionen mehr in den Bus einsteigen (d. h. bestätigt werden). Eine oft zitierte Kennzahl, wenn es um die Funktionalität von Bitcoin geht, sind Transaktionen pro Sekunde. Ein Block in Bitcoin kann maximal 1 Megabyte groß sein. Eine durchschnittliche Transaktion ist 400 Byte groß. Das bedeutet, dass im Durchschnitt 2.500 Transaktionen in einen Block passen können. Etwa alle 10 Minuten wird ein neuer Block gefunden. Folglich kann das Bitcoin-System etwa 4 Transaktionen pro Sekunde verarbeiten.

Das sogenannte "SegWit"-Upgrade erlaubt nun aber auch Blöcke bis zu 4 MB, wird aber noch nicht von allen Nodes unterstützt. Mit dem SegWit-Update für Bitcoin im Jahr 2017 wurde eine intelligente Lösung gefunden, um diese Grenze zu umgehen. Dadurch erhöhte sich die mögliche Anzahl der Transaktionen pro Sekunde um das Vierfache.

Während die Bitcoin-Blockchain bei mehr als vier Transaktionen pro Sekunde ihre Grenze erreicht, kann PayPal bis zu 115 Transaktionen pro Sekunde verarbeiten. Das Visa-Zahlungsnetzwerk behauptet, bis zu 24.000 Transaktionen pro Sekunde verarbeiten zu können. Das SegWit-Update hilft bei der Skalierbarkeit, erreicht aber nicht die Zahlen des Visa-Zahlungsnetzwerks.

Ein Mechanismus in Bitcoin ist, dass sich Transaktionen durch ihre Transaktionsgebühr einen Platz im Bus sichern können. Das heißt, wenn Alice eine wichtige Transaktion an Bob senden möchte, die einen Platz im nächsten Bus finden sollte, kann sie eine überdurchschnittlich hohe Gebühr zahlen. Der "Busfahrer" (der Miner) muss die Transaktion nicht fahren lassen, obwohl er eine relativ hohe Transaktionsgebühr verdienen kann, wenn er es tut. Folglich hat er einen wirtschaftlichen Anreiz, der Transaktion einen Platz in seinem Bus zu verschaffen.

Das Problem entsteht, wenn jeder, der versucht, eine Transaktion zu senden, eine überdurchschnittlich hohe Gebühr verlangt. Der Platz auf der Blockchain, der Platz auf dem nächsten Block, auf dem nächsten Bus, ist fest. Da immer mehr Menschen das Bitcoin-Geldsystem nutzen wollen, da immer mehr Transaktionen in den Bus drängen, steigen die Transaktionsgebühren. Das liegt daran, dass die Transaktionen über ihre Gebühren um einen Platz auf der Blockchain konkurrieren. Im Dezember 2017 konnte man ein Beispiel für dieses Ansteigen der Transaktionsgebühren sehen. Die Transaktionsgebühr hängt also nicht davon ab, wie viel Bitcoin Sie zu senden versuchen, sondern von der Konkurrenz durch andere unbestätigte Transaktionen und davon, wie hoch die Transaktionsgebühr ist, die sie bieten.

Bei der Diskussion um die Skalierbarkeit müssen jedoch auch zwei Nuancen erwähnt werden: Die Transaktionsgröße und die Endgültigkeit einer Transaktion.

Bei Bitcoin spielt es für die Gebühren und das Netzwerk keine Rolle, ob ein Betrag von 0,001 BTC oder 10.000 BTC gesendet wird. Was zählt, ist die Anzahl der Ein- und Ausgänge der Transaktion. Bei alternativen Zahlungssystemen wie Visa und PayPal zahlen Sie stattdessen normalerweise eine prozentuale Gebühr auf den Transaktionsbetrag. Das Versenden großer Beträge ist entsprechend teurer.

Die Endgültigkeit der Transaktion beschreibt die Möglichkeit, dass die Transaktion rückgängig gemacht werden kann. Bei Bitcoin ist das sehr schwierig: Ist eine Transaktion einmal abgeschickt und in einen Block geschrieben, kann sie kaum noch rückgängig gemacht werden. Das ist ein Vorteil, denn so können Verkäufer sicher sein, dass der vermeintlich freundliche Kunde sie nicht im Nachhinein betrügen wird. Anders bei PayPal und Visa: Hier gibt es eine Frist (meist 30 bis 120 Tage), in der die Zahlung widerrufen werden kann. Das ist möglich, weil PayPal oder Visa die zentrale Instanz im Geldsystem sind. Sie bestimmen die Historie der Transaktionen und können sie auch im Nachhinein ändern.

Während Bitcoin bei der Transaktionshäufigkeit noch hinterherhinkt, kann die Technologie bei der Transaktionsgröße und der finanziellen Finalität bereits massiv punkten.

Lösungsansätze für die Skalierung: On-Chain vs. Off-Chain

Die Frage der Transaktionskapazität wird oft auch als Skalierungsfrage bezeichnet. In ihrem Kern hat sie den gleichen Charakter wie die Gretchenfrage in Goethes Faust angenommen:

> "Sagen Sie mir, wie sieht es mit der Skalierung aus?"

Die Antworten lassen sich im Wesentlichen in zwei Lager unterteilen: On-Chain-Skalierung und Off-Chain-Skalierung.

Um auf das Beispiel des Busses zurückzukommen, wird in der Kette der Ansatz verfolgt, den Bus zu vergrößern. Das heißt, um die Blöcke auf 1 Megabyte zu begrenzen, wird eine neue Obergrenze für den Block festgelegt. Auf diese Weise können mehr Transaktionen auf den Bus passen, der immer noch alle 10 Minuten fährt. Angenommen, die Blockgröße steigt auf 10 Megabyte, dann steigt auch die Anzahl der Transaktionen pro Sekunde um den Faktor 10. Das bedeutet, dass dann etwa 40 Transaktionen pro Sekunde verarbeitet werden können. Die Möglichkeit, die Kapazität der Blockchain durch eine Erhöhung der Blockgröße zu verbessern, kommt in der Bitcoin-Hardfork Bitcoin Cash (BCH) zum Ausdruck.

Die Alternative dazu ist die Off-Chain-Skalierung. Hier geht es nicht darum, die Transaktionskapazität der Blockchain selbst zu verbessern, sondern eine zweite Schicht für Transaktionen zu schaffen, die an die erste Schicht, die Blockchain, andockt. Diese zweite Schicht würde die Sicherheitsaspekte von Bitcoin übernehmen und auch eine Größenordnung mehr Transaktionen ermöglichen. Anstatt linear zu skalieren, wie beim On-Chain-Ansatz, könnte die zweite Ebene Millionen von Transaktionen verarbeiten. Und diese könnten sofort, für sehr kleine Beträge und mit ähnlicher Sicherheit wie das Bitcoin-System selbst durchgeführt werden. Diese Methode der Skalierung von Bitcoin außerhalb der Blockchain wird auch als Lightning Network bezeichnet.

Lightning-Netzwerk

Das Lightning Network ist ein zeitgesperrter Off-Chain-Zahlungskanal. Das bedeutet, dass Nutzer BTC off-chain, d.h. außerhalb der Bitcoin-Blockchain, festlegen und an andere Nutzer senden können. Das Senden von Werten erfolgt fast sofort und erfordert, ähnlich wie bei On-Chain-Transaktionen, keine vertrauenswürdige dritte Partei. Das Lightning Network wird als vielversprechende Skalierungslösung für Bitcoin angesehen.

Für viele Bitcoin-Befürworter ist das Lightning Network (LN) die logische Weiterentwicklung des Bitcoin-Zahlungssystems. Sie können sich die Architektur wie eine Torte mit mehreren Schichten vorstellen. Die Bitcoin Blockchain ist die unterste, die sogenannte Basisschicht. Das Lightning Network würde darauf aufgebaut. Bestimmte Merkmale der Basisschicht könnten übernommen werden, wie z. B. die Sicherheit, während andere Beschränkungen nicht mehr gelten, wie z. B. die begrenzte Anzahl von Transaktionen. Die Verbindung zwischen der Basisschicht und dem Lightning Network wird durch eine Reihe von kryptografischen Mechanismen hergestellt.

Zahlungskanäle

Das Herzstück des Lightning Network sind Zahlungskanäle. Einen Zahlungskanal kann man sich als Tunnel zwischen zwei Parteien, Alice und Bob, vorstellen. Er verbindet Alice und Bob direkt miteinander. Der Unterschied zwischen einem Zahlungskanal und einer Transaktion auf der Blockchain besteht darin, dass Zahlungen innerhalb des Tunnels nicht in der Blockchain aufgezeichnet werden. Stattdessen können Alice und Bob den Status des Zahlungskanals ständig aktualisieren und den letzten Status erst dann in die Blockchain schreiben, wenn sie "fertig" sind. Die Aktualisierung des Zahlungskanals erfolgt außerhalb der Blockchain und unterliegt nicht deren Beschränkungen. Alice und Bob könnten den Status ihres Kanals mehrere Male pro Sekunde aktualisieren. Mit anderen Worten: Mikrotransaktionen werden nicht nur möglich, sondern auch plausibel. Anstatt mehrere Transaktionen zu senden, wird der geschuldete Betrag nach einer bestimmten Zeit summiert und erst dann auf der Hauptblockchain abgerechnet.

1.2 Bitcoin-Mining- Ein Deep Dive

In Modul 1 haben Sie bereits ein Verständnis für den Zweck und die Funktionsweise des Bitcoin-Mining-Prozesses gewonnen. Jetzt werden Sie im Generation Blockchain Podcast über Bitcoin-Mining in die Details des Minings eintauchen, wie z.B. die Hardware- und Energieanforderungen und die Legalität des Minings in verschiedenen Ländern.

