Lukas Görnert
01/2022

KRYPTO-ASSETS UND BLOCKCHAIN-ÖKOSYSTEME

TEIL 1 – FUNKTIONSWEISE UND TECHNISCHE GRUNDLAGEN

Einleitung

Wie ist es möglich, dass Investoren weltweit mehr als 1,5 Billionen US-Dollar in dezentrale Anwendungen investieren, gegen die sie keine Rechtsmittel einlegen können und die oft nicht älter als 3 Jahr alt sind? Die Antwort auf diese Frage liegt in der Blockchain-Technologie.[1] Die Technologie hat das Potenzial, bestehende Finanzmarkt-Strukturen und das Erbringen von Finanzdienstleistungen nachhaltig zu verändern. Finanzgeschäfte unterliegen seit jeher dem Problem, dass sich die beteiligten Parteien gegenseitig vertrauen müssen, um Transaktionen abzuwickeln. Im uns bisher bekannten Finanzsystem wird **fehlendes Vertrauen** zwischen den Akteuren durch den Einsatz von vertrauenswürdigen Dritten (z.B. Banken und/oder Clearing-Stellen) hergestellt. Die damit erwirkte Sicherheit bei der Abwicklung von Finanzgeschäften ist i. d. R. ineffizient, kostenintensiv und bietet trotz strenger regulatorischer Rahmenbedingungen immer wieder Spielraum für Betrug. Mit Hilfe der Blockchain-Technologie lassen sich ein Großteil dieser Probleme lösen, und Finanzdienstleistungen können **ohne den Einsatz von Intermediären** angeboten werden.

Der vorliegende Beitrag ist der erste Teil einer Beitrags-Reihe, die dabei helfen soll, ein grundsätzliches Verständnis für den Aufbau und die Funktionsweise von Blockchain-Ökosystemen und dezentralen Finanzdienstleistungen zu schaffen. Es werden Unterschiede und

[1] Vgl. Bitkom (2020): DeFi-Whitepaper, S. 5

Gemeinsamkeiten zur bestehenden Finanzmarkt-Infrastruktur und vielversprechende Projekte und Protokolle vorgestellt. Ein wesentlicher Treiber dieser Entwicklung ist vor allem die „Tokenisierung" von Vermögensgegenständen, Zahlungsmitteln und Rechten, die durch kryptografische Verschlüsselungen in einer dezentralen Datenbank digital abgebildet werden können.[2] Zudem wird auf den Entwicklungsstand von zukünftigen und bestehenden Regulierungsbestrebungen eingegangen, sowie die sich aus den daraus ergebenen Implikationen für bereits aktive Banken und Finanzdienstleister.

Die Blockchain-Technologie

Mit dem Aufkommen von virtuellen Währungen, insbesondere der Kryptowährung Bitcoin, ist auch das Interesse an der zugrundeliegenden Distributed-Ledger-Technologie (DLT) stark gestiegen. Im Jahr 2008 veröffentlichte Satoshi Nakamoto das Whitepaper für ein digitales Peer-to-Peer Cash-System, welches auf der Blockchain-Technologie basiert und bis heute die Grundlage für das bestehende Bitcoin-Netzwerk darstellt.[3] Nakamoto ist es nachhaltig gelungen, ein digitales Peer-to-Peer-Zahlungssystem zu entwickeln, welches es Nutzern ermöglicht, Vermögensgegenstände bilateral zu handeln. Das Bitcoin-Netzwerk ist das größte, bekannteste und älteste Blockchain-Netzwerk, welches mittels kryptografischer Verfahren das Double-Spending-Problem beheben konnte und damit den Weg in eine völlig neue Finanz-Architektur ebnet. Eine Blockchain ist eine **verteilte Datenbankarchitektur**, in der ein dezentrales Netz von Akteuren einen sich automatisch abgleichenden Datenbestand verwaltet. Die Transaktionen in der Datenbank stellen Zustandsübergänge dar, die in "Datenblöcken" zwischen den Netzwerkteilnehmern verbreitet werden. Die korrekte Reihenfolge der Blöcke, die den chronologischen Überblick über die Transaktionen in der Datenbank enthalten, wird mit Hilfe von kryptografischen Methoden aufrechterhalten, mit denen alle Beteiligten die Abfolge der Blöcke manuell überprüfen können.[4] Ein Konsens-Mechanismus definiert dabei, was eine legitime Transaktion in der verteilten Datenbank ist und was nicht.

