Decentralised Finance: Dezentrale Kreditplattformen – (ver)sicher(t)?

Stefan Mitzlaff, Lucas Johns
Deutsche Bundesbank, Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main & Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

Dezentrale Kreditplattformen ermöglichen Nutzern die Aufnahme sowie die Bereitstellung von Liquidität in Form von Krypto-Token gegen Verzinsung. Dieser Teil des dynamisch wachsenden Bereichs dezentraler Anwendungen erweist sich zwar als sehr innovativ, birgt jedoch auch Risiken. Dazu zählen insbesondere Kreditrisiken, Liquiditätsrisiken, Marktrisiken und operationelle Risiken. Um diesen Risiken entgegenzuwirken existieren vereinzelt Absicherungsmechanismen. Diese Mechanismen haben durchaus Potenzial die genannten Risiken zu verringern, wenngleich dadurch keine vollumfängliche Risikobewältigung erfolgen kann. Somit verbleiben immer Restrisiken, die letztlich vor allem von den Nutzern zu tragen sind.

1. Einleitung

Der Bereich Decentralised Finance (DeFi) entwickelt sich dynamisch und bringt neue Formen von Finanzdienstleistungen und -produkten hervor. So entstehen etwa Anwendungsfälle in Verbindung mit Krypto-Token, die Ähnlichkeiten zu Leistungen des konventionellen Finanzsystems aufweisen, wie beispielsweise dem Kredit- und Einlagengeschäft oder Versicherungen. Erbracht werden diese Leistungen von sogenannten dezentralen Anwendungen (Decentralised Applications, dApps).

Dezentrale Anwendungen basieren auf einem Distributed Ledger – üblicherweise in Form einer Blockchain – und auf Smart Contracts. Während die Blockchain als Transaktionssystem und -register dient, spezifizieren die darauf aufbauenden Smart Contracts die Anwendungslogik, also welche Bedingungen bei Transaktionen zu prüfen sind und welche Aktivitäten daraus folgen. So können komplexe, aufeinander aufbauende Geschäftsfälle automatisch abgewickelt werden. Im Extremfall können ganze Prozessketten, ähnlich zu Abläufen in Unternehmen, autonom implementiert werden. Der Begriff Dezentralität findet seinen Ursprung dabei insbesondere in dezentralen Prozessen zum Betrieb und zur Weiterentwicklung der Anwendungen [1]. Abbildung 1 zeigt eine Einordnung von dezentralen Anwendungen aus technischer Sicht.

Obwohl sich dezentrale Anwendungen aus technischer Sicht ähneln, können sie unterschiedliche Geschäftsfelder abdecken. Dezentrale Anwendungen etwa, denen Netzwerkakteure Krypto-Token gegen eine Verzinsung bereitstellen und die entsprechende Kredite herausgeben, werden auch als dezentrale Kreditplattformen bezeichnet. Gemessen an der Liquidität, die von Netzwerkakteuren in dezentralen Anwendungen hinterlegt wird, zählen Aave und Compound zu den größten Vertretern solcher Plattformen [2].

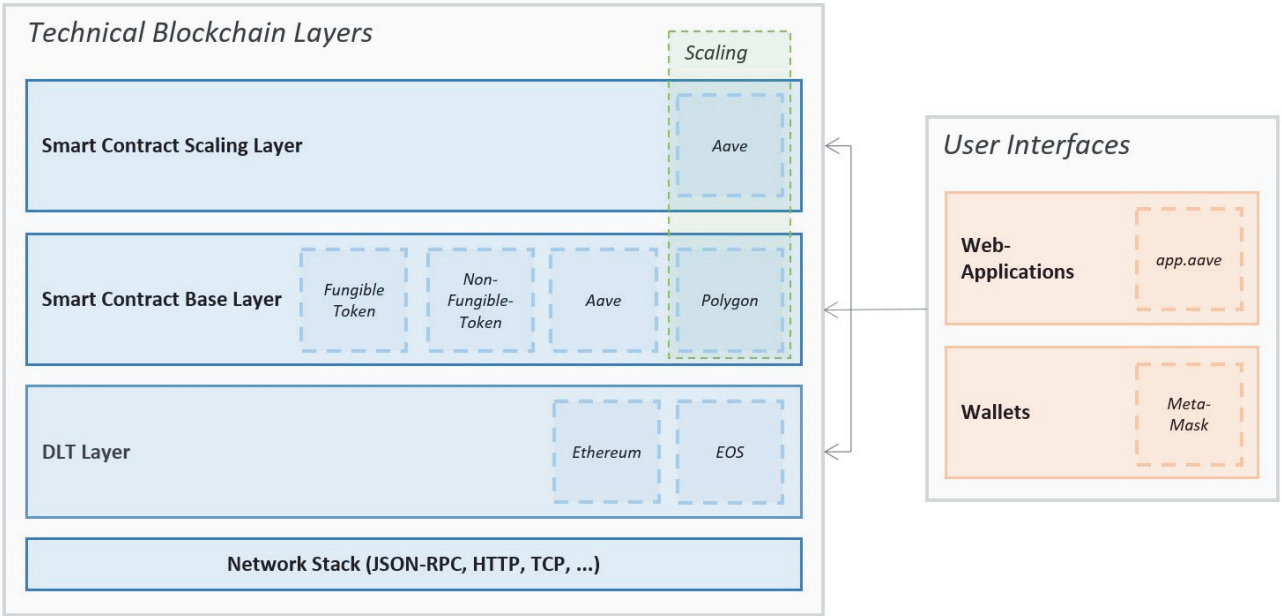

Abbildung 1: Stilisierte technische Darstellung dezentraler Anwendungen, Quelle: Eigene Darstellung. Beachte: Einträge mit gestrichelter Umrandung stellen Beispiele dar.

Die Nutzung dezentraler Anwendungen ist mit verschiedenen Risiken verbunden, die durch unklare oder fehlende Regulierungsanforderungen sowie die mangelnde Einhaltung ebendieser zum Teil verstärkt werden. Dabei ist insbesondere das Kreditrisiko hervorzuheben, das auch im konventionellen Finanzsystem eine der bedeutendsten Risikoarten darstellt. Kreditrisiken in Verbindung mit dezentralen Anwendungen können dadurch auftreten, dass Netzwerkakteure Anwendungen, etwa dezentralen Kreditplattformen Liquidität in Form von Krypto-Token bereitstellen und diese anschließend an andere Netzwerkakteure verliehen wird. Der genaue rechtliche Status dezentraler Anwendungen ist bislang ungeklärt, sodass auch Fragen der Haftung ungewiss sind. Entsprechend übertragen sich Kreditrisiken, die eigentlich durch die Anwendungen eingegangen werden, implizit auf deren Nutzer, die den Anwendungen Liquidität bereitstellen.