Klicken Sie hier, um den Generation Blockchain-Podcast über Bitcoin-Mining anzuhören.

02

MODUL 3

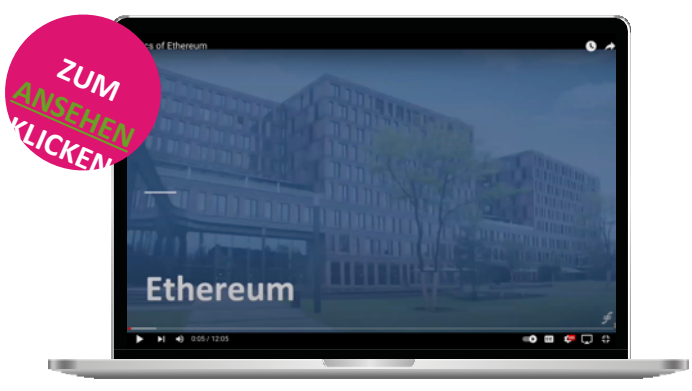
ETHEREUM

2.1 Einführung in Ethereum

Nach Bitcoin ist Ethereum die zweitgrößte Kryptowährung, gemessen an der Marktkapitalisierung. Das Ethereum-Netzwerk ist eine Blockchain-basierte Plattform, die sich auf programmierbare Verträge (Smart Contracts) und dezentralisierte Programme (dApps) konzentriert. Die zugehörige Kryptowährung wird Ether (ETH) genannt. Ethereum wird auch oft als "Weltcomputer" bezeichnet. Der Begriff "Weltcomputer" rührt daher, dass Ethereum nicht nur den Zustand des Währungsbesitzes speichert wie Bitcoin, sondern den Zustand jeder Art von beliebigen Daten verfolgen und jeden Code ausführen kann, der sich in ein binäres Datenformat bringen lässt.

Ethereum (ETH) ist eine dezentralisierte Open-Source-Plattform, die auf der Blockchain-Technologie basiert. Sie ermöglicht es jedem interessierten Entwickler, jeder Einzelperson oder jedem Unternehmen, seine eigene dApp oder sogar eine dezentrale Organisation (DAO) unter Verwendung von Smart Contracts zu betreiben und zu entwickeln. Ethereum verfügt über einen Speicher, in dem sowohl Code als auch Daten gespeichert werden, und nutzt die Ethereum-Blockchain, um zu verfolgen, wie sich dieser Speicher im Laufe der Zeit verändert, ähnlich wie ein allgemeiner Computer mit gespeicherten Programmen. Ethereum kann Code in seine Zustandsmaschine laden und diesen Code ausführen und die daraus resultierenden Änderungen in seiner Blockchain speichern.

Um die Grundlagen von Ethereum zu verstehen, sehen Sie sich dieses Einführungsvideo von Generation Blockchain an. Klicken Sie hier, um das Generation Blockchain-Video über die Grundlagen von Ethereum anzusehen.



Die Erfinder von Ethereum

Vitalik Buterin ist der ursprüngliche Erfinder und Mitbegründer von Ethereum. In den frühen Phasen der Bitcoin-Entwicklung leitete Buterin ein Magazin, das sich mit dem Thema Bitcoin befasste. Dabei identifizierte er Aspekte bei Bitcoin, die er als verbesserungswürdig ansah. Vitalik Buterin gründete dann zusammen mit Anthony Di Iorio, Mihai Alisie und Charles Hoskinson Ethereum. Buterin erläuterte die Ethereum-Blockchain erstmals 2013 in einem Whitepaper. Ethereum sollte das volle Potenzial von Bitcoin freisetzen. Es kombiniert eine Synthese aus radikaler Offenheit und radikaler Privatsphäre. Buterin wollte eine Plattform schaffen, die ein Mining-System ist und eine Plattform für die Entwicklung eigener Software-Anwendungen bietet.

Ether Währungseinheiten

Die Kryptowährung der Ethereum-Blockchain wird Ether genannt. Ether ist ein Zahlungsmittel für jede Transaktion oder Erstellung von Smart Contracts sowie für die Nutzung verschiedener Dienste auf der Ethereum-Plattform. Alle Änderungen, die am Weltzustand von Ethereum vorgenommen werden, kosten Ether. Um mit der Ethereum-Blockchain zu interagieren, muss man Ether kaufen. Ether ist der Treibstoff der gesamten Plattform. Ether wird auch als Belohnung an Ethereum-Staker und -Validierer verteilt. Ether ist in kleinere Einheiten unterteilt, bis hin zur kleinstmöglichen Einheit, die wei genannt wird. 1 Ether ist 1 Quintillion (1018) wei.

Was sind Smart Contracts?

Smart Contracts sind digitalisierte, festgelegte Verträge zwischen zwei oder mehreren Personen oder Softwareprogrammen. Der Code kann entweder die einzige Manifestation der Vereinbarung zwischen den Parteien sein oder auch als Ergänzung zu einem herkömmlichen textbasierten Vertrag fungieren und bestimmte Bestimmungen ausführen, z. B. die Überweisung von Geldern von Partei A an Partei B. Der Code selbst wird über mehrere Knoten einer Blockchain repliziert und profitiert daher von der Sicherheit, Beständigkeit und Unveränderlichkeit, die eine Blockchain bietet. Es ist möglich, intelligente Verträge für die Entwicklung einer DAO oder einer dApp zu verwenden.

Smart Contracts

1 von einem Netzwerk von Computern betrieben werden

2 vereinbarte Schritte automatisch ausführen, wenn ein bestimmtes Ereignis eintritt

3 automatische Verfolgung von Änderungen innerhalb der festgelegten Vertragsbedingungen

4 in der Blockchain gespeichert sind

Im Ethereum-Netzwerk existieren smart contracts als unabhängige Benutzer, mit denen interagiert werden kann, und haben somit denselben Status wie menschliche Benutzer. Das bedeutet auch, dass sie von jedem im Netzwerk eingesehen und überwacht werden können. In den Verträgen werden Bedingungen definiert, die jeder auf ihre Richtigkeit überprüfen kann. Je nachdem, ob das auslösende Ereignis eintritt, führen die Smart Contracts automatisch die damit verbundenen Befehle aus. Diese Smart Contracts werden auf der Ethereum Blockchain gespeichert.

Beispiel für einen Smart Contract

Der Smart Contract beinhaltet zum Beispiel die Vereinbarung, dass eine Person ihr Geld für das Paket erhält, wenn es drei Tage nach der Bestellung eintrifft. Außerdem ist ein solcher Smart Contract mit einer Software verbunden, die den Status des Pakets überprüfen kann (d. h. ob es geliefert wurde oder nicht). Sobald das Paket eingetroffen ist, gibt der Smart Contract automatisch den im Smart Contract gespeicherten Ether-Betrag des Empfängers an den Absender des Pakets frei. Wenn die Software feststellen würde, dass das Paket nicht zugestellt wurde, könnte sich der Smart Contract selbst außer Kraft setzen und der Käufer erhält sein Geld zurück.

Smart Contracts und die Ethereum-Blockchain

Das Besondere an Ethereum sind jedoch die Smart Contracts, die das Ethereum-Netzwerk zu einem dezentralen Computer machen. Smart Contracts sind kleine Programme, die auf dem Ethereum-Netzwerk laufen und zum Beispiel die Bedingungen für Ethereum-Transaktionen regeln können. Im Gegensatz zum Bitcoin-Netzwerk sind die Knotenpunkte des Ethereum-Netzwerks auch für die Bearbeitung dieser Contracts zuständig. Durch Smart Contracts ist es möglich, sogenannte dezentrale Apps zu entwickeln. DApps sind öffentlich zugängliche dezentrale Anwendungen. Da letztlich jeder einen Ethereum-Knoten betreiben kann, haben alle dApps die gleiche Funktionalität und können entsprechend auf der Infrastruktur aufbauende Dienste anbieten.

Ethereum dApps

Überall auf der Welt bauen Entwickler dApps auf Ethereum auf und kreieren innovative dApps. Der dApp-Entwicklung sind fast keine Grenzen gesetzt. Es gibt Finanzanwendungen, dezentrale Börsen (DEX), Social-Media-Plattformen, Messenger-Dienste,

Spiele, was nur ein paar Beispiele für dApps sind. Smart Contracts können als Back-End-APIs betrachtet werden, die auf der Blockchain laufen, während dApps das Front-End oder die UX darstellen. Sie stellen die sichtbare Schicht dar, die Nutzer oder andere Anwendungen mit den in der Blockchain laufenden Smart Contracts verbindet. Sie denken dabei vielleicht an App-Stores, die wir bereits kennen. Genau wie bei dApps gibt es heute unzählige Apps im App Store. Diese Apps vertrauen dem App-Store bei der Zahlungsabwicklung und involvieren somit eine dritte Partei und die Notwendigkeit eines etablierten Vertrauens. Auch traditionelle Entwickler sind auf die Gunst des App Stores angewiesen. App Stores können als letzte Instanz Apps aus ihren Stores entfernen. Die Entscheidung des Verbrauchers hängt also auch vom Einfluss Dritter wie Google oder Apple ab. In der Konsequenz bedeutet dies, dass die von ihnen erzeugten Inhalte in den Händen Dritter liegen und von ungeschriebenen Regeln der Branche beeinflusst werden. Anders verhält es sich bei dApps, die auf Ethereum aufgebaut sind. Hier befinden sich die Daten in den Händen der Nutzer. Entwickler können dApps frei und unabhängig von einem App-Store-Anbieter anbieten, wodurch die Vorauswahl eines App-Stores gänzlich entfällt. Der Betrieb eines Ethereum-Knotens ist keine Voraussetzung für die Implementierung von DApps. Stattdessen gibt es private Angebote in der Cloud, die Zugang zu bestehenden Nodes bieten können.

