# Decentralized Finance und die Zukunft des Finanzwesens

Eine Untersuchung möglicher Auswirkungen auf den traditionellen Finanzsektor

Whitepaper


Total Value Locked in DeFi-Protokollen, 2018–2026 · Daten: DeFiLlama, Stand: 02.08.2026

Martin Janda

martin@janda.io

Überarbeitete Fassung der Diplomarbeit, AKAD University · **Stand: August 2026**

**Über dieses Dokument.** Dieses Whitepaper basiert auf der vom Autor an der AKAD University eingereichten und angenommenen Diplomarbeit „Decentralized Finance und die Zukunft des Finanzwesens“ (Mai 2023). Für die Veröffentlichung wurden Marktdaten und regulatorischer Stand auf August 2026 aktualisiert und einzelne Kapitel überarbeitet. Prüfungsbezogene Bestandteile der eingereichten Fassung sind nicht Teil dieser Veröffentlichung.

**Danksagung.** Mein besonderer Dank gilt Prof. Dr. Philipp Sandner (†), Gründer und Leiter des Frankfurt School Blockchain Center. Als externer Experte im Netzwerk des FSBC habe ich in verschiedenen Projekten im Kryptoumfeld mit ihm zusammengearbeitet; der fachliche Austausch mit ihm hat mich zum Thema dieser Arbeit inspiriert. Sein früher Tod im Januar 2024 ist ein großer Verlust für die deutsche Blockchain-Community.

**Hinweis.** Dieses Dokument dient ausschließlich Informationszwecken und stellt keine Anlage-, Rechts- oder Steuerberatung dar.

**Lizenz.** Dieses Werk ist lizenziert unter einer Creative-Commons-Lizenz „Namensnennung 4.0 International“ (CC BY 4.0), `https://creativecommons.org/licenses/by/4.0/deed.de`.

**Kontakt.** Martin Janda, martin@janda.io

# Vorwort zur überarbeiteten Fassung

Diese Arbeit entstand 2023 als Diplomarbeit an der AKAD University. Kaum ein Gegenstand verändert sich so schnell wie der hier untersuchte: Die Regulierung, die damals erst Konturen annahm, ist mit MiCA und dem GENIUS Act Realität geworden; die untersuchten Protokolle haben Generationswechsel, Rebrandings und Konsolidierung durchlaufen; und mit Spot-ETFs und tokenisierten Fonds hat die institutionelle Adoption eine neue Stufe erreicht.

Für diese Veröffentlichung habe ich die Arbeit deshalb umfassend optimiert und auf den Stand von August 2026 gebracht: Alle Marktdaten beruhen auf einem einheitlichen, reproduzierbaren Datenstand mit ausgewiesenen Stichtagen, Methodik und Analyse wurden geschärft — unter anderem um ein durchgängiges Analyseraster und eine systematische Risikobetrachtung —, und die Entwicklungen der Jahre 2023 bis 2026 sind in neuen, gekennzeichneten Abschnitten ergänzt, einschließlich eines Prüfstands der damaligen Einschätzungen am tatsächlichen Verlauf.

Die Arbeit bleibt, was sie war: der Versuch, eine schnelllebige Technologie mit wissenschaftlicher Sorgfalt einzuordnen. Wenn diese Fassung dazu beiträgt, die Debatte um dezentrale Finanzsysteme faktenbasierter zu führen, hat sie ihren Zweck erfüllt.

Im August 2026
Martin Janda

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| AMM | Automated Market Maker |
| API | Application Programming Interface (Programmierschnittstelle) |
| APY | Annual Percentage Yield (jährliche prozentuale Rendite) |
| BaFin | Bundesanstalt für Finanzdienstleistungsaufsicht |
| BGP | Byzantinisches Generalsproblem |
| BIS | Bank for International Settlements (Bank für Internationalen Zahlungsausgleich) |
| BMF | Bundesministerium der Finanzen |
| CASP | Crypto-Asset Service Provider (Krypto-Dienstleister nach MiCA) |
| CBOT | Chicago Board of Trade |
| CDM | Collateralized Debt Market |
| CDP | Collateralized Debt Position |
| CeFi | Centralized Finance |
| CEX | Centralized Exchange (zentralisierte Kryptobörse) |
| CFMM | Constant Function Market Maker |
| CFTC | Commodity Futures Trading Commission (US-Derivateaufsicht) |
| dApp | Decentralized Application (dezentrale Anwendung) |
| DeFi | Decentralized Finance |
| DEX | Decentralized Exchange (dezentrale Kryptobörse) |
| EBA | European Banking Authority (Europäische Bankenaufsichtsbehörde) |
| EH/s | Exahashes pro Sekunde ($10^{18}$ Hashes/s) |
| ERC | Ethereum Request for Comments (Token-Standard-Verfahren) |
| ESMA | European Securities and Markets Authority (Europäische Wertpapieraufsicht) |
| ETF | Exchange Traded Fund (börsengehandelter Fonds) |
| ETH | Ether (native Kryptowährung der Ethereum-Blockchain) |
| FF | Forschungsfrage |
| FSB | Financial Stability Board (Finanzstabilitätsrat) |
| KMAG | Kryptomärkteaufsichtsgesetz |
| KWG | Kreditwesengesetz |

| | |
|---|---|
| KYC | Know Your Customer (Identitätsprüfung) |
| LP | Liquidity Provider (Liquiditätsanbieter) bzw. Liquiditätspool |
| MiCA | Markets in Crypto-Assets (Verordnung (EU) 2023/1114) |
| NPP | Neue-Produkte-Prozess |
| P2P | Peer-to-Peer |
| PoS | Proof of Stake |
| PoW | Proof of Work |
| PSD2 | Payment Services Directive 2 (Zweite EU-Zahlungsdiensterichtlinie) |
| RWA | Real World Assets (tokenisierte reale Vermögenswerte) |
| SEC | U.S. Securities and Exchange Commission (US-Wertpapieraufsicht) |
| SPV | Simplified Payment Verification |
| TradFi | Traditional Finance (traditionelles Finanzwesen) |
| TVL | Total Value Locked |
| wBTC | Wrapped Bitcoin |

# 1. Einführung

In den letzten Jahren hat sich eine neue Art des Finanzwesens etabliert, die auf dezentralen Technologien wie der Blockchain und Smart Contracts basiert und unter dem Namen Decentralized Finance (DeFi) bekannt ist. DeFi-Protokolle ermöglichen es den Nutzern, auf Finanzdienstleistungen wie Kredite, Handel und Versicherungen zuzugreifen, ohne auf traditionelle Finanzinstitutionen wie Banken angewiesen zu sein. Als Vorteile werden vor allem geringere Transaktionskosten, der Wegfall von Antrags- und Prüfprozessen sowie die Verfügbarkeit ohne bestehende Kontobeziehung genannt [vgl. 100]. Die Verfügungsgewalt über die eingesetzten Vermögenswerte verbleibt — bei eigener Schlüsselverwahrung — beim Nutzer; bei Einlagen in Protokoll-Pools tritt an die Stelle des Intermediärs allerdings das Smart-Contract- und Governance-Risiko (Abschnitt 4.5.1). Mittlerweile hat DeFi ein beträchtliches Marktvolumen erreicht und wird als mögliche Ergänzung des traditionellen Finanzwesens diskutiert (Abschnitt 5.2.2).

Während das traditionelle Finanzwesen auf einer zentralisierten Struktur basiert, in der Banken und Finanzinstitutionen als Vermittler und Garanten fungieren, setzt DeFi auf eine dezentrale Struktur, in der Intermediäre durch Algorithmen und Smart Contracts ersetzt werden (Abbildung 1.1). In der Krypto-Literatur wird das zentralisierte Gegenstück häufig als Centralized Finance (CeFi) bezeichnet [vgl. 100]; im engeren Sinn meint CeFi zentralisierte Krypto-Dienstleister wie Handelsplattformen, im weiteren Sinn — und so wird der Begriff in dieser Arbeit verwendet — das intermediärbasierte, zentral organisierte Finanzwesen insgesamt.

DeFi verspricht, Finanzdienstleistungen schneller, günstiger und transparenter verfügbar zu machen, ohne dass Nutzer auf Dritte angewiesen sind. Allerdings betonen kritische Stimmen die Risiken und Herausforderungen: Bedenken bestehen hinsichtlich der Sicherheit von DeFi-Protokollen, der Skalierbarkeit von DeFi-Systemen und der Regulierung von DeFi [vgl. 100]. Zudem wird argumentiert, dass DeFi noch nicht ausgereift genug sei, um als Ersatz für das traditionelle Finanzwesen zu dienen.

## 1.1. Hintergrund und Motivation

Die Entstehung von DeFi ist eng mit der Entwicklung der Blockchain-Technologie verbunden, die erstmals 2008 durch die Veröffentlichung des Bitcoin-Whitepapers von Satoshi Nakamoto bekannt gemacht wurde [vgl. 81]. Die Blockchain-Technologie ermöglichte erst-

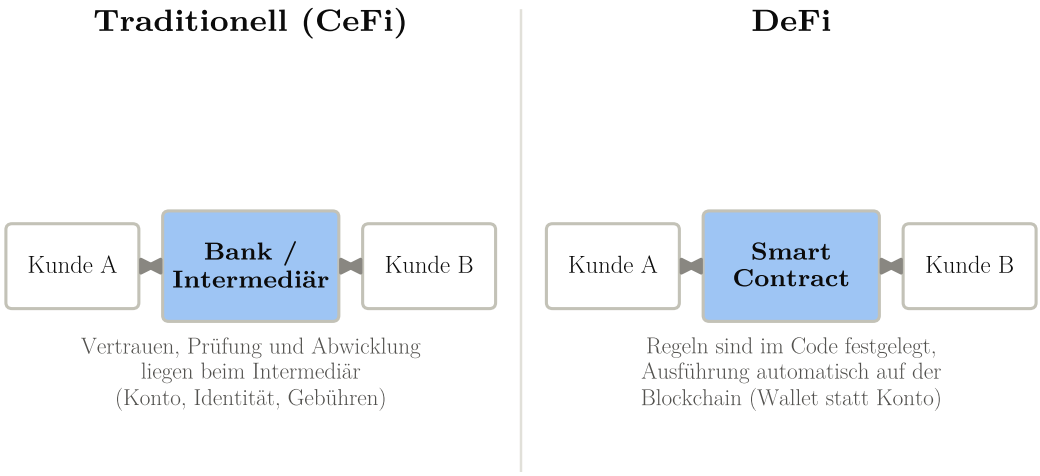



Abbildung 1.1.: CeFi und DeFi im Vergleich: Intermediär versus Smart Contract. Eigene Darstellung [vgl. 103].

mals die Schaffung einer dezentralen digitalen Währung, die unabhängig von zentralen Behörden oder Banken funktioniert. Bitcoin fand in den Folgejahren zunehmende Verbreitung und inspirierte die Schaffung weiterer dezentraler Anwendungen, darunter DeFi. Durch den Einsatz der Blockchain-Technologie sind DeFi-Protokolle in der Lage, Finanzdienstleistungen ohne die Notwendigkeit traditioneller Finanzinstitutionen anzubieten und dadurch eine höhere Autonomie und Effizienz zu ermöglichen.

Die DeFi-Protokolle nutzen Blockchain-Technologie und Smart Contracts, um eine Vielzahl von Finanzdienstleistungen zu ermöglichen, darunter Kredite, Handel und Versicherungen. DeFi-Protokolle sind im Grundsatz erlaubnisfrei zugänglich: Voraussetzung ist eine Wallet und die Fähigkeit, Transaktionsgebühren zu tragen, nicht eine Identitätsprüfung oder Kontoeröffnung. Faktisch bestehen jedoch Zugangshürden — etwa Transaktionskosten, technisches Vorwissen und Zugangsbeschränkungen vieler Nutzeroberflächen; die Abschnitte 4.5 und 5.2.1 greifen dies auf.

DeFi wird in der Literatur ein erhebliches Potenzial zugeschrieben [vgl. 100]: DeFi-Protokolle können dazu beitragen, die Kosten und die Zeit für die Durchführung von Finanztransaktionen zu reduzieren und die Transparenz von Finanzdienstleistungen zu verbessern. Insbesondere in Ländern mit schwach ausgebautem Finanzsystem, in denen viele Menschen keinen Zugang zu traditionellen Bankdienstleistungen haben, könnte DeFi dazu beitragen, Finanzdienstleistungen für eine breitere Bevölkerungsschicht zugänglich zu machen. Ob dieses Potenzial realisiert wird, hängt allerdings wesentlich davon ab, wie die in dieser Arbeit untersuchten Risiken und Regulierungsfragen adressiert werden.

Trotz aller Herausforderungen und Risiken hat DeFi seit 2020 eine ausgeprägte Wachstums- und Konsolidierungsphase durchlaufen. Der Gesamtwert der in DeFi-Protokollen gebundenen Vermögenswerte (Total Value Locked, TVL — die gebräuchlichste Größenkennzahl

des Sektors) lag zum Jahreswechsel 2020/21 bei rund 15,3 Mrd. US-Dollar, erreichte am 9. November 2021 mit rund 177 Mrd. US-Dollar seinen bisherigen Höchststand, fiel bis Anfang 2023 auf rund 38 Mrd. US-Dollar, erreichte am 07.10.2025 mit 171,0 Mrd. US-Dollar einen zweiten Gipfel und liegt aktuell bei 74,2 Mrd. US-Dollar (Stand: 02.08.2026) [48]. Der Verlauf ist damit ausgeprägt zyklisch. Da der TVL in US-Dollar bewertet wird, bildet er neben Zu- und Abflüssen stets auch die Kursentwicklung der hinterlegten Token ab — eine Einschränkung, die bei der Interpretation dieser Kennzahl mitzudenken ist (vgl. Abschnitt 4.6).

Die Motivation für diese Arbeit besteht darin, ein besseres Verständnis für die Potenziale und Herausforderungen von DeFi zu vermitteln und eine kritische Bewertung der Zukunftsperspektive vorzunehmen.

Im nachfolgenden Abschnitt werden die Forschungsfragen vorgestellt. Ziel ist es zu untersuchen, ob DeFi das traditionelle Finanzwesen ergänzt oder substituiert und welche Vor- und Nachteile DeFi im Vergleich zum traditionellen Finanzwesen hat. Durch eine detaillierte Analyse der Vor- und Nachteile von DeFi wird eine umfassende Einschätzung der Rolle von DeFi in der aktuellen und zukünftigen Finanzlandschaft ermöglicht.

## 1.2. Zielsetzung und Forschungsfragen

DeFi hat in den letzten Jahren ein starkes Wachstum erfahren und wird von vielen als vielversprechende Ergänzung des traditionellen Finanzwesens gesehen. DeFi-Protokolle nutzen Blockchain-Technologie und Smart Contracts, um eine Vielzahl von Finanzdienstleistungen auf dezentrale und automatisierte Weise anzubieten, ohne auf traditionelle Finanzinstitutionen wie Banken angewiesen zu sein. Damit verbindet sich das Versprechen, Finanzdienstleistungen schneller, günstiger und transparenter verfügbar zu machen und insbesondere Menschen in Ländern mit schwachem Finanzsystem oder ohne Zugang zu traditionellen Bankdienstleistungen neue Möglichkeiten zu eröffnen.

Die Arbeit untersucht vier Forschungsfragen:

**FF1 — Marktentwicklung und Potenzial:** Wie haben sich Größe und Struktur des DeFi-Marktes entwickelt, und welche Auswirkungen auf die Finanzbranche lassen sich daraus ableiten? Untersucht werden die Entwicklung des TVL, die zentralen Anwendungskategorien sowie die führenden Protokolle je Kategorie.

**FF2 — Ergänzung oder Substitution:** Inwieweit eignet sich DeFi als Ergänzung oder Substitution des traditionellen Finanzwesens, und welche Synergieeffekte können durch eine Integration von DeFi-Protokollen in das traditionelle Finanzwesen entstehen? Bewertungsmaßstab sind die Dimensionen Kosten, Geschwindigkeit, Transparenz und Zugang.

**FF3 — Risiken und Regulierung:** Welche technischen, ökonomischen, Governance- und regulatorischen Risiken und Herausforderungen stehen einer breiteren Nutzung von

DeFi entgegen, und wie können diese bewältigt werden? Betrachtet werden Sicherheitslücken, Skalierbarkeit und der regulatorische Rahmen sowie die Rolle, die Regulierung und traditionelles Finanzwesen dabei spielen können.

**FF4 — Akteursperspektiven:** Wie bewerten Investoren und Entscheidungsträger des traditionellen Finanzwesens DeFi, und welche Konsequenzen ergeben sich daraus für Nutzung, Investition und Integration? Diese Perspektiven tragen maßgeblich dazu bei, ob und wie DeFi-Protokolle genutzt werden und sich in das traditionelle Finanzwesen integrieren lassen.

Die Zuordnung von Forschungsfragen und Kapiteln ist wie folgt: FF1 wird in den Abschnitten 4.1–4.4 und 4.6 sowie in Abschnitt 5.1 bearbeitet; die Abschnitte 5.2.1 bis 5.2.4 beantworten die vier Forschungsfragen in dieser Reihenfolge explizit; FF3 stützt sich zusätzlich auf Abschnitt 4.5, und FF4 mündet in die Handlungsempfehlungen in Abschnitt 5.3.

Die Ergebnisse dieser Arbeit sollen Entscheidungsträgern und Investoren dabei helfen, bessere Entscheidungen zu treffen. Insbesondere werden sie bei der Beurteilung unterstützt, ob und wie sie DeFi-Protokolle nutzen und in sie investieren sollten. Zudem sollen die Ergebnisse dazu beitragen, eine Grundlage für weitere Diskussionen und Forschungen im Bereich DeFi und traditionellem Finanzwesen zu schaffen.

## 1.3. Methodik

Die vorliegende Arbeit basiert auf einer qualitativen Forschungsmethode, bei der verschiedene Forschungsansätze kombiniert werden, um die gestellten Forschungsfragen umfassend zu beantworten: eine strukturierte Literaturanalyse, die Auswertung von Sekundärdaten (Marktdaten) sowie Fallstudien ausgewählter DeFi-Protokolle. Damit die Ergebnisse nachvollziehbar und überprüfbar sind, wird diese Methodik im Folgenden operationalisiert.

**Aufbau der Untersuchung.** Kapitel 2 erläutert die technischen Grundlagen (Blockchain, Smart Contracts) auf Basis wissenschaftlicher Literatur sowie Berichten von Experten und Institutionen. Kapitel 3 führt in DeFi ein und arbeitet je Anwendungskategorie die Merkmale heraus, die als Analyseraster dienen (siehe unten). Kapitel 4 untersucht Fallstudien konkreter Protokolle entlang dieses Rasters und analysiert die Marktentwicklung. Kapitel 5 beantwortet die Forschungsfragen und leitet Handlungsempfehlungen ab; Kapitel 6 fasst zusammen, reflektiert die Grenzen der Untersuchung und gibt einen Ausblick.

**Auswahl der Fallstudien.** Die in Kapitel 4 untersuchten Protokolle (Aave, Compound, Uniswap, PancakeSwap, Nexus Mutual, Opyn) werden anhand von drei Kriterien ausgewählt: (1) Marktbedeutung — je Anwendungskategorie (Kreditvergabe, dezentrale Exchanges, Versicherungs- und Absicherungsprodukte) werden zwei Protokolle betrachtet, die zum Untersuchungszeitpunkt der Erstfassung nach Total Value Locked zu den führenden ihrer Kategorie zählten [vgl. 43]; (2) Marktbestand — die Protokolle waren zu diesem

Zeitpunkt seit mindestens zwei Jahren produktiv im Einsatz; (3) Dokumentationslage — Whitepaper bzw. technische Primärdokumentation sind öffentlich verfügbar. Dabei ist eine Abweichung transparent zu machen: Bei den dezentralen Exchanges wies Anfang 2023 Curve den höchsten TVL aus; ausgewählt wurden dennoch Uniswap — als Referenzimplementierung des in Abschnitt 3.5.3 erläuterten Constant-Product-Market-Makers und nach Handelsvolumen führend — und PancakeSwap, das den Vergleich über zwei Blockchains (Ethereum, BNB Chain) ermöglicht; Abschnitt 4.3 greift diese Abweichung auf. Die Kategorienwahl deckt mit Kreditvergabe und dezentralem Handel zwei der zum Untersuchungszeitpunkt nach TVL größten Anwendungskategorien ab [vgl. 43]; Versicherungs- und Absicherungsprodukte werden wegen ihrer Bedeutung für das Risikomanagement (FF3) einbezogen. Stablecoins und Staking werden nicht als eigenständige Fallstudien geführt, sondern als Querschnittsthemen behandelt (Abschnitte 3.5.1, 3.5.2 und 3.5.6). Die überarbeitete Fassung überprüft in Kapitel 4 zusätzlich, ob die ausgewählten Protokolle ihre Marktstellung seit 2023 behaupten konnten.

**Analyseraster.** Für jede Anwendungskategorie und jedes Fallstudien-Protokoll werden sechs Merkmale erhoben und verglichen: (M1) die ersetzte bzw. abgebildete Intermediärfunktion, (M2) Art und Höhe der Besicherung, (M3) Kosten und Abwicklungsgeschwindigkeit, (M4) Zugangsvoraussetzungen, (M5) das Risikoprofil (technisch, ökonomisch, Governance) und (M6) die regulatorische Einordnung. Abschnitt 3.5 arbeitet diese Merkmale je Kategorie heraus, Kapitel 4 vergleicht die Fallstudien entlang des Rasters, und Kapitel 5 nutzt dasselbe Raster für den strukturierten Vergleich zwischen DeFi und traditionellem Finanzwesen.

**Quellen- und Gütekriterien.** Für Belege gilt folgende Hierarchie: (1) Primärdokumente — Whitepaper und technische Dokumentation der Protokolle sowie regulatorische Originaltexte; Whitepaper dienen dabei als Quelle für Funktionsweise und Design eines Protokolls, nicht als Beleg für dessen Markterfolg oder Sicherheit; (2) wissenschaftliche Literatur sowie Publikationen von Zentralbanken und Aufsichtsbehörden (u. a. BIS, EZB, ESMA, BaFin); (3) Fachpresse, ausschließlich ergänzend und zur Dokumentation von Ereignissen. Marktdaten werden durchgängig von Datenaggregatoren mit offengelegter Methodik (DeFiLlama, blockchain.com) bezogen und stets mit Quelle und Stichtag angegeben. Sonstige Unternehmenskommunikation und Blogbeiträge dienen nicht als alleiniger Beleg zentraler Aussagen. Für die Güte der qualitativen Analyse gelten vier Kriterien: Verfahrensdokumentation (Auswahl, Analyseraster und Datenstände sind offengelegt), Regelgeleitetheit (alle Fallstudien werden entlang desselben Rasters M1–M6 erhoben), Triangulation (zentrale Aussagen werden auf mindestens zwei unabhängige Quellentypen gestützt) sowie argumentative Absicherung der Interpretation (Gegenpositionen werden benannt und geprüft).

**Datenbasis für FF4.** Die Perspektiven von Investoren und Entscheidungsträgern werden nicht primärempirisch erhoben. Ausgewertet werden dokumentierte Sekundärquellen:

Geschäftsberichte, Positionspapiere und Produktankündigungen von Banken und Vermögensverwaltern, Umfragen Dritter mit offengelegter Methodik sowie Stellungnahmen von Aufsichtsbehörden. Aussagen zu FF4 sind daher als Auswertung öffentlich dokumentierter Positionen zu lesen, nicht als repräsentative Erhebung; diese Limitation wird im Fazit (Kapitel 6) aufgegriffen.

**Datengrundlage und Reproduzierbarkeit.** Alle datenbasierten Abbildungen dieser Arbeit sind Eigenanfertigungen und werden aus dokumentierten Abfragen öffentlicher Datenschnittstellen (DeFiLlama, blockchain.com) mit eingefrorenem Datenstand erzeugt; die Abfrageskripte und Rohdatenstände sind Teil der Veröffentlichung. Damit sind alle datenbasierten Abbildungen und die daraus im Text abgeleiteten Marktzahlen reproduzierbar.

Insgesamt soll die gewählte Methodik dazu beitragen, ein umfassendes und fundiertes Verständnis der Potenziale und Herausforderungen von DeFi zu vermitteln und die gestellten Forschungsfragen aus verschiedenen Perspektiven zu beantworten.

# 2. Blockchain-Grundlagen

## 2.1. Theoretische Grundlagen

Blockchain lässt sich in die unterliegende Datenstruktur und das zugehörige Verwaltungssystem unterscheiden. Die Blockchain ist nach Condos et al. (2016) ein elektronisches Register für digitale Datensätze, Ereignisse oder Transaktionen [vgl. 36]. In dieser Datenbank erfolgen Einträge in Blöcken, die in chronologischer Reihenfolge verknüpft sind. Die Verknüpfung erfolgt durch kryptografische Verfahren, wodurch jeder Block die Transaktionen, die seit dem Hinzufügen des letzten Blocks entstanden sind, enthält. Im Kontrast zu zentralen Datenbanken übernimmt ein dezentrales Verwaltungssystem die Verifikation des Netzwerkstatus. Blockchain-Verwaltungssysteme basieren auf Kryptografie und Peer-to-Peer-Prinzipien (P2P).

Peer-to-Peer bezeichnet eine dezentrale Kommunikationsarchitektur, bei der einzelne Knoten („Peers“) direkt miteinander kommunizieren, statt über zentrale Server. Jeder Peer nimmt dabei zugleich die Rolle eines Clients und eines Servers ein und stellt dem Netzwerk Hardware-Ressourcen wie Bandbreite, Speicherplatz oder Rechenleistung zur Verfügung — diese bereitgestellten Ressourcen sind die Leistungsgrundlage jedes dezentralen Netzwerks. Während in klassischen Netzwerken eine zentrale Instanz für die Kommunikation zwischen den Teilnehmern sorgt, erfolgt der Datenaustausch in P2P-Netzwerken direkt zwischen den Teilnehmern, ohne zentrale Koordinations- und Kommunikationsinstanz [vgl. 101]. Bekannte Anwendungen dieser Architektur sind File-Sharing-Systeme wie BitTorrent — und eben Blockchains wie Bitcoin. Der Verzicht auf zentrale Punkte macht solche Netzwerke widerstandsfähig gegen Ausfälle und Angriffe auf einzelne Stellen; er bedeutet aber auch, dass Sicherheit und Vertrauen ohne zentrale Kontrollinstanz hergestellt werden müssen — die zentrale Herausforderung, die in diesem Kapitel Schritt für Schritt entwickelt wird.

## 2.2. Kryptografische Grundlagen: Hash-Funktionen

Bevor die Funktionsweise der Blockchain erläutert wird, werden die kryptografischen Bausteine eingeführt, auf denen sie beruht — allen voran die Hash-Funktion, die in nahezu jedem der folgenden Abschnitte eine Rolle spielt.

Eine Hash-Funktion ist ein mathematischer Algorithmus, der Daten beliebiger Länge (Eingabe) auf eine Ausgabe fester Länge (Hash-Wert) abbildet. Kryptografische Hash-

Funktionen haben dabei folgende Eigenschaften [vgl. 104]:

- **Determinismus:** Für dieselbe Eingabe wird immer derselbe Hash-Wert erzeugt.
- **Effizienz:** Die Berechnung des Hash-Werts ist schnell und effizient möglich.
- **Einwegfunktion:** Es ist praktisch unmöglich, vom Hash-Wert auf die ursprünglichen Daten zu schließen — die Funktion ist nicht umkehrbar.
- **Avalanche-Effekt:** Selbst kleinste Änderungen der Eingabe führen zu einem völlig anderen Hash-Wert.
- **Kollisionsresistenz:** Es ist praktisch unmöglich, zwei unterschiedliche Eingaben zu finden, die denselben Hash-Wert ergeben.

Im Bitcoin-Netzwerk kommt die Hash-Funktion SHA-256 („Secure Hash Algorithm“, 256 Bit) aus der SHA-2-Familie zum Einsatz. Sie erzeugt aus beliebigen Eingaben einen 256-Bit-Wert, der üblicherweise als 64-stellige Hexadezimalzahl dargestellt wird [vgl. 104, 122]. Der Avalanche-Effekt lässt sich daran unmittelbar zeigen: Die Eingabe „Blockchain“ ergibt einen SHA-256-Wert, der mit `625da44e...` beginnt; ändert man nur den Anfangsbuchstaben zu „blockchain“, beginnt der Wert mit `ef7797e1...` — die beiden Ausgaben haben nichts erkennbar Gemeinsames.

Neben Hash-Funktionen nutzt Bitcoin digitale Signaturen: Jeder Teilnehmer besitzt ein Schlüsselpaar aus privatem und öffentlichem Schlüssel. Mit dem privaten Schlüssel werden Transaktionen signiert; jeder andere Teilnehmer kann die Signatur mit dem öffentlichen Schlüssel prüfen, ohne den privaten Schlüssel zu kennen. So ist sichergestellt, dass ausschließlich der Inhaber einer Bitcoin-Adresse über deren Guthaben verfügen kann [vgl. 81].

Diese beiden Bausteine — Hash-Funktionen und digitale Signaturen — genügen, um die im Folgenden beschriebene Funktionsweise der Blockchain vollständig nachzuvollziehen.

## 2.3. Funktionsweise der Blockchain

Die grundlegende Funktionsweise der Blockchain lässt sich am Beispiel der Bitcoin-Blockchain erklären. Die Bitcoin-Blockchain wurde 2008 von Satoshi Nakamoto in dem Paper „Bitcoin: A Peer-to-Peer Electronic Cash System“ [vgl. 81] eingeführt. Das Problem, das die Bitcoin-Blockchain zu lösen versuchte: Handel im Internet ist auf Finanzinstitutionen angewiesen, um Vertrauen zwischen Käufer- und Verkäuferseite einer Transaktion herzustellen. Die Finanzinstitutionen als Intermediäre erhöhen die Transaktionskosten, was kleine Transaktionen unrentabel macht. Um Vertrauen zwischen den Vertragsparteien herstellen zu können, benötigen sie zudem vermehrt persönliche Daten ihrer Kunden. Die Bitcoin-Blockchain löst dieses Problem, indem Dritte aus dem Prozess herausgelöst werden und die Vertrauensbasis durch Kryptografie hergestellt wird, wodurch die Vertragsparteien direkt miteinander handeln können [vgl. 81].

### 2.3.1. Das Double-Spend-Problem

Ein Problem, das normalerweise von zentralen Instanzen bewältigt wird und nun der Blockchain obliegt, ist das Double-Spend-Problem. Es beschreibt die Anforderung, dass digitales Geld nicht mehrfach ausgegeben werden darf. Der Verkäufer einer Ware kann bei rein digitalem Geld nicht ohne Weiteres verifizieren, ob der Käufer dieselbe Geldeinheit bereits zuvor ausgegeben hat. In zentralisierten Systemen obliegt diese Prüfung einer zentralen Instanz: Sie emittiert das Geld, führt die Konten und bürgt für die Gültigkeit jeder Zahlung. In einem dezentralen System muss dieselbe Aufgabe ohne vertrauenswürdige zentrale Instanz gelöst werden.

Bitcoin adressiert das Problem durch eine dezentrale, verteilte Architektur, in der mehrere Schlüsselelemente zusammenwirken:

1. **Dezentralisierung:** Bitcoin setzt auf ein P2P-Netzwerk (Abschnitt 2.1), in dem sämtliche Teilnehmer (Knoten) direkt miteinander interagieren. Hierdurch entfällt die Notwendigkeit einer zentralen Instanz oder eines Vermittlers.