Der Artikel zielt darauf ab, zu einem besseren Verständnis der Risiken beizutragen, die mit der Nutzung dezentraler Kreditplattformen verbunden sind. Dabei spielen neben den Kreditrisiken auch Liquiditätsrisiken, Marktrisiken und operationellen Risiken eine Rolle. Diese vier Risikokategorien werden gemäß den Mindestanforderungen an das Risikomanagement (MaRisk) auch im Rahmen der Ausgestaltung des Risikomanagements von Kreditinstituten als wesentlich angesehen, weshalb sich der Artikel auf diese Risikoauswahl beschränkt [3]. Zudem wird aufgezeigt, welche anwendungsinhärenten sowie externen Absicherungsmechanismen gegen diese Risiken existieren.

Dezentrale Anwendungen befinden sich in einem frühen Entwicklungsstadium und entwickeln sich dynamisch weiter. Ein besseres Verständnis der Risiken, die innerhalb des Ökosystems dezentraler Anwendungen existieren, könnte zu einer besseren Regulierung dieses Bereiches beitragen. Denn eine effektive Regulierung könnte das Vertrauen in den Bereich stärken, wenngleich die Regulierung dabei vor besonderen Herausforderungen steht.

2. Arten dezentraler Kreditvergabe

Dezentrale Kreditplattformen ermöglichen Nutzern die Aufnahme sowie die Bereitstellung von Liquidität in Form von Krypto-Token gegen Verzinsung. Anders als Kreditinstitute betreiben sie dabei allerdings keine Geldschöpfung. Das klassische Beispiel für die Buchgeldschöpfung wäre die Kreditgewährung einer Bank an eine Nichtbank, bei der der Kreditbetrag auf einem Konto des Kreditnehmers gutgeschrieben wird. Auf der Bankbilanz entstehen eine Forderung und eine Verbindlichkeit, sodass es zu einer Bilanzverlängerung kommt. Im Ergebnis wurde Buchgeld geschaffen [4]. Dezentrale Kreditplattformen reichen hingegen lediglich Krypto-Token aus, die ihnen zuvor bereitgestellt wurden, sodass im Rahmen der Kreditvergabe keine neuen Krypto-Token geschaffen werden.

Dabei vermitteln dezentrale Kreditplattformen üblicherweise nicht direkt zwischen Kreditgebern und Kreditnehmern, wie es etwa bei Plattformen für Peer-To-Peer-Kredite der Fall ist. Stattdessen basieren dezentrale Kreditplattformen in der Regel auf sogenannten Lending Pools [5]. Eine direkte Kreditvergabe zwischen einzelnen Netzwerkakteuren kann jedoch etwa im Zusammenhang mit der Besicherung sogenannter Non Fungible Token (NFT) erfolgen. Dabei hinterlegt ein Nutzer Krypto-Token in einem Smart Contract und erhält im Gegenzug individuelle Kreditangebote von anderen Nutzern [6]. Nutzer können dabei also nicht unmittelbar ein Geschäft abschließen, sondern müssen zunächst immer erst einen geeigneten Kontrahenten finden. Dadurch ist die direkte Kreditvergabe zwischen Netzwerkakteuren im Vergleich zur Kreditvergabe mittels Lending Pools üblicherweise umständlicher und weniger liquide, weshalb sie seltener zur Anwendung kommt [7]. Lending Pools werden, wie in Abbildung 2 dargestellt, mittels Smart Contracts implementiert. Netzwerkakteure können den Pools Liquidität in Form von Krypto-Token bereitstellen. Im Gegenzug erhalten

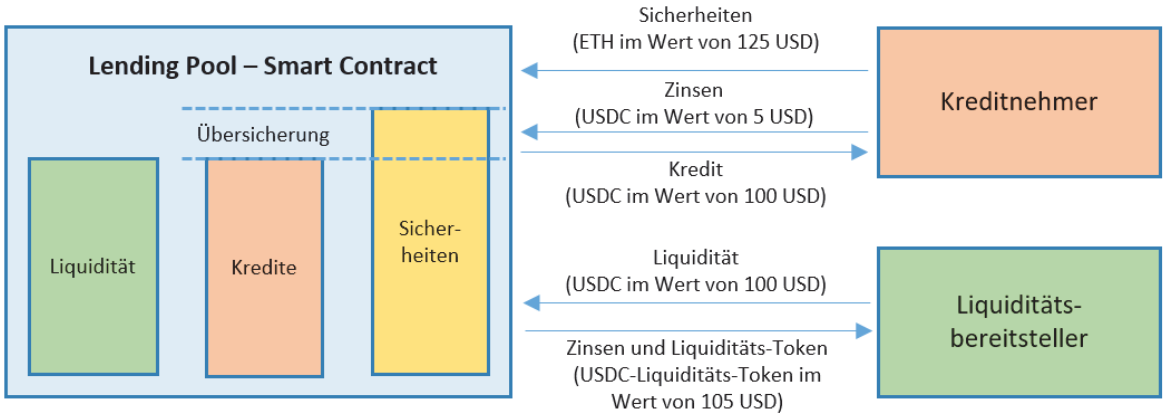

Abbildung 2: Exemplarische Funktionsweise von Lending Pools am Beispiel USD Coin (USDC), Quelle: Eigene Darstellung.

sie sogenannte Liquiditäts-Token, die ihre eingebrachte Liquidität repräsentieren und über welche die Zuteilung der Verzinsung abgebildet wird. Durch Rückgabe der Liquiditäts-Token kann die ursprünglich eingebrachte Liquidität wieder entnommen werden. Kreditnachfrager können dem Pool Liquidität entnehmen, sofern sie entsprechende Sicherheiten bereitstellen. Um einen Anreiz zur Rückzahlung zu schaffen und aufgrund der hohen Volatilität und Illiquidität vieler als Sicherheit verwendeter Krypto-Token müssen Kreditnehmer ihre Verbindlichkeiten oftmals überbesichern. Wie viel Kredit man erhält, hängt von der Art der Sicherheit ab [8]. Die Sicherheiten werden in einem Smart Contract hinterlegt und wieder freigegeben sobald der Kredit getilgt wurde [9, 10].

Unbesicherte Kredite können in Form sogenannter Flash Loans vergeben werden. Diese müssen innerhalb desselben Blockchain-Blocks zurückbezahlt werden, andernfalls erfolgt eine Rückabwicklung bzw. Nicht-Ausführung des gesamten Geschäfts. Dies wird durch die sequentielle Verarbeitung von Transaktionen der zugrundeliegenden Blockchain ermöglicht. Dabei wird ein Smart Contract verwendet, über welchen ein Kredit aufgenommen wird. Mit dieser Liquidität werden dann Transaktionen ausgeführt und der Kredit plus Zinsen im Anschluss automatisch zurückgezahlt. Diese Schritte müssen gebündelt und innerhalb eines Blockintervalls, also dem Zeitfenster zwischen der Erstellung zweier Blöcke, erfolgen. Ohne Rückzahlung würde eine Rückabwicklung sämtlicher vorher ausgeführter Schritte erfolgen, sodass auch die Kreditaufnahme nicht auf die Blockchain geschrieben wird [9, 11].