Ether-Versorgung

Im Gegensatz zu Bitcoin, bei dem die maximale Anzahl an Bitcoin auf 21 Millionen begrenzt ist, gibt es bei Ether kein Limit. Es wird nie ein Ende der Ether-Produktion geben. Wie viele Ether es gibt, hat einen direkten Einfluss auf den Preis. Generell gilt: Je mehr Münzen öffentlich verfügbar sind, desto niedriger ist ihr Wert. Die Gesamtmenge an Ether ist immer noch fließend, da die jüngste Umstellung des Netzwerks auf PoS eine Zunahme und Abnahme des Ether-Angebots in beide Richtungen möglich gemacht hat.

Die Unterschiede zwischen Ethereum und Bitcoin

Bitcoin und Ethereum unterscheiden sich in vielen Aspekten. Während Bitcoin eine Kryptowährung ist, ist Ethereum eine Plattform. Aus diesem Grund ist Bitcoin in erster Linie ein Wertaufbewahrungs- und Tauschmittel, während Ethereum als Allzweck-Blockchain angesehen wird. Ether ist der native Token auf der Ethereum-Blockchain. Gemessen an der Marktkapitalisierung ist und war Bitcoin die größte Kryptowährung, während Ethereum die zweitgrößte ist. Transaktionen sind im Ethereum-Netzwerk schneller als im Bitcoin-Netzwerk, da die Ethereum-Blockchain etwas schneller ist als die Bitcoin-Blockchain. Es ist auch wichtig zu beachten, dass Ethereum als Ergänzung zu Bitcoin und nicht als Konkurrenz geschaffen wurde. Während Bitcoin sich als Kryptowährung etablieren konnte, zielt Ethereum darauf ab, einen dezentralen Weltcomputer zu schaffen. In diesem Sinne ist ein Vergleich zwischen den beiden Kryptowährungen schwierig.

2.2 Ethereum-Transaktionen

Wie Ethereum-Transaktionen mit Smart Contracts funktionieren, erfahren Sie in der Podcast-Episode Generation Blockchain zu diesem Thema.

Klicken Sie hier, um die Episode des Generation Blockchain Podcasts über Ethereum-Transaktionen und Smart Contracts anzuhören.

2.3 Ethereum Smart Contracts

In einem vorangegangenen Abschnitt haben Sie bereits einen groben Überblick über Smart Contracts erhalten, der im Folgenden vertieft werden soll.

Wie Sie bereits wissen, sind Smart Contracts eine Art Ethereum-Konto. Sie haben also ein Guthaben und können das Ziel von Transaktionen sein. Smart Contracts müssen nicht von einem Nutzer kontrolliert werden, sondern werden im Netzwerk bereitgestellt und laufen wie zuvor programmiert. Tatsächliche Benutzerkonten können mit einem Smart Contract interagieren, indem sie Transaktionen verschicken, die eine im Smart Contract definierte Funktion ausführen. Smart Contracts können wie ein regulärer Vertrag Regeln festlegen und diese automatisch über den Code durchsetzen. Smart Contracts können standardmäßig nicht gelöscht werden, und Interaktionen mit ihnen sind unumkehrbar. Sie können nur von autorisierten Parteien überschrieben werden. Smart Contracts sind einfache Programme, die auf einer Blockchain gespeichert sind und ausgeführt werden, wenn bestimmte Bedingungen erfüllt sind.

Sie werden in der Regel eingesetzt, um die Ausführung einer Vereinbarung zu automatisieren, so dass alle Beteiligten sofort Gewissheit über das Ergebnis haben, ohne dass ein Vermittler eingeschaltet werden muss oder Zeit verloren geht. Sie können auch einen Arbeitsablauf automatisieren und die nächste Aktion auslösen, wenn die Bedingungen erfüllt sind.

Was die Implementierung betrifft, so haben Vitalik und seine Mitgründer die sogenannte Ethereum Virtual Machine (EVM) für die Ausführung von Byte-Code in der Blockchain entwickelt. Jeder Knoten im Netzwerk führt diese EVM aus und ist in der Lage, jeden beliebigen Code auszuführen. Um einen neuen Vertrag in der Blockchain zu erstellen, muss die Programmdarstellung in Bytecode als Teil der Transaktionsdaten gesendet werden. Sobald der EVM die Transaktion ausführt und der Block dem Ledger hinzugefügt wird, erhält der Programmierer die öffentliche Adresse, an der er veröffentlicht wurde. Von dort aus kann jeder, der Zugang dazu hat, mit dem Vertrag unter dieser Adresse interagieren.

Es gibt drei wichtige Aspekte von intelligenten Verträgen. Der Ausführungskontext, die Gasgebühr und die Unveränderlichkeit.

Ausführungskontext

Smart Contracts laufen isoliert, d. h. sie können nur die auf der Ethereum-Blockchain verfügbaren Daten einsehen oder andere Smart Contracts aufrufen. Sie können also keine Dienste aufrufen oder Daten von außerhalb der Ethereum-Blockchain abfragen. Einige Verträge auf Ethereum fungieren als Orakel. Externe Nutzer oder Anwendungen können diese Orakel-Verträge mit externen Daten füttern, so dass andere sie konsumieren können.

Gasgebühr

Die Ausführung von Code im EMV ist ohne die Zahlung einer Gasgebühr nicht möglich, da Rechenressourcen und Speicherplatz knapp sind und für die Validierer nicht kostenlos sind. Die Kosten für die Nutzung von Ethereum-Diensten werden in einer Einheit ausgedrückt, die als Gas bezeichnet wird und kurze Bruchteile von Ether (in WEI) darstellt. Für jede Transaktion, die eingereicht wird, muss Gas bezahlt werden, da der Code sonst nicht ausgeführt werden kann. Gas wird durch die Ausführung von Codezeilen oder die Zuweisung von Speicherplatz verbraucht. Wenn einer Transaktion das Gas ausgeht, führt dies zum Abbruch der Transaktion. In diesem Fall werden die Token oder Gelder trotzdem ausgegeben. Technisch gesehen handelt es sich bei Gas um eine Einheit und nicht um einen Preis, da der Preis für die Transaktion bei deren Erstellung festgelegt wird. Je höher der Preis ist, den man zahlt oder zu zahlen bereit ist, desto höher ist die Priorität der Transaktion in der Ausführungswarteschlange. Die Prüfer haben einen Anreiz, Transaktionen auszuführen, die mehr kosten, da sie die Gasgebühren erhalten. Man kann auch ein Gaslimit für die Transaktion festlegen. Damit wird ausgedrückt, wie viel man bereit ist, für die Ausführung auszugeben. Wenn die Transaktion mehr kostet, wird sie abgebrochen, und die nicht verwendeten Mittel werden an den Absender zurückgegeben.

Unveränderlichkeit

Smart Contracts sind unveränderbar. Daher können sie per Definition (Byte-Code) nicht geändert oder aktualisiert werden, sobald sie auf der Ethereum-Blockchain bereitgestellt wurden. Wenn ein bestehender Smart Contract geändert werden soll, muss eine neue Version an einer neuen Adresse bereitgestellt werden. Einmal eingeführte Fehler können nicht mehr behoben werden.

03

MODUL 3

DEZENTRALES FINANZWESEN

Bevor wir uns mit dem dezentralen Finanzwesen (DeFi) beschäftigen, müssen wir zunächst unser derzeitiges Finanzsystem auf einer grundlegenden Ebene verstehen, um die Parallelen zwischen dem traditionellen Finanzwesen (TradFi) und DeFi zu erkennen.

3.1 Traditionelles Finanzsystem

Jedes Finanzsystem, wie wir es heute kennen, ist ein hochgradig vernetztes Netz von Vermittlern, Moderatoren und Märkten, das folgenden Zwecken dient:

1 Zuteilung von Kapital,

2 Teilung der Risiken, und

3 Erleichterung aller Arten von Handel, einschließlich des intertemporalen Austauschs.

Was auf den ersten Blick uninteressant klingt, ist in einem kapitalistischen System eine der wichtigsten Säulen für das menschliche Wohlergehen. Ohne dieses Finanzsystem hätte der technische Fortschritt der letzten zwei Jahrhunderte (z. B. die Erfindung von Dampfmaschinen, Autos, Flugzeugen, Festnetztelefonen, Computern, Genmanipulationen und Mobiltelefonen) nicht stattgefunden, zumindest nicht in diesem Tempo.

Der Zweck des Finanzsystems

Die Hauptfunktion des Systems besteht darin, Kreditnehmer und Kreditgeber effizient miteinander zu verbinden. Zu den Kreditnehmern gehören Erfinder, Unternehmer, Privathaushalte, Regierungen, Unternehmen und Start-ups mit potenziell rentablen Geschäftsideen, aber begrenzten finanziellen Ressourcen, bei denen die Ausgaben höher sind als die Einnahmen. Kreditgeber oder Sparer sind ebenfalls unterschiedlich kalibriert und können in Form von Privathaushalten, Unternehmen, Regierungen und Investoren mit überschüssigen Mitteln auftreten, bei denen die Einnahmen höher sind als die Ausgaben. Das Finanzsystem trägt auch dazu bei, risikoscheue Unternehmen, so genannte Hedger, mit Spekulanten zu verbinden.