Konsens-Mechanismen

Die bedeutendsten Konsens-Mechanismen sind **Proof-of-Work (PoW)** und **Proof-of-Stake (PoS)**. PoW ist ein Konsens-Mechanismus, der zuerst vom Bitcoin-Netzwerk verwendet wurde. Für das Validieren von Transaktionen werden große Mengen an Rechenleistung benötigt. Netzwerkteilnehmer, die diese Rechenleistung zur Verfügung stellen, werden mit sog. Rewards

[2] Vgl. Brühl (2021): DeFi - wie die Tokenisierung die Finanzindustrie verändert, S. 1

[3] Vgl. Nakamoto (2008): Bitcoin: A Peer-to-Peer electronic Cash System

[4] Vgl. Jensen et al. (2021): An Introduction to Decentralized Finance (DeFi), S. 2

(native Token des Netzwerks z. B. BTC) belohnt. Ziel der Validatoren ist es, die Validierung der Transaktion so schnell wie möglich durchzuführen, da nur die schnellste Validierung einen Anspruch auf den Reward hat. Sofern der Wert einer Kryptowährung steigt, steigt automatisch der Anreiz, Rechenleistung zur Verfügung zu stellen. Während beim PoW ausschließlich die Rechenleistung dafür erforderlich ist, dass Transaktionen schnell und zuverlässig abgewickelt werden, verknüpft PoS die Sicherstellung der Transaktionen mit spieltheoretischen Ansätzen. Im PoS-Verfahren müssen Validatoren eine gewisse Anzahl an Krypto-Token als Sicherheit im Netzwerk hinterlegen. Dieses „Collateral" berechtigt dazu, Rechenknoten im Netzwerk zu betreiben und Rewards zu erhalten, wenn die Transaktionen korrekt durchgeführt und abgesichert werden. Sollten Validatoren bei diesem Vorgang betrügen, fällt dies aufgrund der dezentralen Datenhaltung auf und Teile der hinterlegten Sicherheit gehen verloren bzw. werden durch das Netzwerk automatisch vernichtet. Indem wohlwollendes oder böswilliges Verhalten langfristig automatisch belohnt bzw. bestraft wird, wird die Integrität des DLT-Netzwerks dauerhaft sichergestellt.[5] Die Höhe der Rewards ist von Netzwerk zu Netzwerk unterschiedlich. In der Regel bemessen sich die Rewards beim PoS-Verfahren anhand der hinterlegten Sicherheiten. Je höher die hinterlegte Sicherheit, desto höher ist die Wahrscheinlichkeit, die Rewards gutgeschrieben zu bekommen. Dies stellt die **Integrität des gesamten Datenbestands** sicher und eignet sich gut für eine Peer-to-Peer Übertragung von (digitalen) Vermögensgegenständen, ohne dass der Einsatz eines Intermediärs notwendig ist. Hinsichtlich der technischen Ausgestaltung von DLT-Netzwerken kann auf mehrere verschiedenen Architekturen zurückgegriffen werden, deren wesentliche Unterscheidungsmerkmale u. a. in der Art der Verteilung der Rechnerknoten liegt.[6] Die Merkmale, anhand derer sich Blockchain-Netzwerke besonders gut differenzieren lassen, sind **Dezentralität, Sicherheit und Transaktionsgeschwindigkeit**.

Es handelt sich dabei um konträre Merkmale, deren gleichzeitige Erfüllung i.d.R. nicht oder nur sehr eingeschränkt möglich ist (vgl. Abb. 1).