2. **Blockchain:** Die Blockchain ist ein öffentlich einsehbares, digitales Hauptbuch, das sämtliche bestätigten Transaktionen in chronologischer Reihenfolge erfasst. Jeder vollständige Knoten im Netzwerk verfügt über eine Kopie der Blockchain, wodurch Transparenz und Nachvollziehbarkeit gewährleistet werden.

3. **Unabhängige Validierung:** Jeder Knoten prüft jede empfangene Transaktion selbstständig gegen die Konsensregeln des Netzwerks: Ist die digitale Signatur gültig (Abschnitt 2.2)? Existieren die auszugebenden Geldeinheiten, und wurden sie nicht bereits ausgegeben? Nur Transaktionen, die diese Prüfungen bestehen, werden weitergeleitet und können in Blöcke aufgenommen werden. Die Gültigkeit einer Transaktion wird also nicht durch das Mining hergestellt, sondern durch die unabhängige Prüfung aller Knoten [vgl. 4].

4. **Konsensmechanismus:** Bitcoin nutzt den Proof-of-Work-Mechanismus (im Detail in Abschnitt 2.4): Miner konkurrieren darum, neue Transaktionsblöcke an die Blockchain anzuhängen, und werden dafür mit neu erzeugten Bitcoin belohnt — seit dem Halving im April 2024 mit 3,125 Bitcoin je Block [12]. Der Konsensmechanismus legt fest, in welcher Reihenfolge Transaktionen in die gemeinsame Historie eingehen — und macht es damit mit jeder weiteren Bestätigung unwahrscheinlicher, dass dieselbe Geldeinheit ein zweites Mal ausgegeben werden kann (probabilistische Endgültigkeit, Abschnitte 2.4 und 2.5.4).

5. **Kryptografische Verkettung:** Die Blöcke sind über Hash-Werte miteinander verkettet (Abschnitt 2.5.2). Einmal bestätigte Transaktionen können dadurch nicht mehr unbemerkt verändert werden.

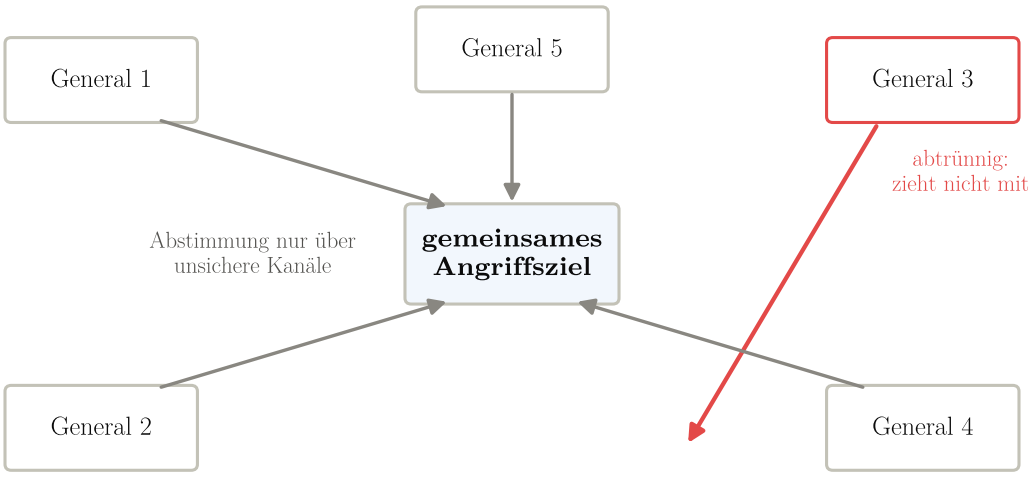



Abbildung 2.1.: Das byzantinische Generalsproblem: Konsens trotz unzuverlässiger Teilnehmer und unsicherer Kommunikationskanäle. Eigene Darstellung.

Diese Kombination aus Dezentralisierung, unabhängiger Validierung, Konsensmechanismus und kryptografischer Verkettung ermöglicht, dass das Bitcoin-Netzwerk ohne zentrale Instanz funktioniert und dabei ein hohes Maß an Sicherheit und Vertrauen bietet.

### 2.3.2. Das Konsensproblem in verteilten Systemen

Das byzantinische Generalsproblem (BGP) ist ein fundamentales Konsensproblem in verteilten Systemen, das die Schwierigkeiten bei der Koordination und Kommunikation zwischen unterschiedlichen Teilnehmern eines dezentralen Netzwerks veranschaulicht. In diesem hypothetischen Szenario müssen Generäle, die von verschiedenen Standorten aus operieren, einen gemeinsamen Angriffsplan koordinieren [vgl. 77, S. 382–384]. Die Herausforderung entsteht durch die Möglichkeit, dass einige Generäle unzuverlässig oder sogar feindlich gesinnt sein könnten, und dadurch, dass die Kommunikation zwischen den Generälen über unsichere Kanäle stattfindet. In Abbildung 2.1 ist die Absicht eines abtrünnigen Generals durch den roten Pfeil dargestellt, der nicht auf das gemeinsame Angriffsziel gerichtet ist. Die Folge wäre eine Schwächung des Angriffs und daraus resultierend ein mögliches Scheitern.

Das Hauptziel bei der Lösung des BGP besteht darin, einen Konsens unter den Teilnehmern eines verteilten Systems zu erreichen, selbst wenn einige Knoten im Netzwerk fehlerhaft oder bösartig sind. Um dieses Problem effektiv zu lösen, muss das System zwei Bedingungen erfüllen:

1. Alle ehrlichen Knoten müssen sich auf denselben Wert einigen.
2. Eine kleine Anzahl bösartiger Knoten darf das System nicht kompromittieren können.

Da Bitcoin ein dezentrales Netzwerk ist, in dem die Knoten unabhängig voneinander arbeiten und potenziell Fehlinformationen oder bösartige Angriffe auftreten können, ist das BGP hier von zentraler Bedeutung. Bitcoins Antwort darauf ist der Proof-of-Work-Mechanismus: Wer einen Block anhängen will, muss dafür nachweisbar Rechenaufwand investieren. Wie dieser Mechanismus im Einzelnen funktioniert und warum er zugleich das ökonomische Fundament des Netzwerks bildet, erläutert der folgende Abschnitt.

## 2.4. Mining, Proof of Work und das ökonomische Anreizsystem

Mining ist der Prozess, der im Bitcoin-Netzwerk neue Blöcke erzeugt, Transaktionen in die gemeinsame Historie aufnimmt und dabei zugleich neue Bitcoin in Umlauf bringt. Miner sind Teilnehmer, die Rechenleistung einsetzen, um das kryptografische Rätsel des Proof-of-Work-Mechanismus zu lösen [vgl. 82].

**Der Proof-of-Work-Mechanismus.** Das „Rätsel“ besteht darin, einen Blockheader (Abschnitt 2.5.1) so zu vervollständigen, dass sein SHA-256-Hash-Wert unter einem vom Protokoll vorgegebenen Schwellenwert liegt. Dazu variiert der Miner die sogenannte Nonce — ein Freifeld im Blockheader: Er setzt einen Wert ein, berechnet den Hash des Headers und prüft das Ergebnis (in der Praxis werden bei erschöpftem Nonce-Raum zusätzlich Felder wie der Zeitstempel und die Coinbase-Transaktion variiert). Wegen des Avalanche-Effekts (Abschnitt 2.2) führt jede Änderung der Nonce zu einem völlig anderen Hash-Wert; nach heutigem Kenntnisstand existiert kein effizienteres Verfahren als systematisches Ausprobieren. Ein gültiger Hash lässt sich daher nur durch massenhaftes Ausprobieren finden — das erfordert Rechenleistung und damit Zeit und Energie —, während jeder andere Knoten mit einer einzigen Hash-Berechnung überprüfen kann, dass die gefundene Lösung korrekt ist [vgl. 63]. Der Schwellenwert wird vom Protokoll regelmäßig angepasst, sodass die durchschnittliche Blockzeit bei etwa zehn Minuten bleibt, auch wenn sich die Gesamtrechenleistung des Netzwerks stark verändert. Hat ein Miner eine gültige Lösung gefunden, propagiert er den Block an alle Netzwerkteilnehmer; diese prüfen den Block und seine Transaktionen und beginnen, auf dem neuen Block aufbauend am nächsten zu arbeiten.

**Das Anreizsystem.** Für die erfolgreiche Lösung wird der Miner über die sogenannte Coinbase-Transaktion belohnt — einen speziellen Transaktionstyp, der neue Coins erzeugt und ohne vorherige Transaktionseingänge an eine vom Miner definierte Adresse sendet; zusätzlich sammelt sie die Transaktionsgebühren des Blocks ein. Diese Belohnung setzt den Anreiz, Rechenleistung bereitzustellen und ehrlich zu agieren. Zugleich steuert sie die Geldschöpfung des Systems: Die anfängliche Belohnung betrug 50 Bitcoin pro Block und halbiert sich alle 210.000 Blöcke — bei etwa zehn Minuten Blockzeit entspricht das rund vier

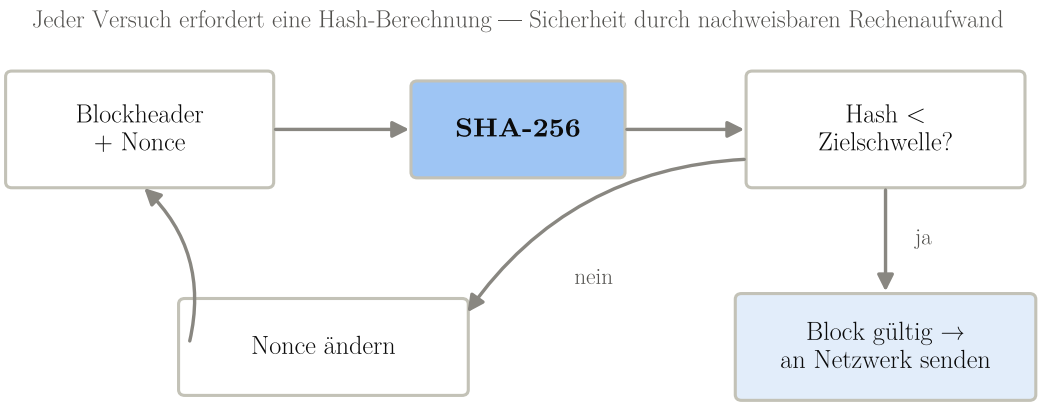
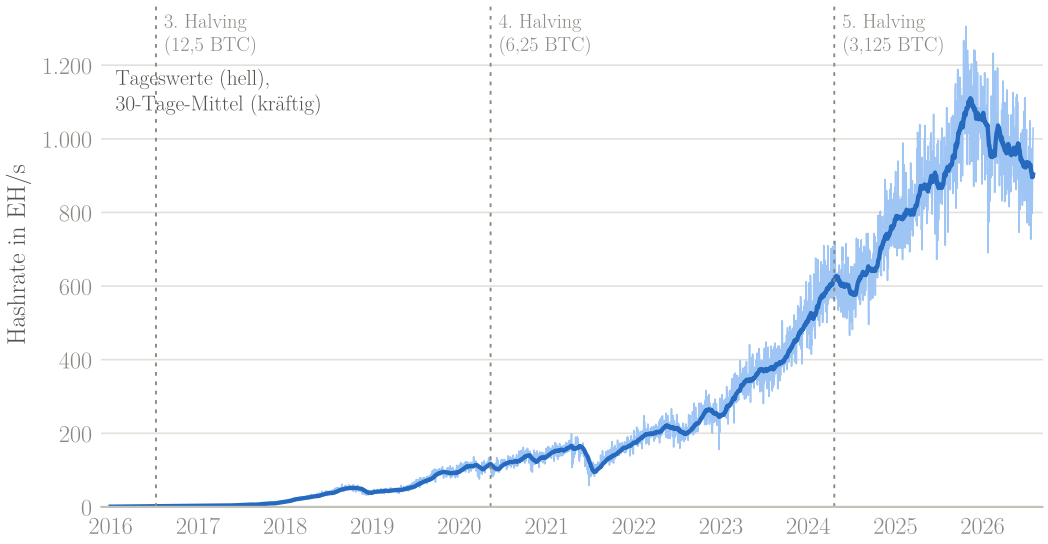



Abbildung 2.2.: Der Proof-of-Work-Zyklus: Nonce variieren, hashen, gegen die Zielschwelle prüfen. Eigene Darstellung.

Jahren. Dieses Ereignis ist als „Halving“ bekannt [vgl. 81, 4]. Zuletzt wurde die Belohnung im April 2024 (Block 840.000) auf aktuell 3,125 Bitcoin halbiert; die nächste Halbierung wird turnusgemäß für das Frühjahr 2028 erwartet [12]. Der Prozess wird fortgesetzt, bis alle 21 Millionen Bitcoin geschöpft sind. Ökonomisch war das Mining ursprünglich als Mechanismus zur breiten Verteilung neuer Einheiten angelegt; mit der Industrialisierung des Minings hat sich diese Verteilungswirkung relativiert (vgl. die Pool-Konzentration unten). Erhalten geblieben ist die zweite Funktion: eine kontrollierte, im Voraus planbare Geldmengenentwicklung.

**Hashrate und Netzwerksicherheit.** Die Gesamthashrate bezeichnet die kombinierte Rechenleistung aller Miner, gemessen in Hashes pro Sekunde (H/s) bzw. deren Vielfachen bis hin zu Exahashes pro Sekunde (1 EH/s = 10^18 H/s). Abbildung 2.3 zeigt ihre Entwicklung seit 2016: Im April 2023 lag das 30-Tage-Mittel bei rund 330 EH/s; bis August 2026 hat es sich auf rund 900 EH/s nahezu verdreifacht, Tageswerte überschritten zeitweise 1.000 EH/s (Stand: 01.08.2026) [12].

Die Hashrate ist ein Indikator für die Angriffskosten auf das Netzwerk: Ein Angreifer, der die Transaktionshistorie umschreiben oder eigene Double-Spends durchsetzen wollte, müsste dauerhaft mehr als die Hälfte der gesamten Rechenleistung kontrollieren — ein sogenannter 51-%-Angriff [vgl. 82]. Die Hardware- und Energiekosten eines solchen Angriffs steigen proportional zur Gesamthashrate: Bei einem 30-Tage-Mittel von rund 900 EH/s müsste ein Angreifer eine Rechenleistung aufbauen und dauerhaft betreiben, die die gesamte übrige Mining-Industrie übertrifft. Selbst ein erfolgreicher Angriff wäre zudem für jeden Beobachter sichtbar und würde das Vertrauen in das System — und damit den Wert der erbeuteten Coins und der Mining-Ausrüstung des Angreifers — untergraben. Da Miner erhebliche Ressourcen investieren, haben sie einen starken wirtschaftlichen Anreiz, das




Daten: blockchain.com (api.blockchain.info/charts/hash-rate), Stand: 01.08.2026 · Eigene Darstellung

Abbildung 2.3.: Entwicklung der Bitcoin-Hashrate seit 2016 (Tageswerte und 30-Tage-Mittel) mit den Halving-Zeitpunkten. Eigene Darstellung; Datenquelle: blockchain.com [12].

Netzwerk zu schützen statt es anzugreifen. Aus der hohen Hashrate folgt allerdings nur die Sicherheit gegen diese Klasse von Angriffen auf die Transaktionshistorie: Risiken wie Protokollfehler, der Diebstahl privater Schlüssel oder die Konzentration großer Teile der Hashrate in wenigen Mining-Pools bleiben davon unberührt. Die verbreitete Einschätzung, Bitcoin sei das sicherste dezentrale Transaktionssystem, ist in diesem eingeschränkten Sinn zu verstehen — als Aussage über die Kosten eines Historien-Angriffs, nicht als pauschale Sicherheitsgarantie.

**Energieverbrauch und Alternativen.** Der Arbeitsnachweis hat seinen Preis: Das Cambridge Centre for Alternative Finance schätzt den jährlichen Stromverbrauch des Bitcoin-Netzwerks auf rund 170–180 TWh (annualisierte Schätzung, Stand: Anfang 2026) — gut ein halbes Prozent der weltweiten Stromerzeugung und in der Größenordnung des Jahresverbrauchs mittelgroßer Industriestaaten [23]. Dieser Ressourceneinsatz ist kein Nebeneffekt, sondern der Kern des Sicherheitsmodells — genau deshalb ist PoW jedoch umstritten. Als energiesparsame Alternative hat sich Proof of Stake (PoS) etabliert: Statt Rechenleistung hinterlegen Validatoren dort Kapital in Form von Token („Stake“) und werden in Abhängigkeit von ihrem Einsatz zufällig ausgewählt, den nächsten Block zu erzeugen; Fehlverhalten wird durch den Verlust des Einsatzes sanktioniert [vgl. 97]. Die Erzeugung neuer Einheiten erfolgt hier nicht durch Mining, sondern wird als Minting bezeichnet und ist deutlich weniger rechen- und energieintensiv [vgl. 5]. Prominentester Vertreter ist Ethereum, das sein Konsensverfahren im September 2022 („Merge“) von PoW auf PoS umgestellt hat [vgl. 118, 53]. Der Vergleich beider Verfahren — Sicherheit durch

externe Ressourcen (Energie) versus Sicherheit durch internes Kapital — wird in Kapitel 3 und 5 wieder aufgegriffen, da die meisten DeFi-Anwendungen auf PoS-Blockchains laufen.

## 2.5. Aufbau der Bitcoin-Blockchain

Die Struktur der Bitcoin-Blockchain basiert auf kryptografisch gesicherten, chronologisch verknüpften Datenblöcken, die Transaktionen enthalten und eine unveränderliche Aufzeichnung aller jemals stattgefundenen Transaktionen im Netzwerk ermöglichen. Die folgenden Abschnitte erläutern die Schlüsselkomponenten im Detail.

### 2.5.1. Blöcke

Ein Block ist die grundlegende Einheit der Bitcoin-Blockchain und besteht aus drei Hauptelementen:

1. **Blockheader:** Der Blockheader enthält wichtige Metadaten, wie die Version des Blocks, den Zeitstempel, den aktuellen Schwierigkeitsgrad des kryptografischen Rätsels, die Nonce (Abschnitt 2.4) und den Hash des vorherigen Blocks, wodurch die Verkettung der Blöcke entsteht.

2. **Merkle-Root:** Die Merkle-Root ist der Hash-Wert, der aus den Hash-Werten aller im Block enthaltenen Transaktionen erzeugt wird (im Detail in Abschnitt 2.5.3). Dieser Wert wird im Blockheader gespeichert und ermöglicht eine effiziente Überprüfung der Transaktionen innerhalb des Blocks.

3. **Transaktionsliste:** Die Transaktionsliste enthält alle im Block enthaltenen Bitcoin-Transaktionen. Jede Transaktion besteht aus Informationen wie den Eingangs- und Ausgangsadressen, den Beträgen und den kryptografischen Signaturen der Beteiligten.

### 2.5.2. Verkettung der Blöcke

Die Bitcoin-Blockchain erhält ihre Integrität und Unveränderlichkeit durch die Verkettung der Blöcke mittels kryptografischer Hash-Funktionen: Jeder Block enthält den Hash-Wert des vorherigen Blocks in seinem Blockheader, wodurch eine chronologische Kette entsteht.

Eine nachträgliche Änderung in einem Block würde dessen Hash-Wert verändern (Avalanche-Effekt, Abschnitt 2.2) — und damit die Verweise aller nachfolgenden Blöcke ungültig machen. Ein Angreifer müsste also nicht nur den betroffenen Block, sondern auch sämtliche darauf folgenden Blöcke neu berechnen, und das schneller, als das ehrliche Netzwerk die Kette verlängert. Die Verkettung macht Manipulationen dadurch nicht unmöglich, aber mit wachsender Tiefe eines Blocks exponentiell aufwendiger — hier greifen Datenstruktur (dieser Abschnitt) und Konsensmechanismus (Abschnitt 2.4) ineinander.

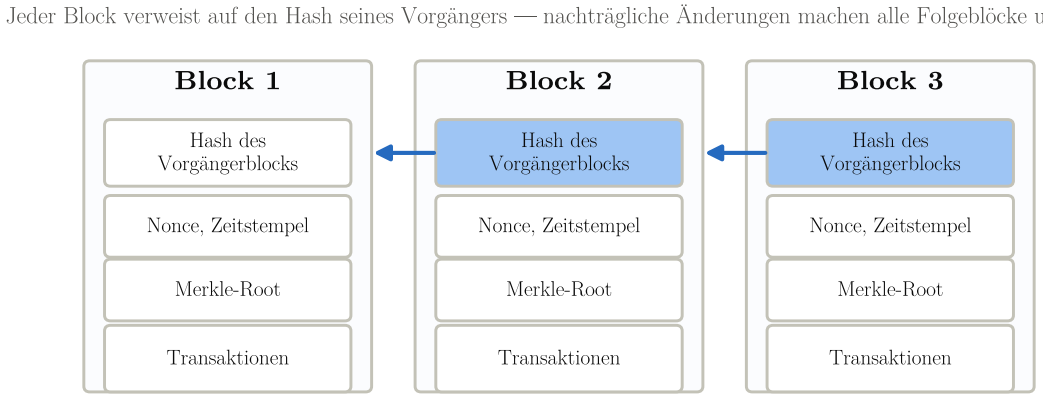



Abbildung 2.4.: Verkettung der Blöcke über den Hash des Vorgängerblocks. Eigene Darstellung.

### 2.5.3. Der Merkle-Baum

Innerhalb eines Blocks werden die Transaktionen nicht einzeln im Blockheader referenziert, sondern in einer Baumstruktur zusammengefasst, dem Merkle-Baum. Das Prinzip lässt sich an einem kleinen Beispiel vollständig durchrechnen. Angenommen, ein Block enthält vier Transaktionen:

| Transaktion | Inhalt | SHA-256-Wert (gekürzt) |
|---|---|---|
| T1 | Alice zahlt Bob 5 BTC | `cd3ee612...` |
| T2 | Bob zahlt Carol 2 BTC | `2521f323...` |
| T3 | Carol zahlt Dave 1 BTC | `bc9ff84d...` |
| T4 | Dave zahlt Alice 3 BTC | `1a772b6a...` |

Im ersten Schritt wird jede Transaktion einzeln gehasht (H1 bis H4, die „Blätter“ des Baums). Anschließend werden die Hash-Werte paarweise zusammengefügt und erneut gehasht: Aus H1 und H2 entsteht H12 (`9b63d12d...`), aus H3 und H4 entsteht H34 (`14a0103f...`). Im letzten Schritt werden H12 und H34 zusammengefügt und ein letztes Mal gehasht — das Ergebnis ist die Merkle-Root (`717b1b8f...`), ein einziger Hash-Wert, der sämtliche Transaktionen des Blocks repräsentiert und im Blockheader gespeichert wird (Abbildung 2.5). Bei mehr Transaktionen wird das Verfahren einfach über mehr Ebenen fortgesetzt; bei ungerader Anzahl wird der letzte Hash-Wert dupliziert. Bitcoin verwendet dabei statt des hier zur Vereinfachung gezeigten einfachen SHA-256 eine doppelte Anwendung der Hash-Funktion; im Beispiel werden zudem die hexadezimalen Darstellungen der Hash-Werte verkettet [vgl. 4].

Der Nutzen dieser Konstruktion liegt in drei Eigenschaften:

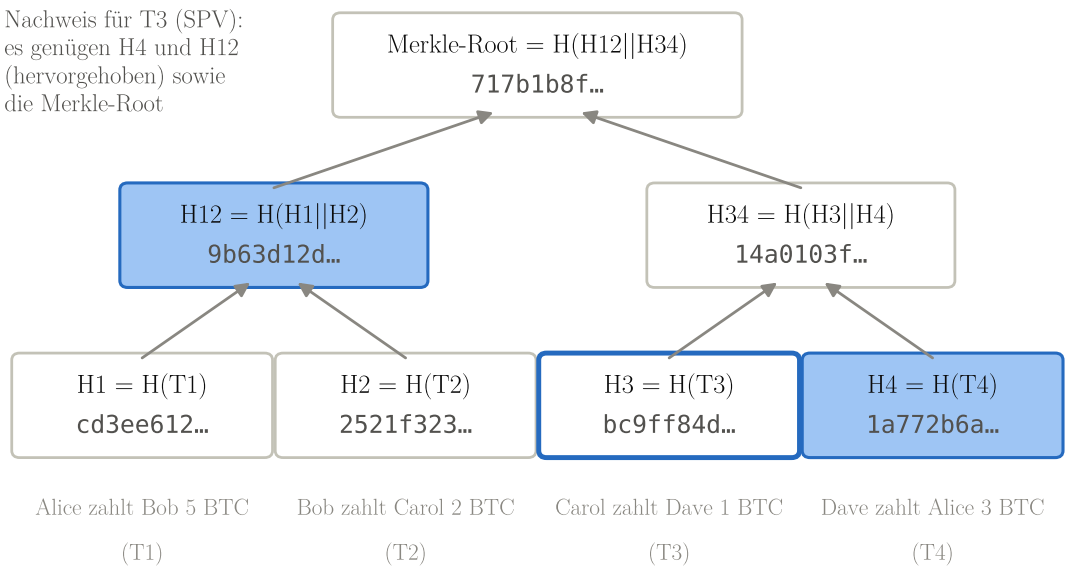



Abbildung 2.5.: Merkle-Baum mit vier Transaktionen und durchgerechneten (gekürzten) SHA-256-Werten. Hervorgehoben ist der Nachweispfad für T3: Zum Existenznachweis genügen H4 und H12 sowie die Merkle-Root. Eigene Darstellung.

- **Kompaktheit:** Eine beliebig große Zahl von Transaktionen wird in einem einzigen Hash-Wert zusammengefasst; der Blockheader bleibt dadurch konstant klein.
- **Effiziente Nachweise:** Um zu belegen, dass eine bestimmte Transaktion in einem Block enthalten ist, genügt der Pfad von der Transaktion zur Wurzel. Im Beispiel reicht für den Nachweis von T3 die Kenntnis von H4 und H12: Daraus lassen sich H34 und die Merkle-Root nachrechnen und mit dem Blockheader vergleichen — zwei Hash-Werte statt aller vier Transaktionen, und der Vorteil wächst mit der Blockgröße, da der Aufwand nur logarithmisch mit der Transaktionszahl steigt. Genau darauf beruhen Simplified-Payment-Verification-Clients (SPV): leichtgewichtige Anwendungen wie Smartphone-Wallets, die nur die Blockheader speichern und die Existenz einzelner Transaktionen überprüfen können, ohne die gesamte Blockchain zu laden [vgl. 81].
- **Manipulationssicherheit:** Ändert sich auch nur ein Zeichen einer Transaktion, ändert sich ihr Hash — und kaskadierend alle Werte bis zur Merkle-Root, die dann nicht mehr zum Blockheader passt.

Die Verlässlichkeit des gesamten Verfahrens steht und fällt dabei mit der Kollisionsresistenz der Hash-Funktion (Abschnitt 2.2): Gelänge es einem Angreifer, zwei unterschiedliche Transaktionen mit demselben Hash-Wert zu konstruieren, könnte er eine bestätigte Transaktion unbemerkt gegen eine andere austauschen, ohne dass sich die Merkle-Root ändert — sämtliche Integritätsgarantien wären hinfällig. Die Sicherheit der Blockchain reduziert sich an dieser Stelle vollständig auf die Sicherheit der verwendeten Hash-Funktion; für SHA-256

sind bis heute (Stand: August 2026) keine praktikablen Kollisionsangriffe bekannt [vgl. 104]. Dass diese Annahme nicht zeitlos gilt, zeigt die Vorgängerfunktion SHA-1, für die 2017 die erste praktische Kollision demonstriert wurde [vgl. 105].

### 2.5.4. Forks und die längste Kette

In einigen Fällen kann es vorkommen, dass zwei Miner gleichzeitig gültige Blöcke finden und an die Blockchain anhängen. Dies führt zu einer vorübergehenden Abspaltung der Kette, die als Fork bezeichnet wird. In solchen Situationen arbeiten die Miner an derjenigen Kette weiter, die die meiste Proof-of-Work-Anstrengung aufweist — die „längste Kette“. Schließlich wird einer der Zweige länger als der andere, und die Miner, die am kürzeren Zweig gearbeitet haben, wechseln zur längeren Kette. Der kürzere Zweig wird verworfen, und die darin enthaltenen Transaktionen kehren in den Mempool zurück, um in zukünftige Blöcke aufgenommen zu werden. Dieser Mechanismus stellt sicher, dass die Bitcoin-Blockchain eine konsistente und einheitliche Aufzeichnung aller Transaktionen beibehält [vgl. 81, 4].

## 2.6. Bitcoin und das Vertrauensproblem

Das grundlegende Problem, das ein dezentrales Transaktionssystem wie Bitcoin lösen muss, ist das Vertrauensproblem. In der klassischen Finanzwelt wird dieses Problem durch Intermediäre gelöst.

Bei einer Kreditkartenzahlung übermittelt der Kunde seine Kreditkartendaten (Kreditkartennummer, Gültigkeitsdatum und Kartenprüfnummer) an den Händler. Die Daten werden anschließend zur Autorisierung und Genehmigung an einen sogenannten Kreditkarten-Acquirer weitergeleitet. Acquirer sind Institutionen, die für den Händler die Autorisierung und Abrechnung von Kreditkartenzahlungen abwickeln.

Bei erfolgreicher Autorisierung wird ein Autorisierungscode ausgegeben, der bestätigt, dass das Kreditkartenkonto existiert und belastet werden kann. Der Acquirer bucht anschließend den Betrag vom Kreditkartenkonto des Kunden ab und schreibt ihn, abzüglich des vereinbarten Entgelts (Disagio), dem Händlerkonto gut. Das Disagio setzt sich aus dem — in der EU seit der Verordnung (EU) 2015/751 auf 0,3 % (Kreditkarten) bzw. 0,2 % (Debitkarten) gedeckelten — Interbankenentgelt, den Systementgelten der Kartenorganisationen und der Marge des Acquirers zusammen; es liegt im europäischen Handel typischerweise im niedrigen einstelligen Prozentbereich und variiert nach Branche, Umsatz und Kartenprodukt [vgl. 60].

In der dezentralen Ökonomie übernimmt die Blockchain die Aufgabe, Vertrauen zwischen den Parteien herzustellen, um Transaktionen ohne Intermediäre wie Banken oder Kreditkarteninstitute zu vollziehen. Eine solche Transaktion läuft wie folgt ab: Zunächst erstellt ein Benutzer mithilfe seines Wallets eine Transaktion, um Bitcoin an eine andere Bitcoin-

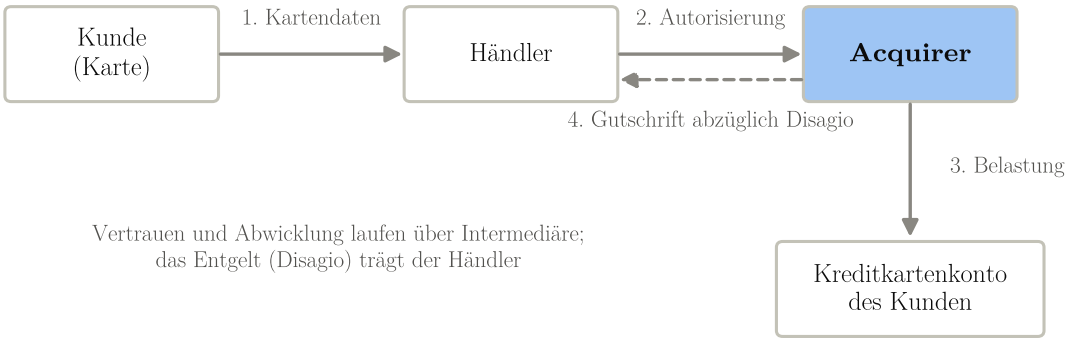



Abbildung 2.6.: Ablauf einer Kreditkartenzahlung mit Intermediären (vereinfacht). Eigene Darstellung in Anlehnung an ibi research [vgl. 74].