Es kommt vor, dass Einzelpersonen und Unternehmen, insbesondere kleine Unternehmen oder solche, die auf schnell wachsenden Märkten tätig sind, über genügend Vermögen (d. h. einen Bestand) und Einkommen (d. h. einen Geldfluss) verfügen, um ihre Ideen ohne finanzielle Unterstützung von außen umzusetzen, indem sie ihre Gewinne zurückführen, was auch als Innenfinanzierung bezeichnet wird. Der häufigere Fall ist jedoch, dass Menschen und Unternehmen, die gute Ideen haben, nicht über die erforderlichen Mittel verfügen, um Entwürfe zu erstellen, Prototypen zu entwickeln, Büros oder Produktionsräume zu mieten, Mitarbeiter zu bezahlen, Genehmigungen und Lizenzen zu erhalten oder die Risiken zu tragen, die mit der Markteinführung einer Ware oder Dienstleistung verbunden sind. Ausreichende finanzielle Mittel sind unerlässlich, um unsere Ideen beruflich und privat zu verfolgen und zu verwirklichen. Dieser Kurs über Blockchain zum Beispiel ist kostenlos, weil die EU Bildung als eine Notwendigkeit ansieht, die nicht nur denjenigen Studenten zugänglich gemacht werden sollte, die die Mittel haben, sie zu bezahlen.

Die Notwendigkeit eines Finanzsystems (?)

Warum leihen sich Privatpersonen und Unternehmen nicht einfach von anderen Privatpersonen und Unternehmen, wenn sie es müssen?

Wie bei den meisten anderen Waren und Dienstleistungen ist die Kreditvergabe am effizientesten und billigsten, wenn sie von Spezialisten und Unternehmen durchgeführt wird, die sich auf eine einzige Sache (oder ein paar verwandte Tätigkeiten) konzentrieren und diese sehr gut ausführen. Erstens haben sie durch die Praxis und die Forschung, die sie im Laufe der Zeit gesammelt haben, und zweitens können sie auch Größenvorteile nutzen. So sind beispielsweise die Fixkosten für die Kreditvergabe (d. h. Werbung für Kreditnehmer, Kauf und Wartung von Computern, Anmietung geeigneter Büroräume und Ausarbeitung von Verträgen) recht hoch. Um diese Fixkosten auszugleichen und eine große Gewinnspanne zu erzielen, müssen die Kreditgeber viele Geschäfte abschließen. Daher können kleine Unternehmen in einem stark konzentrierten Markt nicht rentabel sein. Das soll jedoch nicht heißen, dass größer immer besser ist, sondern nur, dass Finanzunternehmen ein Minimum an effizienter Größe überschreiten müssen, um effizient zu sein.

Asymmetrische Informationen

Im Finanzbereich gibt es noch ein weiteres Problem, das nicht leicht zu lösen ist, nämlich das Konzept der Opportunitätskosten (d.h. um X zu erhalten, muss man Y aufgeben). Darüber hinaus gibt es ein weiteres Problem, das als asymmetrische Information bezeichnet wird. Wenn in einem Finanzsystem ein Verkäufer (d. h. ein Kreditnehmer, ein Verkäufer von Wertpapieren) mehr weiß als ein Käufer (d. h. ein Kreditgeber oder ein Anleger, ein Käufer von Wertpapieren), dauert es nicht lange, bis sich die Probleme zeigen. Die beiden Hauptprobleme dabei sind die adverse Selektion vor der Vertragsunterzeichnung und das moralische Risiko, das eine Sünde nach dem Vertragsabschluss eintreten lassen kann.

Ungünstige Auswahl

Ironischerweise sind die riskantesten Kreditnehmer auch diejenigen, die am stärksten Kredite nachfragen. Wenn sich die Kreditgeber dieser Selektionsverzerrung nicht bewusst sind, werden sie immer mehr zögern, ihr Geld zu verleihen. Solange dies nicht erkannt und wirksam bekämpft wird, führt Moral Hazard zu demselben suboptimalen Ergebnis.

Moralisches Risiko

Selbst wenn die adverse Selektion kein Problem darstellen würde, werden gutwillige Kreditnehmer nach der Unterzeichnung manchmal zu Dieben, weil sie merken, dass sie mit dem Geld anderer Leute spielen können. Diese Art der Veruntreuung ist weit verbreitet, und die Kreditnehmer sind am Ende oft nicht mehr in der Lage, den Kredit zurückzuzahlen.

Das derzeitige Finanzsystem beseitigt die Informationsasymmetrie nicht, aber es verringert ihren Einfluss, und zwar bei den Vermittlern durch die Prüfung von Versicherungs- und Kreditantragstellern und deren anschließende Überwachung sowie auf den Märkten durch die Bereitstellung von Preisinformationen und Analysen. Unternehmen und andere Kreditnehmer können Geldmittel und Versicherungen so günstig erhalten, dass sie trotz asymmetrischer Informationen effizienter werden, innovativ sind, Erfindungen machen und in neue Märkte expandieren können. Eine andere Sichtweise ist die, dass das Finanzsystem den intertemporalen Handel, also den Handel über die Zeit hinweg, erleichtert. Anstatt sofort für Lieferungen bezahlen zu müssen, nutzen Unternehmen das Finanzsystem, um das zu erwerben, was sie heute für ihren Betrieb benötigen, und es zu einem bestimmten Zeitpunkt in der Zukunft zu bezahlen, so dass sie Zeit haben, ihre Produkte herzustellen und zu vertreiben.

Finanzinstrumente

Finanzinstrumente sind rechtsverbindliche Verträge, in denen die Verpflichtungen ihrer Aussteller, d. h. der Personen, Regierungen oder Unternehmen, die sie ausgeben und Zahlungen versprechen, und die Rechte ihrer Inhaber, d. h. der Personen, Regierungen oder Unternehmen, die sie derzeit besitzen und Zahlungen erwarten, aufgeführt sind. Sie dienen dem Zweck, festzulegen, wer wem was schuldet, wann oder unter welchen Bedingungen die Zahlung fällig ist und wie und wo die Zahlung zu erfolgen hat.

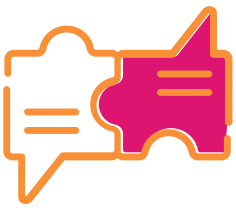
Es gibt im Wesentlichen drei Formen von Finanzinstrumenten:

Verschuldung

Schuldtitel, wie z. B. Anleihen, sind eine Kreditgeber-Kreditnehmer-Beziehung, bei der der Kreditnehmer verspricht, dem Kreditgeber zu einem bestimmten Zeitpunkt oder über einen bestimmten Zeitraum einen bestimmten Betrag und Zinsen zu zahlen.

Eigenkapital

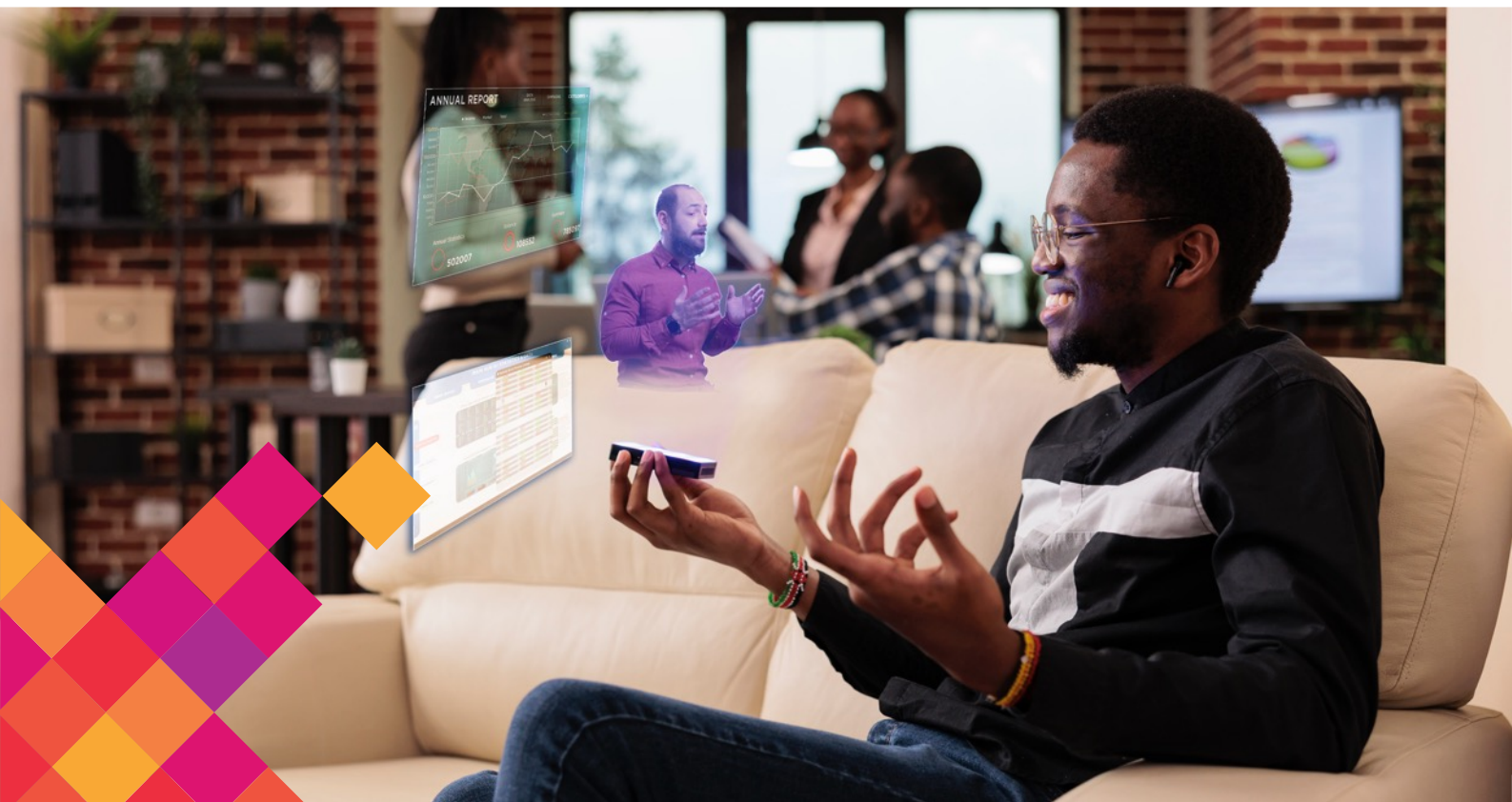
Eigenkapitalinstrumente, wie z. B. Aktien, stellen einen Eigentumsanteil dar, bei dem der Inhaber des Instruments einen Teil der Gewinne des Emittenten erhält.