[5] Vgl. Antonopoulous / Wood (2018): Mastering Ethereum: Building Smart Contracts and DApps

[6] Vgl. Walport (2015): DLT beyond Blockchain (2015), S. 35

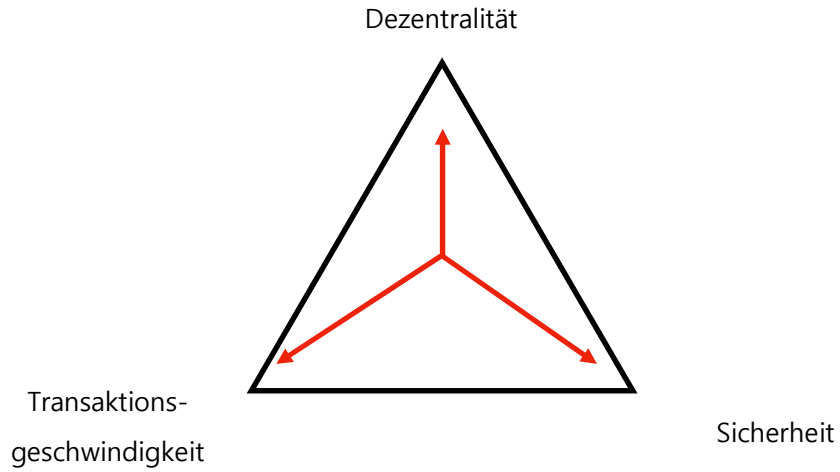

Abb. 1: Charakteristiken von DLT-Layer 1 - Systemen. vgl. Buterin (2021)

Das Bitcoin-Netzwerk gilt als sehr sicheres Netzwerk. Die abgewickelten Transaktionen sind jederzeit öffentlich einsehbar und manipulative Eingriffe sind so gut wie ausgeschlossen. Der Nachteil dabei ist jedoch, dass die Transaktionsgeschwindigkeit stark begrenzt ist, was die Skalierbarkeit der Transaktionen behindert.

Smart-Contracts

Zudem ist das Netzwerk nicht in der Lage, sog. **Smart-Contracts**, die für die Implementierung von dezentralen Anwendungen notwendig sind, zu verarbeiten. Smart-Contracts sind im Blockchain-Netzwerk installierte Programme, die Transaktionen automatisch ausführen können, wenn zuvor definierte Ereignisse eintreten. Es handelt sich dabei nicht um „Verträge" im formaljuristischen Sinne, sondern um simple „Wenn-Dann-Beziehungen", die im jeweiligen DLT-Netzwerk programmiert, implementiert und automatisch ausgeführt werden können. Die Kombination aus dem Einsatz von Smart-Contracts und der fälschungssicheren, dezentralen Datenhaltung eines Blockchain-Systems führt dazu, dass auf manuelle Eingriffe und Intermediärs-Dienstleistungen beim Finanzdienstleistungs-Prozess verzichtet werden kann. Das Erstellen dieser Smart-Contract-Codes ist vergleichsweise leicht und erfordert verglichen mit der Software-Architektur von verteilten Datenbanksystemen wenige Programmierkenntnisse.[7] Blockchain-Netzwerken, die den Einsatz von Smart-Contracts ermöglichen, werden die größten Wachstumspotenziale zugeschrieben. Um die Vorteile der Blockchain-Technologie vollständig

[7] Es gibt bereits Lösungen, die vorgefertigte Skripte bereitstellen, die das Erstellen und Befüllen eines Smart-Contracts sehr einfach gestalten. (Link: https://t3n.de/magazin/entwickeln-fur-ethereum-blockchain-schritt-244427/)

nutzen zu können, ist der Aufbau und der **Betrieb von Blockchain-Ökosystemen** notwendig, die u. a. den Handel und die Transaktionen von kryptografischen Token ermöglichen.