Adresse zu senden. Das Wallet signiert diese Transaktion mit dem privaten Schlüssel des Senders (Abschnitt 2.2). Anschließend wird die Transaktion über das Netzwerk verbreitet; die Knoten validieren sie unabhängig (Abschnitt 2.3.1). Miner nehmen die Transaktion in einen Block auf und suchen per Proof of Work nach einer gültigen Lösung (Abschnitt 2.4). Wird sie gefunden, prüfen die übrigen Knoten den Block und bauen auf ihm auf — sie drücken damit ihre Zustimmung aus. Nachdem mehrere weitere Blöcke angehängt wurden — üblich ist die Konvention von sechs Bestätigungen —, gilt die Transaktion als endgültig bestätigt [vgl. 4, S. 34–35].

Obwohl die Bitcoin-Blockchain als Pionier für dezentrale Finanztransaktionen diente, sind ihre Anwendungsmöglichkeiten aufgrund der eingeschränkten Programmierbarkeit begrenzt. Bitcoins integrierte Skriptsprache kann nur einfache Bedingungen wie zeitverzögerte Transaktionen abbilden; sie kennt insbesondere keine Schleifen oder allgemeinen Kontrollstrukturen. Um komplexere Szenarien umzusetzen, ist eine Turing-vollständige Programmiersprache erforderlich — also eine Sprache, die (abgesehen von Ressourcengrenzen) jede berechenbare Funktion ausdrücken kann [vgl. 110, 70]. Wie eine Blockchain mit einer solchen Sprache kombiniert werden kann und welche neuen Anwendungen daraus entstehen, zeigt der folgende Abschnitt.

## 2.7. Smart Contracts

### 2.7.1. Einführung

Vitalik Buterin — Mitgründer des Fachmagazins Bitcoin Magazine (2011) und Autor des Ethereum-Whitepapers — erkannte frühzeitig das Potenzial einer Turing-vollständigen

Skriptsprache in Verbindung mit einer Blockchain. Den ersten Entwurf des Whitepapers „Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform“ veröffentlichte er im November 2013; die im Literaturverzeichnis geführte kanonische Fassung datiert auf 2014 [vgl. 20]. Auf dieser Grundlage entstand die Ethereum-Blockchain: eine Plattform, die die Blockchain-Technologie mit einer Turing-vollständigen Programmierumgebung kombiniert und bis heute das führende Ökosystem für dezentrale Finanzanwendungen ist — auf Ethereum entfallen rund 55 % des gesamten in DeFi-Protokollen gebundenen Kapitals (Stand: 02.08.2026) [44] (Kapitel 3). Die zugehörige native Kryptowährung Ether (ETH) ist das Gegenstück zu Bitcoin auf der Bitcoin-Blockchain: Sie dient als Zahlungsmittel und wird darüber hinaus benötigt, um die Ausführung von Smart Contracts zu bezahlen, insbesondere wenn diese schreibende, zustandsändernde Operationen beinhalten.

Das Konzept, auf dem Ethereum aufbaut, ist älter als die Blockchain selbst: Nick Szabo prägte bereits 1994 den Begriff der „Smart Contracts“ — in digitaler Form spezifizierte Versprechen samt der Protokolle, in denen die Parteien diese Versprechen erfüllen [vgl. 107]. Die heute übliche Zusatzeigenschaft — automatische, nach Bereitstellung nicht mehr änderbare Ausführung — kam erst mit der Blockchain als Ausführungsumgebung hinzu. Smart Contracts sind digitale, sich selbst ausführende Verträge, die nicht auf zentralen Servern, sondern auf einer Blockchain liegen und dort ausgeführt werden [vgl. 63]. Die Software-Entwicklung erfolgt bei Ethereum über die eigens dafür entwickelte, Turing-vollständige Programmiersprache Solidity. Transaktionen auf der Ethereum-Blockchain lassen sich im Grunde mit denen der Bitcoin-Blockchain vergleichen — sie enthalten jedoch nicht nur den Transfer einer virtuellen Währung, sondern können zusätzlich Vertragsbedingungen formal erfassen, die ohne den Einfluss Dritter ausgeführt und durchgesetzt werden. Dabei kann es sich beispielsweise um den Verkauf virtueller Güter oder die Erfassung und Übertragung des Eigentums virtuell abgebildeter realer Güter handeln. In der Regel erfolgt der Transfer automatisch anhand vordefinierter Bedingungen, die im Smart Contract festgelegt sind [vgl. 63].

Durch Smart Contracts können komplexe Abläufe modelliert werden, die auf Zustände und Zustandsänderungen der Blockchain reagieren. Ein Beispiel ist die Ausgabe und Verwaltung eigener Token unter vordefinierten Bedingungen. Eine weitere Einsatzmöglichkeit ist die Programmierung dezentraler Anwendungen (dApps), die beispielsweise traditionelle Finanzdienstleistungen auf der Blockchain anbieten und automatisiert ausführen können [vgl. 63].

### 2.7.2. Token: Klassifikation und Standards

Token sind digitale Einheiten, die mithilfe von Smart Contracts erstellt werden, um Werte oder Rechte abzubilden — etwa Unternehmensanteile, Besitzverhältnisse, Nutzungsrechte

oder digitale Identitäten [vgl. 63]. Ein Coin ist demgegenüber die digitale Geldeinheit einer Kryptowährung: Alle Coins sind Token, aber nicht alle Token sind Coins, da Token über den reinen Werttransfer hinaus zusätzliche Rechte abbilden können [vgl. 63].

Gemäß Oliveira et al. (2018) lassen sich Token in drei Klassen einteilen [vgl. 87]:

**Payment Token** wie Bitcoin dienen ausschließlich als Tauschmittel für dezentrale Transaktionen im Zahlungsverkehr.

**Security Token** sind digitale Wertpapiere, die als Investitionsverträge oder Vermögenswerte fungieren und ihren Besitzern bestimmte Rechte gewähren — etwa Stimmrechte bei Unternehmensentscheidungen oder Ansprüche auf zukünftige Gewinne. Sie repräsentieren traditionelle Finanzinstrumente auf einer dezentralen Plattform.

**Utility Token** sind mit einer digitalen Dienstleistung auf der Blockchain verbunden und beschreiben Mitglieds- und Mitwirkungsrechte in einem Protokoll oder Ökosystem. Sie ermöglichen es Benutzern, bestimmte Dienstleistungen innerhalb des Ökosystems zu erwerben oder zu nutzen, und können auch als Belohnung für Beiträge zum Netzwerk dienen [vgl. 87].

Neben dieser Klassifikation lassen sich Token nach technischen Standards untergliedern; die Ethereum-Standards tragen die Bezeichnung ERC (Ethereum Request for Comments) nach dem Verfahren, in dem sie vorgeschlagen werden. Als Basis dienen hier die Standards der für DeFi-Applikationen meistgenutzten Blockchain Ethereum (rund 55 % des DeFi-TVL, Stand: 02.08.2026 [44]) [vgl. 51].

Auf Ethereum abgebildete Coins, Payment Token und Utility Token verwenden in der Regel den **ERC-20**-Standard, der die Erstellung und Verwaltung fungibler Token vereinheitlicht und vereinfacht [vgl. 63]. Er ist der am häufigsten eingesetzte Standard und bildet einfache Funktionalitäten wie den Token-Transfer auf Ethereum-kompatiblen Blockchains ab.

Der **ERC-721** Non-Fungible Token Standard beschreibt Token, die einzigartig und voneinander unterscheidbar sind. Dieser Standard ermöglicht die Nachverfolgung unterscheidbarer Vermögenswerte; Eigentumsverhältnisse an individuellen Assets wie Kunstwerken, Grundstücken oder Immobilien lassen sich damit eindeutig abbilden [vgl. 51].

Der **ERC-777**-Standard (2017) baut auf ERC-20 auf und führt Callback-Funktionen („Hooks“) ein, mit denen Sender und Empfänger automatisiert auf Transfers reagieren können — etwa um Transaktionen bestimmter Adressen abzulehnen; das zweistufige Freigabeverfahren von ERC-20 entfällt dadurch [vgl. 42]. Diese Hooks erwiesen sich in der Praxis jedoch als Angriffsfläche: Über den Empfänger-Hook des ERC-777-Tokens imBTC wurden im April 2020 ein Uniswap-V1-Pool und die Kreditplattform Lendf.me (Verlust rund 25 Mio. US-Dollar) per Reentrancy angegriffen [vgl. 123]; der Standard hat sich deshalb nicht auf breiter Front durchgesetzt.

Der **ERC-1155** Multi Token Standard kombiniert ERC-20 und ERC-721: Fungible und nicht-fungible Token können in einem einzigen Smart Contract verwaltet und mehrere

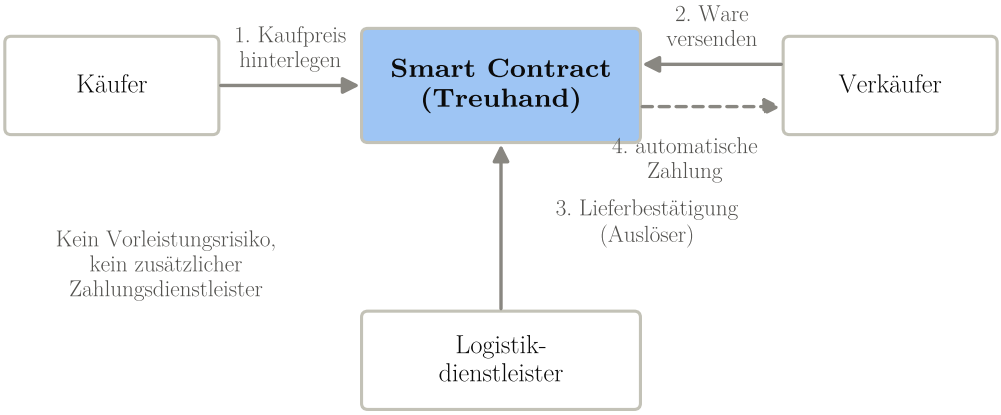



Abbildung 2.7.: Ablauf eines Smart Contracts im E-Commerce: Treuhand ohne zusätzlichen Zahlungsdienstleister. Eigene Darstellung.

Tokenarten mit einer Transaktion transferiert werden [vgl. 51]. Während bei ERC-20 und ERC-721 jeder Erwerb in einer einzelnen Transaktion abgebildet wird, erlaubt ERC-1155 das Bündeln von Elementen: Der Tausch von zehn Assets gegen zehn andere benötigt nicht 20 Transaktionen, sondern zwei. Dies entlastet das Netzwerk und steigert die Effizienz [vgl. 94].

### 2.7.3. Beispiel eines Smart Contracts

Als Beispiel dient ein Smart Contract im E-Commerce-Bereich in Verbindung mit einem Logistikunternehmen: Wenn ein Endverbraucher Ware bei einem Verkäufer bestellt, liefert dieser die Ware an das Logistikunternehmen. Auf den ersten Blick unterscheiden sich diese Schritte nicht von einem konventionellen Geschäftsprozess. Der Unterschied besteht in einer vertraglichen Vereinbarung, die die Zahlung des Kaufpreises an den Verkäufer erst freigibt, sobald der Paketdienstleister die Ware ausgeliefert hat. Der Vorteil für den Endkunden: Er muss das Geld nicht im Voraus überweisen und geht kein Vorleistungsrisiko ein. Der Händler wiederum erhält das Geld sicher und unmittelbar nach der Lieferung. Heute wird dieses Risiko häufig durch einen zusätzlichen Zahlungsdienstleister abgedeckt, der sich diese Absicherung bezahlen lässt; durch Smart Contracts entfällt dieser Kostenfaktor [vgl. 96].

**Zwischenfazit.** Für die weitere Untersuchung sind aus diesem Kapitel drei Eigenschaften zentral: Erstens entsteht Vertrauen in Blockchains nicht durch einen Intermediär, sondern durch unabhängige Validierung und ein ökonomisches Anreizsystem — das ist der Referenzpunkt für Merkmal M1 (Intermediärfunktion) des in Abschnitt 1.3 eingeführten Analyserasters. Zweitens sind die Sicherheitsgarantien eng umgrenzt und kostenbasiert,

nicht absolut — darauf baut die Risikoanalyse (M5) in den Kapiteln 4 und 5 auf. Drittens machen Smart Contracts aus einer reinen Zahlungsinfrastruktur eine Programmierplattform — die technische Voraussetzung dafür, dass sich klassische Finanzdienstleistungen ohne Intermediär abbilden lassen. Kapitel 3 setzt genau hier an.

# 3. Grundlagen der Decentralized Finance

## 3.1. Definition von Decentralized Finance

Decentralized Finance (DeFi) ist ein Begriff, der sich auf eine wachsende Zahl von Finanzdienstleistungen und -anwendungen bezieht, die auf dezentralisierten Netzwerken wie Blockchains basieren. Im Gegensatz zum traditionellen Finanzwesen, bei dem Finanzdienstleistungen von zentralisierten Institutionen wie Banken und Versicherungen angeboten werden, sind DeFi-Protokolle dezentralisiert und automatisiert. Sie nutzen Blockchain-Technologie und Smart Contracts (Kapitel 2), um Finanzdienstleistungen wie Kredite, Zahlungen und Handel auf dezentralisierte Weise anzubieten.

Ein zentrales Merkmal von DeFi ist die Möglichkeit, Finanzdienstleistungen ohne eine zentrale Autorität anzubieten. Jeder kann an DeFi-Protokollen teilnehmen und Finanzdienstleistungen nutzen, ohne auf eine zentrale Institution wie eine Bank angewiesen zu sein — mit den in Abschnitt 1.1 benannten faktischen Zugangshürden. Ein weiteres Merkmal ist das Versprechen, Finanzdienstleistungen schneller, günstiger und transparenter verfügbar zu machen: Da DeFi-Protokolle automatisiert sind, können Transaktionen ohne menschliches Eingreifen durchgeführt werden; die Kosten für Intermediäre entfallen, und Transaktionen werden öffentlich in der Blockchain aufgezeichnet. Ob und in welchem Umfang dieses Versprechen eingelöst wird, untersucht Kapitel 5 entlang der Merkmale M3 (Kosten und Geschwindigkeit) und M4 (Zugang).

Ein drittes Merkmal von DeFi ist die Möglichkeit, verschiedene Finanzdienstleistungen zu kombinieren und komplexe Finanzinstrumente zu erstellen. So können mehrere DeFi-Protokolle miteinander verknüpft werden, um beispielsweise einen Kredit zu erhalten, der mit hinterlegten Token einer Kryptowährung besichert wird. Durch die Kombination unterschiedlicher DeFi-Protokolle können neuartige Finanzprodukte geschaffen werden. Zu den bekanntesten DeFi-Anwendungen gehören Kreditprotokolle wie Compound und Aave, dezentrale Exchanges wie Uniswap, Curve und PancakeSwap sowie Stablecoins wie DAI [vgl. 38].

Herausforderungen und Risiken — etwa Sicherheitslücken und Regulierungsfragen — werden in Abschnitt 4.5 systematisch behandelt.

## 3.2. Historischer Hintergrund von DeFi

Die Idee, traditionelle Finanzdienstleistungen zu dezentralisieren und auf eine Blockchain-Plattform zu bringen, ist nicht neu. Bereits 2008 wurde mit der Einführung von Bitcoin das Potenzial erkannt, die Kontrolle über Finanzdienstleistungen aus den Händen von Regierungen und Banken zu nehmen und in die Hände der Nutzer zu legen. In den folgenden Jahren entstanden immer mehr Kryptowährungen, die als alternatives Zahlungssystem genutzt werden konnten.

Die erste Anwendung von DeFi-Prinzipien erfolgte mit der Einführung von Ethereum im Jahr 2015. Ethereum ermöglichte es Entwicklern, Smart Contracts zu erstellen, die automatisch ausgeführt werden, sobald bestimmte Bedingungen erfüllt sind (Abschnitt 2.7). Dies eröffnete neue Möglichkeiten für dezentrale Anwendungen, einschließlich dezentraler Finanzanwendungen.

Die ersten DeFi-Anwendungen auf Ethereum waren einfache dezentrale Exchanges wie EtherDelta, mit denen Nutzer Ether und andere ERC-20-Token direkt handeln konnten. Die Notwendigkeit einer zentralen Börse entfiel damit. Im Laufe der Zeit wurden immer komplexere DeFi-Protokolle entwickelt, die es Nutzern ermöglichten, verschiedene Finanzdienstleistungen dezentral zu nutzen, einschließlich Krediten, Derivaten, Staking und Liquiditätspools. Ein bedeutender Meilenstein war die Einführung von MakerDAO im Jahr 2017 — das erste große Protokoll für dezentrale, besicherte Kreditvergabe, das den Weg für viele weitere DeFi-Protokolle geebnet hat.

Insbesondere seit 2020 hat DeFi stark an Aufmerksamkeit und Bedeutung gewonnen: Der Gesamtwert des in DeFi-Protokollen gebundenen Kapitals (TVL, Abschnitt 1.1) stieg im Jahresverlauf 2020 von unter einer auf rund 15,3 Mrd. US-Dollar, überschritt am 11. Februar 2021 erstmals die Marke von 40 Mrd. US-Dollar und erreichte seinen bisherigen Höchststand von rund 177 Mrd. US-Dollar am 9. November 2021 (vgl. Abschnitt 4.6) [48]. Diese Entwicklung zeigt, dass dezentrale Finanzdienstleistungen erhebliches Interesse auf sich ziehen — sie verlief allerdings, wie Abschnitt 4.6 zeigen wird, ausgeprägt zyklisch.

## 3.3. DeFi-Einführung

Decentralized Finance, zu Deutsch dezentralisierte Finanzdienstleistungen, ist eine auf der Blockchain-Technologie basierende Finanzinfrastruktur. Der Begriff DeFi wird grundsätzlich für offene, genehmigungsfrei zugängliche und interoperable Smart-Contract-Protokolle verwendet [vgl. 100, S. 153–174]. DeFi-Protokolle sind auf öffentlichen Blockchains wie Ethereum, Solana oder der BNB Chain implementiert [44]. DeFi nimmt traditionelle Finanzdienste — wie das Leihen von Währungen bei Banken oder den Handel an Devisenmärkten — und repliziert diese als programmierte Smart Contracts auf öffentlichen Blockchains. Dies wird mit dem Ziel eines dezentralen Finanzsystems vorangetrieben, bei

dem der Nutzer unabhängig von zentralen Instanzen wie Banken oder Intermediären wie Börsen ist. Konträr zum klassischen Finanzsystem werden Verträge nicht durch Intermediäre wie Notare geschaffen, sondern in programmierten Smart Contracts festgehalten [vgl. 100, S. 153–174].

DeFi-Dienstleistungen lassen sich durch vier Eigenschaften beschreiben: non-custodial, genehmigungsfrei, öffentlich überprüfbar und zusammensetzbar [vgl. 121]. Non-custodial (verwahrungsfrei) bedeutet, dass Nutzer zu jedem Zeitpunkt die Kontrolle über ihre Besitztümer wie Coins und Token behalten; keine zentrale Instanz kann diese konfiszieren. Genehmigungsfrei bedeutet, dass grundsätzlich jeder mit dezentralen Finanzdienstleistungen interagieren kann — auch Nutzer, denen der Zugang zum traditionellen Finanzmarkt verwehrt ist. Öffentlich überprüfbar sind DeFi-Protokolle, weil jeder Nutzer den zugrunde liegenden Programmcode und jede Transaktion verifizieren kann. Die Zusammensetzbarkeit schließlich beschreibt, wie aus einzelnen, primitiveren Finanzdienstleistungen komplexe Finanzkonstrukte zusammengesetzt werden können [vgl. 121].

## 3.4. DeFi-Architektur

Im Folgenden wird vor allem die Eigenschaft „zusammensetzbar“ betrachtet: Die DeFi-Infrastruktur lässt sich nutzen, um aus einzelnen Protokollen neuartige DeFi-Produkte zu orchestrieren. DeFi-Komponenten lassen sich dazu am besten in einer mehrschichtigen Architektur betrachten, wie sie Schär (2021) vorschlägt [vgl. 100, S. 156]. Jede Schicht hat einen bestimmten Zweck; die Schichten bauen aufeinander auf und schaffen eine offene Infrastruktur, die es jedem ermöglicht, auf anderen Teilen des Stacks aufzubauen (Abbildung 3.1).

- **Abwicklungsschicht (Settlement Layer):** Sie besteht aus der Blockchain und dem zugehörigen Protokoll-Asset. Sie ermöglicht dem Netzwerk die sichere Speicherung von Eigentumsinformationen und stellt sicher, dass alle Zustandsänderungen mit den Regeln des Netzwerks übereinstimmen (Kapitel 2).

- **Vermögensschicht (Asset Layer):** Sie besteht aus allen Token, die auf der Abwicklungsschicht ausgegeben werden — das native Protokoll-Token sowie alle zusätzlichen Token nach den unterstützten Token-Standards (Abschnitt 2.7.2).

- **Protokollschicht (Protocol Layer):** Sie bietet Standards für bestimmte Anwendungsfälle wie dezentrale Börsen, Schuldenmärkte, Derivate und Vermögensverwaltung. Diese Standards sind als Smart Contracts implementiert und können von jedem Benutzer und jeder Anwendung genutzt werden — sie sind in hohem Maße interoperabel. Im klassischen Finanzwesen lässt sich diese Öffnung am ehesten mit der Payment Services Directive 2 (PSD2) vergleichen — jener EU-Richtlinie (2015


Abbildung 3.1.: Der DeFi-Stack: fünf aufeinander aufbauende Schichten. Die Sicherheit jeder Schicht hängt von den darunterliegenden ab. Eigene Darstellung in Anlehnung an Schär (2021) [vgl. 100].

verabschiedet, seit Januar 2018 anwendbar), die Banken verpflichtet, Drittanbietern über standardisierte Schnittstellen (APIs) Zugriff auf Kontoinformationen und Zahlungsauslösung zu gewähren [vgl. 17, S. 367–381, 49]. Ein Ziel dieser Öffnung ist es, den Wettbewerb zu fördern und FinTechs — Unternehmen, die Finanzdienstleistungen mit modernen Technologien anbieten oder verbessern [vgl. 92] — neuartige Bankdienstleistungen zu ermöglichen.

- **Anwendungsschicht (Application Layer):** Hier werden benutzerorientierte Anwendungen erstellt, die sich mit den einzelnen Protokollen verbinden. Die Interaktion mit den Smart Contracts erfolgt in der Regel über ein Web-Frontend, das die Nutzung erleichtert.

- **Aggregationsschicht (Aggregation Layer):** Aggregatoren schaffen nutzerzentrierte Plattformen, die mehrere Anwendungen und Protokolle verbinden, komplexe Aufgaben vereinfachen und relevante Informationen übersichtlich zusammenfassen.

Entscheidend ist die hierarchische Sicherheitsabhängigkeit dieses Aufbaus: Jede Schicht ist nur so sicher wie die darunterliegenden. Wird die Blockchain der Abwicklungsschicht kompromittiert, sind alle darauf aufbauenden Schichten unsicher; wäre die zugrunde liegende Blockchain faktisch nicht dezentral, wären alle Dezentralisierungsbemühungen auf höheren Schichten bedeutungslos [vgl. 99].

Ein Beispiel macht das Zusammenspiel konkret: Wer über einen DEX-Aggregator (Aggregationsschicht) den Stablecoin DAI gegen Ether tauscht, nutzt dessen Web-Frontend

(Anwendungsschicht), das den Tausch an ein Handelsprotokoll wie Uniswap weiterreicht (Protokollschicht); gehandelt werden ERC-20-Token (Vermögensschicht), und abgewickelt wird die Transaktion endgültig auf der Ethereum-Blockchain (Abwicklungsschicht). Ein Fehler auf einer beliebigen Schicht — vom Frontend bis zum Konsens — gefährdet das Ergebnis des Nutzers; diese Beobachtung wird in der Risikoanalyse (Abschnitt 4.5, Merkmal M5) wieder aufgegriffen.

## 3.5. DeFi-Anwendungen

Die folgenden Unterabschnitte stellen die zentralen Anwendungskategorien von DeFi vor. Um die Kategorien vergleichbar zu machen und die spätere Analyse vorzubereiten, wird jede Kategorie am Ende entlang des in Abschnitt 1.3 eingeführten Analyserasters zusammengefasst: (M1) ersetzte Intermediärfunktion, (M2) Besicherung, (M3) Kosten und Abwicklungsgeschwindigkeit, (M4) Zugang, (M5) Risikoprofil und (M6) regulatorische Einordnung. Kapitel 4 vergleicht die Fallstudien-Protokolle entlang dieses Rasters; Kapitel 5 stellt DeFi und traditionelles Finanzwesen einander gegenüber.

### 3.5.1. Stablecoins

Stablecoins sind Assets, die versuchen, Preisstabilität gegenüber einer Zielwährung zu erreichen. Diese Zielwährung ist meistens eine Fiatwährung wie der US-Dollar, kann jedoch auch ein anderes Asset sein [vgl. 121]. Eine Fiatwährung ist eine Währung, die nicht durch einen physischen Rohstoff wie Gold gedeckt ist, sondern auf dem Vertrauen in das Währungssystem und die emittierende Institution beruht; sie wird von Regierungen und Zentralbanken ausgegeben und in ihrer Menge gesteuert [vgl. 55]. Grundsätzlich können mit Stablecoins, die den Wert des US-Dollars widerspiegeln, Waren bezahlt werden. Stablecoins werden meistens im Austausch gegen Fiatwährung an Nutzer ausgegeben und so in Umlauf gebracht. Um die Wertstabilität zu bewahren, hat der Stablecoin-Besitzer die Möglichkeit, seine Coins wieder gegen Fiatwährung einzutauschen. Der Wert wird stabil gehalten, indem ein Sicherheiten-Pool — ähnlich dem historischen Goldstandard einer Zentralbank [vgl. 54] — zum Tragen kommt. Anders als bei Zentralbanken bestehen die Reserven nicht aus Gold, sondern aus versicherten Einlagen, Staats- und Unternehmensanleihen, Wertpapieren oder digitalen Assets [vgl. 91].

Nach der Art der Besicherung lassen sich drei Typen unterscheiden:

**Off-chain besicherte Stablecoins** wie USDT (Tether) und USDC halten ihre Reserven außerhalb der Blockchain bei zentralen Emittenten und sind u. a. als ERC-20-Token auf mehreren Blockchains verfügbar; ihre 1:1-Bindung hängt von der Qualität und Verfügbarkeit dieser Off-Chain-Reserven ab [vgl. 100, S. 153–174]. Ähnlich funktionieren wrapped Token wie wBTC, die den Wert eines Assets einer anderen Blockchain abbilden und es so über

Blockchain-Grenzen hinweg handelbar machen (vgl. Abschnitt 3.5.3).

**On-chain (krypto-)besicherte Stablecoins** hinterlegen Kryptowährungen als Sicherheit in einem Smart Contract. Dieses Verfahren kommt beim DAI-Stablecoin zum Einsatz: Durch das Hinterlegen von Ether werden Coins erzeugt, die an den Wert des US-Dollars gekoppelt sind — notwendigerweise überbesichert, da die hinterlegte Sicherheit selbst volatil ist (im Detail in Abschnitt 3.5.2).

**Algorithmische Stablecoins** verzichten ganz oder teilweise auf Besicherung und versuchen, die Bindung allein über programmierte Angebotsmechanismen zu halten. Dieses Modell ist spektakulär gescheitert: Im Mai 2022 verlor der algorithmische Stablecoin TerraUSD (UST) seine Dollar-Bindung. UST wies zuvor eine Marktkapitalisierung von rund 18 Mrd. US-Dollar auf; im Zusammenspiel mit dem Kurssturz des verbundenen Token LUNA wurden binnen weniger Tage rund 40 Mrd. US-Dollar Marktwert vernichtet, mit Kettenreaktionen im gesamten Kryptomarkt [vgl. 16]. Der Fall gilt seither als Lehrstück dafür, dass Stabilität ohne werthaltige Besicherung von reflexivem Vertrauen abhängt — er wird in der Risikoanalyse (Abschnitt 4.5.1) wieder aufgegriffen. *(Ergänzung der überarbeiteten Fassung.)*

Der Umlauf US-Dollar-gebundener Stablecoins beträgt rund 307 Mrd. US-Dollar — davon USDT rund 183 Mrd. und USDC rund 72 Mrd. — und beträgt damit mehr als das Vierfache des gesamten in DeFi-Protokollen gebundenen TVL (74,2 Mrd. US-Dollar, Abschnitt 1.1) (Stand: 02.08.2026) [47].

**Merkmalsprofil (M1–M6).** Stablecoins bilden die Funktion des E-Geld-Emittenten bzw. der Giralgeld-Bereitstellung ab; die geldpolitische Stabilisierungsfunktion der Zentralbank ersetzen sie nicht, sondern importieren sie über die Bindung an die Referenzwährung (M1). Die Besicherung reicht von Off-Chain-Reserven über Krypto-Überbesicherung bis zu rein algorithmischen Mechanismen (M2). Transfers erfolgen weltweit in Minuten zu Netzwerkgebühren (M3); Halten und Transferieren sind genehmigungsfrei, Ausgabe und Rücktausch bei Off-Chain-Modellen dagegen an Identitätsprüfung gebunden (M4). Das Risikoprofil (M5) gliedert sich in technische Risiken (Smart-Contract-Fehler bei On-Chain-Modellen), ökonomische Risiken (Qualität und Verfügbarkeit der Reserven, strukturelles Depeg-Risiko algorithmischer Modelle, Liquidationsrisiken der Überbesicherung) und Governance-Risiken (Ermessen und Bonität des zentralen Emittenten). In der EU unterwirft die Verordnung (EU) 2023/1114 (MiCA) E-Geld-Token und vermögenswertreferenzierte Token seit dem 30. Juni 2024 einem eigenen Zulassungs-, Reserve- und Rücktauschregime (M6, im Detail Abschnitt 4.5.2).

### 3.5.2. Kreditvergabe und -aufnahme (Lending/Borrowing)

Das Leihen und Verleihen von Krypto-Assets stellt einen der wichtigsten Mechanismen im DeFi-Raum dar [vgl. 100, S. 153–174]. Im traditionellen Finanzmarkt erfüllen Banken

durch die Kreditvergabe diese Rolle [vgl. 119]. Ein Verleiher stellt seine Krypto-Assets wie Bitcoin oder Ether dem Protokoll zur Verfügung und erhält Zinsen auf das eingesetzte Kapital. Im Gegenzug zahlt der Leihende Zinsen auf das geliehene Kapital, von denen das Protokoll und der Verleiher profitieren. Dezentrale Plattformen für Kreditgeschäfte unterscheiden sich drastisch von traditionellen Kreditinstituten: Durch ein einprogrammiertes Sicherheitsnetz muss keine zentrale Entität die Identität oder Kreditwürdigkeit der Teilnehmer prüfen. Kreditvergabe und -nahme werden dezentral und automatisiert durch Smart Contracts geregelt. Der Kreditgeber wird, je nach Protokoll, durch zwei unterschiedliche Mechanismen geschützt: durch die Atomarität von Flash Loans oder durch das Hinterlegen von Sicherheiten.