Hybride

Hybride Instrumente (z. B. Vorzugsaktien) weisen einige Merkmale sowohl von Schuldtiteln als auch von Eigenkapitalinstrumenten auf. Wie eine Anleihe versprechen Vorzugsaktien feste Zahlungen zu bestimmten Terminen, aber wie Stammaktien nur, wenn die Gewinne des Emittenten dies rechtfertigen. Wandelanleihen hingegen sind hybride Instrumente, da sie den Inhabern die Möglichkeit bieten, Schuldtitel in Aktien umzuwandeln.

Heute werden die meisten Finanzinstrumente nur noch in Form von elektronischen Buchungseinträgen gehalten, die mit einem bestimmten Vertrag verbunden sind. Aktien wurden früher in Papierform ausgegeben.



Finanzmärkte

Das derzeitige Finanzsystem ist kein direktes Finanzsystem. Es ist immer ein Vermittler erforderlich, um eine Transaktion abzuwickeln, es sei denn, die Transaktion erfolgt in Form von Bargeld. So erleichtern beispielsweise Makler die Sekundärmärkte, indem sie Verkäufer und Käufer von Wertpapieren gegen eine Gebühr oder eine Provision, einen Prozentsatz des Verkaufspreises, zusammenbringen. Händler "machen einen Markt", indem sie Wertpapiere kaufen und verkaufen und dabei von der Arbitrage, d. h. der Differenz zwischen dem Verkaufs- und dem Kaufkurs, profitieren. Makler bieten in der Regel beides an - Makeln und Handeln - und beraten ihre Kunden auch bei Investitionsentscheidungen. Investmentbanken unterstützen die Primärmärkte, indem sie Aktien- und Anleiheemissionen übernehmen (d. h. zum Weiterverkauf an Investoren kaufen) und die direkte Platzierung von Anleihen arrangieren. Investmentbanken können auch als Makler tätig sein, indem sie Wertpapieremittenten bei Anlegern vorstellen.

Wie die Finanzmärkte sind auch die Finanzintermediäre hoch spezialisiert. Finanzintermediäre haben sehr unterschiedliche Funktionen, von der Geldanlage über die Beratung bis hin zur Nutzung unterschiedlicher Preise für ein und denselben Vermögenswert zu einem bestimmten Zeitpunkt und viele andere. Sie werden in der Regel nach ihrer Eigentumsstruktur kategorisiert. So geben beispielsweise Einlageninstitute (d. h. Geschäftsbanken, Sparkassen und Kreditgenossenschaften) kurzfristige Einlagen aus und kaufen langfristige Wertpapiere. Traditionell haben sich Geschäftsbanken auf die Ausgabe von Sicht-, Transaktions- oder Giroeinlagen und die Vergabe von Krediten an Unternehmen spezialisiert. Sparkassen gaben Termin- oder Spareinlagen aus und vergaben Hypothekarkredite an Haushalte und Unternehmen, während Kreditgenossenschaften Termineinlagen ausgaben und Verbraucherkredite vergaben. Fast alle Geschäftsbanken und viele Sparkassen sind Aktiengesellschaften. Einige Sparkassen und alle Kreditgenossenschaften sind Aktiengesellschaften auf Gegenseitigkeit und damit im Besitz derjenigen, die bei ihnen Einlagen getätigt haben. Der heutige Finanzmarkt ist sehr komplex und das Ergebnis jahrelanger Entwicklungen.

Verordnung

Das Finanzsystem ist im Vergleich zu anderen Sektoren in kapitalistischen Ländern relativ stark reguliert. Die Regulierungsbehörden erfüllen vier wichtige Funktionen:

1 Asymmetrische Informationen abbauen

Sie versuchen dies zu erreichen, indem sie Transparenz fördern und einfordern. Das bedeutet in der Regel, dass sowohl die Finanzmarktteilnehmer als auch die Intermediäre verpflichtet sind, den Anlegern genaue Informationen in klarer und rechtzeitiger Form offenzulegen.

2 Schutz der Verbraucher

Die Regulierungsbehörden müssen die Verbraucher vor Betrügern und vor dem Konkurs ehrlicher, aber schlecht geführter Finanzinstitute schützen. Sie tun dies, indem sie die Arten von Vermögenswerten, mit denen Finanzinstitute Geschäfte machen dürfen, direkt beschränken und Mindestreserven und eine Mindestkapitalisierung vorschreiben.

3 Förderung des Wettbewerbs und der Effizienz des Finanzsystems

Die Regulierungsbehörden fördern den Wettbewerb, indem sie dafür sorgen, dass der Markteintritt und -austritt von Unternehmen so einfach und kostengünstig wie möglich ist.

4 Sicherstellung der Solidität des Finanzsystems

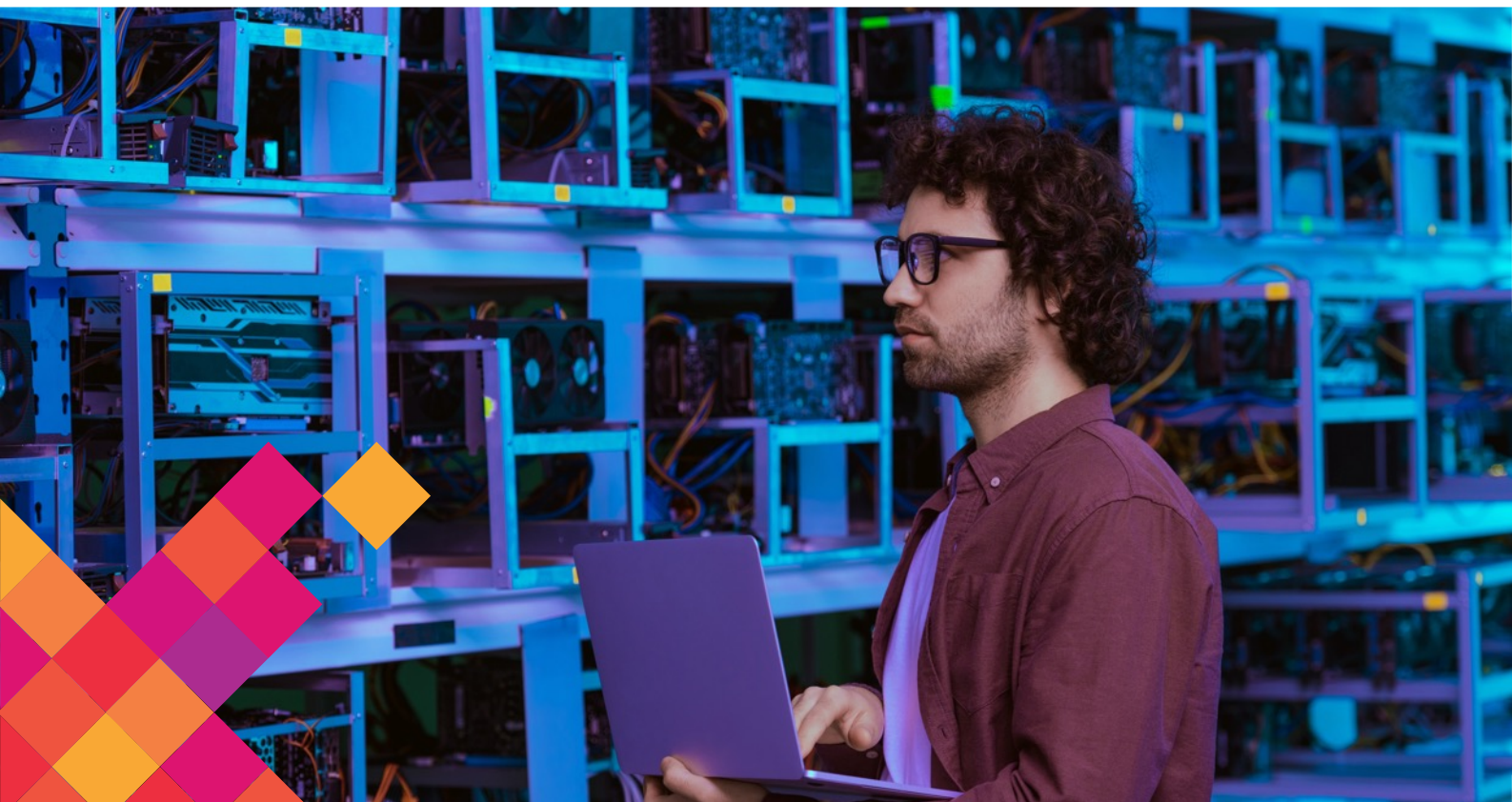
Ziel der Regulierungsbehörde ist es, die Solidität des Finanzsystems zu gewährleisten, indem sie als Kreditgeber letzter Instanz fungiert, eine Einlagensicherung vorschreibt und den Wettbewerb durch Beschränkungen des Marktzugangs und der Zinssätze einschränkt, was einen umstrittenen Eingriff in den Markt darstellt. Auch die Regulierungsbehörden können den Wettbewerb auf dem Markt einschränken, um die Sicherheit zu gewährleisten. Dadurch werden jedoch bestehende Institute gegenüber neuen Instituten privilegiert, weshalb bestehende Unternehmen häufig Befürworter der Regulierung sind.