3. Mögliche Gründe für Kreditaufnahme

Die Vergabe von Krediten durch dezentrale Kreditplattformen grenzt sich aufgrund der Pseudo-Anonymität der Netzwerkakteure und den daraus resultierenden Sicherheitsanforderungen von traditionellen Bankkrediten deutlich ab. Durch die Übersicherung mit äquivalenten Vermögensgegenständen – in Form von Krypto-Token – oder der sehr kurzfristigen Laufzeit einiger Kreditarten gerät die Motivation eines Kreditnehmers sich Liquidität zu Konsum- oder Investitionszwecken zu beschaffen in den Hintergrund. Vielmehr dürften andere Gründe für eine Kreditaufnahme bei dezentralen Kreditplattformen sprechen, wie etwa Belohnungen, Leveraging, Arbitrage und dolose Handlungen.

Belohnungen: Anwendungen belohnen Nutzer – sowohl Liquiditätsbereitsteller als auch Kreditnehmer – zum Teil mit Governance-Token [7,12]. Governance-Token können eingesetzt werden, um dezentrale Governance-Prozesse mithilfe von kollektiven Abstimmungsverfahren abzubilden. Einige Anwendungen schütten zudem Erträge an die Inhaber der Governance-Token aus – vergleichbar mit einer Dividende. Governance-Token können dann sowohl zum Zweck der Stimmrechtsausübung als auch mit Ertragsaussichten gehalten oder veräußert werden. Die Nutzung einer dezentralen Kreditplattform könnte demnach mit der Erwartung auf Belohnungen in Form von Governance-Token einhergehen (sog. Liquidity Mining), und erhält dadurch einen Selbstzweck, da das eigentliche Kreditgeschäft von eher nachrangiger Bedeutung ist.

Leveraging: Die besicherte Kreditaufnahme kann beispielsweise dem Hebeln eigener Positionen dienen. Hält man Krypto-Token etwa in der Erwartung steigender Kurse, können diese als Kreditsicherheit verwendet werden [7, 12]. Wird der Kredit nun in Form von Stablecoins aufgenommen, können diese gegen volatilere Krypto-Token mit angenommenen Kurspotenzial getauscht werden. Dieser Anwendungsfall deckt sich damit, dass Kredite üblicherweise in Form von Stablecoins aufgenommen werden, wohingegen volatilere Krypto-Token eher als Kreditsicherheit verwendet werden [8]. Steigen die erworbenen Krypto-Token im Wert, kann der Kreditnehmer einen Gewinn erzielen, sofern der Wertzuwachs größer ist als der Zinsaufwand des Kredites zuzüglich Transaktionskosten [13]. Die aufgenommenen Krypto-Token könnten ihrerseits als Kreditsicherheit verwendet werden. Derartige Strategien werden in Verbindung mit dem Erzielen von Belohnungen auch als Yield Farming bezeichnet, bei dem die Nutzer das vorrangige Ziel der Gewinnmaximierung verfolgen [14].

Arbitrage: Flash Loans eignen sich für Arbitrage-Zwecke, etwa durch das monetarisieren von Preisunterschieden an verschiedenen dezentralen Handelsplattformen [13, 15]. Dabei würde in einem ersten Schritt ein Flash Loan aufgenommen werden. Die aufgenommen Krypto-Token könnten dann an einer dezentralen Handelsplattform veräußert werden. Idealerweise können die Krypto-Token dann an einer anderen dezentralen Handelsplattform zu einem niedrigeren Preis zurückgekauft werden. Dadurch könnten einerseits die ursprünglich geliehenen Krypto-Token im Rahmen des Flash Loans sowie dafür anfallende Zinsen zurückgegeben werden. Andererseits ergäbe sich ein Gewinn sofern die Transaktionskosten des Vorgangs niedriger ausfallen als der Handelsgewinn.

Dolose Handlungen: Flash Loans können beispielsweise für schädliche Attacken auf dezentrale Anwendungen eingesetzt werden, etwa durch den Erwerb von Governance-Token und anschließender Änderung des Programmcodes der jeweiligen Anwendung zum eigenen Vorteil [5, 14, 15].

4. Risiken und Absicherungsmechanismen

Die von dezentralen Kreditplattformen angebotenen Leistungen ähneln in Ansätzen dem Kredit- und Einlagegeschäft von konventionellen Banken, inklusive den damit einhergehenden Risiken. Diese sind zwar vergleichbar mit den Risiken, denen auch Kreditinstitute im Rahmen ihres Risikomanagements ausgesetzt sind.

Allerdings sind im Fall von dezentralen Kreditplattformen insbesondere die Nutzer von den Risiken betroffen, während die Plattformen selbst keinerlei Haftung unterliegen. Zur Verringerung der Risiken existieren vereinzelte anwendungsinhärente Absicherungsmechanismen und externe Versicherungen.

4.1 Kreditrisiken

Netzwerkakteure, die Lending Pools Liquidität bereitstellen, sind grundsätzlich dem Risiko ausgesetzt, dass sie die von ihnen eingereichte Liquidität zuzüglich der zustehenden Zinsen nicht vollumfänglich wiedererhalten. Dieses Risiko vergrößert sich insbesondere dadurch, dass die Lending Pools die Liquidität ohne Bonitätsprüfung an pseudoanonyme Netzwerkakteure verleihen. Ohne adäquate Absicherungsmechanismen hätten Kreditnehmer kaum einen Anreiz geliehene Krypto-Token zurückzuzahlen. Zudem achten dezentrale Kreditplattformen nicht auf Risikokonzentrationen, etwa mit Hilfe von kreditnehmerbezogenen Limiten wie es beispielsweise für Banken im Rahmen der MaRisk vorgeschrieben ist. Abbildung 3 zeigt am Beispiel von Aave mehrere aufeinanderfolgende Mechanismen, die Liquiditätsbereitsteller vor Verlusten ihrer Krypto-Token schützen sollen. Diese Kaskade besteht aus vier wesentlichen Stufen:

1) Um die Rückzahlung von Krediten trotz der Pseudo-Anonymität der Netzwerkakteure und ohne vorherige Bonitätsprüfung zu gewährleisten, müssen Kreditnehmer diese mit Krypto-Token besichern. Damit Wertschwankungen der Sicherheiten keinen direkten Einfluss auf den Wert eines Lending Pools haben und um einen möglichst hohen Anreiz zur Rückzahlung des Kredites zu schaffen erfolgt die Besicherung üblicherweise zu Quoten von mehr als 100%. Sinkt der Wert der Sicherheiten, muss der Kreditnehmer Sicherheiten nachschießen, um das Recht zur Auslösung seiner Sicherheiten zu erhalten [8, 9, 11].

2) Schießt der Kreditnehmer keine Sicherheiten nach, sodass diese anschließend unter einen bestimmten Schwellenwert fallen, erhalten sogenannte Liquidatoren die Möglichkeit die Sicherheiten mit einem Abschlag zu erwerben. Dieser Mechanismus soll eine Unterdeckung des Lending Pools verhindern, sofern Kreditnehmer keine ausreichende Besicherung mehr bereitstellen [12].