**Flash Loans**

Flash Loans sind Darlehensgeschäfte, bei denen Kapital innerhalb einer einzigen Transaktion geliehen, genutzt und zuzüglich der anfallenden Zinsen zurückgegeben wird. Im traditionellen Finanzwesen gibt es kein vergleichbares Produkt. Da jedes Darlehensgeschäft innerhalb einer Transaktion gestartet und beendet wird, nennt man diese Art von Geschäft atomar — es ist nicht teilbar [vgl. 100, S. 153–174]. Nutzer können große Mengen Kapital aus dem Protokoll-Pool leihen; die leihbare Menge hängt vom im Smart Contract gesperrten Kapital ab, das Kreditgeber bereitgestellt haben [vgl. 119]. Läuft die Transaktion aus, ohne dass das geliehene Kapital zuzüglich Zinsen zurückgezahlt wurde, ist die gesamte Transaktion ungültig — als wäre der Kredit nie vergeben worden [vgl. 100, S. 153–174]. Das ermöglicht auch Nutzern ohne großes Eigenkapital, von Arbitragegeschäften zu profitieren: Wer einen Preisunterschied eines Tokens auf zwei dezentralen Börsen identifiziert, kann diese Arbitragemöglichkeit mit geliehenem Kapital ausnutzen [vgl. 119].

Ein Beispiel liefert eine Transaktion vom 15. Februar 2020 auf der Ethereum-Blockchain. 10.000 Ether wurden per Flash Loan von der dYdX-Plattform geliehen. 5.500 ETH wurden auf Compound als Sicherheit hinterlegt, um 112 wrapped Bitcoin (wBTC) zu leihen [vgl. 71] — wBTC ist ein ERC-20-Token, der den Wert von Bitcoin auf der Ethereum-Blockchain abbildet [vgl. 22]. Weitere 1.300 ETH dienten auf der Handelsplattform bZx [vgl. 21] als Margin für eine fünffach gehebelte Short-Position ETH gegen wBTC. Deren Ausführung tauschte ein Vielfaches des Margin-Betrags über eine dezentrale Börse (Uniswap) in wBTC — bei der dort vorhandenen dünnen Liquidität stieg der wBTC-Preis dadurch stark an. Da bZx genau diesen Marktpreis als Referenz verwendete, blieb die Manipulation für das Protokoll unbemerkt. Die auf Compound geliehenen 112 wBTC wurden anschließend zu diesem überhöhten Preis gegen ETH verkauft, der Flash Loan in derselben Transaktion zurückgezahlt und ein Gewinn von rund 1.193 ETH (nach damaligem Kurs etwa 350.000 US-Dollar) realisiert [vgl. 71, 93].

Die Risikoverteilung von Flash Loans muss dabei nach Perspektive getrennt werden — das Original ließ diese Unterscheidung offen, was zu einem scheinbaren Widerspruch mit der Risikoanalyse führte:

- **Für den Kreditgeber** (den Pool) ist der Flash Loan konstruktionsbedingt abgesichert: Wird nicht zurückgezahlt, ist die gesamte Transaktion ungültig, das Kapital hat den Pool faktisch nie verlassen. Bei korrekter Implementierung des Protokolls riskiert der Kreditgeber nichts; der Kreditnehmer riskiert lediglich die Transaktionsgebühren.
- **Für die angegriffenen Protokolle** sind Flash Loans dagegen ein Angriffsverstärker: Sie stellen jedermann kurzfristig beliebig großes Kapital bereit, mit dem sich Marktpreise und Preisorakel innerhalb einer Transaktion manipulieren lassen — wie im geschilderten bZx-Fall, in dem nicht bZx selbst, sondern dessen externe Preisquelle manipuliert wurde [vgl. 93]. Flash Loans erzeugen diese Verwundbarkeiten nicht, aber sie machen ihre Ausnutzung kapitallos möglich. Diese Perspektive vertieft Abschnitt 4.5.1.

**Kreditvergabe durch Besicherung mit Krypto-Assets**

Alternativ können Krypto-Assets geliehen werden, indem Sicherheiten hinterlegt werden — meist in Form anderer ERC-20-Token. Da in einem dezentralen Finanzsystem die Identitäten der Vertragsparteien nicht verifiziert werden, muss der Smart Contract das Vertrauen herstellen: Der als Sicherheit hinterlegte Betrag wird gesperrt und dem Kreditnehmer erst wieder zur Verfügung gestellt, nachdem der Kredit samt Zinsen zurückgezahlt wurde. Besicherte Kreditvergabe-Protokolle lassen sich in Collateralized Debt Positions (CDP) und Collateralized Debt Markets (CDM) einteilen [vgl. 100, S. 153–174].

**Collateralized Debt Position.** Eine CDP ist eine durch hinterlegte Sicherheiten erzeugte Schuldposition. Der Kreditnehmer stellt dem Protokoll Kryptowährungen als Sicherheit zur Verfügung, um eine andere Währung zu minten oder zu leihen. Die leihbare Menge hängt vom Wert der hinterlegten Sicherheit, dem Preis des zu leihenden Tokens und dem vom Protokoll vorgeschriebenen Besicherungsgrad ab. Diese Methode ermöglicht es dem Nutzer, gleichzeitig an der Wertentwicklung der hinterlegten Krypto-Assets teilzuhaben und Zugriff auf liquide Mittel zu haben [vgl. 100, S. 164–165].

Ein Beispiel liefert MakerDAO: Der Nutzer hinterlegt ETH als Sicherheit im Smart Contract, um den Stablecoin DAI zu leihen; ein DAI entspricht stets circa einem US-Dollar [vgl. 10]. CDP-besicherte Kredite sind immer überbesichert — der Kreditnehmer muss Sicherheiten hinterlegen, deren Wert das geliehene Kapital überschreitet; die Überbesicherung ersetzt die im traditionellen Kreditgeschäft übliche Informationsbeschaffung über den Schuldner [vgl. 121, 6]. Bei MakerDAO betrug die Besicherungsquote 2023 beispielsweise 150 %: Für Sicherheiten im Wert von 100 US-Dollar erhält der Kreditnehmer DAI im Wert von 66,66 US-Dollar; die Quote ist je nach Sicherheiten-Typ („Vault“) variabel [vgl. 10]. (MakerDAO firmiert seit August 2024 unter dem Namen Sky [vgl. 31]; das DAI-System besteht fort und wird um den Nachfolge-Stablecoin USDS ergänzt, dessen Umlauf den von DAI inzwischen übersteigt [47] — die Fallstudie in Kapitel 4 greift dies auf.)

Der Kreditgeber ist in diesem Prozess durch den Smart Contract geschützt: Sinkt der Wert der Sicherheit unter einen definierten Schwellenwert, wird die Position liquidiert.

Liquidatoren — funktional vergleichbar mit Insolvenzverwaltern — können die liquidierte Position zu einem reduzierten Wert aufkaufen; Verluste des Kreditgebers und Protokollgebühren werden so automatisiert aus dem Verkauf der Sicherheiten gedeckt [vgl. 121].

Der Schwellenwert wird im Aave-Ökosystem über den Health Factor (Gesundheitsfaktor) ausgedrückt. Aave ist wie MakerDAO eine Plattform für dezentrale, besicherte Kreditvergabe. Der Gesundheitsfaktor $H_f$ ist der Quotient aus dem Wert der hinterlegten Sicherheiten — gewichtet mit der jeweiligen Liquidationsschwelle — und dem Gesamtwert des geliehenen Kapitals zuzüglich Zinsen [vgl. 3]:

$$H_f = \frac{\sum (\text{Sicherheit}_i \times \text{Liquidationsschwelle}_i)}{\text{geliehenes Kapital} + \text{Zinsen}} \tag{3.1}$$

Fällt der Gesundheitsfaktor unter 1, kann die Kreditposition liquidiert und von Liquidatoren aufgekauft werden [vgl. 3]. Um eine CDP-Position regulär zu schließen, zahlt der Nutzer den Kredit zuzüglich Zinsen zurück und erhält Zugriff auf die hinterlegten Sicherheiten [vgl. 100, S. 164–165].

**Collateralized Debt Markets.** Im Gegensatz zu CDPs werden bei CDMs keine neuen Token erzeugt, sondern bestehende Krypto-Assets verliehen, indem das Protokoll Kreditgeber und -nehmer zusammenbringt. Auch hier hinterlegt der Kreditnehmer Sicherheiten. Das Zusammenbringen kann auf zwei Arten geschehen: Bei P2P-Paarungen stellt der Kreditgeber sein Kapital einer bestimmten, von ihm ausgewählten Gegenpartei zu vordefiniertem Zinssatz und Laufzeit zur Verfügung — Erträge fallen nur an, wenn sich eine leihende Partei findet. Bei gepoolten Krediten wird das Kapital aller Kreditgeber in einem Smart Contract zusammengefasst und aus dem Pool verliehen; die Zinssätze passen sich über den programmierten Nutzungsgrad flexibel an den Markt an (Kredite werden günstiger, wenn viel ungenutztes Kapital bereitsteht), und Kreditgeber profitieren von durchgängigen, anteiligen Zinszahlungen des gesamten Pools [vgl. 100, S. 165–166].

**Merkmalsprofil (M1–M6).** Lending-Protokolle ersetzen die Kreditintermediation der Bank durch einen Smart-Contract-Pool (M1). An die Stelle der Bonitätsprüfung tritt Überbesicherung mit automatischer Liquidation — bzw. bei Flash Loans die Atomarität der Transaktion (M2). Kredite sind ohne Antragsprozess sofort verfügbar, die Zinsbildung erfolgt algorithmisch nach Angebot und Nachfrage (M3); der Zugang ist genehmigungsfrei und anonym (M4). Das Risikoprofil (M5) gliedert sich in technische Risiken (Smart-Contract-Fehler, Orakel-Manipulation), ökonomische Risiken (Volatilität der Sicherheiten, Liquidationskaskaden bei dünner Liquidität) und Governance-Risiken (Änderung von Parametern wie Liquidationsschwellen durch Token-Mehrheiten). Regulatorisch besteht keine der Bankenaufsicht vergleichbare Einordnung; die Kreditvergabe ohne Intermediär entzieht sich bislang den bestehenden Kategorien (M6, Abschnitt 4.5.2).

### 3.5.3. Dezentrale Handelsplätze (Decentralized Exchanges)

Die meisten Krypto-Assets werden auf zentralisierten Kryptobörsen oder Centralized Exchanges (CEX) gehandelt [vgl. 100, S. 153–174]. Zentralisierte Kryptobörsen wie Binance oder Coinbase agieren ähnlich wie klassische Börsen am Kapitalmarkt: Sie unterhalten ein digitales Register aller offenen Kauf- und Verkaufspositionen, bringen Käufer und Verkäufer zusammen und legen den aktuellen Marktpreis automatisiert fest [vgl. 67]. Zentrale Kryptobörsen haben jedoch den Nachteil, dass Nutzer ihre Assets zuerst bei der Börse einzahlen müssen, um handeln zu können. Dadurch entsteht eine einseitige Vertrauensbeziehung: Unprofessionelle oder wenig vertrauenswürdige Börsen können Assets konfiszieren, verlieren oder durch Angriffe gestohlen bekommen.

Dezentrale Kryptobörsen (Decentralized Exchanges, DEX) lösen dieses Problem, indem das benötigte Vertrauen minimiert wird: Nutzer müssen ihre Krypto-Assets nicht in zentralen Systemen hinterlegen, sondern behalten jederzeit die Verfügungsgewalt. Der Handel erfolgt atomar — Kauf und Verkauf werden in einer Transaktion durch einen Smart Contract vollzogen [vgl. 100, S. 160–161].

DEX-Plattformen erlauben grundsätzlich nur den Handel mit Assets, die auf derselben Blockchain beheimatet sind: Eine DEX auf der Ethereum-Blockchain ermöglicht nur den Handel mit Ether und dort ausgegebenen Token [vgl. 121]. Diese Einschränkung lässt sich durch wrapped Token wie wBTC umgehen (Abschnitt 3.5.1), wodurch die in Bitcoin gehaltene Liquidität für DeFi-Anwendungen nutzbar wird — auf der Bitcoin-Blockchain selbst lassen sich mangels Turing-vollständiger Skriptsprache (Abschnitt 2.6) keine komplexen DeFi-Protokolle umsetzen; entsprechende Ansätze setzen auf Sidechains und Layer-2-Protokolle auf [vgl. 22]. Dezentrale Kryptobörsen lassen sich nach Preisbildung und Protokoll in verschiedene Typen unterteilen:

**Dezentrale Orderbuch-Börsen.** Orderbuch-Börsen nutzen Smart Contracts für Transaktionen, die Käufer und Verkäufer zusammenbringen, unterscheiden sich aber darin, wo die Orderdaten gespeichert werden. Vollständig dezentrale Orderbuch-Börsen speichern sie On-Chain — das benötigt keine Drittanbieter, kostet aber bei jeder Orderänderung Transaktionsgebühren und Zeit. Viele Orderbuch-Börsen verwenden deshalb ein Hybridmodell: Die Orderbücher werden Off-Chain durch Drittanbieter verwaltet, die eigentliche Transaktion wird On-Chain vollzogen.

Ein Beispiel eines hybriden Orderbuchs ist das 0x-Protokoll, dessen Handelsprozess in sieben Schritte unterteilt ist: Nutzer A genehmigt dem Protokoll den Zugriff auf die zu tauschende Kryptowährung, definiert eine Transaktion (Menge, Wechselkurs, Verfallszeitpunkt), signiert sie und übermittelt sie an das Netzwerk. Nutzer B findet die Transaktion, genehmigt dem Smart Contract den Zugriff auf seine Assets und signiert die bereits signierte Transaktion. Der Smart Contract verifiziert beide Signaturen, prüft Verfallszeitpunkt und ob die Order bereits gefüllt wurde, und transferiert dann die Assets zum

definierten Wechselkurs [vgl. 120]. Dieser atomare Aufbau — die Transaktion wird erst ausgeführt, wenn beide Parteien den Konditionen zugestimmt haben — ist charakteristisch für dezentrale Orderbuch-Börsen [vgl. 100, S. 161–162].

**Automated Market Maker (AMM).** Ein Problem von Orderbuch-Börsen ist, dass in illiquiden Märkten oft Tauschpartner fehlen. AMMs sind Smart-Contract-Protokolle, die dem Nutzer ständig einen Tauschpartner zur Verfügung stellen: einen Liquiditätspool, der mindestens zwei Kryptowährungen als Tauschpaar hält. Der Nutzer handelt direkt mit dem Pool, statt auf die Ordererfüllung eines individuellen Gegenparts zu warten. Die Wechselrate wird algorithmisch als Funktion der im Smart Contract hinterlegten Krypto-Assets berechnet: Je weniger von einer Währung im Pool hinterlegt ist, desto höher fällt die Wechselrate aus, um in dieses Asset zu tauschen. Traditionelle Orderbücher sind nicht erforderlich [vgl. 100, S. 153–174].

**Constant Function Market Maker (CFMM).** Das Charakteristikum, das CFMMs von anderen AMMs unterscheidet, ist die Preisbildung über eine konstante Funktion: Jeder Tausch muss die Reserven des Pools so verändern, dass das Produkt der Bestände konstant bleibt [vgl. 100, S. 161–162, 9]. Die Konstante lässt sich durch die Funktion $x \cdot y = k$ darstellen, wobei $x$ und $y$ die im Pool hinterlegten Token-Bestände sind. Für jeden Tausch muss gelten:

$$(x + \Delta x) \cdot (y - \Delta y) = k \tag{3.2}$$

Durch diese Funktion entsteht ein Liquiditätspool, der nie vollständig leer werden kann: Strebt die Reserve eines Tokens gegen null, strebt sein relativer Preis gegen unendlich (Abbildung 3.2) [vgl. 100, S. 153–174].

Nutzer können nicht nur über einen CFMM handeln, sondern auch davon profitieren, dem Pool Liquidität zur Verfügung zu stellen. Das Protokoll erhebt bei jedem Handel eine kleine Gebühr und kann von einer Geld-Brief-Spanne profitieren — der Differenz zwischen höchstem Kauf- und niedrigstem Verkaufsangebot, deren Enge die Liquidität eines Marktes anzeigt [vgl. 76]. Die erhobenen Gebühren erhöhen das $k$ der CFMM-Funktion stetig — die Kurve verschiebt sich nach außen (Abbildung 3.2) [vgl. 9]. An diesen Protokollgewinnen werden die Liquiditätsanbieter beteiligt [vgl. 100, S. 153–174]. Dem stehen Kursrisiken gegenüber: Verschiebt sich das Preisverhältnis der Poolpaare, kann der Wert der Position hinter das bloße Halten beider Token zurückfallen — dieser Effekt wird als *impermanenter Verlust* (impermanent loss) bezeichnet und in den Fallstudien in Abschnitt 4.3 wieder aufgegriffen. Neben der hier erläuterten Produkt-Funktion lassen sich CFMMs auch durch Summen-, Durchschnitts- oder Hybridfunktionen modellieren [vgl. 9].

Für das Funktionieren einer dezentralen Exchange wirken mehrere Akteure zusammen [vgl. 8]:

- **Trader** sind DeFi-Nutzer, die Token tauschen (swappen).

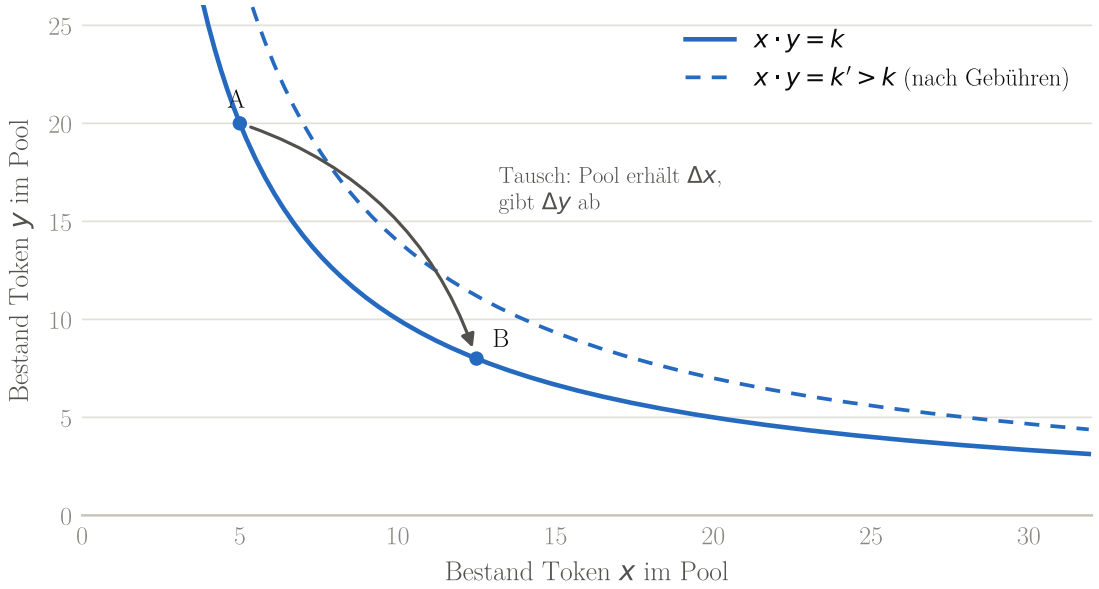



Abbildung 3.2.: Preisbildung eines Constant Function Market Makers: Ein Tausch bewegt die Reserven entlang der Kurve $x \cdot y = k$ (durchgezogen); Handelsgebühren vergrößern $k$ mit der Zeit und verschieben die Kurve nach außen (gestrichelt). Eigene Darstellung in Anlehnung an Schär (2021) [vgl. 100].

- **Liquiditätsprovider** stellen Liquidität für ein Handelspaar zur Verfügung (Token $x$ und $y$) und können diese jederzeit wieder entnehmen.
- **Arbitrageure** gleichen die Zusammensetzung der Pools aus, wenn ein Ungleichgewicht zu externen Marktpreisen entsteht.
- **Governance-Nutzer** halten Governance-Token, haben damit Stimmrechte über Protokollparameter wie Gebühren und erhalten einen Anteil der Gebühren als Entlohnung. Beim Start einer dezentralen Exchange werden über die sogenannte „Genesis Allocation“ frühe Investoren mit Governance-Token bedacht.

**Smart-Contract-basierte Reserve-Aggregatoren.** Eine weitere Form dezentraler Handelsplätze aggregiert Krypto-Reserven großer Liquiditätsanbieter (Liquidity Provider, LPs). Der Nutzer sendet eine Handelsanfrage an den Smart Contract; dieser vergleicht die Angebotspreise der am Markt agierenden LPs, akzeptiert den günstigsten und führt den Handel atomar aus [vgl. 78]. Anders als bei AMMs werden die Preise von den LPs gesetzt und nicht algorithmisch aus der Poolallokation berechnet. Der Nutzer kennt den Wechselkurs bereits beim Senden der Anfrage — dadurch tritt kein Slippage auf, also keine Abweichung zwischen erwartetem und tatsächlichem Ausführungspreis, wie sie sonst durch Marktschwankungen oder geringe Liquidität entsteht [vgl. 80]. Monopolistische Tendenzen bei unpopulären Handelspaaren können durch eine Mindestzahl an LPs entschärft werden; zusätzlich können große LPs über Know-Your-Customer-Verfahren (KYC) verifiziert werden, um Kollusionsrisiken zu verhindern [vgl. 100, S. 163]. Ein verwandtes, aber auf der Aggregationsschicht (Abschnitt 3.4) angesiedeltes Modell sind DEX-Aggregatoren wie

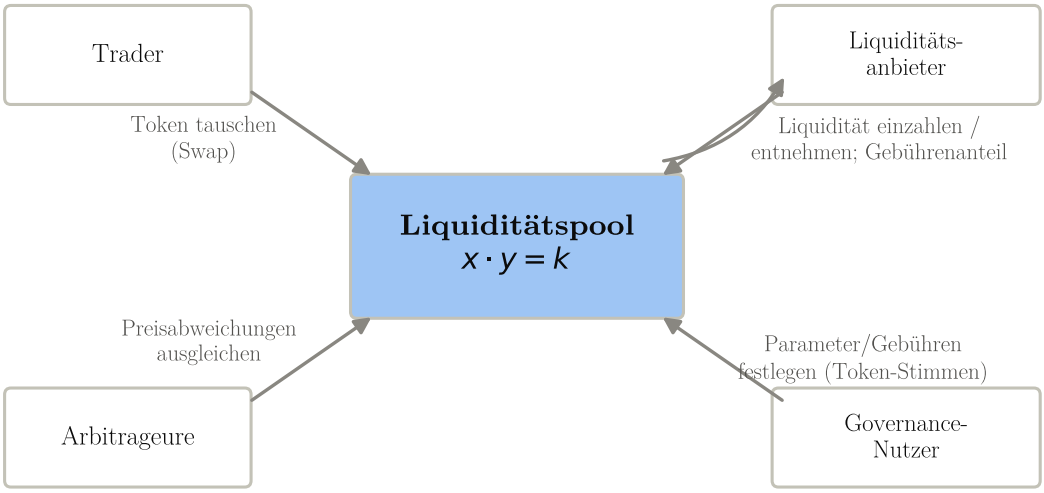



Abbildung 3.3.: Akteure einer dezentralen Exchange rund um den Liquiditätspool. Eigene Darstellung in Anlehnung an Auer/Choi/Kundu [vgl. 8].

1inch: Sie setzen keine eigenen Reserven ein, sondern durchsuchen bestehende Börsen und Liquiditätspools nach dem besten Ausführungspreis bei minimalen Gasgebühren [vgl. 13].

**P2P-Protokolle.** Bei Peer-to-Peer-Protokollen erfolgt der Handel vollständig zwischen den Nutzern: Nutzer A sucht im Netzwerk einen Nutzer B für den gewünschten Tausch, der Wechselkurs wird bilateral verhandelt, anschließend führt ein Smart Contract den Handel On-Chain aus. Off-Chain-Indexer beschleunigen den Prozess, indem sie Handelsanfragen vermitteln [vgl. 100, S. 163]. Ein Beispiel ist AirSwap: Die Verhandlung erfolgt Off-Chain, der Abschluss On-Chain. Zusätzlich können Oracles eingesetzt werden — Dienste, die Off-Chain-Daten wie Marktpreise von Drittanbietern auf die Blockchain übertragen (vgl. Anhang-Glossar) —, damit beide Parteien vor Annahme eines Handels einen fairen Wechselkurs abfragen können [vgl. 89]. Da sich die Beteiligten auf einen festen Wechselkurs geeinigt haben, wird Slippage vollständig vermieden.

**Merkmalsprofil (M1–M6).** DEX-Protokolle ersetzen Börse und Broker durch Smart Contracts, im AMM-Fall zusätzlich den Market Maker durch einen algorithmischen Pool (M1). Kredit-Besicherung entfällt; die Handelsliquidität stammt von Liquiditätsanbietern (M2). Der Tausch erfolgt atomar in einer Transaktion, zu Protokollgebühren im Promille- bis Prozentbereich zuzüglich Netzwerkgebühren (M3); der Zugang ist genehmigungsfrei (M4). Das Risikoprofil (M5) gliedert sich in technische Risiken (Smart-Contract-Fehler, Preismanipulation über Orakel und dünne Liquidität — vgl. den bZx-Fall in 3.5.2), ökonomische Risiken (impermanenter Verlust der Liquiditätsanbieter, Slippage) und Governance-Risiken (Gebühren- und Parameterhoheit der Token-Inhaber). Aufsichtsrechtlich sind DEX-Protokolle mangels zentraler Betreiber bislang schwer zu fassen (M6, Abschnitt 4.5.2).

### 3.5.4. Derivate

Derivate sind Finanzinstrumente, deren Wert vom Wert anderer Assets abhängt. Im traditionellen Finanzsystem sind z. B. Aktienoptionen Derivate, die vom Preis einer zugrunde liegenden Aktie abhängen; grundsätzlich können Derivate von jeder messbaren Variable wie Rohstoffpreisen, Zinsraten oder Strompreisen abgeleitet werden [vgl. 72]. Ähnlich wie traditionelle Derivate können Optionen oder Futures auch dezentral in Smart Contracts gehandelt werden. Der weit überwiegende Teil des Derivatehandels findet auf zentralen Börsen wie der Chicago Board of Trade (CBOT) statt [vgl. 121]; es existieren jedoch DeFi-Protokolle, die den Derivatehandel dezentralisieren. Auch im Kryptomarkt stellt der Derivatehandel — gemessen am Handelsvolumen — inzwischen den größten Teilmarkt: Allein Perpetual-Futures setzen an zentralen Kryptobörsen monatlich über drei Billionen US-Dollar um [vgl. 108]. Er wird deshalb nachfolgend ausführlicher behandelt: zuerst Futures und Perpetual Swaps, anschließend deren DeFi-Umsetzung.

**Futures.** Futures sind Vereinbarungen, ein Asset zu einem bestimmten Zeitpunkt in der Zukunft zu einem bestimmten Preis zu kaufen [vgl. 72]. Die ursprüngliche Anwendung war die Reduktion des Preisrisikos von Landwirten und Händlern [vgl. 39]: Ein Händler kann im Januar an einer Börse wie der CME Group 5.000 Scheffel Mais zur Lieferung im Mai kaufen (Long-Position), während ein anderer zur gleichen Zeit verkaufen möchte (Short-Position); durch den elektronischen Handel wird ein Preis zwischen beiden Positionen festgelegt. Da Future-Verträge meist Spekulationen über den zukünftigen Preis sind, werden die Positionen in der Regel vor Lieferung geschlossen; Gewinn oder Verlust hängt von der Preisentwicklung zwischen Öffnen und Schließen ab [vgl. 72]. Neben der Risikoreduktion werden Futures primär für Spekulations- und Arbitragegeschäfte verwendet [vgl. 39].

Das Synthetix-Protokoll implementiert Derivate als dezentrale Blockchain-Anwendung: Nutzer können synthetische Derivate („Synths“), die an den Wert zugrunde liegender Assets gekoppelt und durch Sicherheiten gedeckt sind, veröffentlichen und handeln. Die Liquidität stammt aus einem Pool hinterlegter Sicherheiten. Grundsätzlich kann zu jedem Asset ein synthetisches Derivat geschaffen werden; praktisch basieren die Synths auf Preisen von Krypto-Assets, Währungen und Gold. Um Synths zu erzeugen, müssen Nutzer den protokolleigenen SNX-Token erwerben und zu einer Besicherungsquote von 400 % hinterlegen — SNX im Wert von 400 Euro für Synths im Wert von 100 Euro (Stand der Protokollversion v2; auf Layer-2-Netzwerken 500 %) [106, vgl. 25]. Die hohe Quote dient der Absicherung stark schwankender Synths.

**Perpetual Swaps.** Perpetual Swaps sind mit Futures vergleichbar, haben jedoch kein Ablaufdatum. Investoren können damit auf Kursbewegungen von Krypto-Assets spekulieren, ohne ein Fälligkeitsdatum festzulegen — auf steigende wie fallende Kurse, auch gehebelt. Da es kein Fälligkeitsdatum gibt, muss das gehebelte Kapital nicht zurückgezahlt, sondern nur verzinst werden; deshalb werden Perpetual Swaps auch als ewige Anleihen

bezeichnet [vgl. 11].

**Merkmalsprofil (M1–M6).** Derivate-Protokolle ersetzen Terminbörse und zentrales Clearing durch besicherte Smart-Contract-Pools (M1). Die Besicherung erfolgt durch teils sehr hohe Übersicherung mit protokolleigenen Token (Synthetix: 400 %) (M2). Der Handel ist kontinuierlich und global möglich (M3); der Zugang ist genehmigungsfrei — das *Erzeugen* synthetischer Positionen setzt allerdings den Erwerb und die Hinterlegung protokolleigener Token voraus, der Handel bereits emittierter Synths nicht (M4). Das Risikoprofil (M5) gliedert sich in technische Risiken (Orakel-Abhängigkeit der Preisreferenzen), ökonomische Risiken (Volatilität der Sicherheiten, Hebeleffekte) und Governance-Risiken (Parametrisierung von Quoten und Gebühren durch die Protokoll-Governance); die aufsichtsrechtliche Einordnung des dezentralen Derivatehandels ist ungeklärt (M6, Abschnitt 4.5.2).

### 3.5.5. Blockchain-basierte Vermögensverwaltung

On-Chain Asset Management ermöglicht es Investoren, diversifiziert in unterschiedliche Krypto-Assets zu investieren, ohne einzelne Assets selbst halten zu müssen. Traditionelle Vermögensverwalter verwahren die Guthaben ihrer Kunden bei einer Verwahrstelle wie einer Depotbank; bei Blockchain-basierter Verwaltung werden die Assets stattdessen in einem Smart Contract verwahrt. Das Portfolio-Management kann passiv durch programmierte Strategien erfolgen oder aktiv durch Portfoliomanager, die ähnlich wie Fondsmanager arbeiten [vgl. 100, S. 153–174].

Die Parallele zum klassischen Finanzmarkt liefern börsengehandelte Indexfonds (ETFs) als Vorlage passiv gemanagter Verwaltung, während aktiv gemanagte Portfolios dem System aktiv gemanagter Fonds folgen. Deren Manager sind durch vordefinierte Regeln gebunden, die vor Auflage definiert und durch Smart Contracts durchgesetzt werden — ein Portfoliomanager wird technisch zum Einhalten der Strategie gezwungen. Jeder Fonds hat ein Risikoprofil und einen festgelegten Absicherungsanteil, der das Investitionsrisiko reduzieren, aber auch die mögliche Rendite mindern kann [vgl. 98, S. 130].