Je nach Gerichtsbarkeit gibt es in der Regel mehr als eine lokale Aufsichtsbehörde, an die man sich halten muss. In den USA zum Beispiel überwachen und regulieren die Securities and Exchange Commission (SEC, die Börsen und OTC-Märkte beaufsichtigt), die New York Stock Exchange (NYSE, die sich selbst als SRO oder selbstregulierende Organisation beaufsichtigt) und die Commodities Futures Trading Commission (CFTC, die Terminmarktbörsen beaufsichtigt) die Finanzmärkte. Neben diesen drei großen Aufsichtsbehörden gibt es noch weitere Regulierungsbehörden, darunter das Office of the Comptroller of the Currency (das die staatlich gecharterten Geschäftsbanken beaufsichtigt), die Federal Deposit Insurance Corporation (FDIC, die fast alle Einlageninstitute beaufsichtigt) und verschiedene staatliche Banken- und Versicherungsausschüsse, die die Finanzintermediäre überwachen. Akteure, die versuchen, sich aufgrund der hohen Kosten einer aufsichtsrechtlichen Kontrolle zu entziehen, neigen dazu, statt der Märkte auf Intermediäre zurückzugreifen.

3.2 Dezentrales Finanzsystem

Mit dem Versprechen, den Zugang und die Effizienz von Finanzdienstleistungen zu verbessern, hat DeFi in den letzten Jahren erhebliche Aufmerksamkeit (und eine gewisse Zugkraft auf dem Markt) erlangt. Im Wesentlichen nutzt DeFi die sichere Blockchain-Technologie zur Erleichterung von Peer-to-Peer-Finanztransaktionen, einschließlich Kreditaufnahme, Kreditvergabe und Handel. DeFi zielt darauf ab, die traditionelle Finanzdienstleistungsbranche durch die Automatisierung komplexer Finanzprozesse zu unterbrechen und zu dezentralisieren. Die Funktionen von vertrauenswürdigen Dritten, wie Maklerfirmen, Banken und anderen zentralisierten Finanzinstituten, werden durch intelligente Verträge ersetzt. Obwohl es sich bei DeFi im Großen und Ganzen noch um ein Nischenphänomen handelt, dessen langfristige Auswirkungen auf die Finanzdienstleistungsbranche noch nicht absehbar sind, bedeutet das Potenzial der Disintermediation, dass es wichtig ist, dass etablierte Finanzinstitute verstehen, wie es die operative Landschaft umgestalten könnte und wie sie selbst das Konzept der Dezentralisierung annehmen könnten. Sicher ist, dass im Bereich der digitalen Vermögenswerte im Jahr 2022 eine große Marktkorrektur im Gange ist.

Es gibt bereits eine breite Palette von Finanzdienstleistungen oder -produkten im DeFi-Bereich, darunter Handel, Kreditvergabe, Investitionen, Einlagen und Zahlungsdienste. Außerdem sind dezentrale Anwendungen hochgradig modular. Das bedeutet, dass sie sehr oft kombiniert werden können und interoperabel sind, um neue Anwendungen zu schaffen. Die steigende Popularität von DeFi lässt sich zum Teil durch reale und wahrgenommene strukturelle Probleme in der derzeitigen Finanzdienstleistungsbranche erklären. DeFi entstand aus dem Wunsch heraus, Finanzdienstleistungen von der Kontrolle zentralisierter Institutionen und Regierungen zu befreien, wie im vorangegangenen Abschnitt beschrieben, und so mehr Menschen finanzielle Integration zu ermöglichen. Die Befürworter von DeFi argumentieren, dass die traditionellen Finanzdienstleistungen von großen Institutionen dominiert werden und oft durch einen streng kontrollierten Zugang gekennzeichnet sind, was zu organisch gewachsener Ineffizienz, hohen und undurchsichtigen Gebühren sowie zu finanzieller Ausgrenzung führt. Darüber hinaus verweisen sie darauf, dass das hohe Maß an Regulierung in den meisten Ländern der Welt ein Umfeld fördert, das bahnbrechenden Technologien oder innovativen Geschäftsmodellen generell feindlich gegenübersteht. Während einige Branchenkommentatoren die Nachhaltigkeit vollständig dezentralisierter Finanzdienstleistungen bezweifeln, glauben andere, dass DeFi ein echtes Potenzial hat, die traditionellen Finanzdienstleistungsmärkte zu stören.



Die Schichten von DeFi

Ein grundlegendes Verständnis der verschiedenen Technologieebenen, die für DeFi-Anwendungen verwendet werden, schafft eine mentale Landkarte, die bei der Analyse und Bewertung spezifischer DeFi-Implementierungen hilfreich ist (siehe unten).

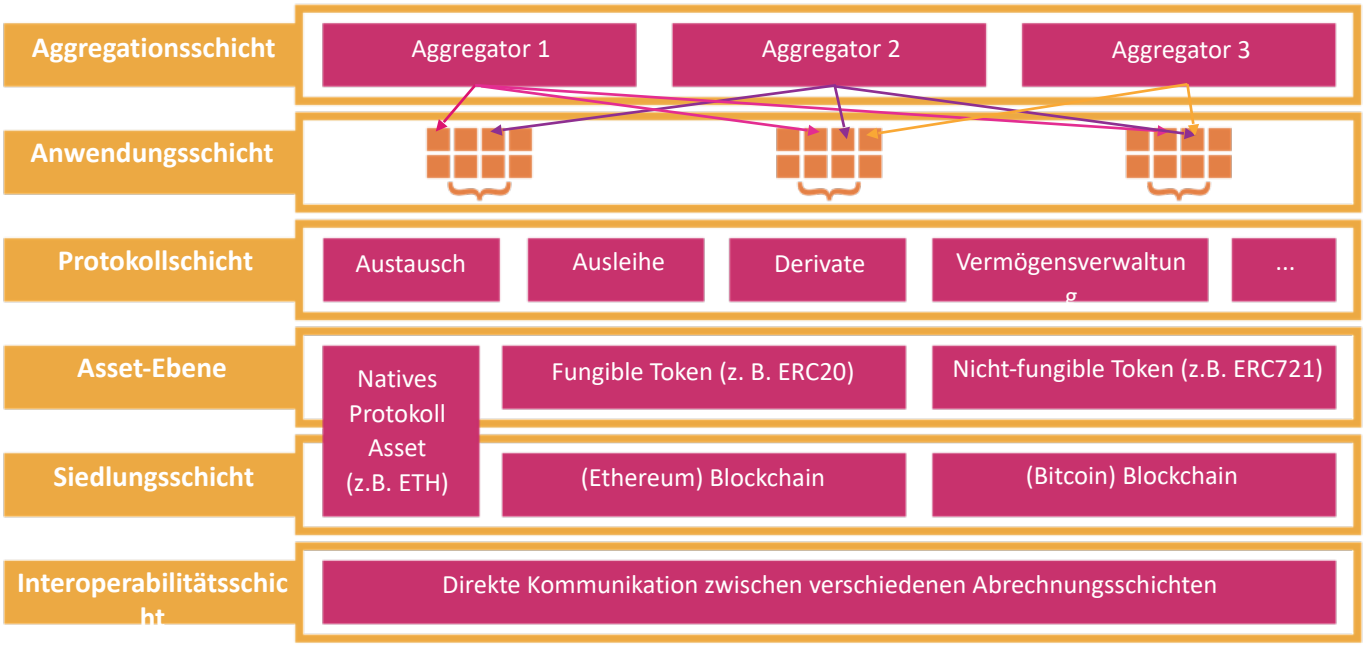
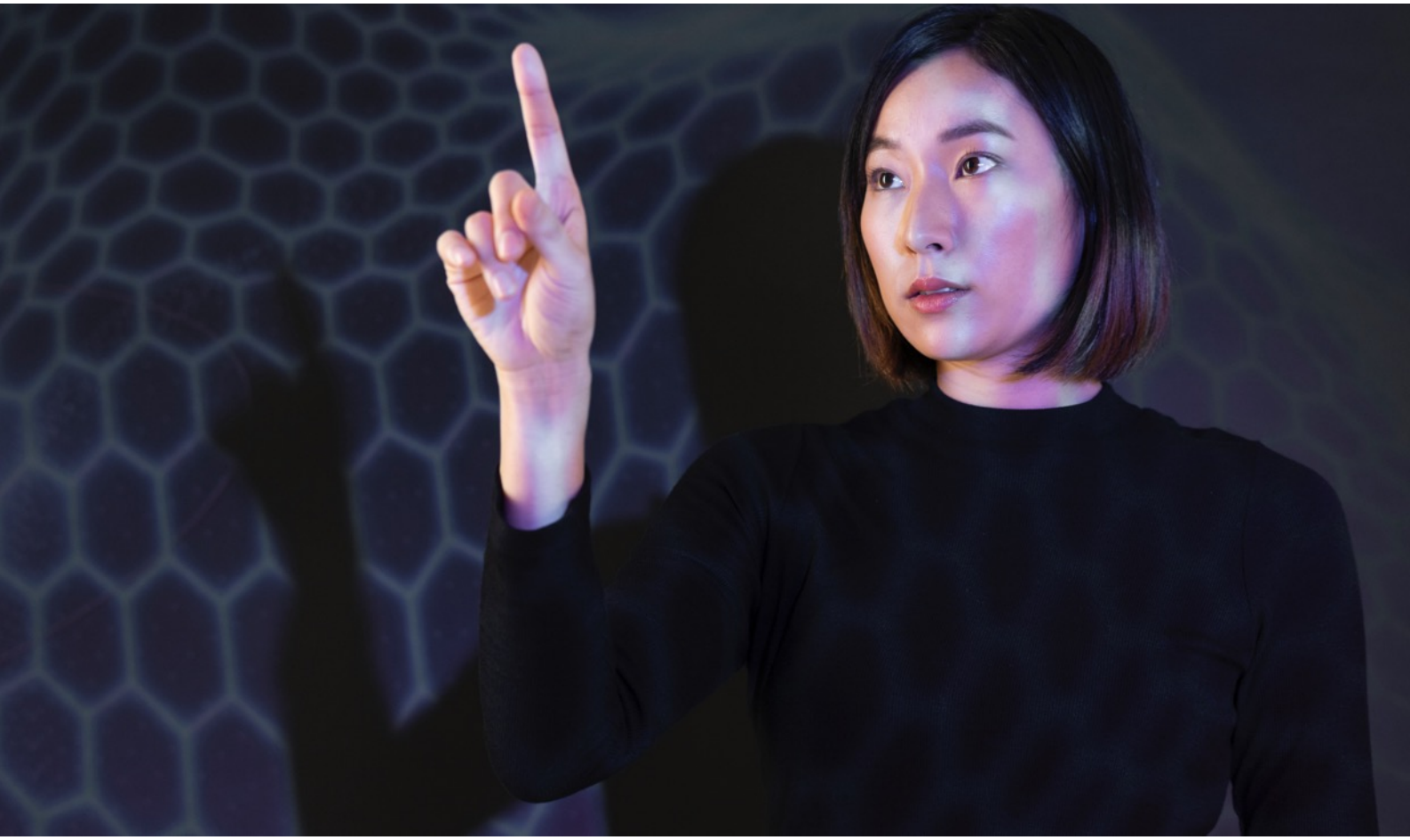