3) Durch einen plötzlichen Wertverfall von Sicherheiten kann es dazu kommen, dass etwaige Liquidierungsereignisse nicht genügend Liquididatoren finden und es dadurch zur Unterdeckung eines Lending-Pools kommt [12]. Aave sieht in einem solchen Fall ex ante einen Ausgleich für die Liquiditätsbereitsteller durch ein sogenanntes Safety Module vor – vergleichbar mit einem Verlustabsorptionspuffer. Diesem können AAVE-Token gegen eine Verzinsung bereitgestellt werden. Dabei handelt es sich um die Governance-Token der dezentralen Kreditplattform Aave. Die Token können mit einer Frist von sieben Tagen wieder aus dem Safety Module entnommen werden – was etwa mit der Kündigungsfrist von Genossenschaftsanteilen verglichen werden kann, wenngleich diese üblicherweise deutlich länger ist. Die Unterdeckung eines Lending Pools würde durch die Aave Governance festgestellt werden, woraufhin die Liquidierung der Token des Safety Module angestoßen werden würde. Die AAVE-Token würden dann gegen die entsprechenden Krypto-Token verkauft werden, bei deren Lending Pool es zu einer Unterdeckung gekommen ist. Der Verkaufserlös würde dem Lending Pool solange zugeführt werden, bis die Unterdeckung ausgeglichen ist [16].

4) Reichen die Erlöse des Safety Module nicht aus, kann ex post eine zusätzliche Reserve aktiviert werden, um die Unterdeckung auszugleichen. Zu diesem Zweck kann die Aave Governance die Ausgabe zusätzliche AAVE-Token beschließen und diese veräußern [16]. Deren Verkaufserlös wiederum kann zum Ausgleich der Unterdeckung verwendet werden. Gleichzeitig würde jedoch der Kurs der AAVE-Token verwässert werden: Der Anteil der Alt-Inhaber verringert sich hierdurch und es kommt effektiv zu einem Verlust – vergleichbar mit einer Gläubigerbeteiligung. Dabei ist es im Vorfeld jedoch nicht klar, ob die neu geschaffenen AAVE-Token ausreichend Abnehmer finden werden, um die Liquiditätsbereitsteller zu entschädigen.

Grundsätzlich sollten anwendungsinhärente Absicherungsmechanismen die Nutzung einer Anwendung im Vergleich zu anderen – ohne entsprechende Mechanismen – verteuern. So sind die Zinsen, die Governance-Token Inhaber für die Speisung eines Verlustabsorptionspuffers erhalten, ceteris paribus letztlich von den Nutzern in Form höherer Kreditzinsen, niedrigerer Einlagenzinsen oder zusätzlicher Gebühren zu tragen. Zudem dürften Governance-Token-Inhaber die Gefahren einer Gläubigerbeteiligung in ihre Renditekalkulation einpreisen und sich entsprechend höhere Gewinne auszahlen, was ebenfalls zulasten der Nutzer gehen dürfte. Fehlende anwendungsinhärente Absicherungsmechanismen würden für die Liquiditätsbereitsteller jedoch mit größeren Kreditrisiken einhergehen, was wiederum in die individuelle Renditekalkulation einbezogen werden müsste.

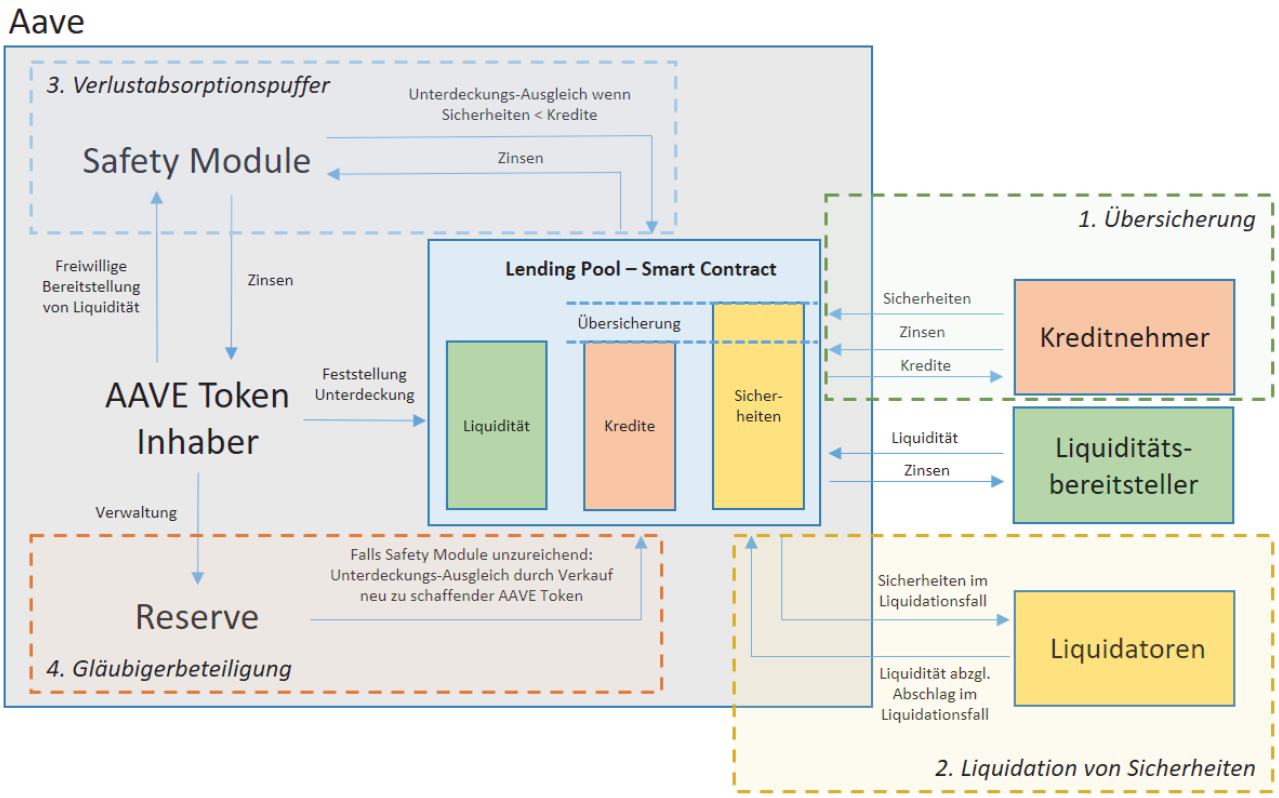

Abbildung 3: Anwendungsinhärente Absicherungsmechanismen am Beispiel Aave, Quelle: Eigene Darstellung nach [9, 11, 16].