Krypto-Token

Krypto-Token (auch Krypto-Assets) sind **digitale Wertgegenstände**, die mittels kryptografischer Verfahren verschlüsselt werden und in einem dezentralen Datenbank-Netzwerk fälschungssicher gespeichert, gehandelt und transferiert werden können.[8] Diese digitalen Wertgegenstände können es dem Eigentümer / Besitzer z. B. ermöglichen, die Abwicklung von (digitalen) Zahlungsvorgängen vorzunehmen oder sich an Investitionen in Unternehmen oder Projekten zu beteiligen.[9] An dieser Stelle empfiehlt es sich, die unterschiedlichen Token-Kategorien aufzuzeigen, die sich in den vergangenen Jahren etabliert haben. In die erste Kategorie fallen sog. **Payment-Token**. Sie sind virtuelle „Zahlungsmittel" in den jeweiligen DLT-Netzwerken, die aufgrund ihrer Ausgestaltung jedoch keine akzeptierten Währungen im klassischen Sinne darstellen. Sie dienen ausschließlich dazu, Zahlungen in den jeweiligen digitalen Ökosystemen vorzunehmen. Bekannte Payment-Token sind der BTC (Bitcoin-Netzwerk), ETH (Ethereum-Netzwerk), ADA (Cardano-Netzwerk), SOL (Solana-Netzwerk) und DOT (Polkadot-Netzwerk). Ergänzt wird die Gruppe der Payment-Token durch die sog. **Stablecoins**, die von einer oder mehreren Währungen (z.B. USD, EUR, GBP etc.), Edelmetallen oder Bonds gedeckt sind. Die bekanntesten Stablecoins sind Tether (USDT), USD Coin (USDC) oder BUSD (Binance USD). Stablecoins dienen vor allem dazu, eine gewisse Preisstabilität auf dem Krypto-Markt herzustellen und erfüllen i. d. R. wichtige Eigenschaften, wie Rechnungseinheit, Tauschmittel und Wertaufbewahrung.[10] In der zweiten Kategorie sind die sog. **Utility-Token** zu nennen. Utility-Token räumen dem Nutzer das Recht ein, unterschiedlichste Dienstleistungen oder Produkte des Coin-Herausgebers in Anspruch zu nehmen.[11] Häufig werden Utility-Token formaljuristisch nicht als Finanzinstrumente, Wertpapiere oder Vermögensgegenstände eingestuft, was dazu führt, dass sie nicht oder nur eingeschränkt der Finanzaufsicht unterliegen. Die dritte Kategorie sind sog. **Investment-Token (auch Security-Token)**, die aufgrund ihrer Beschaffenheit am ehesten einen wertpapierähnlichen Charakter haben. Sie haben, ähnliche wie Aktien und Schuldtitel, mitgliedschaftliche Rechte oder schuldrechtliche Ansprüche auf Vermögensgegenstände

[8] Vgl. Kim, Sarin und Verdi (2018): Crypto-Assets Unencrypted

[9] Vgl. Brühl (2021): DeFi, S. 2

[10] Vgl. https://blockchainwelt.de/stablecoins-sind-preisstabile-kryptowaehrungen-moeglich/

[11] Vgl. EU-Kommission (2020): MiCa, Artikel 3 (1) - (5)

und/oder Zahlungen.[12] Anleihen, die auf der Blockchain ausgegeben werden, können in eine beliebige Anzahl an Token unterteilt werden. Somit kann beispielsweise eine Anleihe über eine Gesamtsumme von 1 Mio. EUR auf 10.000 Security-Token verteilt werden. Jeder Token repräsentiert demzufolge einen Nennwert von 100 EUR, welcher auf der jeweiligen Blockchain gespeichert wird. Security-Token können nach deutschem Recht als **Finanzinstrument** deklariert werden.

Tokenisierung

Darüber hinaus ist es technisch möglich, die sog „**Tokenisierung" von Vermögenswerten** vorzunehmen. Dazu kann nahezu jeder beliebige Vermögenswert digital mittels Token auf öffentlichen Blockchains abgebildet werden. Dies hat den Vorteil, dass Assets wie z. B. Immobilien, Kunst oder Oldtimer in digitale Einzelteile unterteilt und handelbar werden.[13] Die allgemeine Idee der Tokenisierung besteht darin, den Zugang zu Vermögenswerten zu erleichtern und Transaktionen effizienter zu gestalten.[14] Der bisher gängigste Standard zur Tokenisierung von Vermögensgegenständen ist der ERC-20-Token-Standard. Der überwiegende Teil der gelisteten Token wird aktuell auf der Ethereum-Blockchain begeben.[15] Wie sich die jeweiligen Aufsichtsbehörden in diesem auch juristisch neuen Themenbereich positionieren, ist aus heutiger Sicht noch nicht abschließend erkennbar. Der Umstand, dass es weltweit inzwischen mehrere Tausend verschiedene Krypton-Token gibt, denen vielfach unterschiedliche Anwendungsbereiche und Konzepte zu Grunde liegen, hat den Wunsch nach Standardisierung, Transparenz und Übersicht hervorgebracht. Die **International Token Standardization Association (ITSA)** hat sich daher zum Ziel gesetzt, diese Transparenz mit Hilfe eines universellen Klassifizierungsmodells zu konstruieren. Ferner soll, vergleichbar mit einer WKN oder ISIN, jeder Token mittels Identifizierungsnummer eindeutig bestimmbar sein und in einer Token-Datenbank gelistet werden.[16] Damit könnte eine verlässliche Datenbasis geschaffen werden, die sich zukünftig z. B. in ISO-Normen, Gesetzgebungsverfahren oder anderen rechtlichen Rahmenbedingungen wiederfinden. Das bis heute wichtigste und größte Smart-Contract-fähige DLT-Netzwerk ist das **Ethereum-Netzwerk (ETH)**, welches aufgrund seiner Open-Source-Architektur und seiner inzwischen mehr als 200.000 Entwickler in den