Abbildung 9: Der DeFi-Stapel (basierend auf IOSCO 2022 und Schär 2021)

Protokoll-, Vermögens- und Abwicklungsschicht bilden den Kern des DeFi-Technologie-Stacks. Die Protokollschicht besteht aus DeFi-Anwendungen, die eine Art von Finanzdienstleistungsfunktionalität wie Handel oder Kreditvergabe anbieten. Die Vermögensebene definiert, welche digitalen Vermögenswerte von einem DeFi-Protokoll verarbeitet werden können. Dabei ist zu beachten, dass ein bestimmtes DeFi-Protokoll seine Dienste in der Regel nur für einige wenige spezifische digitale Vermögenswerte anbietet, z. B. einen fungiblen Token oder ein Paar fungibler Token. Schließlich bildet die Abwicklungsschicht die zugrunde liegende Infrastruktur. Sowohl die DeFi-Anwendungen als auch die digitalen Vermögenswerte befinden sich auf Layer-1-Protokollen (z. B. Ethereum).

Dieses Layer-1-Protokoll ist von entscheidender Bedeutung, da es die Ausführungs- und Abwicklungsschicht für alle Transaktionen darstellt. Zusätzlich zu diesen Kernschichten können drei weitere Schichten eine Rolle spielen. Die Interoperabilitätsschicht am unteren Ende des Stapels ermöglicht es den verschiedenen Abwicklungsschichten, direkt miteinander zu kommunizieren. Sie kann genutzt werden, um DeFi-Anwendungen die Möglichkeit zu geben, verschiedene Layer-1-Protokolle in ihre Funktionalität einzubinden. An der Spitze des Stacks stellt eine Anwendungsschicht normalerweise Benutzerschnittstellen bereit. Eine Aggregationsschicht schließlich ermöglicht es, die Funktionalität mehrerer DeFi-Anwendungen zusammenzufassen.

DeFi-Lösungen gibt es für die wichtigsten Funktionen wie Handel, Kreditvergabe, Geldanlage, Einlagen und Zahlungsverkehr, und es kommen laufend weitere Dienste hinzu. Nachstehend finden Sie einen Überblick über Finanzdienstleistungen mit Beispielen von Lösungen für das traditionelle Finanzwesen (TradFi), das zentralisierte Finanzwesen (CeFi) und DeFi. Beim Vergleich von TradFi mit CeFi und DeFi ist es wichtig, zwischen Infrastrukturen und Vermögenswerten zu unterscheiden. DeFi (und CeFi)-Lösungen konzentrieren sich derzeit auf die Verarbeitung von digitalen Vermögenswerten wie Kryptowährungen, während TradFi mit traditionellen Vermögenswerten wie Anleihen oder Aktien arbeitet. Es wäre jedoch auch denkbar, dass DeFi-Lösungen digitalisierte Versionen traditioneller Vermögenswerte verarbeiten (z. B. tokenisierte Anleihen).



	Traditionelle Finanzierung (TradFi)	Zentralisierte Finanzierung (CeFi)	Dezentralisierte Finanzen
Handel	Börsen/Broker (z.B. Xetra)	Krypto-Börsen (z. B. Binance)	Dezentrale Börse (z. B. Uniswap)
Ausleihe	Gesichert und ungesichert (z. B. befristete Darlehen)	Kreditvergabeplattformen (z. B. BlockFi)	Verleihprotokolle (z. B. Aave)
Investieren	Investmentfonds (z. B. ETFs)	Krypto-Fonds (z. B. Graustufen)	Dezentrale Vermögensverwaltung (z. B. Cosmos)
Einlagen	Sparbücher (z. B. Geschäftsbanken)	Pool für Einsätze (z.B. Coinbase)	dStaking Dienstleistungen (z. B. Cosmos)
Zahlungen	Zahlungsplattformen (z. B. SEPA, T2)	Zentralisierte Stablecoins (z.B. USDC)	DeFi-Stablecoins (z.B. DAI)

Abbildung 10: Hauptkategorien von Finanzdienstleistungen im traditionellen Finanzwesen, im zentralisierten Finanzwesen und im dezentralisierten Finanzwesen.

Wie bereits erwähnt, sind DApps derzeit für Nutzer von Finanzdienstleistungen wie Handel, Kreditvergabe, Investitionen, Einlagen und Zahlungslösungen verfügbar.

Handel:
In DeFi übernehmen dezentrale Börsen (DEXs) die Funktion zentraler Börsen, indem sie intelligente Verträge verwenden. DEXs ermöglichen es den Nutzern, digitale Vermögenswerte auszutauschen, ohne auf Vermittler oder Verwahrer zurückgreifen zu müssen. Zu den wichtigsten DEX-Protokollen gehören Uniswap und Sushiswap.

Ausleihe:
DeFi-Kreditprotokolle bieten Kreditdienstleistungen an. Diese Lösungen werden in der Regel in einer von zwei Varianten angeboten. Bei poolbasierten Kreditprotokollen stellen interessierte Einzelpersonen Liquidität oder Mittel für einen Pool zur Verfügung, aus dem andere Personen Kredite aufnehmen können.

Nutzer, die ihr Vermögen in den Pool einbringen, können im Gegenzug ein zinsähnliches Einkommen erzielen. Bei der Peer-to-Peer-Kreditvergabe leihen sich Einzelpersonen direkt bei einem bestimmten Kreditgeber. In diesem Fall ermöglichen dezentrale Kreditprotokolle den Kreditnehmern die Aufnahme von Krediten mit minimalen Barrieren. Zu den wichtigsten DeFi-Kreditprotokollen gehören Aave, Maker und Compound.

Investieren

DeFi DApps können auch zur Ausführung automatisierter Handelsstrategien verwendet werden. TokenSets zum Beispiel ist eine DApp-basierte Plattform für das Portfoliomanagement. Die Nutzer geben die Randbedingungen und Investitionsziele vor, und TokenSets handelt, bilanziert und setzt Strategien um, um die Ziele der Nutzer automatisch zu erreichen. Dies ermöglicht es den Nutzern, in einen Korb von digitalen Vermögenswerten zu investieren, ohne dass sie einzelne Vermögenswerte kaufen müssen.

Einlagen (Absteckung)

Während es im DeFi-Ökosystem keine Einlagen im herkömmlichen Sinne gibt, existiert ein sehr ähnlicher Mechanismus (genannt Staking). Unter Staking versteht man das Sperren digitaler Vermögenswerte gegen eine Gebühr. Es ist also vergleichbar mit dem Einzahlen von Geld bei einer normalen Bank. Genauso wie eine Bankeinlage einen kurzfristigen Kredit darstellt, der der Bank gewährt wird, können gestockte Kryptowährungen als ein kurzfristiger Kredit an ein Protokoll angesehen werden. Für die Zeit, in der Vermögenswerte eingesetzt werden, erzielen sie ein kleines Einkommen. Allerdings können sie in dieser Zeit von ihren Besitzern nicht verkauft oder anderweitig genutzt werden. Auf diese Weise gesperrte digitale Vermögenswerte werden in der Regel für angrenzende Prozesse verwendet (z. B. für die Unterstützung des Transaktionsvalidierungsmechanismus des zugrunde liegenden Blockchain-Netzwerks).