4.2 Liquiditätsrisiken

Liquiditätsrisiken können auftreten, wenn Netzwerkakteure einer Plattform Liquidität bereitstellen und sie diese nicht zu einem gewünschten Zeitpunkt wieder abrufen können. So können Lending Pools illiquide werden, sobald die Summe aller ausgegebenen Kredite der Summe der eingereichten Liquidität entspricht. In diesem Fall müssten Netzwerkakteure, die ihre Liquidität entnehmen wollen, darauf warten, dass Kredite getilgt werden oder weitere Netzwerkakteure dem Lending Pool Liquidität bereitstellen. Die Gefahr der Illiquidität eines Lending Pools soll durch variable Zinssätze verringert werden [17, 18]. Sinkt die verfügbare Liquidität im Pool, steigen die Einlagen- und Kreditzinsen, sowohl für Neu- als auch Bestandsgeschäft. Einleger haben dadurch einen größeren Anreiz Liquidität bereitzustellen, wohingegen Kreditnehmer einen größeren Anreiz haben, ihre Kredite zu tilgen. Selbiges Prinzip gilt in umgekehrter Logik für den Fall eines Überangebots an Liquidität [5, 18]. Die Funktion, derer die Zinssätze dabei folgen, kann verschiedene Formen annehmen. Aave und Compound etwa setzen auf Funktionen mit linear ansteigendem Verlauf und „Knickstelle“, ab der die Funktion deutlich steiler verläuft. Wesentliche Einflussgröße ist dabei die Utilisation Rate *U*, welche das Verhältnis aus Krediten *L* und Einlagen *D* für einen bestimmten Lending Pool angibt [18]:

$$U = \frac{L}{D}$$

Sodass sich der Kreditzins i_b wie folgt ergeben kann:

$$i_b = \begin{cases} \alpha + \beta U & wenn\ U < U_{optimal} \\ \alpha + \beta U_{optimal} + \gamma(U - U_{optimal}) & wenn\ U \geq U_{optimal} \end{cases}$$

wobei α eine Konstante ist und β die Steigung des Zinses im Verhältnis zur Utilisation Rate widergibt. Überschreitet U ein gewisses Optimum am Punkt $U_{optimal}$ erzeugt γ einen Multiplikator-Effekt, der zu einem steileren Anstieg führt. $U_{optimal}$ wird üblicherweise für jeden Lending Pool individuell festgelegt und kann beispielsweise einem Verlauf wie in Abbildung 4 annehmen.

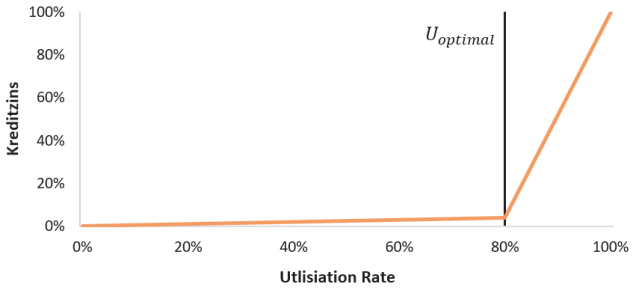

Abbildung 4: Exemplarische Kreditzinskurve mit Knickstelle, Quelle: Eigene Darstellung nach [18].

Darüber hinaus existieren Anwendungen, deren Zinssätze linearen oder nichtlinearen Verläufen folgen. Unabhängig von der Art der Zinssatzermittlung kann sich dieses Anreizsystem jedoch als unzureichend erweisen, etwa im Fall von abrupten

Liquiditätsabflüssen – vergleichbar mit einem Bank Run. Nutzer sind dann möglicherweise nicht mehr dazu bereit Liquidität trotz hoher Verzinsung bereitzustellen. Demnach kann das Risiko der Illiquidität von Lending Pools zwar verringert, aber nicht ausgeschlossen werden [5].

4.3 Marktrisiken (einschließlich Zinsänderungsrisiken)

Marktrisiken sind gemäß Artikel 4 Nr. 141 Verordnung (EU) Nr. 575/2013 (Kapitaladäquanzverordnung) Verlustrisiken, die aus Markpreisbewegungen, einschließlich Wechselkurs- oder Warenpreisbewegungen erwachsen. In Bezug auf die Nutzung dezentraler Kreditplattformen können sich entsprechende Marktrisiken für Kreditnehmer aus Wertschwankungen der zu hinterlegenden Sicherheiten und Veränderungen der variablen Zinssätze ergeben. Letztere stellen somit auch für die Liquiditätsbereitsteller ein Risiko dar.

Krypto-Token, die als Kreditsicherheit verwendet werden, unterliegen üblichen Kursschwankungen. Diese Wertschwankungen können von Kreditnehmern im Zusammenhang mit Leveraging-Strategien zwar bewusst in Kauf genommen werden. Gleichwohl existieren ohnehin keine anwendungsinhärenten Absicherungsmechanismen gegen derartige Wertschwankungen, die entsprechend durch die Kreditnehmer zu tragen sind.

Zinsänderungsrisiken, als Teil der Marktrisiken, ergeben sich sowohl für Kreditnehmer als auch Liquiditätsbereitsteller, da die Zinssätze dezentraler Kreditplattformen üblicherweise variabel sind. Dabei sind die Risiken für Liquiditätsbereitsteller gleichwohl geringer, da diesen keine negativen Zinssätze vergeben werden, und sie, im Fall geringer ausstehender Liquidität im Lending Pool, von steigenden Zinsen profitieren würden. Demgegenüber würde es in einem solchen Szenario zu einem starken Anstieg der Kreditzinsen kommen, mit entsprechend negativen Auswirkungen für die Kreditnehmer.

Um die Zinsänderungsrisiken für Kreditnehmer zu verringern bietet etwa Aave die Möglichkeit fixer Zinssätze an. Allerdings ist die Stabilität dieser Zinssätze an Bedingungen geknüpft. Kommt es beispielsweise zu einem Rückgang der verfügbaren Liquidität in einem Lending Pool, sodass die Utilisation Rate über 95% steigt, werden die fixen Zinssätze angepasst. Für Krypto-Token, deren Lending Pools hohen Liquiditätsrisiken ausgesetzt sind, sodass die Utilisation Rate häufig in den Bereich von 100% steigt, werden von vornherein keine fixen Zinssätze angeboten. Kreditnehmer müssen für dieses anwendungsinhärente Angebot zur Verringerung der Zinsänderungsrisiken höhere Zinssätze in Kauf nehmen. Diese liegen in der Regel im einstelligen Prozentpunkte-Bereich über den variablen Zinssätzen [18].

4.4 Operationelle Risiken

Während Kredit-, Liquiditäts- und Marktrisiken im Wesentlichen die Nutzung dezentraler Kreditplattformen betreffen, stellen operationelle Risiken eine Gefahr für die Nutzung sämtlicher dezentraler Anwendungen dar. Denn Softwarefehler und missbräuchliches Verhalten einzelner Netzwerkakteure können trotz externer Sicherheitsüberprüfungen und