Die Funktionsweise ähnelt dem klassischen Investmentfonds: Der Investor hinterlegt Krypto-Assets in einem Smart Contract und erhält dafür Fonds-Token, die sein anteiliges Eigentum am Fondsvolumen abbilden [vgl. 100, S. 153–174]. Die Strategien entstehen durch Transaktionen auf anderen DeFi-Protokollen; Erträge stammen aus Zinsen auf das eingelegte Kapital oder Token-Vergütungen anderer Protokolle — vom einfachen Portfolio-Rebalancing bis zu komplexen Ertragsmaximierungsstrategien [vgl. 121].

Als Beispiel dient Yearn Finance: Zahlt ein Investor etwa den Stablecoin USDC ein, erhält er den Protokoll-Token yUSDC als Eigentumsnachweis am Pool. Der Smart Contract legt das Kapital in demjenigen Protokoll an, das aktuell die höchsten Erträge bietet. Der Investor muss also nicht täglich die Konditionen mehrerer Protokolle vergleichen und

umschichten — was sich für Privatanleger wegen der Transaktionskosten ohnehin nicht lohnen würde; durch das Umschichten auf Fondsebene verteilen sich diese Kosten auf alle Investoren [vgl. 14]. Zur Auflösung gibt der Investor seine yUSDC-Token zurück und erhält Einlage plus Erträge.

Den passiv gemanagten Pools stehen die Yearn Vaults gegenüber, die aktiv gemanagte Strategien umsetzen — etwa die Erzielung von Erträgen aus Liquiditätspools von Curve Finance [vgl. 14]. Anfang 2023 verdienten Liquiditätsanbieter im crvCOMP-Pool beispielsweise ca. 12,82 % jährliche Rendite (APY) aus Handelsgebühren und zusätzlich 24,72 % APY an Belohnungen im Governance-Token CRV, sofern sie ihre LP-Token im „Curve Gauge“ hinterlegten — einem Smart-Contract-System zur Verteilung von Belohnungen an Liquiditätsanbieter, dessen Mechanik die Curve-Dokumentation beschreibt [vgl. 41]. Durch Hinterlegen der CRV-Belohnungen in einem weiteren Modul ließ sich die Rendite auf bis zu 61,81 % APY steigern, abhängig von Einzahlung und Poolgröße [vgl. 40]. Die genannten Renditewerte geben den Datenstand der Erstfassung wieder (Anfang 2023); die seinerzeit genutzte Übersichtsseite ist nicht mehr abrufbar. Sie sind Momentaufnahmen und illustrieren die Mechanik, nicht dauerhaft erzielbare Renditen. Schließt der Investor seine Position, werden die Fonds-Token an den Smart Contract zurückgegeben und vernichtet („verbrannt“); sein Anteil wird auf einer DEX verkauft und ihm gutgeschrieben [vgl. 100, S. 153–174].

**Merkmalsprofil (M1–M6).** On-Chain-Vermögensverwaltung ersetzt Fondsmanager, Depotbank und Verwahrstelle durch Smart-Contract-Vaults mit einprogrammierten Anlageregeln (M1). Die Einlagen selbst liegen als Sicherheit im Contract; eine gesonderte Besicherung entfällt (M2). Strategien werden automatisiert ausgeführt, Umschichtungskosten auf alle Anleger verteilt (M3); der Zugang ist genehmigungsfrei ab Kleinstbeträgen (M4). Das Risikoprofil (M5) kumuliert technisch die Smart-Contract-Risiken aller genutzten Protokolle — die Zusammensetzbarkeit, die die Renditestrategien ermöglicht, vervielfacht die Angriffsfläche —, ökonomisch das Markt- und Strategierisiko der gewählten Anlagepolitik und auf Governance-Ebene das Risiko nachträglicher Regel- oder Strategieänderungen. Eine der Fondsregulierung (Verwahrung, Prospektpflichten) vergleichbare Aufsicht existiert nicht (M6, Abschnitt 4.5.2).

### 3.5.6. Staking

In Abschnitt 2.4 wurde die theoretische Grundlage zu Proof-of-Stake-Blockchains gelegt, die die Voraussetzung für Staking bilden. Die Ethereum-Blockchain hat ihr Konsensprotokoll im September 2022 („Merge“) von PoW zu PoS gewechselt. Proof-of-Stake-Blockchains benötigen Validatoren, um einen verteilten Konsens im Netzwerk zu erreichen. Diese Validatoren setzen Kapital in Form von Ether ein und übernehmen die Aufgaben, die Miner in einer Proof-of-Work-Blockchain haben: das Validieren von Transaktionen sowie

das Erstellen und Anhängen von Blöcken. Ein Nutzer muss mindestens 32 ETH einsetzen (staken), um Validator zu werden; bei jeder Blockerstellung wird ein Validator zufällig ausgewählt [vgl. 118].

Die übrigen Validatoren prüfen und bestätigen die korrekte Blockerstellung. Das eingesetzte Kapital dient als Anreiz, nicht böswillig zu handeln: Bei Fehlversuchen — etwa wenn ein Validator offline geht — können Teile des Stakes einbehalten werden; vorsätzlich böswilliges Verhalten kann zur Konfiszierung des gesamten Einsatzes führen („Slashing“). Der Anreiz zu staken ist der monetäre Ertrag: Jede Blockerstellung und Validierung generiert Erträge, die dem Validator in Form von Token ausgeschüttet werden [vgl. 118].

Der Mindesteinsatz von 32 ETH hindert viele potenzielle Teilnehmer an der direkten Teilnahme. Dieses Problem lösen Staking-Pools: Anleger legen Kapital in einem Smart Contract ein, der Pool agiert als Validator, und die Erträge werden proportional zum hinterlegten Kapital ausgeschüttet [vgl. 68].

**Entwicklungen seit der Erstfassung (2023–2026).** *Dieser Absatz ist eine Ergänzung der überarbeiteten Fassung.* Aus den Staking-Pools hat sich mit dem Liquid Staking eine der beiden kapitalstärksten DeFi-Kategorien entwickelt — mit rund 35 Mrd. US-Dollar gebundenem Kapital knapp hinter dem Lending (rund 41 Mrd.; Stand: 03.08.2026) [45]: Protokolle wie Lido geben für gestakte ETH einen liquiden Vertreter-Token (z. B. stETH) aus, der die Staking-Erträge fortlaufend abbildet und zugleich in anderen DeFi-Protokollen als Sicherheit oder Handelsgut einsetzbar bleibt — die Einlage ist also nicht mehr gebunden. Darauf aufbauend entstand ab 2023 das Restaking (prominentester Vertreter: EigenLayer), bei dem bereits gestakte ETH zusätzlich zur Absicherung weiterer Dienste eingesetzt werden — was die Kapitaleffizienz erhöht, aber Risiken kaskadiert, weil derselbe Einsatz mehrere Systeme gleichzeitig besichert. Die Größenordnungen belegen die Bedeutung: Lido ist mit rund 17,6 Mrd. US-Dollar das kapitalstärkste DeFi-Protokoll überhaupt, das Restaking-Protokoll EigenLayer (inzwischen EigenCloud) bindet rund 5,0 Mrd. US-Dollar (Stand: 02.08.2026) [46].

**Merkmalsprofil (M1–M6).** Staking hat keine direkte Entsprechung im traditionellen Finanzwesen; am ehesten ersetzt es die Kombination aus verzinslicher Einlage und dem Betrieb von Finanzinfrastruktur (M1). Der Stake selbst ist die Besicherung — Fehlverhalten wird durch Slashing sanktioniert (M2). Erträge stammen aus Protokollemission und Gebühren und fallen laufend an (M3); der Zugang erfordert 32 ETH oder die Teilnahme an Pools bzw. Liquid-Staking-Protokollen (M4). Das Risikoprofil (M5) gliedert sich in technische Risiken (Slashing durch Fehlbetrieb, Smart-Contract-Fehler der Pool-Protokolle), ökonomische Risiken (Kursrisiken der Vertreter-Token, kaskadierte Besicherung beim Restaking) und Governance-Risiken (Zentralisierungstendenzen großer Anbieter mit Einfluss auf den Konsens). Die aufsichtsrechtliche Einordnung von Staking-Erträgen und -Diensten ist im Fluss (M6, Abschnitte 4.5.2 und 5.2.3).

### 3.5.7. Versicherungs- und Absicherungsprodukte

*(Ergänzung der überarbeiteten Fassung: führt die Kategorie der Fallstudien aus Abschnitt 4.4 bereits in den Grundlagen ein.)*

Auch das Versicherungsgeschäft lässt sich dezentral abbilden. Zwei Ansätze haben sich herausgebildet: Erstens kapitalgedeckte Risiko-Pools, bei denen Mitglieder Kapital einlegen, um definierte Risiken — typischerweise Smart-Contract-Fehler anderer Protokolle — gemeinschaftlich zu decken; über Auszahlungen im Schadensfall entscheidet eine Governance-Abstimmung der Mitglieder oder ein Orakel-Mechanismus. Der bekannteste Vertreter ist Nexus Mutual [vgl. 83]. Zweitens optionsbasierte Absicherung: Protokolle wie Opyn bilden Put- und Call-Optionen als Smart Contracts ab — funktional ein Spezialfall der Derivate aus Abschnitt 3.5.4, der zur Absicherung von Preis- und Protokollrisiken eingesetzt werden kann. Beide Ansätze werden in Abschnitt 4.4 als Fallstudien vertieft.

**Merkmalsprofil (M1–M6).** Absicherungsprotokolle ersetzen Versicherer und Rückversicherung durch kapitalgedeckte Risiko-Pools mit tokenisierten Ansprüchen (M1). Die Deckung ist vollständig durch eingezahltes Kapital besichert, nicht durch versicherungsmathematische Reserven (M2). Prämien bilden sich nachfragegetrieben; die Auszahlung erfolgt nach Governance- oder Orakel-Entscheid (M3). Der Zugang ist grundsätzlich genehmigungsfrei — mit Ausnahme mitgliedschaftsbasierter Modelle, die eine Identitätsprüfung verlangen (Abschnitt 4.4.1) —, die Deckungssumme jedoch durch die Poolgröße begrenzt (M4). Das Risikoprofil (M5) gliedert sich in technische Risiken (Smart-Contract-Fehler des Absicherungsprotokolls selbst), ökonomische Risiken (Unterdeckung bei korrelierten Schäden) und Governance-Risiken (Ermessen bei der Schadensfeststellung). Aufsichtsrechtlich fehlt bislang eine Einordnung als Versicherungsgeschäft (M6, Abschnitt 4.5.2).

# 4. DeFi in der Praxis

## 4.1. Auswahl der Fallstudien und Vorgehen

In den folgenden Abschnitten werden wichtige DeFi-Protokolle als Fallstudien untersucht. Die Auswahl folgt den in Abschnitt 1.3 definierten Kriterien: Marktbedeutung (nach TVL zu den führenden der Kategorie zählend, Stand der Erstfassung Anfang 2023), Marktbestand von mindestens zwei Jahren und öffentlich verfügbare Primärdokumentation. Untersucht werden je zwei Protokolle aus drei Anwendungskategorien des Kapitels 3.5: Kreditvergabe (Aave, Compound), dezentrale Handelsplätze (Uniswap, PancakeSwap) sowie Versicherungs- und Absicherungsprodukte (Nexus Mutual, Opyn). Die in Abschnitt 1.3 transparent gemachte Abweichung — Curve führte Anfang 2023 die DEX-Kategorie nach TVL an — wird in Abschnitt 4.3 aufgegriffen. Eine zweite Abweichung ist hier offenzulegen: Opyn zählte Anfang 2023 nach TVL nicht zu den führenden Protokollen seiner Kategorie, wurde aber als einer der wenigen etablierten Vertreter der optionsbasierten Absicherung einbezogen (Abschnitt 3.5.7); gerade sein weiterer Verlauf erweist sich als analytisch aufschlussreich (Abschnitt 4.4.2).

Das Vorgehen ist für alle Fallstudien gleich: Jedes Protokoll wird beschrieben, entlang der Merkmale M1–M6 (Abschnitt 1.3) eingeordnet und seine Marktstellung wird zum Stand der Erstfassung (Anfang 2023) und zum Stand dieser überarbeiteten Fassung (02.08.2026) ausgewiesen; Datenquelle ist durchgängig der eingecheckte DeFiLlama-Protokoll-Snapshot [46]. TVL-Angaben sind kaufmännisch gerundet und summieren, wo nicht anders ausgewiesen, alle Versionen eines Protokolls. Abschnitt 4.7 wertet die Fallstudien vergleichend aus.

## 4.2. Kreditvergabe

Die Kategorie folgt dem Merkmalsprofil aus Abschnitt 3.5.2: Kreditintermediation ohne Bank, Überbesicherung statt Bonitätsprüfung, algorithmische Zinsbildung.

### 4.2.1. Aave

Aave ist ein dezentrales Finanzprotokoll, das es Benutzern ermöglicht, Kredite aufzunehmen oder zu vergeben, ohne dass eine zentrale Partei als Vermittler benötigt wird [vgl. 2]. Das

Protokoll wurde auf der Ethereum-Blockchain gestartet und ist vollständig quelloffen — jeder Benutzer kann den Code einsehen und überprüfen [vgl. 3].

Das Aave-Protokoll ermöglicht es Benutzern, eine Vielzahl von Vermögenswerten als Sicherheit zu hinterlegen, darunter Ether und verschiedene ERC-20-Token. Die Höhe des möglichen Kredits hängt vom Wert der hinterlegten Sicherheiten und deren Liquidationsschwellen ab (Health Factor, Formel 3.1). Das früher zusätzlich angebotene Stable-Rate-Modell (fester Zinssatz) wurde im November 2023 protokollweit deaktiviert und später vollständig entfernt — Kredite werden heute ausschließlich variabel verzinst [vgl. 1]. Ein zentrales Merkmal von Aave ist die Vergabe von Flash Loans (Abschnitt 3.5.2), die das Protokoll als einer der ersten Anbieter eingeführt hat. Über „Credit Delegation“ können Kreditlinien an Dritte delegiert werden, ohne dass diese selbst Sicherheiten hinterlegen [vgl. 2]. Liquiditätsanbieter können zusätzlich den Governance-Token AAVE verdienen, der Stimmrechte über Protokolländerungen verleiht.

**Entwicklung seit 2023.** Aave hat seine Marktführerschaft ausgebaut: Version v3 (seit 2022, mit Effizienzmodus und Isolationsmechanismen für riskantere Sicherheiten) hält mit rund 13,9 Mrd. US-Dollar TVL den mit Abstand größten Anteil der Kategorie; eine vierte Protokollgeneration (v4) mit Hub-and-Spoke-Architektur durchlief 2025 die Testnetzphase und ging 2026 auf dem Mainnet in Betrieb (rund 0,2 Mrd. US-Dollar TVL), und mit „Horizon“ adressiert Aave die Tokenisierung realer Vermögenswerte (Real World Assets, tokenisierte reale Vermögenswerte wie Anleihen und Fonds; rund 0,26 Mrd. US-Dollar; alle Werte Stand 02.08.2026, Summe über alle Versionen — v3 13,9, Horizon 0,26, v2/v1-Restbestände 0,1 sowie kleinere Instanzen — rund 14,4 Mrd.) [46, vgl. 1]. Aave ist damit das nach TVL größte Kreditprotokoll und liegt unter den DeFi-Protokollen — ohne die von Datenanbietern mitgeführten zentralen Verwahrbestände — nur hinter dem Liquid-Staking-Protokoll Lido [46].

### 4.2.2. Compound

Die Compound-Plattform ist ein DeFi-Protokoll, das es Benutzern ermöglicht, Kredite zu vergeben und aufzunehmen, indem Kryptowährungen als Sicherheit hinterlegt werden [vgl. 35]. Compound ist auf der Ethereum-Blockchain aufgebaut; Benutzer hinterlegen ERC-20-Token als Sicherheit, um Kredite in anderen ERC-20-Token zu erhalten. Anders als im traditionellen Kreditgeschäft, in dem ein einzelner Kreditgeber das Ausfallrisiko trägt, teilen sich bei Compound die Einleger eines Pools das Risiko und die Zinserträge (gepoolter Collateralized Debt Market, Abschnitt 3.5.2).

Ein zentraler Aspekt der Plattform ist die jederzeitige Verfügbarkeit: Es gibt keine festen Laufzeiten; Benutzer können ihre Schulden jederzeit begleichen und ihre Einlagen abheben. Die Zinssätze werden algorithmisch durch Angebot und Nachfrage — den Nutzungsgrad des Pools — bestimmt und passen sich fortlaufend an [vgl. 35]. Inhaber des Governance-

Tokens COMP stimmen über Protokolländerungen ab. Über API-Schnittstellen können Entwickler Compound in eigene Anwendungen integrieren — Compound war damit ein früher Baustein der Zusammensetzbarkeit (Abschnitt 3.3).

**Entwicklung seit 2023.** Compound hat seine einstige Stellung als zweitgrößtes Kreditprotokoll verloren: Mit rund 1,2 Mrd. US-Dollar TVL (v2 und v3 zusammen, Stand 02.08.2026) liegt es deutlich hinter Aave (rund 14,4 Mrd.) und wurde zudem vom Wettbewerber Morpho überholt (2022 als Optimierungsschicht über Aave und Compound gestartet, seit Januar 2024 mit „Morpho Blue“ eigenständige Kreditinfrastruktur [vgl. 79]; rund 7,6 Mrd.) [46]. Der Fall illustriert, dass Marktpositionen im DeFi-Sektor nicht dauerhaft gesichert sind — der Wettbewerb findet auf Protokollebene statt und Kapital wandert schnell (vgl. Abschnitt 4.7).

**Vergleich der Kategorie.** Beide Protokolle setzen dasselbe Grundmodell um (M1: Kreditintermediation durch Smart-Contract-Pools; M2: Überbesicherung mit automatischer Liquidation; M4: genehmigungsfreier Zugang). Auch bei Kosten und Geschwindigkeit (M3) gleichen sie sich: Kredite sind ohne Antragsprozess sofort verfügbar, die Kosten bestehen aus algorithmisch bestimmten Zinsen plus Netzwerkgebühren. Unterschiede liegen im Produktspektrum: Aave bietet mehr (Flash Loans, Credit Delegation, RWA-Vorstöße), Compound das puristischere Pool-Modell. Die Risikoprofile (M5) sind strukturgleich — technisch dominieren Smart-Contract- und Orakelrisiken, ökonomisch die Liquidationsrisiken volatiler Sicherheiten, auf Governance-Ebene die Parameterhoheit der Token-Inhaber. Die Marktentwicklung 2023–2026 zeigt eine deutliche Konzentration auf den Marktführer.

## 4.3. Dezentrale Handelsplätze

Die Kategorie folgt dem Merkmalsprofil aus Abschnitt 3.5.3. Zur Einordnung der Auswahl: Anfang 2023 führte Curve die Kategorie nach TVL an; Uniswap wurde dennoch als Fallstudie gewählt (Referenzimplementierung des CFMM, höchstes Handelsvolumen), PancakeSwap als Vertreter einer zweiten Blockchain (Abschnitt 1.3). Die Marktentwicklung bis 2026 hat die Kategorieführung erneut verschoben: Zum Stand 02.08.2026 liegt Uniswap (alle Versionen zusammen rund 3,1 Mrd. US-Dollar TVL) wieder vor Curve (rund 1,3 Mrd.); PancakeSwap hält rund 2,1 Mrd. US-Dollar [46].

### 4.3.1. Uniswap

Das Uniswap-Protokoll nutzt einen Automated Market Maker (AMM, Abschnitt 3.5.3): Für jedes unterstützte Handelspaar existiert ein Liquiditätspool, der von Benutzern befüllt wird; der Tauschpreis ergibt sich algorithmisch aus der Poolzusammensetzung nach dem Constant-Product-Modell (Formel 3.2) [vgl. 117]. Liquiditätsanbieter erhalten einen Anteil der Handelsgebühren; Inhaber des Governance-Tokens UNI stimmen über Protokolländerungen

ab. Uniswap stellt zudem offene Schnittstellen bereit, auf denen zahlreiche Anwendungen aufbauen — von Aggregatoren bis zu komplexeren Finanzinstrumenten auf Basis der Liquiditätspools.

Für Liquiditätsanbieter ist neben den Gebührenerträgen der in Abschnitt 3.5.3 eingeführte impermanente Verlust relevant, der sich am Constant-Product-Modell quantifizieren lässt: Verdoppelt sich der Preis eines der beiden Pool-Token relativ zum anderen, liegt der Wert der Pool-Position rund 5,7 % unter dem bloßen Halten beider Token; bei einer Vervierfachung sind es bereits rund 20 % (eigene Berechnung nach der Konstantprodukt-Formel; ohne Berücksichtigung der Gebührenerträge, die den Verlust kompensieren können) [vgl. 9]. Die Bereitstellung von Liquidität ist also keine risikolose Zinsanlage, sondern eine Position mit eigenem Marktrisiko.

**Entwicklung seit 2023.** Uniswap hat seit dem v2-Modell mit einheitlichen Pools zwei Generationswechsel vollzogen: Version v3 (2021) führte konzentrierte Liquidität ein — Anbieter können ihre Liquidität auf Preisbereiche beschränken und so kapitaleffizienter einsetzen —, Version v4 (Januar 2025) ergänzte sogenannte Hooks, mit denen Entwickler Pools um eigene Logik (z. B. dynamische Gebühren oder Limit-Orders) erweitern können [vgl. 117]. Zum Stand 02.08.2026 verteilt sich der TVL auf v3 (1,43 Mrd. US-Dollar), v4 (0,82 Mrd.) und v2 (0,80 Mrd.) — zusammen die in Tabelle 4.1 ausgewiesenen rund 3,1 Mrd. [46].

### 4.3.2. PancakeSwap

PancakeSwap ist ein dezentrales Börsenprotokoll, das im September 2020 auf der BNB Chain (vormals Binance Smart Chain) gestartet ist und dem AMM-Modell von Uniswap folgt — die Gemeinsamkeit liegt im Funktionsprinzip, nicht in der zugrunde liegenden Blockchain. Es ermöglicht Nutzern, Kryptowährungen direkt zu tauschen, ohne dass eine zentrale Börse benötigt wird, und entwickelte sich schnell zum meistgenutzten DEX-Protokoll der BNB Chain.

Auch dieses Protokoll stellt Liquidität über Pools bereit: Nutzer legen Kryptowährungen ein und erhalten dafür einen Anteil der Handelsgebühren. Darüber hinaus setzt PancakeSwap stark auf Anreizprogramme: Beim Yield Farming hinterlegen Nutzer ihre Liquiditäts-Zertifikate (LP-Token) in Farming-Pools und erhalten zusätzliche Erträge im protokolleigenen Token CAKE; in „Syrup Pools“ können CAKE-Token gestakt werden, um weitere Token zu verdienen. PancakeSwap ist damit zugleich ein Beispiel für die tokenbasierte Anreizökonomie vieler DeFi-Protokolle — und für deren Verwässerungsrisiken (M5, Governance/Ökonomie).

**Entwicklung seit 2023.** PancakeSwap ist längst nicht mehr auf die BNB Chain beschränkt, sondern auf mehreren Blockchains aktiv (u. a. Ethereum und diverse Layer-2-Netzwerke); mit Version v3 (2023) übernahm es das Modell konzentrierter Liquidität; die

Nachfolgegeneration „Infinity“ (vormals v4) ist seit April 2025 produktiv [vgl. 90], hält aber bislang nur rund 0,07 Mrd. US-Dollar TVL. Insgesamt liegt der TVL bei rund 2,1 Mrd. US-Dollar über alle Versionen (Stand: 02.08.2026) [46].

**Vergleich der Kategorie.** Beide Protokolle teilen das AMM-Grundmodell (M1: Börse und Market Maker werden durch den Pool ersetzt; M4: genehmigungsfrei) und haben sich technisch konvergent entwickelt (konzentrierte Liquidität, Multichain-Präsenz). Die Handelskosten (M3) liegen bei beiden in gestaffelten Gebührenstufen im Promille- bis Prozentbereich zuzüglich Netzwerkgebühren, bei atomarer Abwicklung in einer Transaktion. Unterschiede liegen in der Herkunfts-Blockchain und der Anreizpolitik: Uniswap setzt auf minimale Protokoll-Eingriffe und Entwickler-Erweiterbarkeit (Hooks), PancakeSwap auf breite Token-Anreizprogramme. Das Risikoprofil (M5) ist strukturgleich (Smart Contract, Orakel/Preismanipulation, impermanenter Verlust); bei PancakeSwap tritt die Abhängigkeit von der Token-Emissionspolitik hinzu.

### 4.3.3. Entwicklung der Kategorie seit der Erstfassung: Perpetual-DEXs und Hyperliquid

*(Ergänzung der überarbeiteten Fassung: Der Abschnitt ergänzt die 2023 ausgewählten Spot-Fallstudien um die seither bedeutendste Entwicklung der Börsenkategorie; er ist keine nachträgliche Fallstudie, da die Auswahlsystematik aus Abschnitt 4.1 auf dem Stichtag der Erstfassung beruht.)*

Die Fallstudien dieser Kategorie sind Spot-Börsen nach dem AMM-Modell. Seit der Erstfassung hat sich das Gewicht des dezentralen Handels jedoch deutlich in Richtung Derivate verschoben — konkret zu den in Abschnitt 3.5.4 eingeführten Perpetual-Kontrakten. Prägend für diese Entwicklung ist Hyperliquid, eine 2023 gestartete dezentrale Derivatebörse, die architektonisch einen Gegenentwurf zum AMM darstellt: Statt eines Liquiditätspools mit Preisformel betreibt das Protokoll ein vollständig On-Chain geführtes zentrales Limit-Orderbuch auf einer eigens dafür entwickelten Layer-1-Blockchain (Konsensverfahren HyperBFT); das Funding der Perpetual-Kontrakte wird stündlich zwischen Long- und Short-Seite verrechnet, berechnet aus der Abweichung des Kontraktpreises von einem Spot-Orakelpreis [vgl. 73].

Für das Analyseraster heißt das: Die Intermediärfunktion der Börse (M1) wird hier nicht durch einen Pool, sondern durch protokollbasiertes Matching ersetzt — das Marktmodell der traditionellen Terminbörse, ausgeführt ohne deren Betreiber; die Rolle des Market Makers übernimmt teilweise ein gemeinschaftlich befüllter Market-Making-Vault (HLP), dessen Erträge und Verluste die Einleger tragen. Die Handelskosten (M3) folgen einer Maker/Taker-Gebührenstaffel wie an zentralen Terminbörsen, die Abwicklung erfolgt mit Blockzeiten im Subsekundenbereich [vgl. 73]. Bemerkenswert ist auch das Verteilungsmodell: Das Protokoll verzichtete auf Risikokapitalfinanzierung und teilte bei der Einführung des

eigenen Tokens am 29. November 2024 rund 31 % des Bestands direkt den Nutzern zu [vgl. 15].

Die Marktbedeutung ist erheblich: Im März 2026 wickelte Hyperliquid ein Monatsvolumen von knapp 200 Mrd. US-Dollar ab — knapp 6 % des globalen Perpetual-Handels einschließlich der zentralen Börsen (nach etwa 3,5 % ein Jahr zuvor) und mit Abstand der größte Anteil des dezentralen Perpetual-Handels [109, vgl. 108]. Im Protokoll-Snapshot dieser Arbeit stehen die Brücken-Einlagen der Börse bei rund 5,9 Mrd. US-Dollar, das DeFi-Ökosystem der zugehörigen Blockchain bei rund 1,2 Mrd. US-Dollar (Stand: 02.08.2026) [46, 44]. Die Erstfassung hatte den Derivatehandel noch als Randerscheinung des DeFi-Sektors behandelt (Abschnitt 3.5.4) — inzwischen ist er ein tragender Teil des dezentralen Handelsgeschehens.

Zugleich illustriert der Fall die Grenzen der Dezentralität (M1/M5) schärfer als die AMM-Fallstudien: Im März 2025 geriet der HLP-Vault durch eine gezielte Preismanipulation des Memecoins JELLY zeitweise mit rund 13,5 Mio. US-Dollar in Rückstand; die kleine Validatorenmenge der Blockchain stimmte daraufhin kurzfristig dafür, den Kontrakt vom Handel zu nehmen und zu einem für den Vault vorteilhaften Preis abzurechnen — Nutzer wurden entschädigt, doch der Eingriff zeigte, dass ein handlungsfähiges Governance-Gremium Marktergebnisse nachträglich korrigieren kann [vgl. 32]. Was im Krisenfall Verluste begrenzt, relativiert zugleich das Kernversprechen der Neutralität — dieselbe Spannung zwischen Dezentralitätsanspruch und faktischer Steuerbarkeit, die Abschnitt 4.5.1 als Governance-Risiko systematisiert. Aufsichtsrechtlich gilt das in Abschnitt 4.5.2 Gesagte entsprechend: Als Protokoll ohne zentralen Betreiber ist Hyperliquid von MiCA nicht erfasst; der Handel mit gehebelten Kontrakten wäre bei zentralen Anbietern hingegen erlaubnispflichtig — die Kategorie verschärft damit die dort beschriebene Regulierungslücke.

## 4.4. Versicherungs- und Absicherungsprodukte

Die Kategorie folgt dem Merkmalsprofil aus Abschnitt 3.5.7: kapitalgedeckte Risiko-Pools bzw. optionsbasierte Absicherung statt klassischer Versicherer.

### 4.4.1. Nexus Mutual

Nexus Mutual ist ein dezentrales Absicherungsprotokoll auf der Ethereum-Blockchain, das 2018 von Hugh Karp gegründet wurde [vgl. 83]. Es folgt dem Konzept der Versicherungsgegenseitigkeit („mutual insurance“): Die Mitglieder tragen Risiken gemeinsam und sichern sich gegenseitig ab. Mitglied wird, wer den protokolleigenen Token NXM erwirbt — dies setzt bei Nexus Mutual eine Identitätsprüfung (KYC) voraus, womit das Protokoll bewusst von der sonst üblichen Genehmigungsfreiheit abweicht (M4).

Abgesichert werden vor allem Risiken aus dem DeFi-Umfeld selbst: Das aktuelle Produktspektrum umfasst Deckungen gegen Fehlfunktionen und Exploits von DeFi-Protokollen (Protocol Cover), Ausfälle von Verwahrstellen (Custody Cover), Stablecoin-Depegs (Depeg Cover) sowie Slashing-Risiken von Validatoren [vgl. 85]. Die Prämien richten sich nach der Nachfrage und dem Kapital, das Mitglieder auf das jeweilige Risiko staken; über Schadensfälle entscheiden die Mitglieder in einem Governance-Verfahren [vgl. 85]. Damit spielen die Nutzer eine aktive Rolle in Risikoprüfung und Schadensregulierung — die klassischen Kernfunktionen eines Versicherers werden auf die Gemeinschaft verlagert (M1). Die 2023 angekündigte Ausweitung auf Risiken außerhalb des Kryptoumfelds wurde mit einer Kooperation mit dem regulierten Rückversicherungsdienstleister Ensuro (2024) begonnen [vgl. 84], blieb bislang aber ohne wesentliche Marktbedeutung; die gezeichneten Deckungen konzentrieren sich weiterhin auf On-Chain-Risiken (vgl. den Prognosen-Check in Abschnitt 6.2).

**Entwicklung seit 2023.** Nexus Mutual bleibt der führende Vertreter der Kategorie, allerdings auf niedrigem Niveau: Der TVL — der Kapitalpool der Gegenseitigkeit; die aktiv gezeichnete Deckungssumme liegt darunter — beträgt rund 0,09 Mrd. US-Dollar (Stand: 02.08.2026) [46]. Gegenüber den Kredit- und Handelskategorien ist die Absicherungskategorie klein geblieben; gemessen am abzusichernden Kapital des Gesamtmarkts (TVL rund 74 Mrd. US-Dollar) deckt der Sektor nur einen Bruchteil ab. Das Missverhältnis wird in der Risikoanalyse (4.5.1) und der Bewertung (Kapitel 5) aufgegriffen.