Zahlungen und Stablecoins

Die hohe Volatilität von Kryptowährungen wie Bitcoin und Ether erschwert ihre Verwendung für Zahlungszwecke. An dieser Stelle kommen Stablecoins ins Spiel. Stablecoins sind digitale Vermögenswerte, die an (einen Korb von) Fiat-Währungen oder einen anderen stabilen Vermögenswert gekoppelt sind. Sie sollen ein Zahlungsmittel mit einer ähnlichen Volatilität wie Fiat-Währungen sein. Da Stablecoins digitale Vermögenswerte sind, können sie nahtlos in andere DeFi-Anwendungen integriert werden. Nutzer können mit diesen Münzen innerhalb von Sekunden On-Chain-Transaktionen durchführen, ohne die traditionellen Finanzinfrastrukturen nutzen zu müssen. Stablecoins gibt es in verschiedenen Varianten:

Asset-backed Stablecoins sind Blockchain-basierte Token, deren Wert an ein Reserve-Asset wie eine andere digitale Währung, Fiat-Geld oder einen Rohstoff gekoppelt ist. Im Gegensatz dazu versuchen algorithmische Stablecoins, ihren Wert stabil zu halten, indem sie das Angebot der Münze auf der Grundlage der Nachfrage der Nutzer verwalten. Der jüngste Zusammenbruch von Terra (Luna) hat jedoch gezeigt, dass algorithmische Stablecoins ihren Wert nur schwer halten können und als Zahlungsmittel eher ungeeignet sind.

Auch die Angemessenheit der Rücklagen von mit Vermögenswerten unterlegten Stablecoin-Projekten wurde kürzlich öffentlich in Frage gestellt. Zu den beliebtesten Stablecoins gehören USD Coin (USDC), Binance USD (BUSD) und Dai (DAI). Neben diesen vom Privatsektor betriebenen Stablecoins prüfen Zentralbanken auf der ganzen Welt die Möglichkeiten von Zentralbank-Digitalwährungen (CBDC), die die Einführung eines Stablecoins beinhalten können. Während die oben genannten Beispiele die wichtigsten Lösungen darstellen, die derzeit im DeFi-Bereich beobachtet werden, gibt es viele andere DeFi-Finanzdienstleistungen, die getestet werden (z. B. Versicherungsdienstleistungen, Derivate und Prognosemärkte).

Dezentrale Exchanges

Einer der am schnellsten wachsenden Bereiche von DeFi sind die dezentralen Börsen (DEX). Mit dem Aufkommen von Kryptowährungen und anderen digitalen Vermögenswerten nach der Finanzkrise von 2008 suchten die Nutzer nach Dienstleistungsangeboten, die ihnen den Handel mit diesen neuen Anlageklassen ermöglichen. Traditionelle Finanzdienstleister boten keine Handelsdienstleistungen für Besitzer von digitalen Vermögenswerten an. Infolgedessen entstand eine neue Klasse von Finanzvermittlern. In der Anfangsphase nahm dies in Form von zentralisierten Börsen (CEXs) Gestalt an. CEXs replizieren die Angebote von TradFi in der CeFi-Welt. Um die Dienste einer CEX in Anspruch zu nehmen, muss sich ein Nutzer bei der CEX registrieren (d.h. KYC- und AML-Prozesse) und dann vor dem Kauf oder Verkauf von digitalen Vermögenswerten sein Konto entweder mit Kryptowährungen (z.B. Bitcoin) oder einer traditionellen Zahlungsform (z.B. Banküberweisung) auffüllen. Dieser rezentralisierte Ansatz für DeFi bedeutet, dass man die Kontrolle über alle Vermögenswerte aufgibt. Im Grunde genommen kontrolliert die CEX das Konto des Nutzers.

Bei CEXs müssen die Nutzer der Börse ihr Geld anvertrauen. Dies macht sie anfällig für ein gewisses Kontrahentenrisiko. Zu Beginn war dies besonders problematisch, da es sich bei den meisten CEXs um neu gegründete Unternehmen mit unerprobten Abläufen und minimaler bis gar keiner Überwachung durch die Finanzmarktbehörden handelte. Infolgedessen waren Hacks, Betrügereien und andere illegale Aktivitäten in den ersten Jahren des CeFi-Raums keine Seltenheit, was häufig zu einem Kapitalverlust für die Nutzer dieser Dienste führte. In einem späteren Modul werden Sie mehr über die Anfangsphase von Börsen erfahren. Um dieses Problem zu lösen, entstanden die dezentralen Börsen (DEX). Das Hauptziel einer DEX ist die vollständige Disintermediation durch die Eliminierung von Zwischenhändlern und die Möglichkeit für jeden Nutzer, direkt mit anderen Nutzern auf einer Peer-to-Peer-Basis zu handeln. Indem die Handelsfunktionalität über intelligente Verträge direkt auf die Blockchain verlagert wird, dient eine DEX als vertrauenslose Plattform für den Handel mit digitalen Vermögenswerten. Ähnlich wie traditionelle Börsen und CEX koordinieren diese Plattformen Angebot und Nachfrage von vielen Nutzern. Allerdings verbleiben die Vermögenswerte entweder in der Obhut des Nutzers oder (für eine begrenzte Zeit) auf einem Treuhandkonto des vollautomatisierten Smart Contracts.

Haupttypen von DEXs

DEXs gibt es in verschiedenen Formen. Im Laufe der Jahre wurden verschiedene Entwürfe vorgeschlagen und umgesetzt, die alle darauf abzielten, frühere Projekte zu verbessern und die Funktionalität der Lösung und die Benutzerfreundlichkeit weiter zu optimieren. Es gibt die folgenden drei Haupttypen von DEX:

Automatisierte Market-Maker-basierte DEXs (AMMs)

AMMs nutzen Pools digitaler Vermögenswerte, die von sogenannten "Liquiditätsanbietern" bezogen werden, um ihren Nutzern Handelsdienstleistungen zu ermöglichen. Die Preise werden automatisch von dem zugrunde liegenden intelligenten Vertrag gestellt, daher der Name "Automated Market Maker". Der Hauptzweck der Schaffung eines AMM besteht darin, stets Liquidität zu gewährleisten.

Orderbuchbasierte DEXs

Orderbuch-DEXs stellen die Details aller offenen Kauf- und Verkaufsaufträge für ein bestimmtes Paar digitaler Vermögenswerte zusammen. Ein Kaufauftrag bedeutet, dass ein Händler ein Gebot für einen Vermögenswert zu einem bestimmten Preis abgeben möchte. Ein Verkaufsauftrag hingegen zeigt an, dass ein Händler bereit ist, einen bestimmten Vermögenswert zu einem bestimmten Preis zu verkaufen. Ähnlich wie bei traditionellen Börsen werden diese Aufträge in den Auftragsbüchern von DEXs zusammengeführt.

Hybride/alternative Plattformen

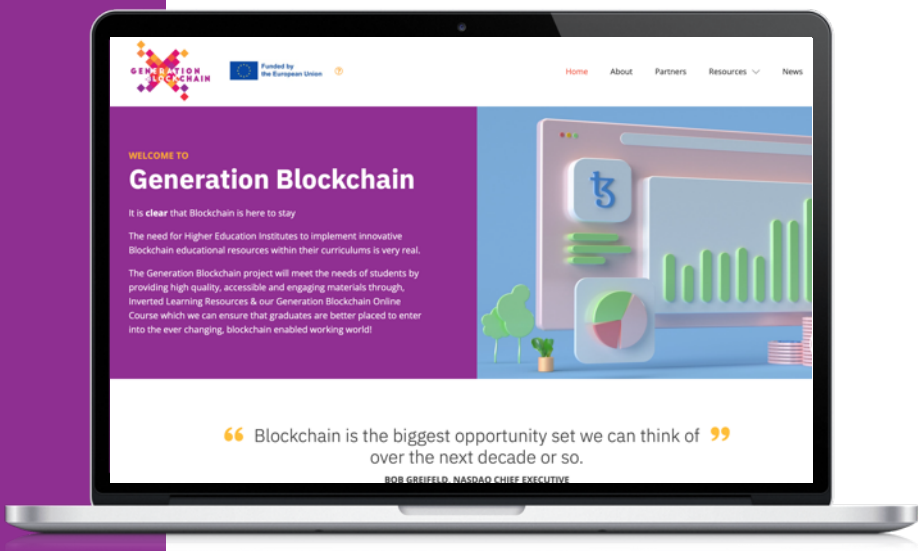
Während die meisten DEX entweder als AMM- oder als Orderbuch-basiert eingestuft werden können, beginnt eine wachsende Zahl von Plattformen, die Konzepte dieser beiden Typen zu verschmelzen, um neue, hybride DEX zu schaffen. Dies geschieht, um zusätzliche Funktionen zu ermöglichen (z. B. können Nutzer ihre Vermögenswerte nahtlos über mehrere Blockchains hinweg handeln).

Ein bemerkenswertes Phänomen ist außerdem der Aufstieg von DEX-Aggregatoren, die es den Nutzern ermöglichen, Preise und Liquidität über mehrere DEXs hinweg zu suchen. Wie der Name schon sagt, aggregieren sie die Liquidität verschiedener DEXs, um den Nutzern innerhalb kürzester Zeit den besten Ausführungskurs zu bieten und gleichzeitig die Slippage bei großen Aufträgen zu verringern und die Gebühren zu optimieren.

04

LERNKONTROLLE FÜR MODUL 3

Um Ihr Wissen zu testen, beenden Sie diese Lernkontrolle als Teil Ihrer Gesamtnote für den Kurs. Klicken Sie hier.



Folgen Sie Ihrer Lernreise

www.generationblockchain.eu

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Co-funded by the European Union

Frankfurt School Blockchain Center · momentum [educate + innovate] · European E-Learning Institute · Amsterdam University of Applied Sciences · U.PORTO