[12] Vgl. BaFin (2018): Perspektiven Digitalisierung

[13] weitere Informationen siehe: Sandner et al. (2021): Studie zur Tokenisierung von Immobilien (Tokenisierung von Immobilien)

[14] Vgl. Schaer (2021): DeFi , S. 6

[15] Vgl. Schaer (2021): DeFi, S. 6

[16] Vgl. ITSA (2021): ITSA FAQ

vergangenen Jahren starkes Wachstum erfahren hat. Das Ethereum-Netzwerk ist ein sog. **Layer-1-Netzwerk**, welches die technische Basis des Blockchain-Ökosystems ist. Neben Ethereum bieten auch andere DLT-Netzwerke, wie z.B. **Cardano, Solana, Polkadot und Avalanche** die Möglichkeit, Smart-Contracts zu implementieren. Inwieweit sich die einzelnen Blockchain-Netzwerke unterscheiden, wird in der nachfolgenden Tabelle skizziert.

Layer 1 – Blockchain-Systeme

	ethereum	CARDANO	SOLANA	Polkadot.	AVALANCHE
Token	ETH	ADA	SOL	DOT	AVA
Konsens-Mechanismus	Proof-of-Stake	Proof-of-Stake	Proof-of-Stake	Proof-of-Stake	Proof-of-Stake
Anzahl der Validatoren	ca. 300.000	ca. 2.100	ca. 1.100	ca. 300	ca. 1.100
Umlaufversorgung (max)	Kein Limit aber (Burnrate)	45 Mrd. Token	Kein Limit	Kein Limit	720 Mio. Token
Transaktionen pro Sekunde	15	250	50.000	1.000 – 3000	4.500
Transaktionsgebühr	10 – 50 $	ca. 0,40 $	0,00025 $	15 $	0,005 – 0,05 $
Total Value Locked (TVL)	155 Mrd. $	-	ca. 12 Mrd. $	-	ca. 7 Mrd. $
Ökosystem	5000+ Projekte	200+ Projekte	350+ Projekte	500+ Projekte	300+ Projekte
Marktkapitalisierung (Stand: 22.12.2021)	ca. 477 Mrd. $	ca. 43 Mrd. $	ca. 55 Mrd. $	ca. 24 Mrd. $	ca. 29 Mrd. $

Übersicht Layer-1-Blockchains
Alle Angaben haben den Stand: Dezember 2021

Der Wert und Nutzen dieser DLT-Ökosysteme hängen maßgeblich auch von der Anzahl der Anwendungen und User ab. Je mehr Entwickler die Plattform nutzen, desto mehr Anwendungen werden auf ihr entwickelt. Je mehr Anwendungen auf einer Plattform verfügbar sind, desto mehr Nutzer werden generiert, was diese Plattform i. d. R. wertvoller macht. Diese Netzwerk-Effekte konnte man bereits in der Vergangenheit bei den Betreibern von Social-Media-Plattformen oder Betriebssystem-Betreibern erkennen. Der Einsatz der oben beschriebenen Technologie kann dazu beitragen, dass sich die etablierten Prozesse in der Finanzdienstleistung-Industrie nachhaltig verändern und die Transaktionskosten zwischen den beteiligten Parteien

massiv sinken.[17] Im **zweiten Teil** unserer Fachbeitrags-Reihe werden wir Ihnen das Thema **„Blockchain-Ökosysteme"** näherbringen. Dabei gehen wir vor allem auf die unterschiedlichen Akteure von dezentralen Ökosystemen und deren Architektur ein. Sollten Sie Fragen und Anregungen zu den beschriebenen Themen haben, scheuen Sie sich nicht uns zu kontaktieren. Wir unterstützen Sie gerne!