### 4.4.2. Opyn

Opyn wurde 2019 gegründet und basiert auf der Ethereum-Blockchain. Opyn ist kein Versicherungs-, sondern ein **Optionsprotokoll**: Es bildet Put- und Call-Optionen als Smart Contracts ab — Put-Optionen geben das Recht, ein Asset zu einem festgelegten Preis zu verkaufen, Call-Optionen das Recht, es zu kaufen (Abschnitt 3.5.4). Solche Optionen *können* zur Absicherung eingesetzt werden (etwa ein Put als Absicherung gegen Kursverluste einer Position), sind aber Derivate mit eigenständigem Risikoprofil und setzen — anders als eine Versicherung — kein versichertes Interesse voraus. Die Preisbildung orientiert sich an der Volatilität des zugrunde liegenden Assets. Nutzer konnten so beispielsweise Positionen in anderen DeFi-Protokollen gegen Preis- und Ausfallrisiken absichern.

**Entwicklung seit 2023.** Opyn illustriert die Konsolidierung des Sektors — und zugleich die Wirkung regulatorischen Drucks: Nach einem Vergleich mit der US-Derivateaufsicht CFTC im September 2023 (250.000 US-Dollar Zivilstrafe wegen nicht registrierten Derivatehandels) zog sich das Protokoll aus dem US-Markt zurück [vgl. 34]; am 4. November 2024 wurde das Squeeth-Produkt abgeschaltet [vgl. 88], und im Juli 2025 wechselte das Führungsteam zu Coinbase, ohne dass die Protokolle übernommen wurden [vgl. 28]. Zum Stand 02.08.2026 weisen die verbliebenen Verträge zusammen weniger als 2 Mio. US-Dollar

TVL aus [46]. Als Fallstudie bleibt Opyn gleichwohl instruktiv — als Beleg dafür, dass im DeFi-Sektor auch technisch innovative Protokolle ohne tragfähige Nachfrage und unter regulatorischem Druck vom Markt verschwinden.

**Vergleich der Kategorie.** Beide Fallstudien adressieren Absicherungsbedarf, aber mit grundverschiedenen Mechanismen (M1/M2): Nexus Mutual sozialisiert Risiken in einem kapitalgedeckten Pool mit Governance-Schadensentscheid, Opyn individualisiert sie über handelbare Optionskontrakte mit Besicherung. Gemeinsam ist beiden die geringe Marktdurchdringung — die Kategorie ist die kleinste der untersuchten drei (M3/M4: Prämien nachfragegetrieben, Deckungsgrenzen durch Poolgröße; M5: Unterdeckungs- und Governance-Risiken; M6: keine Einordnung als Versicherungsgeschäft, Abschnitt 4.5.2).

## 4.5. Herausforderungen und Risiken von DeFi

### 4.5.1. Sicherheitsrisiken

Die Risikoanalyse folgt der in den Merkmalsprofilen (M5) verwendeten Taxonomie und zerlegt jedes Risiko nach Quelle, betroffenen Akteuren und Schadensmechanik — statt Risiken lediglich aufzuzählen.

**Technische Risiken.** Die größte Risikoquelle sind Fehler in Smart Contracts. Smart Contracts führen einprogrammierte Bedingungen automatisch aus (Abschnitt 2.7); enthalten sie Fehler oder Sicherheitslücken, können Angreifer sie ausnutzen und hinterlegtes Kapital entwenden — betroffen sind unmittelbar die Einleger des Protokolls. Das prägende Frühbeispiel ist der Angriff auf „The DAO“ am 18. Juni 2016, bei dem über eine Reentrancy-Schwachstelle rund 3,6 Mio. Ether — nach damaliger Bewertung etwa 60 Mio. US-Dollar — unter die Kontrolle des Angreifers gerieten [vgl. 7]. Die Schadenshöhe solcher Vorfälle ist hoch, die Eintrittswahrscheinlichkeit je Protokoll schwer schätzbar — sie sinkt mit Audits und Betriebsdauer, verschwindet aber nicht: Der Programmcode ist öffentlich, ein erfolgreicher Angriff sofort skalierbar, und die hierarchische Sicherheitsabhängigkeit des DeFi-Stacks (Abschnitt 3.4) überträgt Fehler einer Schicht auf alle darüberliegenden. In dieselbe Klasse fällt die Manipulation von Preisorakeln: Protokolle, die Marktpreise von externen Quellen beziehen, können über diese Quellen angegriffen werden. Flash Loans (Abschnitt 3.5.2) wirken hier als Angriffsverstärker, weil sie beliebig großes Kapital für die Dauer einer Transaktion bereitstellen — der bZx-Fall von 2020 verband beide Elemente: manipulierte Preisquelle plus geliehenes Kapital [vgl. 93]. Das Risiko trägt das angegriffene Protokoll bzw. dessen Einleger; der Angreifer benötigt kein Eigenkapital. Eine dritte technische Risikoklasse liegt in der Infrastruktur selbst: In Phasen hoher Netzauslastung steigen die Transaktionsgebühren sprunghaft und Transaktionen verzögern sich — was nicht nur die Nutzbarkeit einschränkt, sondern direkt in die ökonomische Risikoklasse durchschlägt, wenn etwa Liquidationen oder Absicherungsgeschäfte nicht rechtzeitig ausgeführt werden

können. Die Verlagerung auf Layer-2-Netzwerke mindert dieses Skalierungsrisiko, verlagert es aber zugleich auf zusätzliche Infrastrukturschichten (Abschnitt 5.2.3).

**Ökonomische Risiken.** Neben Angriffskosten drohen Verluste aus der Marktmechanik selbst: Liquidationskaskaden, wenn fallende Preise viele überbesicherte Positionen gleichzeitig unter ihre Schwellen drücken und die Zwangsverkäufe die Preise weiter belasten; impermanente Verluste der Liquiditätsanbieter (Abschnitt 4.3.1); und Konstruktionsfehler ökonomischer Mechanismen. Das größte Lehrstück der letzten Kategorie ist der Terra/UST-Kollaps vom Mai 2022 (Abschnitt 3.5.1): Der Stabilisierungsmechanismus des algorithmischen Stablecoins versagte unter Abverkaufsdruck, rund 40 Mrd. US-Dollar Marktwert wurden vernichtet, und die Kettenreaktion riss überproportional exponierte Kreditgeber und Fonds mit [vgl. 16]. Betroffen sind hier nicht nur die Nutzer des fehlerhaften Protokolls, sondern über die Zusammensetzbarkeit (Abschnitt 3.3) auch verbundene Protokolle — Vernetzung wirkt als Ansteckungskanal.

**Governance- und Betrugsrisiken.** Governance-Token verleihen Mehrheiten die Macht, Parameter (etwa Liquidationsschwellen oder Gebühren) zu ändern oder Protokollkapital umzuwidmen; konzentrierter Token-Besitz wird damit selbst zum Risiko. Hinzu kommen klassische Betrugsformen im Umfeld der Protokolle: gefälschte Frontends und Phishing zielen auf die privaten Schlüssel der Nutzer — hier liegt das Risiko beim einzelnen Anwender, nicht im Protokoll. Da DeFi-Anwendungen keine zentrale Instanz haben, die Transaktionen rückabwickeln könnte, sind Verluste in aller Regel endgültig.

Für die Bewertung in Kapitel 5 ist festzuhalten: Die Risiken sind strukturell — sie folgen aus Offenheit, Automatisierung und Zusammensetzbarkeit, also genau den Eigenschaften, die die Effizienzvorteile erzeugen. Absicherungsmärkte (Abschnitt 4.4) decken bislang nur einen kleinen Teil des exponierten Kapitals; Sicherheitsprüfungen (Audits) und formale Verifikation mindern die technische Risikoklasse, adressieren die ökonomische und die Governance-Klasse aber nicht.

### 4.5.2. Regulierung

*(Für die überarbeitete Fassung vollständig neu geschrieben — die Regulierungslage hat sich seit 2023 grundlegend entwickelt.)*

**Strukturelle Herausforderungen.** Die Gründe, aus denen sich DeFi schwer regulieren lässt, bestehen fort und erklären die Architektur der inzwischen erlassenen Regelwerke: Dezentrale Protokolle haben keinen Betreiber, der als Adressat von Pflichten dienen könnte; Nutzer bleiben pseudonym, was Geldwäscheprävention erschwert; die Zusammensetzbarkeit verwischt Produktgrenzen; und die globale Nutzbarkeit führt dazu, dass mehrere Rechtsordnungen gleichzeitig berührt sind. Hinzu kommt die technische Komplexität des Gegenstands, die auch die Aufsichtsbehörden selbst vor Kapazitäts- und Wissensprobleme stellt. Regulierung setzt deshalb bislang vor allem dort an, wo zentrale Akteure greifbar

sind: bei Emittenten, Verwahrern und Handelsplattformen.

**Europäische Union: MiCA.** Mit der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA) hat die EU als erster großer Rechtsraum ein umfassendes Regelwerk geschaffen [61]. Die Verordnung trat im Juni 2023 in Kraft und ist seit dem 30. Juni 2024 für Stablecoins (vermögenswertreferenzierte Token und E-Geld-Token: Zulassungs-, Reserve- und Rücktauschpflichten für Emittenten) und seit dem 30. Dezember 2024 vollständig anwendbar — einschließlich der Zulassungspflicht für Krypto-Dienstleister (Crypto-Asset Service Provider, CASP) wie Handelsplattformen und Verwahrer. Für DeFi enthält MiCA eine folgenreiche Aussparung: Kryptowerte-Dienstleistungen, die „in vollständig dezentralisierter Weise ohne Intermediär“ erbracht werden, fallen nicht in den Anwendungsbereich (Erwägungsgrund 22). Wo die Grenze zwischen „vollständig dezentral“ und faktisch zentral gesteuerten Protokollen verläuft — etwa bei Frontends, Governance-Token-Mehrheiten oder Entwicklerfirmen —, ist ungeklärt; die Kommission ist nach Art. 142 MiCA beauftragt, den DeFi-Sektor zu bewerten und gegebenenfalls Regulierungsvorschläge vorzulegen. EBA und ESMA haben dazu im Januar 2025 einen gemeinsamen Bericht vorgelegt, der DeFi mit rund 4 % des globalen Kryptomarktwerts als Nischensegment einordnet [62]; im Mai 2026 hat die Kommission zudem eine gezielte Konsultation zur Überprüfung der Verordnung eröffnet (Frist: 30. September 2026) [vgl. 57]. Ein eigener Bericht der Kommission lag bis zum Redaktionsschluss dieser Fassung (August 2026) nicht vor.

**Deutschland: BaFin-Praxis.** Deutschland hatte mit der Erlaubnispflicht für das Kryptoverwahrgeschäft (KWG) bereits seit 2020 einen nationalen Rahmen; mit Anwendbarkeit von MiCA ist die Aufsicht auf das europäische Regime übergeleitet worden — die BaFin ist zuständige Behörde für die CASP-Zulassung, flankiert durch das nationale Kryptomärkteaufsichtsgesetz [18]. Die Übergangsfristen sind inzwischen abgelaufen: Der deutsche Bestandsschutz für Institute mit KWG-Erlaubnis endete nach § 50 KMAG spätestens am 31. Dezember 2025 [vgl. 50], die MiCA-eigene Übergangsregelung für Bestandsanbieter EU-weit am 1. Juli 2026 (Art. 143 Abs. 3 MiCA) — seither ist die Erbringung von Kryptowerte-Dienstleistungen ohne Zulassung bzw. Notifizierung unzulässig [vgl. 61]. Für die Fallstudien dieses Kapitels bedeutet das: Zentrale Anbieter mit EU-Bezug (Börsen, Verwahrer, Stablecoin-Emittenten) benötigen eine Zulassung; die untersuchten Protokolle selbst agieren mangels Betreiber weiterhin außerhalb dieses Rahmens.

**USA: Kurswechsel und Stablecoin-Gesetz.** Die USA verfolgten bis 2024 einen primär durchsetzungsgetriebenen Ansatz („regulation by enforcement“) über die Wertpapieraufsicht SEC. Seit 2025 hat sich die Linie deutlich verschoben: Mit dem GENIUS Act wurde im Juli 2025 erstmals ein Bundesgesetz für Zahlungs-Stablecoins geschaffen (Zulassungs-, Reserve- und Transparenzpflichten für Emittenten) [112]. Wirksam sind diese Pflichten allerdings noch nicht: Das Gesetz greift erst 120 Tage nach Erlass der finalen Ausführungsvorschriften, spätestens im Januar 2027. Die im Gesetz angelegte Jahresfrist

für diese Vorschriften lief am 18. Juli 2026 ab, ohne dass finale Regeln vorlagen — die Rechtsetzung der beteiligten Behörden (u. a. OCC, Entwurf Februar 2026; FinCEN/OFAC, Entwurf April 2026) dauerte zum Redaktionsschluss an, sodass die Pflichten voraussichtlich erst zum Auffangtermin im Januar 2027 greifen [112]. Ein umfassendes Marktstruktur-Gesetz — der Digital Asset Market Clarity Act (H.R. 3633), der auch Ausnahmen für dezentrale Protokolle vorsieht — hat im Juli 2025 das Repräsentantenhaus passiert, war zum Redaktionsschluss aber noch nicht verabschiedet [vgl. 111]. Parallel hat die SEC ihre Aufsichtslinie neu ausgerichtet — mit der Einrichtung einer Crypto Task Force und der Einstellung mehrerer Verfahren gegen große Handelsplattformen, darunter im Februar 2025 das Verfahren gegen Coinbase [vgl. 115]. Mit der im Juli 2025 angekündigten Initiative „Project Crypto“ geht die Behörde noch einen Schritt weiter: Angekündigt ist unter anderem eine „Innovation Exemption“, die neuartigen — ausdrücklich auch dezentralen — Geschäftsmodellen einen regelgebundenen Markteintritt außerhalb des klassischen Wertpapierregimes ermöglichen soll; die formelle Rechtsetzung dazu stand zum Redaktionsschluss noch aus [vgl. 114].

**Steuerliche Behandlung in Deutschland.** Ertragsteuerlich gelten Kryptowerte in Deutschland als „andere Wirtschaftsgüter“: Veräußerungsgewinne im Privatvermögen sind nach § 23 EStG nach einer Haltefrist von einem Jahr steuerfrei; Erträge aus Staking und Lending zählen zu den sonstigen Einkünften, und die zeitweise diskutierte Verlängerung der Haltefrist auf zehn Jahre für gestakte oder verliehene Kryptowerte ist nicht umgesetzt worden. Maßgeblich ist das BMF-Schreiben zur ertragsteuerrechtlichen Behandlung von Kryptowerten in der Fassung vom 6. März 2025, das auch Ansatz- und Mitwirkungspflichten präzisiert [19].

**Einordnung (M6).** Für das Analyseraster ergibt sich ein gespaltenes Bild: Die Schnittstellen zwischen DeFi und traditionellem Finanzsystem — Stablecoin-Emittenten, Verwahrer, zentrale Handelsplätze — sind in der EU vollständig und in den USA dem Gesetzestext nach reguliert, wobei die US-Pflichten erst mit den Ausführungsvorschriften wirksam werden; die dezentralen Protokolle selbst bleiben in einer beobachteten, aber noch nicht abschließend geregelten Zone — wobei sich mit dem MiCA-Prüfauftrag in der EU und der angekündigten SEC-„Innovation Exemption“ in den USA auf beiden Seiten des Atlantiks erstmals konkrete Regelungsvorhaben für die Protokollebene abzeichnen [vgl. 114]. Für Banken, die DeFi-Bausteine nutzen wollen (Kapitel 5), schafft MiCA erstmals Rechtssicherheit auf der Ebene der Gegenparteien und Basis-Assets, nicht aber auf der Ebene der Protokolle.

## 4.6. Die aktuelle Marktsituation im DeFi-Umfeld

Dieser Abschnitt dokumentiert die Datenlage; die Interpretation und Bewertung erfolgt in Abschnitt 5.1.

Der zentrale Indikator für den Umfang des DeFi-Sektors ist der Total Value Locked (TVL): der Gesamtwert der in den Smart Contracts der Protokolle hinterlegten Kryptowerte (Abschnitt 1.1), hier durchgängig nach der DeFiLlama-Zeitreihe [48]. Abbildung 4.1 zeigt den Verlauf: Ausgehend von rund 0,6 Mrd. US-Dollar Anfang 2020 stieg der TVL bis zum Jahreswechsel 2020/21 auf rund 15,3 Mrd. und erreichte am 9. November 2021 seinen bisherigen Höchststand von rund 177 Mrd. US-Dollar. Im Jahresverlauf 2022 brach der Markt in zwei Wellen ein — im Mai mit dem Terra/UST-Kollaps (Abschnitt 3.5.1), im November mit der Insolvenz der zentralen Börse FTX —, auf rund 38 Mrd. US-Dollar zu Jahresbeginn 2023. Zum Stichtag der Fallstudien-Erhebung dieser Arbeit (09.03.2023) lag der TVL bei rund 46 Mrd. US-Dollar. Danach folgte eine mehrjährige Erholung bis auf einen zweiten Gipfel von rund 171 Mrd. US-Dollar am 7. Oktober 2025. Im Jahresverlauf 2026 ging der Wert erneut deutlich zurück — vom Jahreshoch von rund 128 Mrd. US-Dollar (18.01.2026) um gut 40 % auf rund 74 Mrd. US-Dollar zum Stichtag dieser Fassung (02.08.2026). Dieser Rückgang fällt zusammen mit rückläufigen Token-Bewertungen (zum Bewertungseffekt Abschnitt 5.1) und einer Serie schwerer Sicherheitsvorfälle im ersten Halbjahr 2026: CertiK beziffert die Schäden Web3-weit — also über DeFi-Protokolle hinaus — auf über 1,3 Mrd. US-Dollar, darunter zwei Einzelvorfälle im April 2026 mit 291 bzw. 285 Mio. US-Dollar — wobei sich die Angriffe zunehmend gegen Schlüsselverwaltung und Infrastruktur statt gegen Smart-Contract-Code richteten (vgl. die Risikoklassen in Abschnitt 4.5.1) [vgl. 24]. Der Sektor ist damit hochgradig zyklisch — und da der TVL in US-Dollar bewertet wird, spiegeln die Ausschläge stets auch die Kursentwicklung der hinterlegten Token (Abschnitt 1.1). Hinzu kommt ein Doppelzählungsproblem: Liquid-Staking- und Restaking-Vertreter-Token sowie wrapped Assets können denselben Basiswert in mehreren Protokollen gleichzeitig als TVL erscheinen lassen — gerade weil Liquid Staking inzwischen zu den kapitalstärksten Kategorien zählt [45], sind Niveauvergleiche über die Zeit mit Vorsicht zu interpretieren (vgl. Abschnitt 6.3).

Nach Blockchains konzentriert sich der Sektor weiterhin stark auf Ethereum: Rund 55 % des TVL entfallen auf Ethereum-basierte Protokolle, gefolgt von Tron, der BNB Chain, Solana und der Layer-2-Chain Base mit jeweils rund 6 % (Stand: 02.08.2026) [44]. Nach Anwendungskategorien sind die Kreditvergabe (rund 41 Mrd. US-Dollar) und das Liquid Staking (rund 35 Mrd.; Abschnitt 3.5.6) die beiden kapitalstärksten Felder [45]; größtes Einzelprotokoll unter den DeFi-Protokollen — ohne die vom Datenanbieter mitgeführten zentralen Verwahrbestände und Brücken — ist Lido (rund 17,6 Mrd. US-Dollar), gefolgt vom Kreditprotokoll Aave (rund 14,4 Mrd. über alle Versionen) [46].

## 4.7. Vergleichende Auswertung der Fallstudien

*(Ergänzung der überarbeiteten Fassung: Der Abschnitt führt die Fallstudien entlang des Analyserasters vergleichend zusammen.)*


Daten: DeFiLlama (api.llama.fi/v2/historicalChainTvl), Stand: 02.08.2026 · Eigene Darstellung

Abbildung 4.1.: Entwicklung des Total Value Locked im DeFi-Sektor 2018–2026 mit den Markteinbrüchen 2022 (Terra/UST, FTX). Eigene Darstellung; Datenquelle: DeFiLlama [48].

Tabelle 4.1.: Fallstudien im Vergleich, Teil 1: Intermediärfunktion, Besicherung und Marktstellung (TVL in Mrd. US-Dollar, Stichtage 09.03.2023 und 02.08.2026).

| Protokoll | M1: ersetzte Funktion | M2: Besicherung | TVL 2023 → 2026 |
|---|---|---|---|
| Aave | Kreditintermediär | Überbesicherung, Liquidation | 4,70 → 14,4 |
| Compound | Kreditintermediär | Überbesicherung, Liquidation | 1,89 → 1,2 |
| Uniswap | Börse, Market Maker | Pool-Liquidität | 3,85 → 3,1 |
| PancakeSwap | Börse, Market Maker | Pool-Liquidität | 2,49 → 2,1 |
| Nexus Mutual | Versicherer | Kapitalpool, Staking | 0,21 → 0,09 |
| Opyn | Optionsbörse | besicherte Kontrakte | 0,05 → < 0,01 |

Tabelle 4.2.: Fallstudien im Vergleich, Teil 2: Kosten, Zugang und Regulierungsstatus.

| Protokoll | M3: Kosten/Abwicklung | M4: Zugang | M6: Regulierung |
|---|---|---|---|
| Aave | algorithmischer Zins, sofort | offen | von MiCA nicht erfasst |
| Compound | algorithmischer Zins, sofort | offen | von MiCA nicht erfasst |
| Uniswap | Gebührenstufen, atomar | offen | von MiCA nicht erfasst |

| Protokoll | M3: Kosten/Abwicklung | M4: Zugang | M6: Regulierung |
|---|---|---|---|
| PancakeSwap | Gebührenstufen, atomar | offen | von MiCA nicht erfasst |
| Nexus Mutual | nachfragebasierte Prämie | KYC-Mitgliedschaft | ohne Versicherungslizenz |
| Opyn | Optionsprämie | offen (US-Rückzug) | CFTC-Vergleich 2023 |

Die 2023er-Werte stammen aus der DeFiLlama-Historie zum Stichtag 09.03.2023 (eingecheckter Snapshot `defillama_protokolle_2023.json`), die 2026er-Werte aus dem Protokoll-Snapshot zum 02.08.2026; Summen über alle Protokollversionen, Aave einschließlich Horizon (RWA) [46]. Das Risikoprofil (M5) ist über alle Fälle strukturgleich (technisch/ökonomisch/Governance) und wird deshalb nicht je Protokoll aufgespalten, sondern gebündelt in Abschnitt 4.5.1 behandelt. Auffällig ist am 2023er-Stichtag zudem, dass Curve (4,85 Mrd.) sogar vor Aave lag — die in Abschnitt 1.3 offengelegte Auswahlentscheidung betraf also die damalige Nummer eins des hier verglichenen Feldes.

Aus dem Vergleich lassen sich vier Beobachtungen ableiten:

1. **Konzentration innerhalb der Kategorien, Verschiebung zwischen ihnen:** Innerhalb jeder untersuchten Kategorie hat sich der Marktführer von 2023 behauptet oder ausgebaut (Aave, Uniswap, Nexus Mutual), während zweite Anbieter Marktanteile verloren (Compound, Opyn); im Lending ist mit Morpho ein Neueinsteiger in die Spitzengruppe vorgestoßen. Neues Kapital floss allerdings weniger in die 2023 untersuchten Kategorien selbst als in seither entstandene oder gewachsene Felder — Liquid Staking und Restaking (Abschnitt 3.5.6), tokenisierte Real World Assets (Abschnitt 5.2.4) und den Perpetual-Handel (Abschnitt 4.3.3).
2. **Konvergente Technik:** Die Handelsprotokolle haben sich technisch angeglichen (konzentrierte Liquidität, Multichain-Strategien). Wettbewerbsvorteile entstehen weniger aus dem Grundmodell als aus Ökosystem-Effekten: Integrationen, Liquiditätstiefe, Entwickler-Erweiterbarkeit.
3. **Strukturgleiche Risiken:** Über alle Kategorien hinweg wiederholen sich dieselben M5-Muster (Smart-Contract-, Orakel-, Liquidations-, Governance-Risiken) — die Risikoanalyse in 4.5.1 gilt kategorieübergreifend. Die Besicherungslogik (M2) ersetzt überall die Bonitätsprüfung und koppelt den Zugang zu Krediten an vorhandenes Kapital.
4. **Ungelöste Absicherungslücke:** Die Absicherungskategorie ist um Größenordnungen kleiner als die abzusichernden Risiken — ein strukturelles Defizit des Sektors, das in Kapitel 5 als Integrationshürde für institutionelle Akteure gewertet wird.

# 5. Analyse und Bewertung

## 5.1. Analyse der aktuellen Marktsituation von DeFi

Während Abschnitt 4.6 die Datenlage dokumentiert, ordnet dieser Abschnitt sie ein: Was bedeuten Größe, Struktur und Verlauf des DeFi-Marktes für dessen Rolle im Finanzsystem?

### 5.1.1. Größe des DeFi-Marktes

Der DeFi-Markt hat seit 2020 ein beträchtliches Volumen erreicht, ist über die Marktzyklen hinweg aber kein linear wachsender Markt: Nach der Zeitreihe aus Abschnitt 4.6 stehen dem Höchststand von rund 177 Mrd. US-Dollar (November 2021) und dem zweiten Gipfel von rund 171 Mrd. US-Dollar (Oktober 2025) tiefe Einbrüche gegenüber; zum Stichtag dieser Fassung sind rund 74 Mrd. US-Dollar in DeFi-Protokollen gebunden (02.08.2026) [48].

Für die Interpretation der Kennzahl sind drei Punkte wesentlich. Erstens der Bewertungseffekt: Da der TVL in US-Dollar gemessen wird, spiegeln seine Ausschläge immer auch die Kursentwicklung der hinterlegten Token — ein fallender TVL bedeutet nicht zwingend Kapitalabzug, ein steigender nicht zwingend neue Nutzung (Abschnitt 1.1). Zweitens die Relation: Gemessen am traditionellen Finanzwesen ist DeFi klein. Das globale Finanzvermögen der vom Financial Stability Board erfassten Jurisdiktionen lag 2024 bei rund 500 **Billionen** US-Dollar, davon rund 257 Billionen im Nichtbanken-Sektor [vgl. 65] — der DeFi-Sektor bewegt sich also, selbst auf Zyklushochs, unterhalb eines halben Promille des traditionellen Systems. Drittens das Umfeld: Der Umlauf der US-Dollar-Stablecoins (rund 307 Mrd. US-Dollar, Abschnitt 3.5.1) beträgt inzwischen mehr als das Vierfache des DeFi-TVL — die tokenisierte Form des Dollars hat eine breitere Verwendung gefunden als die dezentralen Finanzprotokolle selbst.

Zusammengenommen zeigt die Marktgröße zweierlei: DeFi hat sich durch zwei vollständige Marktzyklen als dauerhafte Infrastruktur erwiesen — der Sektor ist nach jedem Einbruch zurückgekehrt, mit denselben führenden Protokollen (Abschnitt 4.7). Zugleich blieb das erhoffte Wachstum in die Breite aus; DeFi ist ein etablierter, aber begrenzter Markt geblieben, dessen Bedeutung derzeit weniger in seiner Größe als in seiner Funktion als technologisches Referenzmodell liegt (Abschnitt 5.2.2).

### 5.1.2. Wichtige Akteure und Anwendungen

Im DeFi-Sektor wirken mehrere Akteursgruppen zusammen: die Entwickler(-organisationen) der Protokolle, Nutzer, Liquiditätsgeber, Investoren sowie die Betreiber zentraler Handels- und Verwahrplattformen an den Schnittstellen. Unter den Anwendungen dominieren die in Kapitel 3.5 eingeführten Kategorien: Bei der Kreditvergabe haben sich Aave, Compound und das heute als Sky firmierende MakerDAO etabliert; im Handel Uniswap, PancakeSwap und Curve; bei Absicherungen Nexus Mutual. *(Das früher ebenfalls aktive „Cover Protocol" wurde bereits im September 2021 nach einem Exploit und dem Rückzug des Entwicklerteams eingestellt [vgl. 30].)* Seit 2023 haben sich die Gewichte verschoben: Größte Einzelanwendung ist heute das Liquid-Staking-Protokoll Lido (rund 17,6 Mrd. US-Dollar), und mit Morpho ist ein jüngeres Kreditprotokoll in die Spitzengruppe aufgestiegen (rund 7,6 Mrd. US-Dollar; beide Stand 02.08.2026) [46] (Abschnitt 4.7).

## 5.2. Beantwortung der Forschungsfragen

Die vier Unterabschnitte beantworten die Forschungsfragen FF1–FF4 aus Abschnitt 1.2 in dieser Reihenfolge; jede Antwort stützt sich auf die Merkmalsprofile (M1–M6) und die Fallstudien der Kapitel 3 und 4.

### 5.2.1. FF1 — Marktentwicklung und Potenzial

Der DeFi-Markt ist seit 2020 stark, aber zyklisch gewachsen (Abschnitte 4.6, 5.1.1). Die Nachfrage nach dezentralen Finanzanwendungen speist sich aus den in Kapitel 3 herausgearbeiteten Eigenschaften: genehmigungsfreier Zugang, automatisierte Abwicklung, Zusammensetzbarkeit. Die Fallstudien zeigen zugleich, dass sich der Markt konsolidiert hat — wenige Protokolle je Kategorie binden den Großteil des Kapitals, und die Marktführer von 2023 haben ihre Stellung überwiegend behauptet (Abschnitt 4.7).

Die Auswirkungen auf die Finanzbranche sind bislang mittelbar, aber real: DeFi hat als technologisches Referenzmodell vorgeführt, dass zentrale Funktionen des Finanzwesens — Kreditvergabe, Handel, Marktbildung, Verwahrung — ohne Intermediär als Software abbildbar sind (M1). Messbar ist der Einfluss weniger am eigenen Marktvolumen als an der Reaktion der Branche: an tokenisierten Produkten der Banken und Vermögensverwalter, an regulierten Krypto-Angeboten und an der 2024/2025 entstandenen Regulierungsarchitektur (Abschnitte 4.5.2, 5.2.4).

Das in Abschnitt 1.1 genannte Inklusionsversprechen — Zugang für Menschen ohne Bankverbindung — hat sich dabei nicht in der Breite eingelöst: Genehmigungsfreiheit besteht formal (M4), die faktischen Hürden aus Transaktionskosten, technischem Vorwissen und Schlüsselverwahrung bestehen jedoch fort (Abschnitte 1.1, 3.3), und die tatsächliche Nutzung konzentriert sich auf technik- und risikoaffine Anwender (5.2.3). Wo dezentrale

Technologie Inklusionswirkung entfaltet, geschieht dies bislang eher über Dollar-Stablecoins als Zahlungs- und Wertaufbewahrungsmittel als über DeFi-Protokolle im engeren Sinne.

**Antwort auf FF1:** Der DeFi-Markt hat sich als dauerhafte, aber größenmäßig begrenzte Infrastruktur etabliert; seine Hauptwirkung auf die Finanzbranche liegt in der Rolle als Innovations- und Referenzmodell, das der Tokenisierung des traditionellen Finanzwesens wesentliche Impulse gegeben hat — nicht in einer Verdrängung bestehender Anbieter. Das Inklusionspotenzial ist real, aber bislang nur eingeschränkt realisiert.