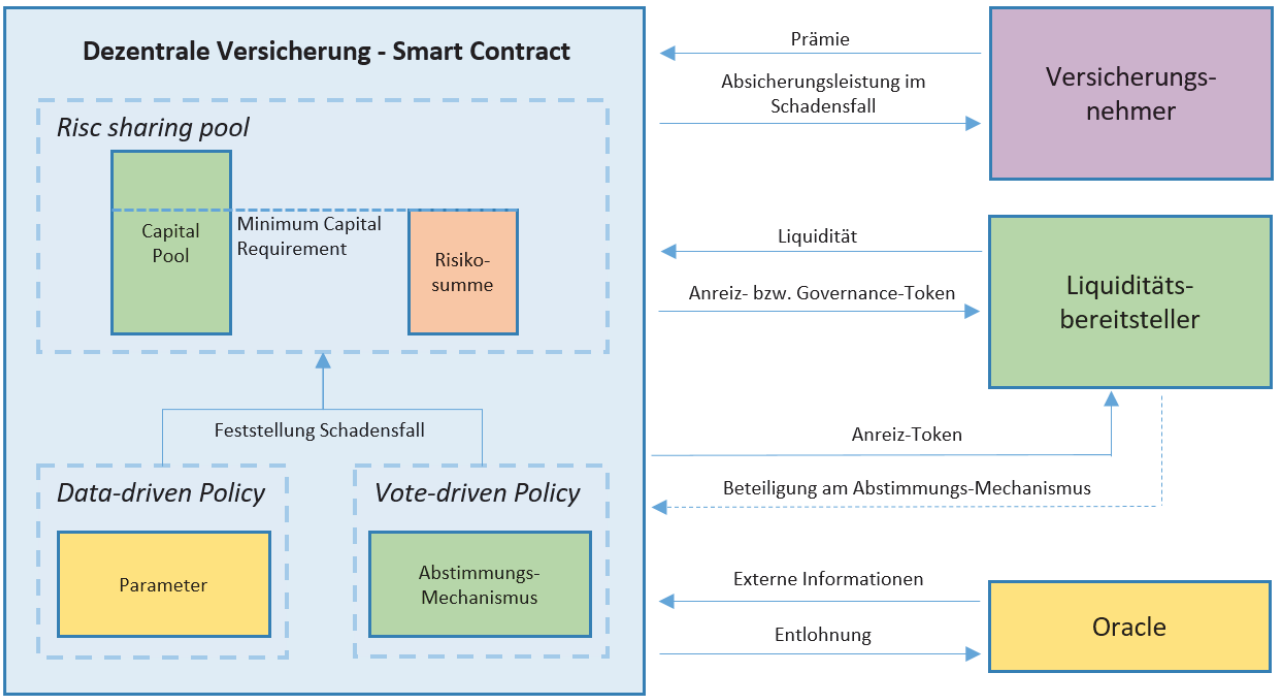

Abbildung 5: Exemplarische Architektur dezentraler Versicherungen, Quelle: Eigene Darstellung.

entsprechender Anreizsystemen die intendierte Funktionsweise dezentraler Anwendungen beeinträchtigen. Gleichzeitig sind schnelle administrative Eingriffe durch eine zentrale Instanz bei dezentralen Anwendungen üblicherweise nicht vorgesehen. Operationelle Risiken sind gemäß Artikel 4 Nr. 52 Verordnung (EU) Nr. 575/2013 (Kapitaladäquanzverordnung) die Risiken von Verlusten, die durch die Unangemessenheit oder das Versagen von internen Verfahren, Menschen, Systemen oder durch externe Ereignisse verursacht werden, einschließlich Rechtsrisiken.

Im Fall von dezentralen Anwendungen können etwa Programmierfehler (sog. Smart Contract Bugs) zu unbeabsichtigten Problemen und damit verbundenen Verlusten für deren Nutzer führen. Durch die Ausnutzung von derartigen Fehlern in Smart Contracts konnten Angreifer in der Vergangenheit immer wieder große Summen erbeuten. Um für einen solchen Fall administrative Eingriffe zu ermöglichen, werden üblicherweise dezentrale Governance-Prozesse implementiert. Dies kann mit Hilfe von Governance-Token erfolgen, mit denen die Entscheidungsprozesse technisch über die zugrundeliegende Blockchain abgebildet werden (sog. On-Chain-Governance). Diese Verfahren sind in der Regel jedoch langsamer als das direkte Einschreiten eines Administrators. Zudem eröffnet sich durch den Einsatz von Governance-Token die Gefahr, dass einzelne Akteure unbemerkt die Stimmenmehrheit erlangen und den Programmcode zu ihren Gunsten ändern (sog. Governance Attack). Diese Gefahr wird durch die Pseudo-Anonymität der Netzwerkakteure und die damit verbundene Intransparenz bezüglich der Entscheidungsstrukturen begünstigt. Die externen Datenquellen der Smart Contracts, sogenannte Oracles, stellen ebenfalls eine kritische Komponente dar, die bei Versagen die Funktionalität der Anwendung gefährdet. Oracles sind gewöhnliche zentrale Informationsquellen wie Sensoren, Dienste oder Institutionen, die einem Smart Contract gewisse Informationen bereitstellen. Daher sind Oracles sämtlichen Bedrohungen, wie Manipulation, Man-in-the-Middle- oder Denial-of-Service-Angriffen ausgesetzt.

Aave etwa sieht für Verluste, die seinen Nutzern aufgrund von Smart Contract Bugs oder Fehlern durch Oracle entstehen, eine Kompensation durch das anwendungsinhärente Safety Module und die Reserve vor [16]. Allerdings können Smart Contract Bugs auch diese Mechanismen selbst betreffen, sodass Nutzer immer Restrisiken ausgesetzt sind. Zudem besteht auch hier Unsicherheit darüber, ob die Mittel des Safety Module und der Reserve ausreichen, um die Nutzer zu entschädigen. Dementsprechend können operationelle Risiken durch die Anwendungen selbst nicht vollumfänglich abgedeckt werden, sodass sich Nutzer gegen diese über Drittanbieter absichern können.

Operationelle Risiken stellen auch den derzeit wesentlichsten Geschäftsfall dezentraler Versicherungslösungen dar. Grundsätzlich sind die existierenden Lösungen ähnlich aufgebaut. Abbildung 5 stellt eine allgemeingültige Architektur dar. Der genaue Aufbau einzelner Komponenten, wie Abstimmungsprozesse, Anreizsysteme, Risikobewertung oder Schadensabwicklung kann je nach Implementierung entsprechend unterschiedlich sein.

Einer der wichtigsten Vertreter ist Nexus Mutual. Diese Plattform bietet beispielsweise Absicherungen gegen Softwarefehler an. Gleichzeitig ist Nexus Mutual selbst eine dezentrale Anwendung. Daher existieren bei derartigen Lösungen große Abhängigkeiten zwischen Versicherer und Schadensereignis, da kritische Ereignissen, die das ganze Ökosystem – in Form der zugrundeliegenden Blockchain – betreffen, ebenfalls für die Versicherungsplattform relevant werden können. Ein Extremereignis könnte somit auch zum Ausfall des Absicherungsgebers führen. Risiken, wie beispielsweise eine kritische Schwachstelle in der Ethereum-Plattform oder in einer kryptografischen Hashfunktion können daher nicht auf diesem Weg abgesichert werden. Obwohl mit einem breiten Anwendungsspektrum und dem Plattformcharakter geworben wird und diese Faktoren auch im White Paper von Nexus Mutual hervorgehoben werden, sind derzeit lediglich Absicherungen von Risiken – insbesondere Softwarefehler – innerhalb des Blockchain-Ökosystems erwerbbar [19].