Glossar

Begriff	Erklärung
Burnrate	In manchen DLT-Netzwerken ist die Anzahl an verfügbaren Coins nicht begrenzt. Um der inflationären Entwicklung der Coins entgegenzuwirken, wird bei Transaktionen ein Teil der Coins an eine Wallet gesendet, auf die niemand Zugriff hat. Dieses Verfahren führt dazu, dass das Angebot der im Umlauf befindlichen Coins reduziert wird. Dadurch wird eine deflationäre Entwicklung erzeugt und die Preisstabilität des Coins kann sichergestellt werden.
Konsens-Mechanismus	Mechanismen, mit denen in Blockchain-Netzwerken ein Konsens darüber hergestellt wird, wie neue Blöcke entstehen und an die bisherigen Blöcke angefügt werden können.
Rewards	Dem DLT-Netzwerk bzw. den Protokollen wird Liquidität in Form von Krypto-Token zur Verfügung gestellt. Diese Dienstleistung erhöht die Stabilität des Netzwerkes und wird durch Rewards belohnt. Die aktuellen Renditen in den jeweiligen Netzwerken können bis zu 10 % p. a. erreichen.
Tokenisierung	Hinzufügen neuer Vermögensgegenstände und Assets zu einer Blockchain bzw. zu einem Blockchain-Ökosystem. Der Token dient als Repräsentant des Assets im Blockchain-Ökosystem.
Total Value Locked (TVL)	Stellt die Summe aller Vermögenswerte dar, die in dezentralen Finanzprotokollen (DeFi) hinterlegt sind. Gemeint sind damit Beträge, die in unterschiedlichen DeFi-Applikationen für einen längeren Zeitraum „weggesperrt" werden und Belohnungen in Form von Zinsen (neue Coins) einbringen.
Validatoren	Validatoren hinterlegen Krypto-Token als Sicherheit im DLT-Netz und sorgen für die technische Abwicklung und die sichere Transaktion von Token. Validatoren werden für böswillige Tätigkeiten bestraft und für die erfolgreiche Abwicklung der Transaktionen mit Rewards belohnt.

[17] Vgl. BaFin (2018): Perspektive FinTech

Umlaufversorgung (max.)	Die maximale Anzahl von Coins / Token, die während der Lebensdauer der Kryptowährung jemals existieren werden. Oft wird dies einem Inflationsschutz gleichgesetzt, da die Menge der Coins / Token nicht beliebig erweitert werden kann. Die maximale Umlaufversorgung der jeweiligen Netzwerke ist i.d.R. auf coinmarketcap.com angegeben.

Literatur

Antonopoulous / Wood, Mastering Ethereum (2018): Building Smart Contracts and DApps.

BaFin (2018): Perspektiven Digitalisierung; https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel.html?nn=11056122.

Bitkom (2020): Decentralized Finance (DeFi) - a new Fintech Revolution.

Brühl, Volker (2021): Decentralised Finance - wie die Tokenisierung die Finanzindustrie verändert, in: ZBW - Leibniz-Informationszentrum Wirtschaft.

EU-Kommission (2020): Markets in Crypto-Assets Regulation (MiCa), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 (aufgerufen am 17.11.2021).

Jensen, J. R., V. von Wachter und O. Ross (2021): An Introduction to Decentralized Finance (DeFi).

Kim, S., A. Sarin und D. Virdi (2018): Crypto-Assets Unencrypted, Journal of Investment Management, 16(2).

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer electronic Cash System.

Schaer, Fabian (2021): Decentralized Finance: On Blockchain and Smart Contract-based Financial Markets, in: Federal Reserve Bank of St. Louis, Second Quarter 2021.

Walport, Mark (2015): Distributed Ledger Technology, beyond block chain, A report by the UK Government Chief Scientific Adviser.