### 5.2.2. FF2 — Ergänzung oder Substitution des traditionellen Finanzwesens

Der systematische Vergleich entlang des Analyserasters M1–M6, ergänzt um die in FF2 genannte Dimension Transparenz, stellt der in den Kapiteln 2–4 erarbeiteten DeFi-Seite das traditionelle Finanzwesen als Referenzsystem gegenüber. Dessen Merkmale werden hier — soweit nicht bereits in Kapitel 2 eingeführt (Kartenabwicklung und Disagio, Abschnitt 2.6) — mit den maßgeblichen Rechtsquellen belegt: der Einlagensicherung bis 100.000 Euro je Einleger nach Richtlinie 2014/49/EU [vgl. 58], den Abwicklungsfristen im Wertpapiergeschäft nach der Zentralverwahrer-Verordnung [vgl. 59], den Interbankenentgelt-Obergrenzen nach VO (EU) 2015/751 [vgl. 60] sowie den Laufzeiten grenzüberschreitender Zahlungen nach dem Monitoring der G20-Roadmap [vgl. 33]:

Tabelle 5.1.: DeFi und traditionelles Finanzwesen im Vergleich entlang des Analyserasters.

| Dimension | Traditionelles Finanzwesen | DeFi | Grundlage |
|---|---|---|---|
| Intermediär (M1) | Bank, Börse oder Versicherer als verantwortliche Gegenpartei | Smart-Contract-Protokoll ohne Betreiber | 3.5, 4.2–4.4 |
| Besicherung (M2) | Bonitätsprüfung, teilbesicherte Kredite, Einlagensicherung | Überbesicherung, automatische Liquidation, keine Sicherungssysteme | 3.5.2, 4.2 |
| Kosten (M3) | Intermediärsmargen (Karte: gedeckeltes Entgelt plus Margen) | Netzwerk- und Protokollgebühren, betragsunabhängig | 2.6, 3.5.1, 3.5.3 |
| Geschwindigkeit (M3) | Sekunden (Karte) bis Tage (Ausland, Wertpapiere) | Minuten, unwiderruflich, rund um die Uhr, global einheitlich | 2.6, 3.5.3, 4.5.1 |

| Dimension | Traditionelles Finanzwesen | DeFi | Grundlage |
|---|---|---|---|
| Zugang (M4) | Konto- und Identitätspflicht, länderabhängig | genehmigungsfrei (Ausnahme: KYC-Modelle, 4.4.1); faktische Hürden bleiben | 1.1, 3.3 |
| Transparenz (FF2) | institutionsinterne Bücher, Aufsichtsberichte | öffentliche Transaktionshistorie, offener Code | 2.3, 3.3 |
| Risiko (M5) | Gegenpartei- und Systemrisiken, durch Aufsicht abgefedert | Smart-Contract-, Orakel-, Liquidations-, Governance-Risiken; Verluste endgültig | 4.5.1 |
| Rechtsrahmen (M6) | umfassend reguliert | Schnittstellen reguliert, Protokolle nicht | 4.5.2 |

Quantifizieren lässt sich der Kostenunterschied an einem Zahlungsvorgang: Im Kartengeschäft ist allein das Interbankenentgelt in der EU auf 0,3 % (Kreditkarte) bzw. 0,2 % (Debitkarte) des Umsatzes gedeckelt, zuzüglich Systementgelten und Acquirer-Marge (Abschnitt 2.6) [vgl. 60]; ein Stablecoin-Transfer kostet dagegen die Netzwerkgebühr der jeweiligen Blockchain — unabhängig vom Betrag. Der Vorteil kehrt sich bei kleinen Beträgen und hoher Netzauslastung um und ist auch sonst nicht kostenlos: Beim Handel treten Protokollgebühren im Promille- bis Prozentbereich hinzu (Abschnitt 3.5.3), beim Bereitstellen von Liquidität der impermanente Verlust — rund 5,7 % bei einer Kursverdopplung, rund 20 % bei einer Vervierfachung (Abschnitt 4.3.1). Der Effizienzvorteil von DeFi liegt damit nicht pauschal in niedrigeren Gebühren, sondern in der Betragsunabhängigkeit und im Wegfall der mehrstufigen Abwicklungskette.

Der Vergleich zeigt ein klares Komplementaritätsmuster: DeFi ist dort überlegen, wo Automatisierung und globale Einheitlichkeit zählen (Abwicklungsgeschwindigkeit, Verfügbarkeit, Transparenz, Zusammensetzbarkeit); das traditionelle System ist dort überlegen, wo Vertrauensschutz zählt (Einlagensicherung, Rechtsdurchsetzung, Verbraucherschutz, unbesicherte Kredite auf Bonitätsbasis — die DeFi mangels Identität strukturell nicht abbilden kann, M2/M4). Substitution scheitert derzeit an drei Punkten: an der Risikolage (4.5.1) samt ungelöster Absicherungslücke (4.4), am fehlenden Zugang zu unbesichertem Kredit und an der Nutzerkomplexität. Synergiepotenziale bestehen dagegen konkret: Banken können Abwicklungs- und Verwahrinfrastruktur tokenisieren, Stablecoins und tokenisierte Fonds als Produkte nutzen und über White-Label-Frameworks — wie das Crypto-Exchange-Integrator-Framework von NTT DATA [vgl. 86] — Kundenzugang zu Krypto-Märkten anbieten, ohne eigene Protokoll-Infrastruktur zu betreiben (Abbildung

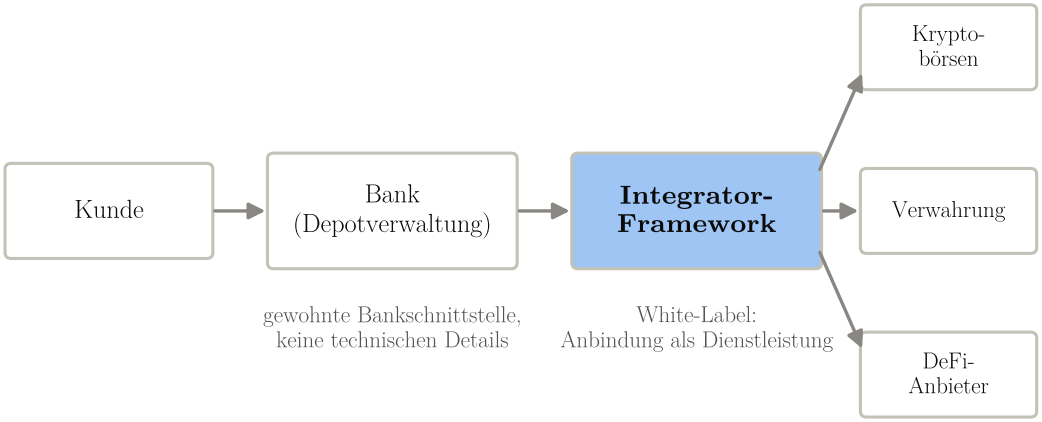



Abbildung 5.1.: Integrator-Framework als White-Label-Schnittstelle zwischen Bank und Krypto-Infrastruktur. Eigene Darstellung in Anlehnung an NTT DATA [vgl. 86].

5.1).

**Antwort auf FF2:** DeFi eignet sich auf absehbare Zeit als Ergänzung, nicht als Substitution des traditionellen Finanzwesens; die Synergien realisieren sich über regulierte Schnittstellen — Verwahrung, Stablecoins, tokenisierte Produkte —, nicht über einen Ersatz der Institutionen.

### 5.2.3. FF3 — Risiken und Regulierung

Die Risikoanalyse in Abschnitt 4.5.1 hat die technischen, ökonomischen und Governance-Risiken systematisch zerlegt; sie bilden das größte Hemmnis für eine breitere Nutzung — der Nutzerkreis bleibt auf technik- und risikoaffine Anwender konzentriert, solange Verluste endgültig sind und Absicherungsmärkte nur einen Bruchteil des Kapitals decken.

Bei der Skalierbarkeit hat sich die Lage seit der Erstfassung deutlich verbessert: Ethereum hat nach dem Merge (September 2022) mit dem Dencun-Upgrade (März 2024) die Datenkosten für Layer-2-Netzwerke deutlich gesenkt und mit Pectra (Mai 2025) die Kontenfunktionalität erweitert; ein wachsender Teil des gebundenen Kapitals liegt heute auf Layer-2-Chains wie Base (rund 6 % des TVL, Abschnitt 4.6) [vgl. 56]. Der Umstieg auf PoS hat zudem den Energieeinwand gegen die DeFi-Basisinfrastruktur weitgehend entkräftet (Abschnitt 2.4) und mit den Staking-Erträgen eine eigene Ertragsquelle geschaffen [vgl. 118]. Damit lässt sich auch der in Abschnitt 2.4 angekündigte Sicherheitsvergleich einlösen: PoS verlagert die Angriffskosten von externen Ressourcen (Hardware, Energie) auf internes Kapital — wer den Konsens angreifen will, muss Stake erwerben und riskiert dessen Verlust durch Slashing statt versunkener Energiekosten. Das senkt den Ressourcenverbrauch drastisch, schafft aber neue Zentralisierungsvektoren, wenn sich Stake bei

wenigen Liquid-Staking-Anbietern konzentriert (Abschnitt 3.5.6). Alternative Plattformen haben sich sortiert: Solana zählt neben Tron und der BNB Chain zu den größten Nicht-Ethereum-Ökosystemen (wie die Layer-2-Chain Base jeweils rund 6 % des TVL, Abschnitt 4.6), während andere in der Erstfassung genannte Plattformen (Cardano, Polkadot) im DeFi-Sektor marginal geblieben sind [44].

Die regulatorische Unsicherheit — 2023 das größte Integrationshindernis — ist an den Schnittstellen weitgehend aufgelöst: MiCA schafft seit 2024 einen einheitlichen EU-Rahmen für Emittenten und Dienstleister, die BaFin beaufsichtigt den Übergang, die USA haben mit dem GENIUS Act nachgezogen, und die steuerliche Behandlung in Deutschland ist durch das BMF-Schreiben von 2025 geklärt (im Detail Abschnitt 4.5.2). Offen bleibt die Regulierung der dezentralen Protokolle selbst: Für Nutzer greift das Recht ihres Aufenthaltsstaats, für die Protokolle bislang kein eigenes Regime — erste Regelungsvorhaben auf Protokollebene sind jedoch angekündigt (MiCA-Prüfauftrag, SEC-„Innovation Exemption“; Abschnitt 4.5.2).

**Antwort auf FF3:** Die technischen und ökonomischen Risiken sind strukturell und bleiben die zentrale Hürde; Skalierung und Regulierung — 2023 die beiden anderen zentralen Hemmnisse — sind seither substanziell entschärft. Die Bewältigung der Restrisiken erfordert das Zusammenwirken von Entwicklern (Audits, formale Verifikation), Absicherungsmärkten und Regulierern; ihre vollständige Beseitigung ist nicht zu erwarten, da sie aus denselben Eigenschaften folgen wie die Effizienzvorteile.

### 5.2.4. FF4 — Perspektiven von Investoren und Entscheidungsträgern

*(Datenbasis gemäß Abschnitt 1.3: dokumentierte Produktankündigungen sowie Emittenten- und Aufsichtspublikationen, keine Primärerhebung; Ankündigungen belegen Existenz und Ausgestaltung eines Angebots, nicht dessen Markterfolg.)*

**Banken und Finanzdienstleister** des traditionellen Finanzwesens (Traditional Finance, kurz TradFi) haben ihr Engagement seit 2023 von Ankündigungen zu produktiven Angeboten verschoben — allerdings fast ausschließlich in Form *tokenisierter traditioneller Produkte*, nicht durch Nutzung dezentraler Protokolle: J.P. Morgan betreibt mit Kinexys (vormals Onyx) eine eigene Blockchain-Plattform für Zahlungen und Tokenisierung auf Basis der bankeigenen Infrastruktur [vgl. 75, 37]. Goldman Sachs hat im November 2024 angekündigt, seine Digital-Asset-Plattform GS DAP — auf der u. a. digitale Anleihen emittiert und abgewickelt werden — als eigenständiges, branchengetragenes Unternehmen auszugründen; der Vollzug stand zum Stichtag dieser Fassung noch unter aufsichtsrechtlichem Vorbehalt [vgl. 69]. Bereits 2015 beteiligte sich die Bank an einer Finanzierungsrunde des späteren Stablecoin-Emittenten Circle [vgl. 29], der seit Juni 2025 an der New York Stock Exchange notiert ist [vgl. 26]. UBS bietet mit uMINT einen tokenisierten Geldmarktfonds an [vgl. 116], Citi mit Citi Token Services tokenisierte Einlagen für Firmenkunden

[vgl. 27].

**Vermögensverwalter und Investoren** haben ihren Zugang über regulierte Vehikel gefunden: Die Zulassung von Bitcoin-Spot-ETFs in den USA (Januar 2024) — börsengehandelter Fonds, die Bitcoin physisch halten und wie Wertpapiere im Depot verwahrt werden — hat institutionellen Anlegern erstmals breiten Zugang zu Kryptowerten über gewohnte Anlagevehikel verschafft [vgl. 113]; BlackRock legte im März 2024 mit BUIDL seinen ersten tokenisierten Fonds auf einer öffentlichen Blockchain auf, ausgegeben über die Tokenisierungsplattform Securitize [vgl. 102]; er wuchs bis 2026 auf rund 3,5 Mrd. US-Dollar an [46]. Ein tokenisierter Geldmarktfonds eines großen Vermögensverwalters war zuvor bereits 2021 mit Franklin Templetons FOBXX an den Markt gekommen [vgl. 66]. Die Tokenisierung realer Vermögenswerte (Real World Assets, RWA) — Geldmarktfonds, Anleihen, Private Credit — ist zum sichtbarsten Wachstumsfeld an der Schnittstelle beider Welten geworden; auch DeFi-Protokolle selbst greifen sie auf (Aave Horizon, Abschnitt 4.2.1), und mit BUIDL zählt ein tokenisierter TradFi-Fonds inzwischen zu den zehn größten Positionen des Protokoll-Snapshots (ohne zentrale Verwahrbestände und Brücken) [46].

**Aufsichtsbehörden und Zentralbanken** bewerten DeFi differenziert: als Effizienzversprechen mit systemischen Risiken (Hebelwirkung, Ansteckung über Zusammensetzbarkeit, Stablecoin-Runs) — die BIS-Analysen, auf die sich bereits Kapitel 3 stützt, und der DeFi-Finanzstabilitätsbericht des FSB stehen exemplarisch für diese Linie [vgl. 8, 6, 64]. Die Konsequenz war nicht Verbot, sondern Einhegung über die Schnittstellenregulierung (Abschnitt 4.5.2).

**Antwort auf FF4:** Entscheidungsträger des traditionellen Finanzwesens bewerten die *Technologie* inzwischen als strategisch relevant, das *dezentrale Betriebsmodell* dagegen weiterhin als zu riskant — sie adaptieren Tokenisierung und Blockchain-Abwicklung, meiden aber offene Protokolle. Investoren nutzen bevorzugt regulierte Zugänge (ETFs, tokenisierte Fonds). Für die Integration bedeutet das: Sie findet statt, aber auf den Bedingungen des regulierten Systems — DeFi liefert die Blaupause, die Institutionen bauen die kontrollierte Version.

## 5.3. Handlungsempfehlungen für Banken und Investoren

*(Die folgenden Empfehlungen sind aus den Antworten auf FF1–FF4 abgeleitet und entsprechend referenziert.)*

**Für Banken und Finanzdienstleister:**

1. **Schnittstellen besetzen statt Protokolle betreiben (aus FF2/FF4):** Der belastbare Einstieg liegt in den regulierten Schnittstellen — Kryptoverwahrung und Krypto-Dienstleistungen unter MiCA-Zulassung, Handel über regulierte Plattformen. Die Fallstudien zeigen, dass die Wertschöpfung der offenen Protokolle konzentriert

und umkämpft ist (4.7); die Schnittstellen sind es nicht.

2. **Tokenisierung als Brückenprodukt (aus FF1/FF4):** Tokenisierte Geldmarktfonds, Anleihen und Einlagen übertragen die Effizienzvorteile (M3: Abwicklung, Verfügbarkeit) auf regulierte Produkte — die Beispiele Kinexys, uMINT, BUIDL und Citi Token Services belegen die Machbarkeit. Institute ohne eigene Plattform können über White-Label- und Integrator-Modelle einsteigen — vorgefertigte, unter eigener Marke betreibbare Lösungen, wie sie exemplarisch in Abschnitt 5.2.2 beschrieben sind.

3. **Stablecoin-Strategie entwickeln (aus 5.1.1/4.5.2):** Der Stablecoin-Umlauf übersteigt den DeFi-TVL um ein Mehrfaches; mit MiCA und GENIUS Act ist die Emission von E-Geld-Token bzw. Zahlungs-Stablecoins ein regulierbares Geschäftsfeld — und zugleich eine Verteidigung des Einlagengeschäfts gegen Abflüsse in tokenisierte Dollars.

4. **DeFi-Risikoraster in die Due Diligence übernehmen (aus FF3):** Wo Berührungspunkte zu Protokollen entstehen (Verwahrung von Governance-Token, tokenisierte Sicherheiten, RWA-Protokolle), liefert die Taxonomie aus 4.5.1 (technisch/ökonomisch/Governance, je mit Quelle, Akteur, Schadensmechanik) ein direkt anwendbares Prüfschema; die Absicherungslücke (4.4) ist dabei als nicht versicherbares Restrisiko zu bepreisen.

5. **Den Neue-Produkte-Prozess (NPP) früh und modular ansetzen (aus FF3/FF4):** Der bankinterne NPP — die strukturierte Vorprüfung neuer Produkte auf Risiko-, Rechts- und Reputationsfolgen — war bereits beim Kryptoverwahrgeschäft die maßgebliche Markteintrittsbarriere (Abschnitt 6.1). Da MiCA die Anforderungen an Gegenparteien und Basiswerte vereinheitlicht (4.5.2), lässt sich der NPP auf wiederverwendbare Bausteine ausrichten (Verwahrung, Stablecoin-Akzeptanz, tokenisierte Fondsanteile), statt ihn je Produkt vollständig neu zu durchlaufen; das Risikoraster aus 4.5.1 liefert die Prüfdimensionen.

**Für Investoren:**

1. **Zugangsweg bewusst wählen (aus FF4):** Regulierte Vehikel (ETFs, tokenisierte Fonds) eliminieren Schlüssel- und Protokollrisiken gegen Gebühren und Verzicht auf DeFi-Erträge; direkte Protokollnutzung kehrt das Verhältnis um. Die Entscheidung ist eine Risikoallokation, keine Glaubensfrage.
2. **Ertragsquellen verstehen (aus 3.5/4.7):** DeFi-Renditen stammen aus Handelsgebühren, Zinsspreads, Protokollemissionen oder Staking — nachhaltige Gebührenerträge und verwässernde Token-Emissionen sind zu unterscheiden (PancakeSwap-Fallstudie, impermanenter Verlust in 4.3.1). Renditeversprechen ohne identifizierbare Quelle sind ein Warnsignal (Terra-Lehrstück, 3.5.1).

3. **Konzentrationsbefund nutzen (aus 4.7):** Kapital sammelt sich bei wenigen etablierten Protokollen; Engagements in Randprotokolle tragen das volle M5-Risikoprofil bei geringerer Überlebenswahrscheinlichkeit (Opyn-Fallstudie).
4. **Steuerliche Klarheit nutzen (aus 4.5.2):** Haltefristen sowie Staking- und Lending-Erträge sind in Deutschland seit dem BMF-Schreiben vom 10. Mai 2022 geregelt und mit dem ersetzenden Schreiben vom 6. März 2025 fortgeschrieben — dieses verschärft insbesondere die Aufzeichnungs- und Mitwirkungspflichten, die bei Protokollnutzung von Beginn an mitzuführen sind.

Diese Empfehlungen folgen aus der Analyse dieser Arbeit und sind an die jeweilige Situation und Risikotragfähigkeit anzupassen; sie sind keine Anlageberatung (siehe die Seite „Über dieses Dokument“ am Anfang der Arbeit).

# 6. Fazit

## 6.1. Zusammenfassung der wichtigsten Ergebnisse

Diese Arbeit hat die Grundlagen von Decentralized Finance erläutert (Kapitel 2–3), sechs Protokolle in drei Anwendungskategorien als Fallstudien untersucht (Kapitel 4) und auf dieser Basis die vier Forschungsfragen beantwortet (Kapitel 5). Die Ergebnisse lassen sich entlang der Forschungsfragen zusammenfassen:

DeFi hat sich als dauerhafte, aber größenmäßig begrenzte Finanzinfrastruktur etabliert (FF1): Der Sektor hat zwei vollständige Marktzyklen überstanden, sein Kapitalbestand bleibt jedoch im Promillebereich des traditionellen Finanzvermögens; seine Hauptwirkung liegt in der Rolle als technologisches Referenzmodell, das der Tokenisierung des traditionellen Finanzwesens wesentliche Impulse gegeben hat. DeFi eignet sich als Ergänzung, nicht als Substitution des traditionellen Finanzwesens (FF2): Die Stärken — automatisierte, globale, transparente Abwicklung ohne Intermediär — stehen strukturellen Schwächen gegenüber, allen voran dem Fehlen von Bonitätsprüfung und Vertrauensschutz; hinzu treten die ungelöste Absicherungslücke (Abschnitt 4.4) und die Nutzerkomplexität. Die Integration realisiert sich über regulierte Schnittstellen wie Verwahrung, Stablecoins und tokenisierte Produkte. Die Risiken sind strukturell (FF3): Sie folgen aus denselben Eigenschaften wie die Effizienzvorteile und lassen sich mindern, aber nicht beseitigen; Skalierung und Regulierung — 2023 noch zentrale Hemmnisse — sind seither substanziell entschärft. Die Entscheidungsträger des traditionellen Finanzwesens haben entsprechend reagiert (FF4): Sie adaptieren die Technologie in kontrollierter Form und meiden die offenen Protokolle.

Die vier Antworten hängen zusammen und ergeben ein Bild: Weil die Risiken strukturell aus denselben Eigenschaften folgen wie die Effizienzvorteile (FF3), lässt sich die Substitutionsfrage nicht durch bloße Reifung des Sektors auflösen (FF2); weil die Institutionen deshalb die Technologie übernehmen, nicht das Betriebsmodell (FF4), bleibt die Wirkung von DeFi auf die Finanzbranche mittelbar — als Blaupause, nicht als Wettbewerber (FF1). Aus dieser Verkettung leiten sich die Handlungsempfehlungen in Abschnitt 5.3 ab: Schnittstellen besetzen statt Protokolle betreiben.

Für Banken bleibt dabei ein praktisches Hindernis bestehen, das die Erstfassung zutreffend identifiziert hat: die Einhaltung regulatorischer Anforderungen beim Markteintritt. Der Neue-Produkte-Prozess (NPP, Abschnitt 5.3) ist zeit- und ressourcenintensiv und

stellte bereits bei der Einführung des Kryptoverwahrgeschäfts (Abschnitt 4.5.2) eine bedeutende Markteintrittsbarriere dar [vgl. 52]. Mit MiCA hat sich diese Hürde verschoben, nicht erledigt: Der Rechtsrahmen ist klarer geworden, die Zulassungs- und Compliance-Anforderungen sind zugleich verbindlicher und aufwendiger (Abschnitt 4.5.2).

Bestätigt hat sich auch der Befund zur finanziellen Inklusion — mit der in dieser Fassung ergänzten Einschränkung: DeFi kann Menschen ohne Zugang zu traditionellen Bankdienstleistungen grundsätzlich Finanzdienstleistungen eröffnen (M4), doch koppelt die Überbesicherungslogik (M2) den Kreditzugang an vorhandenes Kapital, und die faktischen Hürden — Technik, Gebühren, Schlüsselverwahrung — begrenzen die Reichweite. Die Dezentralität selbst bleibt für einen Teil der Nutzer der entscheidende Wert: Kontrolle über die eigenen Vermögenswerte ohne Abhängigkeit von zentralen Institutionen.

Insgesamt bietet DeFi erhebliches Potenzial, Finanzdienstleistungen effizienter und offener zu machen — dem von der Erstfassung benannten Potenzial, „die Finanzbranche zu revolutionieren“, ist der Sektor nach zwei Marktzyklen jedoch nicht nähergekommen. Um die Synergieeffekte zu nutzen, bleibt die Zusammenarbeit zwischen Entwicklern, Regulierungsbehörden und traditionellen Finanzinstitutionen unerlässlich: Sie senkt Markteintrittsbarrieren, wie das Beispiel der MiCA-Zulassung zeigt (Abschnitte 4.5.2, 5.3), und adressiert mit Audits und Absicherungsmärkten genau die Risikoklassen, die einzelne Akteure nicht allein bewältigen können (Abschnitt 4.5.1).

## 6.2. Entwicklungen 2023–2026 und Prognosen-Check

*(Ergänzung der überarbeiteten Fassung: Der Abschnitt bilanziert die Entwicklungen seit Mai 2023 und prüft die damaligen Einschätzungen am eingetretenen Verlauf.)*

**Was geschehen ist.** Die Krisen von 2022 — Terra/UST-Kollaps (Abschnitt 3.5.1) und FTX-Insolvenz (Abschnitt 4.6) — prägten die politische Debatte, ohne den EU-Rechtsetzungsprozess auszulösen: Die politische Einigung über MiCA fiel bereits am 30. Juni 2022, wenige Wochen nach Terra und Monate vor dem FTX-Zusammenbruch [vgl. 95]; Terra hat die Stablecoin-Regeln der Verordnung mitgeprägt, FTX vor allem die Debatte um zentrale Verwahrer und den späteren Kurswechsel in den USA (Abschnitt 4.5.2) [vgl. 61]. Vollständig anwendbar ist MiCA seit Ende 2024; die USA haben mit dem GENIUS Act 2025 ein Bundesgesetz für Zahlungs-Stablecoins verabschiedet, dessen Pflichten allerdings erst mit dem Inkrafttreten — spätestens im Januar 2027 — greifen [vgl. 112]. Mit den Bitcoin-Spot-ETFs (Januar 2024) und tokenisierten Fonds (BUIDL, uMINT) wurde die institutionelle Adoption produktiv (Abschnitt 5.2.4). Innerhalb von DeFi verlagerte sich das Kapital: Liquid Staking wuchs zu einer der beiden kapitalstärksten Kategorien heran, Restaking entstand als neue Bausteinschicht (Abschnitt 3.5.6), ein wachsender Teil des gebundenen Kapitals liegt auf Layer-2-Netzwerken (Dencun-Upgrade, Abschnitt 5.2.3), und die Tokenisierung realer Vermögenswerte (RWA) entwickelte sich

zu einem schnell wachsenden Feld an der Schnittstelle beider Welten — mit BUIDL zählt ein tokenisierter TradFi-Fonds inzwischen zu den zehn größten Positionen des Protokoll-Snapshots ohne zentrale Verwahrbestände und Brücken (rund 3,5 Mrd. US-Dollar, Stand 02.08.2026) [46] (Abschnitt 5.2.4). Auf der Ebene der Nutzerfreundlichkeit adressiert die Kontoabstraktion — Wallets, die selbst Smart Contracts sind und dadurch Schlüsselwiederherstellung, Transaktionsbündelung und Gebührenübernahme durch Dritte erlauben (u. a. mit dem in Abschnitt 5.2.3 erwähnten Pectra-Upgrade) — die in dieser Arbeit benannten Zugangshürden Schlüsselverwahrung und Bedienkomplexität (M4). Ihr Verbreitungsgrad ist jedoch nicht aus Quellen belegbar, die den Gütekriterien aus Abschnitt 1.3 genügen; eine Aussage über die Wirkung wäre spekulativ.

**Prognosen-Check.** Vier Einschätzungen der Erstfassung lassen sich nun überprüfen. (1) *DeFi werde das traditionelle Finanzwesen ergänzen, nicht ersetzen* (Erstfassung, Fazit) — **bestätigt**, und zwar deutlicher als dort erwartet: Die Integration verlief fast ausschließlich über tokenisierte Produkte der Institutionen, nicht über deren Nutzung offener Protokolle (Abschnitt 5.2.4). (2) *Zunehmende Regulierung mit offenem Ausgang* — die Erstfassung sah die Regulierung „in den Kinderschuhen“ und ließ ihre Wirkung ausdrücklich offen (sie könne „sowohl Chancen als auch Risiken“ mit sich bringen). **Eingetreten ist an den Schnittstellen die Chancen-Variante**: MiCA hat für Verwahrer, Emittenten und Handelsplätze Rechtssicherheit geschaffen; für die dezentralen Protokolle selbst ist die Frage offen geblieben (Abschnitt 4.5.2). (3) *Marktwachstum* — die Erstfassung traf bewusst keine Punktprognose („Es bleibt abzuwarten, wie sich der Markt in Zukunft entwickeln wird“), zeichnete aber durchgehend das Bild eines stark wachsenden Marktes. Gemessen daran ist der Befund gemischt: Der TVL erreichte mit 171,0 Mrd. US-Dollar (07.10.2025) das Hoch von 2021 (177,5 Mrd., 09.11.2021) fast wieder, liegt zum Stichtag aber bei 74,2 Mrd. US-Dollar (02.08.2026) [48]; nachhaltig gewachsen sind stattdessen Stablecoins (rund 307 Mrd. US-Dollar, Abschnitt 3.5.1) und tokenisierte Produkte. (4) *Die Nexus-Mutual-Roadmap zur Absicherung von „Real-World-Risiken“* (Erstfassung, Ausblick) — **nur ansatzweise eingetreten**: Das Protokoll hat 2024 eine Kooperation mit dem in Bermuda regulierten Rückversicherungsdienstleister Ensuro geschlossen, über die reale Versicherungsrisiken auf das Mitglieder-Kapital transferiert werden können [vgl. 84]; die gezeichneten Deckungen blieben jedoch ganz überwiegend im Kryptoumfeld, und die Absicherungskategorie ist klein geblieben (Abschnitt 4.4.1). Insgesamt haben sich die strukturellen Einschätzungen von 2023 bestätigt; die verbreitete Wachstumszuversicht jener Zeit hat der Verlauf relativiert.

## 6.3. Limitationen und kritische Reflexion

*(Ergänzung der überarbeiteten Fassung.)*

Die Aussagekraft dieser Arbeit ist durch ihre Methodik begrenzt. Erstens beruht sie auf

Literatur- und Sekundärdatenanalyse: Es wurden keine eigenen empirischen Erhebungen durchgeführt; die Antwort auf FF4 stützt sich auf öffentlich dokumentierte Positionen von Instituten und Aufsehern und kann strategische Selbstdarstellung nicht von tatsächlicher Überzeugung trennen (Abschnitt 1.3). Zweitens trägt die zentrale Kennzahl TVL systematische Schwächen — US-Dollar-Bewertungseffekte, Doppelzählungsrisiken bei Liquid Staking und Restaking —, die Niveauvergleiche über die Zeit verzerren können; diese Arbeit begegnet dem durch Stichtage und eine einheitliche Datenquelle, beseitigt das Problem aber nicht. Drittens ist die Fallstudienauswahl auf etablierte Protokolle beschränkt und trägt damit eine Überlebensverzerrung (survivorship bias): Gescheiterte Protokolle sind systematisch unterrepräsentiert — der Opyn-Befund (Abschnitt 4.4.2) deutet an, was eine Ausfallanalyse leisten könnte. Viertens veraltet der Gegenstand schnell; alle Marktangaben gelten für ihre ausgewiesenen Stichtage, und die reproduzierbare Datengrundlage (Abschnitt 1.3) ist der Versuch, diesem Problem methodisch zu begegnen. Fünftens bleibt der Vergleich zwischen DeFi und traditionellem Finanzwesen überwiegend qualitativ: Die Kostendimension (M3) wird strukturell und an Beispielen beschrieben, nicht systematisch gemessen — ein belastbarer Kostenvergleich hätte Transaktionsdaten beider Systeme und eine Normierung auf vergleichbare Vorgänge erfordert; Abschnitt 6.4 führt dies als Anschlussfrage. Sechstens ist die Regulierungsanalyse auf die EU und die USA beschränkt; die für den Sektor bedeutsamen Regime etwa in Singapur, Hongkong und den Vereinigten Arabischen Emiraten bleiben außer Betracht, was die geografische Reichweite der Aussagen zu FF3 und FF4 begrenzt.