Bei Abschluss eines Absicherungsgeschäfts ist durch den Nutzer eine Prämie zu leisten, die prozentual von der Versicherungssumme abhängt und je nach Produkt angefangen bei 2,6% bis zu teilweise 27% betragen kann [19]. Nutzer müssen zudem vor dem Abschluss ein Know-your-Customer-Verfahren (KYC) durchlaufen, d.h. sich mit einem amtlichen Ausweisdokument verifizieren. Der Prozess der Schadensabwicklung sieht bei Nexus Mutual vor, dass im Schadensfall durch den Geschädigten entsprechende Beweise eingereicht werden müssen. Dieser Vorgang wird als Claim Submission bezeichnet. Bei parametrischen Leistungen werden Oracles verwendet, um eine Auszahlung zu genehmigen. Bei anderen Leistungen kommt ein Abstimmungsmechanismus zum Einsatz, bei welchem über die Gültigkeit eines Anspruchs entschieden wird. Im Fall von Nexus Mutual erfolgen die Abstimmungen auf der Basis von NXM-Token, die sowohl für Abstimmungen über Schadensfälle dienen, als auch der operativen Governance, etwa im Fall von Protokolländerungen. Zunächst stimmen nur die dafür vorgesehenen Assessors ab (Assessor Vote), die ihre Token dafür gesondert hinterlegen müssen. Die hinterlegten Token können bei schädlichem Verhalten, ebenfalls abstimmungsbasiert, entzogen werden. Kommt es bei der Abstimmung durch die Assessors zu keinem Ergebnis, wird die diese für alle Mitglieder

Risiken	Auswirkungen für Liquiditäts-bereitsteller	Auswirkungen für Kreditnehmer	Eintritts-wahrscheinlich-keit	Beispiel anwendungs-inhärenter Mechanismen	Beispiel externer Maßnahmen
Kreditrisiken	hoch	–	hoch	▪ Übersicherung ▪ Liquidation von Sicherheiten ▪ Verlust-absorptionspuffer ▪ Gläubiger-beteiligung	–
Liquiditäts-risiken	gering	–	mittel	▪ Variable Zinssätze	–
Marktrisiken	gering	mittel	hoch	▪ Feste Zinssätze	–
Operationelle Risiken	hoch	hoch	gering	▪ Verlust-absorptionspuffer ▪ Gläubiger-beteiligung	▪ Dezentrale Versicherungen

Tabelle 1: Risikoeinschätzung dezentraler Kreditplattformen, Quelle: Eigene Darstellung. Beachte: Es wird angenommen, dass ohne das Vorhandensein entsprechender Absicherungsmechanismen sowohl Liquiditätsbereitsteller als auch Kreditnehmer finanzielle Auswirkungen erleiden, sollten Risiken schlagend werden. Die Eintrittswahrscheinlichkeiten stehen dabei in einem relativen Verhältnis zueinander. Ohne entsprechende Absicherungsmechanismen, sollte ein Risiko mit einer hohen Eintrittswahrscheinlichkeit, häufiger schlagend werden, als ein Risiko mit einer geringen Wahrscheinlichkeit.

freigegeben (Member Vote). Bei einem Assesor Vote muss die Mehrheit mindestens 70% der Stimmen erhalten. Bei einem Member Vote reicht die einfache Mehrheit [20].

Die NXM-Token sind in nativer Form nicht handelbar, sondern lassen sich nur direkt bei Nexus Mutual nach Abschluss eines KYC-Prozesses erwerben. Derzeit ist Nexus Mutual als Limited organisiert und soll langfristig durch eine dezentrale autonome Organisation (DAO) ersetzt werden. Der genaue rechtliche Status und damit auch die Regulierungsanforderungen dieser Art von Unternehmensorganisation sind bislang unklar, wodurch auch der KYC-Prozess entfallen könnte [21].

Das Kapitalmodell ist nach Aussage von Nexus Mutual an die Solvency II-Richtlinie angelehnt und berechnet das Minimum Capital Requirement (MCR) so, dass die Wahrscheinlichkeit, alle Schadensereignisse eines Jahres zu decken, bei 99,5% liegt. Der Kapitalpool von Nexus Mutual muss immer mindestens so groß sein, wie das täglich neu berechnete MCR, sonst können keine Absicherungen erworben werden [22].

5. Risikoeinschätzung

Die Nutzung dezentraler Kreditplattformen erfolgt üblicherweise pseudo-anonym, sodass Kreditnehmer nicht auf ihre Bonität hin überprüft werden können – wie es etwa im konventionellen Bankgewerbe üblich wäre. Dadurch ergeben sich, wie in Tabelle 1 dargestellt, erhebliche Kreditrisiken, die letztlich von den Liquiditätsbereitstellern zu tragen sind. Die Kreditrisiken könnten sich dadurch verstärken, dass Kreditnehmer mit guter Bonität in der Erwartung niedrigerer Zinsen tendenziell auf Plattformen mit Bonitätsprüfungen ausweichen, wodurch letztlich insbesondere Netzwerkakteure mit schlechter Bonität Kredite über dezentrale Kreditplattformen aufnehmen könnten. Um die Kreditrisiken für die Liquiditätsbereitsteller zu verringern, greifen die Anwendungen zum Teil auf verschiedene Mechanismen zurück, wie etwa der Übersicherung von Krediten, der automatischen Liquidation von Sicherheiten, Verlustabsorptionspuffern und der Gläubigerbeteiligung. Vollends ausgeschlossen kann zumindest der teilweise Verlust der eingebrachten Liquidität für deren Bereitsteller dadurch jedoch nicht, sodass immer ein Restrisiko verbleibt.

Liquiditätsrisiken sollten nicht unmittelbar zu Verlusten der Liquiditätsbereitsteller führen. Gleichwohl können sich mittelbare Verluste ergeben, sofern die bereitgestellte Liquidität beispielsweise in Form eines Kredites bei einer anderen Plattform aufgenommen wurde und dort hohe Zinssätze drohen. Dementsprechend sind die Auswirkungen für Liquiditätsbereitsteller eher als gering einzustufen, wenngleich derartige Szenarien – ohne entsprechende anwendungsinhärente Mechanismen – häufig eintreten könnten, da dezentrale Kreditplattformen – im Gegensatz zu herkömmlichen Finanzmarktteilnehmern – keine aktive Liquiditätssteuerung betreiben. Mit Hilfe variabler Zinssätze sollten die Liquiditätsrisiken jedoch verringert werden können, wenngleich es dabei insbesondere im Rahmen von Extremereignissen zu Illiquiditätsereignissen kommen kann.