Kritisch zu reflektieren ist schließlich die zeitgebundene Perspektive: Die Debatte des Jahres 2023 war — quer durch die Literatur — von den Effizienz- und Inklusionsversprechen des Sektors geprägt. Diese Fassung setzt dem die Merkmalsprofile, die Risikotaxonomie und den Prognosen-Check als Korrektive entgegen.

## 6.4. Ausblick

*(Ergänzung der überarbeiteten Fassung: zwei Szenarien und offene Forschungsfragen.)*

Der weitere Weg des Sektors lässt sich nicht seriös als Punktprognose fassen; an die Stelle einer einzelnen Erwartung treten deshalb zwei Szenarien und die Fragen, an denen sich ihr Eintreten entscheidet.

**Integrationsszenario.** Die Tokenisierung traditioneller Vermögenswerte wächst weiter, Stablecoins werden zum regulierten Standard-Zahlungsmedium der Token-Ökonomie, und die Effizienzgewinne der Blockchain-Abwicklung wandern in die Infrastruktur der Institutionen. DeFi-Protokolle bedienen in diesem Szenario eine spezialisierte Nische und liefern weiterhin die technischen Blaupausen; die Grenze zwischen „DeFi“ und „tokenisiertem TradFi“ verwischt zugunsten des letzteren. Die Entwicklungen 2023–2026 stützen dieses Szenario am stärksten.

**Divergenzszenario.** Die dezentralen Protokolle behalten eine eigenständige, wachsende Sphäre — getrieben von Nutzern, für die Verwahrungsfreiheit und Zensurresistenz den Ausschlag geben, und von Anwendungsfällen, die das regulierte System nicht bedient. Voraussetzung wären deutliche Fortschritte bei Nutzerfreundlichkeit (Kontoabstraktion), Absicherungsmärkten und der ungelösten Frage der Protokoll-Governance; die Regulierung „vollständig dezentraler“ Systeme (Abschnitt 4.5.2) bliebe der offene Konfliktpunkt.

**Offene Forschungsfragen.** Aus dieser Arbeit ergeben sich Anschlussfragen: die empirische Messung tatsächlicher Kostenvorteile der Blockchain-Abwicklung gegenüber modernisierten traditionellen Systemen (Echtzeitzahlungen); die Wirksamkeit der MiCA-Schnittstellenregulierung und die künftige Behandlung dezentraler Protokolle (EU-DeFi-Review); Systemrisiken aus Restaking und der Verflechtung tokenisierter TradFi-Produkte mit DeFi-Protokollen; sowie eine Ausfallanalyse gescheiterter Protokolle als Korrektiv der Überlebensverzerrung. Der DeFi-Markt bleibt dynamisch; welche der beiden Entwicklungslinien dominiert, werden die kommenden Marktzyklen zeigen. Das Analyseraster (M1–M6) und die reproduzierbare Datengrundlage dieser Arbeit (Abschnitt 1.3) lassen sich für diese Beobachtung fortschreiben.

# A. Glossar

**Layer 1 / Layer 2** — Layer 1 bezeichnet die Grundebene einer Blockchain: die Kernfunktionalität einschließlich Konsensmechanismus, Blockgröße, Netzwerkarchitektur und Programmierumgebung. Öffentliche Blockchains wie Bitcoin oder Ethereum sind Layer-1-Blockchains. Layer 2 bezeichnet zusätzliche Protokolle, die auf einer Layer-1-Blockchain aufsetzen, um Funktionalität hinzuzufügen oder die Skalierbarkeit zu verbessern — etwa Sidechains oder Off-Chain-Protokolle wie das Lightning-Netzwerk, die Transaktionen schneller und kostengünstiger machen [82].

**Orakel (Oracle)** — Ein Oracle ist eine externe Informationsquelle, die es einer Blockchain ermöglicht, Informationen zu verarbeiten, die nicht innerhalb der Blockchain verfügbar sind (z. B. Marktpreise). Es fungiert als Vermittler zwischen der Blockchain und der realen Welt und ermöglicht Smart Contracts, auf Echtzeitdaten zu reagieren. Ohne Oracles wären viele Blockchain-Anwendungen stark eingeschränkt [vgl. 100].

# Literatur


[1] Aave Labs. *Aave Protocol Documentation (v3/v4)*. 2026. URL: https://aave.com/docs (besucht am 2. August 2026).

[2] Aave Protocol. *Aave*. 2023. URL: https://aave.com/ (besucht am 9. März 2023).

[3] Aave Team. *LendingPoolCore.sol Contract*. 2021. URL: https://github.com/aave/aave-protocol/blob/master/contracts/lendingpool/LendingPoolCore.sol (besucht am 16. März 2023).

[4] Andreas M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA: O'Reilly Media, 2014.

[5] Andreas M. Antonopoulos und Gavin Wood. *Mastering Ethereum: Building Smart Contracts and Dapps*. O'Reilly Media, 2018.

[6] Sirio Aramonte u. a. *DeFi lending: intermediation without information?* BIS Bulletin 57. Bank for International Settlements, 2022. URL: https://www.bis.org/publ/bisbull57.htm (besucht am 2. August 2026).

[7] Nicola Atzei, Massimo Bartoletti und Tiziana Cimoli. „A Survey of Attacks on Ethereum Smart Contracts (SoK)". In: *Principles of Security and Trust (POST 2017)*. 2017. DOI: 10.1007/978-3-662-54455-6_8.

[8] Raphael Auer, Gideon Choi und Samarendra Kundu. *AMM-based Decentralised Exchanges and the role of token governance*. Working Paper 1066. Bank for International Settlements, Februar 2022. URL: https://www.bis.org/publ/work1066.pdf (besucht am 4. April 2023).

[9] Dmitriy Berenzon. *Constant Function Market Makers: DeFi's Zero to One Innovation*. Medium.com. April 2020. URL: https://medium.com/bollinger-investment-group/constant-function-market-makers-defis-zero-to-one-innovation-968f77022159 (besucht am 14. April 2022).

[10] Binance Research. „DeFi Series 1 - Decentralized Cryptoasset Lending Borrowing". In: *Binance Research* (2019).

[11] BitMEX. *Perpetual Contracts Guide*. 2026. URL: https://www.bitmex.com/app/perpetualContractsGuide (besucht am 2. August 2026).

[12] Blockchain.com. *Blockchain Data and Charts API (Hash Rate, Blockdaten)*. 2026. URL: https://api.blockchain.info/charts/hash-rate (besucht am 1. August 2026).

[13] Blockchaincenter.net. *1inch Exchange: A Comprehensive Guide*. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. 2021. URL: https://web.archive.org/web/20231201194041/https://www.blockchaincenter.net/1inch-exchange/ (besucht am 4. April 2023).

[14] blockchainfiles.org. *Yield Farming Optimizer | Yearn Finance*. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. Dezember 2021. URL: https://web.archive.org/web/20240303065910/https://blockchainfiles.org/yearn-finance/ (besucht am 3. August 2026).

[15] Blockworks. *Hyperliquid's HYPE Airdrop Breaks the Mold*. November 2024. URL: https://blockworks.com/news/hyperliquid-hype-airdrop (besucht am 3. August 2026).

[16] Antonio Briola u. a. „Anatomy of a Stablecoin's failure: The Terra-Luna case". In: *Finance Research Letters* 51 (2023). DOI: 10.1016/j.frl.2022.103358.

[17] Rainer Brühl u. a. „Open banking and PSD2—opportunities and challenges". In: *Journal of Payments Strategy & Systems* 13.4 (2019).

[18] Bundesanstalt für Finanzdienstleistungsaufsicht. *Kryptowerte und MiCAR: Aufsicht über Krypto-Dienstleister*. 2026. URL: https://www.bafin.de/DE/unternehmen-maerkte/aufsicht/kryptoinstitute/kryptoinstitute_node.html (besucht am 2. August 2026).

[19] Bundesministerium der Finanzen. *Einzelfragen zur ertragsteuerrechtlichen Behandlung bestimmter Kryptowerte (BMF-Schreiben vom 6. März 2025)*. 2025. URL: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Einkommensteuer/2025-03-06-einzelfragen-kryptowerte.html (besucht am 2. August 2026).

[20] Vitalik Buterin. *Ethereum White Paper. A next generation smart contract decentralized application platform*. 2014. URL: https://ethereum.org/en/whitepaper/ (besucht am 3. August 2026).

[21] bZx LLC. *bZx Litepaper*. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. 2018. URL: https://web.archive.org/web/20210715221325/https://bzx.network/pdfs/bZx_lite_paper.pdf (besucht am 5. April 2022).

[22] Giulio Caldarelli. „Wrapping Trust for Interoperability: A Preliminary Study of Wrapped Tokens". In: *Information* 13.1 (2022). DOI: 10.3390/info13010006. URL: https://www.mdpi.com/2078-2489/13/1/6.

[23] Cambridge Centre for Alternative Finance. *Cambridge Bitcoin Electricity Consumption Index (CBECI)*. 2026. URL: https://ccaf.io/cbnsi/cbeci (besucht am 2. August 2026).

[24] CertiK. *Hack3d: The Web3 Security Report – H1 2026*. Juli 2026. URL: https://www.certik.com/skynet-report/certik-hack3d-h1-2026-report (besucht am 3. August 2026).

[25] Andrea Chello. *DeFi - Derivatives: Synthetix*. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. Dezember 2021. URL: https://web.archive.org/web/20220629090339/https://medium.com/the-quant-journey/defi-derivatives-synthetix-c6cfbb8db6e0?source=post_internal_links---------4---------- (besucht am 3. August 2026).

[26] Circle Internet Group. *Circle Announces Pricing of Upsized Initial Public Offering*. Juni 2025. URL: https://www.circle.com/pressroom/circle-announces-pricing-of-upsized-initial-public-offering (besucht am 3. August 2026).

[27] Citigroup. *Citi Develops New Digital Asset Capabilities for Institutional Clients (Citi Token Services)*. 2023. URL: https://www.citigroup.com/global/news/press-release/2023/citi-develops-new-digital-asset-capabilities-for-institutional-clients (besucht am 2. August 2026).

[28] Coinbase. *Moving Markets Onchain: Welcoming Opyn Markets to Coinbase*. Juli 2025. URL: https://www.coinbase.com/blog/moving-markets-onchain-welcoming-opyn-markets-to-coinbase (besucht am 3. August 2026).

[29] CoinDesk. *Circle Raises $50 Million with Goldman Sachs Support*. 2015. URL: https://www.coindesk.com/markets/2015/04/30/circle-raises-50-million-with-goldman-sachs-support (besucht am 2. August 2026).

[30] CoinDesk. *DeFi Projects Cover, Ruler Are Shutting Down After Development Team Exits*. 2021. URL: https://www.coindesk.com/business/2021/09/05/defi-projects-cover-ruler-are-shutting-down-after-development-team-exits (besucht am 2. August 2026).

[31] CoinDesk. *MakerDAO Is Now 'Sky' as $7B Crypto Lender Rolls Out New Stablecoin, Governance Token*. 2024. URL: https://www.coindesk.com/business/2024/08/27/makerdao-is-now-sky-as-7b-crypto-lender-rolls-out-new-stablecoin-governance-token (besucht am 2. August 2026).

[32] CoinDesk. *HyperLiquid Delists JELLY After Vault Squeezed in $13M Tussle*. März 2025. URL: https://www.coindesk.com/markets/2025/03/26/hyperliquid-delists-jellyjelly-after-vault-squeezed-in-usd13m-tussle (besucht am 3. August 2026).

[33] Committee on Payments and Market Infrastructures. *CPMI Cross-border Payments Programme (G20-Roadmap-Monitoring)*. Bank for International Settlements. URL: https://www.bis.org/cpmi/cross_border.htm (besucht am 2. August 2026).

[34] Commodity Futures Trading Commission. *CFTC Issues Orders Against Operators of Three DeFi Protocols (Opyn, ZeroEx, Deridex)*. 2023. URL: https://www.cftc.gov/PressRoom/PressReleases/8774-23 (besucht am 2. August 2026).

[35] Compound Labs. *Compound Protocol Documentation*. 2026. URL: https://docs.compound.finance/ (besucht am 2. August 2026).

[36] James Condos, William Sorrell und Susan Donegan. *Blockchain Technology: Opportunities and Risks*. Report. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. State of Vermont, 2016. URL: https://web.archive.org/web/20220901084148/https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf (besucht am 26. April 2022).

[37] Consensys. *JPMorgan to Use Ethereum-Based ConsenSys Quorum for Interbank Information Network*. 2019. URL: https://www.consensys.net/blog/press-release/jpmorgan-ethereum-consensys-quorum/ (besucht am 10. März 2023).

[38] Consensys. *What Is Decentralized Finance (DeFi)*. URL: https://consensys.net/blockchain-use-cases/decentralized-finance/ (besucht am 8. März 2023).

[39] Crypto.com. *DeFi Trading: Introduction to Futures*. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. Januar 2021. URL: https://web.archive.org/web/20240527163828/https://crypto.com/university/defi-futures-introduction (besucht am 3. August 2026).

[40] Curve Finance. *Boosting your CRV Rewards*. 2021. URL: https://resources.curve.fi/reward-gauges/boosting-your-crv-rewards (besucht am 11. September 2022).

[41] Curve Finance. *Curve Resources – Reward Gauges und Boosting*. 2026. URL: https://resources.curve.finance/ (besucht am 2. August 2026).

[42] J. Dafflon, J. Baylina und T. Shababi. *ERC-777 Token Standard*. 2015. URL: https://eips.ethereum.org/EIPS/eip-777 (besucht am 3. August 2026).

[43] DeFiLlama. *DeFiLlama*. 2023. URL: https://defillama.com/ (besucht am 9. März 2023).

[44] DeFiLlama. *Chains – TVL je Blockchain (API-Endpunkt v2/chains)*. 2026. URL: https://api.llama.fi/v2/chains (besucht am 2. August 2026).

[45] DeFiLlama. *Protocol Rankings – Kategorien-Aggregation aus dem /protocols-Endpoint (eingecheckter Snapshot)*. Aggregation: abbildungen/snapshot_kategorien.py; Daten: abbildungen/daten/defillama_kategorien.json. 2026. URL: https://api.llama.fi/protocols (besucht am 3. August 2026).

[46] DeFiLlama. *Protocols – TVL je Protokoll (API-Endpunkt protocols)*. 2026. URL: https://api.llama.fi/protocols (besucht am 2. August 2026).

[47] DeFiLlama. *Stablecoins – Marktkapitalisierung je Asset (API-Endpunkt stablecoins)*. 2026. URL: https://stablecoins.llama.fi/stablecoins (besucht am 2. August 2026).

[48] DeFiLlama. *Total Value Locked – historische Zeitreihe (API-Endpunkt historicalChainTvl)*. 2026. URL: https://api.llama.fi/v2/historicalChainTvl (besucht am 2. August 2026).

[49] Deutsche Bundesbank. *PSD2*. 2023. URL: https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/psd2/psd2-775434 (besucht am 4. April 2023).

[50] Deutscher Bundestag. *Kryptomärkteaufsichtsgesetz (KMAG), § 50 Übergangsvorschriften*. 2024. URL: https://www.gesetze-im-internet.de/kmag/__50.html (besucht am 3. August 2026).

[51] Monika Di Angelo und Gernot Salzer. „Tokens, Types, and Standards: Identification and Utilization in Ethereum“. In: *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*. August 2020. DOI: 10.1109/DAPPS49028.2020.00001.

[52] die bank. *Wenn Banken Neuland betreten*. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. 2020. URL: https://web.archive.org/web/20191019145631/http://www.die-bank.de/news/wenn-banken-neuland-betreten-946/ (besucht am 9. März 2023).

[53] Moritz Draht. *Ethereum Merge abgeschlossen: Proof of Stake ist da!* 2023. URL: https://www.btc-echo.de/news/ethereum-merge-abgeschlossen-proof-of-stake-150703/ (besucht am 26. März 2023).

[54] Barry Eichengreen. *Golden Fetters: The Gold Standard and the Great Depression, 1919-1939*. Oxford University Press, 1992.

[55] Barry Eichengreen. *Exorbitant Privilege: The Rise and Fall of the Dollar and the Future of the International Monetary System*. Oxford University Press, 2011.

[56] ethereum.org. *The history of Ethereum – Netzwerk-Upgrades (Merge, Dencun, Pectra)*. 2026. URL: https://ethereum.org/en/history/ (besucht am 2. August 2026).

[57] Europäische Kommission. *Targeted Consultation on the Review of the MiCA Regulation*. Mai 2026. URL: https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-review-mica-regulation_en (besucht am 3. August 2026).

[58] Europäische Union. *Richtlinie 2014/49/EU über Einlagensicherungssysteme*. 2014. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014L0049 (besucht am 2. August 2026).

[59] Europäische Union. *Verordnung (EU) Nr. 909/2014 (Zentralverwahrer-Verordnung, CSDR)*. 2014. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0909 (besucht am 2. August 2026).

[60] Europäische Union. *Verordnung (EU) 2015/751 über Interbankenentgelte für kartengebundene Zahlungsvorgänge*. 2015. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32015R0751 (besucht am 2. August 2026).

[61] Europäische Union. *Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA)*. 2023. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023R1114 (besucht am 2. August 2026).

[62] European Banking Authority und European Securities and Markets Authority. *Joint Report on Recent Developments in Crypto-Assets (Art. 142 MiCAR)*. Report. EBA/ESMA, 2025. URL: https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-esma-analyse-recent-developments-crypto-assets (besucht am 2. August 2026).

[63] Hans-Georg Fill und Andreas Meier. *Blockchain: Grundlagen, Anwendungsszenarien und Nutzungspotenziale*. Springer Fachmedien Wiesbaden GmbH, 2020. DOI: 10.1007/978-3-658-28006-2.

[64] Financial Stability Board. *The Financial Stability Risks of Decentralised Finance*. Report. Financial Stability Board, 2023. URL: https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/ (besucht am 2. August 2026).

[65] Financial Stability Board. *Global Monitoring Report on Nonbank Financial Intermediation 2025*. Report. Financial Stability Board, Dezember 2025. URL: https://www.fsb.org/2025/12/global-monitoring-report-on-nonbank-financial-intermediation-2025/ (besucht am 2. August 2026).

[66] Franklin Templeton. *Franklin OnChain U.S. Government Money Fund (FOBXX) – erster US-registrierter tokenisierter Geldmarktfonds*. 2021. URL: https://www.franklintempleton.com/investments/options/money-market-funds (besucht am 2. August 2026).

[67] Benedict George. *What Is a CEX? Centralized Exchanges Explained*. Februar 2022. URL: https://www.coindesk.com/learn/what-is-a-cex-centralized-exchanges-explained/ (besucht am 14. April 2022).

[68] Hans Gersbach, Akaki Mamageishvili und Manvir Schneider. *Staking Pools on Blockchains*. August 2022. arXiv: 2203.05838. URL: https://arxiv.org/abs/2203.05838 (besucht am 3. August 2026).

[69] Goldman Sachs. *Goldman Sachs Intends to Spin Out Its Digital Asset Platform (GS DAP)*. 2024. URL: https://www.goldmansachs.com/pressroom/press-releases/2024/announcement-18-nov-2024 (besucht am 2. August 2026).

[70] Merunas Grincalaitis. *Mastering Ethereum. Implement advanced blockchain applications using Ethereum-supported tools, services, and protocols*. Hrsg. von Sunith Shetty. Packt Publishing Ltd., 2019.

[71] Florian Gronde. „Flash Loans and Decentralized Lending Protocols: An In-Depth Analysis“. Magisterarb. University of Basel.

[72] John C. Hull. *Options, Futures and other Derivatives*. 9. Aufl. Pearson Education Inc, 2015.

[73] Hyperliquid. *Hyperliquid Documentation – L1 Overview, Trading und Funding*. 2026. URL: https://hyperliquid.gitbook.io/hyperliquid-docs (besucht am 3. August 2026).

[74] ibi research an der Universität Regensburg GmbH. *E-Payment-Verfahren*. 2009. URL: http://www.ecommerce-leitfaden.de/images/big/E-Commerce-Leitfaden_Erfolgreich_im_elektronischen_Internet-Handel_Abb4-5_gross_Ablauf_einer_Zahlung_per_Kreditkarte.jpg (besucht am 7. April 2023).

[75] J.P. Morgan. *Kinexys by J.P. Morgan (vormals Onyx) – Blockchain-Zahlungs- und Tokenisierungsplattform*. 2024. URL: https://www.jpmorgan.com/kinexys (besucht am 2. August 2026).

[76] T. Knecht. *Finanzwissen kompakt*. Springer Gabler, 2019.

[77] Leslie Lamport, Robert Shostak und Marshall Pease. „The Byzantine Generals Problem“. In: *ACM Transactions on Programming Languages and Systems* 4.3 (1982), S. 382–401.

[78] Loi Luu und Yaron Velner. *KyberNetwork: A trustless decentralized exchange and payment service*. 2017. URL: https://whitepaper.io/document/43/kyber-network-whitepaper (besucht am 20. April 2022).

[79] Morpho Labs. *Morpho Blue Launched on the 11th of January (Mitteilung)*. April 2024. URL: https://x.com/Morpho/status/1776228481850098095 (besucht am 3. August 2026).

[80] J. J. Murphy. *Technical Analysis of the Financial Markets*. Prentice Hall, 1999.

[81] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf (besucht am 3. August 2026).

[82] A. Narayanan u. a. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[83] Nexus Mutual. *Nexus Mutual*. 2023. URL: https://nexusmutual.io/ (besucht am 9. März 2023).

[84] Nexus Mutual. *Nexus Mutual and Ensuro Partner to Connect Onchain Capital with Real-World Risk*. November 2024. URL: https://nexusmutual.io/blog/nexus-mutual-and-ensuro-partner-to-connect-onchain-capital-with-real-world-risk (besucht am 2. August 2026).

[85] Nexus Mutual. *Nexus Mutual Documentation – Cover Products*. 2026. URL: https://docs.nexusmutual.io/overview/cover-products/ (besucht am 2. August 2026).

[86] NTT DATA. *Kryptoverwahrung*. 2021. URL: https://de.nttdata.com/insights/expert-guide/kryptoverwahrung (besucht am 14. März 2023).

[87] L. Oliveira u. a. „To token or not to token: Tools for understanding blockchain tokens“. In: *International Conference on Information Systems (ICIS)*. 2018.

[88] Opyn. *Squeeth Has Shutdown*. November 2024. URL: https://medium.com/opyn/squeeth-has-shutdown-a8a3c2869eaa (besucht am 3. August 2026).

[89] Michael Oved und Don Mosites. *Swap: A Peer-to-Peer Protocol for Trading Ethereum Tokens*. 2017. URL: https://www.airswap.io/whitepaper.htm%5C#peer-protocol (besucht am 20. April 2022).

[90] PancakeSwap. *Introducing PancakeSwap Infinity: For Developers, Traders & Every User*. April 2025. URL: https://blog.pancakeswap.finance/articles/introducing-pancake-swap-for-developers-traders-and-every-user (besucht am 3. August 2026).

[91] President's Working Group on Financial Markets, Federal Deposit Insurance Corporation und Office of the Comptroller of the Currency. *Report on Stablecoins*. Report 1. President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, und Office of the Comptroller of the Currency, November 2021. URL: https://home.treasury.gov/news/press-releases/jy0456 (besucht am 3. August 2026).

[92] PwC. *FinTech Global Report 2016*. Report. PwC, 2016. URL: https://www.pwc.co.uk/financial-services/fintech/assets/FinTech-Global-Report2016.pdf (besucht am 6. April 2023).

[93] Kaihua Qin u. a. „Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit“. In: *Financial Cryptography and Data Security (FC 2021)*. 2021. DOI: 10.1007/978-3-662-64322-8_1.

[94] Witek Radomski u. a. *EIP-1155: Multi Token Standard*. Juni 2018. URL: https://eips.ethereum.org/EIPS/eip-1155 (besucht am 31. März 2022).

[95] Rat der Europäischen Union. *Digital Finance: Agreement Reached on European Crypto-assets Regulation (MiCA)*. Juni 2022. URL: https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/ (besucht am 3. August 2026).

[96] Andreas Rauscher und Zoran Cupic. *Blockchain-basierte Smart Contracts*. PDF-Datei. 2018. URL: https://www.syntax-solution.de/wp-content/uploads/sites/7/2018/02/Blockhain-bassierte-Smart-Contract-Andreas-Rauscher-Zoran-Cupic.pdf (besucht am 3. August 2026).

[97] Fahad Saleh. „Blockchain without Waste: Proof-of-Stake“. In: *The Review of Financial Studies* 34 (Juli 2021). DOI: 10.1093/rfs/hhaa075.

[98] Estefania Santacreu-Vasut und Laurent Deville. „Tokenization of Funds: Smart Contract Management and Legal Framework“. In: *Journal of Risk and Financial Management* 12.3 (2019). DOI: 10.3390/jrfm12030130. URL: https://www.mdpi.com/1911-8074/12/3/130.

[99] Fabian Schär. *Decentralised Finance: Hype oder next big thing?* Archivfassung via archive.org; Original-URL nicht mehr erreichbar. Deutsche Bundesbank. 2021. URL: https://web.archive.org/web/20240226195714/https://www.bundesbank.de/de/service/mediathek/videos/fabian-schaer-decentralised-finance-hype-oder-next-big-thing--898858 (besucht am 3. August 2026).

[100] Fabian Schär. „Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets“. In: *Federal Reserve Bank of St. Louis Review* 103.2 (April 2021). Archivfassung via archive.org; Original-URL nicht mehr erreichbar, S. 153–174. DOI: 10.20955/r.103.153-74. URL: https://web.archive.org/web/20230511061645/https://files.stlouisfed.org/files/htdocs/publications/review/2021/04/15/full-issue.pdf (besucht am 12. November 2022).

[101] Vincent Schlatt u. a. *Blockchain: Grundlagen, Anwendungen und Potenziale*. Report. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Institut für Angewandte Informationstechnik FIT, 2016. URL: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf (besucht am 3. August 2026).

[102] Securitize. *BlackRock Launches Its First Tokenized Fund, BUIDL, on the Ethereum Network*. 2024. URL: https://securitize.io/press-releases/blackrock-launches-first-tokenized-fund-buidl-on-the-ethereum-network (besucht am 2. August 2026).

[103] Stably. *Decentralized Finance vs. Traditional Finance: What You Need to Know*. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. August 2020. URL: https://web.archive.org/web/20230925072311/https://stably.io/decentralized-finance-vs-traditional-finance-what-you-need-to-know/ (besucht am 3. August 2026).

[104] William Stallings. *Cryptography and Network Security: Principles and Practice*. 7. Aufl. Pearson, 2016.

[105] Marc Stevens u. a. „The First Collision for Full SHA-1“. In: *Advances in Cryptology – CRYPTO 2017*. 2017. DOI: 10.1007/978-3-319-63688-7_19.

[106] Synthetix. *Synthetix Documentation – Staking and Collateralization Ratio*. 2026. URL: https://docs.synthetix.io/ (besucht am 2. August 2026).

[107] Nick Szabo. *Smart Contracts*. 1994. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (besucht am 31. März 2022).

[108] The Block. *Hyperliquid Gains Ground on Centralized Exchanges as Perps Market Share Nears 6%*. April 2026. URL: https://www.theblock.co/post/395728/hyperliquid-gains-centralized-exchanges-perps-market-share-nears-6 (besucht am 3. August 2026).

[109] The Block. *Hyperliquid vs Exchanges Monthly Perpetual Volumes (Datenreihe)*. 2026. URL: https://www.theblock.co/data/decentralized-finance/derivatives/hyperliquid-vs-exchanges-monthly-perpetual-volumes (besucht am 3. August 2026).

[110] Alan Turing. „On computable numbers, with an application to the Entscheidungsproblem“. In: *Proceedings of the London Mathematical Society*. 2. Ser. 42 (1937), S. 230–265. DOI: 10.1112/plms/s2-42.1.230.

[111] U.S. Congress. *H.R.3633 – Digital Asset Market Clarity Act of 2025*. 2025. URL: https://www.congress.gov/bill/119th-congress/house-bill/3633 (besucht am 3. August 2026).

[112] U.S. Congress. *S.1582 – GENIUS Act of 2025 (Guiding and Establishing National Innovation for U.S. Stablecoins Act)*. 2025. URL: https://www.congress.gov/bill/119th-congress/senate-bill/1582 (besucht am 2. August 2026).

[113] U.S. Securities and Exchange Commission. *Statement on the Approval of Spot Bitcoin Exchange-Traded Products*. 2024. URL: https://www.sec.gov/newsroom/speeches-statements/gensler-statement-spot-bitcoin-011023 (besucht am 2. August 2026).

[114] U.S. Securities and Exchange Commission. *American Leadership in the Digital Finance Revolution (Rede von Chairman Paul S. Atkins, "Project Crypto")*. Juli 2025. URL: https://www.sec.gov/newsroom/speeches-statements/atkins-digital-finance-revolution-073125 (besucht am 3. August 2026).

[115] U.S. Securities and Exchange Commission. *Crypto Task Force*. 2025. URL: https://www.sec.gov/securities-topics/crypto-task-force (besucht am 2. August 2026).

[116] UBS. *UBS Asset Management launches its first tokenized investment fund (uMINT)*. 2024. URL: https://www.ubs.com/global/en/media/display-page-ndp/en-20241101-first-tokenized-investment-fund.html (besucht am 2. August 2026).

[117] Uniswap Labs. *Uniswap Protocol Documentation (v3/v4)*. 2026. URL: https://docs.uniswap.org/ (besucht am 2. August 2026).

[118] Paul Wackerow. *Proof-of-Stake (PoS)*. Juni 2022. URL: https://ethereum.org/de/developers/docs/consensus-mechanisms/pos/ (besucht am 11. September 2022).

[119] Dabao Wang u. a. *Towards understanding flash loan and its applications in defi ecosystem*. arXiv preprint arXiv:2010.12252. 2020. arXiv: 2010.12252. URL: https://arxiv.org/abs/2010.12252 (besucht am 3. August 2026).

[120] Will Warren und Amir Bandeali. *0x: An open protocol for decentralized exchange on the Ethereum blockchain*. Archivfassung via archive.org; Original-URL nicht mehr erreichbar. 0xProject.com. Februar 2017. URL: https://web.archive.org/web/20230329234922/https://www.0x.org/pdfs/0x_white_paper.pdf (besucht am 10. März 2023).

[121] Sam M. Werner u. a. *SoK: Decentralized Finance (DeFi)*. Report. Imperial College London Cornell University, 2021.

[122] Xun (Brian) Wu und Weimin Sun. *Blockchain Quick Start Guide. A beginner's guide to developing enterprise-grade decentralized applications*. Packt Publishing Ltd., 2018.

[123] Liyi Zhou u. a. „SoK: Decentralized Finance (DeFi) Attacks". In: *2023 IEEE Symposium on Security and Privacy (SP)*. 2023. URL: https://arxiv.org/abs/2208.13035 (besucht am 2. August 2026).