Marktrisiken können sich für Kreditnehmer und Liquiditätsbereitsteller durch Änderungen der variablen Zinsen ergeben. Liquiditätsbereitsteller unterliegen

dabei lediglich dem Risiko sinkender Zinsen, wohingegen Kreditnehmer hohen Verlustrisiken in Form stark steigender Kreditzinsen ausgesetzt sind. Zudem unterliegen Kreditnehmer dem Risiko, dass ihre Sicherheiten im Wert schwanken und bei plötzlichem Wertverfall sogar liquidiert werden könnten. Grundsätzlich sollten Marktrisiken jedoch nicht zu einem Totalverlust führen. Gleichwohl müssen insbesondere die Kreditnehmer mit Verlusten rechnen, die mittels fixer Zinssätze nur bedingt verringert werden könnten. Da die Lending Pools kein aktives Liquiditätsmanagement betreiben, sollte die Liquidität in den Pools permanent schwanken und mit ihr die variablen Zinssätze. Zudem sind auch die Kurse vieler Krypto-Token häufigen Schwankungen unterworfen, sodass die Eintrittswahrscheinlichkeit für Marktrisiken durchaus als hoch eingestuft werden kann.

Operationelle Risiken ergeben sich im Fall von dezentralen Anwendungen insbesondere aus Fehlern in den Softwareprotokollen, die wiederum zu erheblichen Schäden bei den Nutzern führen könnten. Der Programmcode dezentraler Anwendungen kann als Open-Source-Software von jedem eingesehen werden. Dadurch können die Netzwerkakteure zumindest potenziell nachvollziehen, wie Anwendungen aufgebaut sind und funktionieren. Zudem sind die Programmcodes vieler Anwendungen Gegenstand regelmäßiger externer Sicherheitsüberprüfungen. Dementsprechend könnten operationelle Risiken im Verhältnis zu Kredit-, Liquiditäts- und Marktrisiken zwar seltener eintreten [23]. Allerdings könnten ihre negativen Auswirkungen nicht zuletzt aufgrund fehlender Eingriffsmöglichkeiten höher ausfallen und im Extremfall zum Verlust der gesamten eingebrachten Liquidität und Sicherheiten führen. Um dem entgegenzuwirken können sich Nutzer mittels dezentraler Versicherungen absichern. Allerdings sind diese mit Unsicherheiten behaften und können zudem keine Extremereignisse absichern, die auch den Ausfall des Absicherungsgebers einschließen, sodass die Nutzung dezentraler Anwendungen immer mit einem Restrisiko verbunden bleibt.

6. Fazit

Dezentrale Kreditplattformen stellen eine innovative Möglichkeit dar, um Krypto-Token gegen eine entsprechende Verzinsung anzulegen oder zu leihen. Gleichwohl sind damit – wie im konventionellen Bankgewerbe – Risiken verbunden, die sich jedoch im Gegensatz zum konventionellen Kredit- und Einlagengeschäft zu einem großen Teil auf die Nutzer abwälzen. Dazu zählen insbesondere Kreditrisiken und operationelle Risiken. Zudem ergeben sich aufgrund der technischen Funktionsweise der Plattformen für die Nutzer zusätzliche Liquiditäts- und Marktrisiken.

Um die Risiken zu verringern, gibt es erste anwendungsinhärente Absicherungsmechanismen. Diese erscheinen geeignet, um zumindest einen Teil der Risiken zu verringern. Allerdings befinden sich die Mechanismen noch in einem frühen Entwicklungsstadium, sodass keine abschließende Beurteilung ihrer Wirkungsweise erfolgen kann. Dennoch lässt sich bereits sagen, dass sie zumindest theoretisch keine vollumfängliche Risikobewältigung ermöglichen. Insofern sollten Nutzer sich der Risiken bewusst sein, die sich aus der Nutzung dezentraler Kreditplattformen ergeben. Entsprechende Regulierungsanforderungen könnten dazu beitragen, die Robustheit der Plattformen zu erhöhen und damit das ihnen entgegengebrachte Vertrauen zu vergrößern.

Literaturverzeichnis

[1] Deutsche Bundesbank, Krypto-Token und dezentrale Finanzanwendungen, Monatsbericht, Juli (2021), S. 33–51.

[2] DeFi Pulse, online, https://defipulse.com, (2021).

[3] Bundesanstalt für Finanzdienstleistungsaufsicht, Mindestanforderungen an das Risikomanagement – MaRisk, Rundschreiben, 09/2017 (2017).

[4] Deutsche Bundesbank, Die Rolle von Banken, Nichtbanken und Zentralbank im Geldschöpfungsprozess, Monatsbericht, April (2017), S. 15–36.

[5] L. Gudgeon, S. Werner, D. Perez, W. J. Knottenbelt, DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency, online, https://arxiv.org/pdf/2006.13922.pdf, Oktober (2020).

[6] NFTfi, NFTfi.com Introduction and FAQ, online, https://nftfi.medium.com/nftfi-com-f9ecf4ab1e7d, Mai (2020).

[7] F. Schaer, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis Review, Vol. 103 (2021), S. 153–74.

[8] Aave, Risk Parameters, online, https://docs.aave.com/risk/asset-risk/risk-parameters, 2021.

[9] Aave, Protocol Whitepaper V1.0, online, https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf, Januar (2020).

[10] R. Leshner, G. Hayes, Compound: The Money Market Protocol, online, https://compound.finance/documents/Compound.Whitepaper.pdf, Februar (2019).

[11] Aave, Protocol Whitepaper V2.0, online, https://github.com/aave/protocol-v2/blob/master/aave-v2-whitepaper.pdf, Dezember (2020).

[12] D. Perez, S. Werner, J. Xu, B. Livshits, Liquidations: DeFi on a Knife-edge, online, https://www.doc.ic.ac.uk/~livshits/papers/pdf/fc21a.pdf, April (2021).

[13] Bitkom, Decentralized Finance (DeFi) – A new Fintech Revolution?, online, https://www.bitkom.org/sites/default/files/2020-

07/200729_whitepaper_decentralized-finance.pdf, (2020).
[14] U. W. Chohan, Decentralized finance (DeFi): an emergent alternative financial architecture, Critical Blockchain Research Initiative, Discussion Paper Series: Notes on the 21st Century, Januar (2021).
[15] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, K. Ren, Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem, online, https://arxiv.org/pdf/2010.12252.pdf, April (2021).
[16] Aave, Safety Module, online, https://docs.aave.com/aavenomics/safety-module, (2021).
[17] DeFi Rate, online, https://defirate.com/lend/, (2021).
[18] Aave, Borrow Interest Rate, online, https://docs.aave.com/risk/liquidity-risk/borrow-interest-rate, (2021).
[19] Nexus Mutual, Buy cover - Nexus Mutual App, online, https://app.nexusmutual.io/cover, 2021.
[20] H. Karp, R. Melbardis, Nexus Mutual A peer-to-peer discretionary mutual on the Ethereum blockchain, White Paper, online, https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf, (2021).
[21] A. Thurman, cointelegraph - Nexus Mutual moves to sunset legal entity, lift KYC requirements, online, https://cointelegraph.com/news/nexus-mutual-moves-to-sundown-legal-entity-lift-kyc-requirements, April (2021).
[22] Nexus Mutual, How-to Guides: How to participate, online, https://nexusmutual.gitbook.io/docs/how-to-use-nexus/how-to-participate, (2021).
[23] D. Perez, B. Livshits, Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited, Proceedings of the 30th USENIX Security Symposium, August (2021).