

Das Dai-Stablecoin-System

Übersicht über das Dai-Stablecoin-System

Beliebte digitale Assets wie Bitcoin (BTC) und Ether (ETH) sind zu volatil, um als Alltagswährung verwendet zu werden. Der Wert des Bitcoins unterliegt oft großen Schwankungen und kann an einem einzigen Tag um bis zu 25% steigen oder fallen, gelegentlich sogar über 300% in einem Monat zulegen.

Dai Stablecoin ist eine kollateral gesicherte Kryptowährung, deren Wert gegenüber dem US-Dollar stabil ist. Wir glauben, dass stabile digitale Assets wie Dai Stablecoin unerlässlich sind, um das volle Potenzial der Blockchain-Technologie auszuschöpfen.

Maker ist eine Smart-Contract-Plattform basierend auf Ethereum, die den Wert von Dai durch ein dynamisches System von Collateralized Debt Positions (CDPs), autonomen Feedback-Mechanismen und entsprechend motivierten externen Akteuren absichert und stabilisiert.

Maker ermöglicht es jedem, seine Ethereum-Reserven zu nutzen, um Dai auf der Maker-Plattform zu generieren. Einmal generiert, kann Dai wie jede andere Kryptowährung verwendet werden: Es kann ohne Einschränkung an andere gesendet, als Zahlungsmittel für Waren und Dienstleistungen verwendet oder langfristig gespart werden. Darüber hinaus schafft die Generierung von Dai die Voraussetzungen für eine robuste dezentrale Margenhandelsplattform.

Collateralized Debt Positions

Jeder, der über Sicherheitsswerte (Collateral Assets) verfügt, kann diese nutzen, um Dai auf der Maker-Plattform zu generieren. Die Smart Contracts die dazu benutzt werden sind so genannte Collateralized Debt Positions (CDPs).

CDPs halten Sicherheiten, die von einem Benutzer hinterlegt wurden. Der Benutzer generiert dadurch Dai aber auch Schulden. Diese Schulden sperren die hinterlegten Sicherheiten innerhalb des CDP, bis sie wieder durch die Rückzahlung des entsprechenden Betrages an Dai gedeckt sind, woraufhin der Eigentümer seine Sicherheiten wieder zurücknehmen kann. Aktive CDPs werden immer im Übermaß besichert, was bedeutet, dass der Wert der Sicherheiten höher ist als der Wert der Schuld.

Der Ablauf der CDP-Interaktion

Schritt 1: Erstellung des CDP und Hinterlegung von Sicherheiten

Der CDP-Benutzer sendet zunächst eine Transaktion an Maker, um das CDP zu erstellen, und sendet dann eine weitere Transaktion, um es mit der Art der Sicherheiten zu bezahlen, die zur Erzeugung von Dai verwendet werden. Ab diesem Zeitpunkt gilt das CDP als besichert.

Schritt 2: Generierung von Dai aus dem besicherten CDP

Der CDP-Nutzer sendet eine Transaktion, um den gewünschten Dai-Betrag vom CDP abziehen. Im Gegenzug verbucht das CDP einen gleichwertigen Schuldenbetrag und sperrt den Zugriff auf die entsprechenden Sicherheiten bis die ausstehende Forderung beglichen ist.

Schritt 3: Rückzahlung von Schulden und Stabilitätsgebühr

Wenn der Nutzer seine Sicherheiten wieder abrufen will, muss er die Schulden im CDP zuzüglich der Stabilitätsgebühr, die kontinuierlich auf die Schulden anfällt, zurückzahlen. Die Stabilitätsgebühr kann nur mit MKR bezahlt werden. Sobald der Benutzer die erforderlichen Dai und MKR an das CDP sendet und somit die Schulden und die Stabilitätsgebühr bezahlt, wird das CDP schuldenfrei.

Schritt 4: Rücknahme von Sicherheiten und Schließung des CDP

Wenn Schulden- und Stabilitätsgebühr bezahlt sind, kann der CDP-Nutzer alle oder einen Teil seiner Sicherheiten in seine Wallet zurückholen, indem er eine Transaktion an Maker sendet. Das Dai-Stablecoin-System wird zunächst mit nur einer Art von Sicherheiten, gebündeltem Ether (pooled Ether, PETH), starten (Single-Collateral Dai). In den nächsten 6-12 Monaten planen wir ein Upgrade von Single-Collateral Dai auf Multi-Collateral Dai. Der Hauptunterschied besteht darin, dass dann eine Vielzahl von CDP-Typen unterstützt werden wird.

Gebündelter Ether (Mechanismus für Single-Collateral Dai)

Zunächst wird gebündelter Ether (PETH) die einzige Sicherheit sein, die von Maker akzeptiert wird. Benutzer, die in dieser ersten Phase der Maker-Plattform ein CDP eröffnen und Dai generieren möchten, müssen zunächst PETH erwerben. Dies geschieht schnell und einfach auf der Blockchain, indem ETH an einen speziellen Smart Contract gesendet werden. Dieser bündelt die ETH von allen Nutzern und gibt ihnen die entsprechende Menge PETH.

Wenn es zu einem plötzlichen Einbruch des ETH Marktes kommt und ein CDP mehr Schulden enthält als seine Sicherheiten wert sind, verwässert die Maker-Plattform automatisch die PETH, um das System zu rekapitalisieren. Dies bedeutet, dass der proportionale Anspruch jedes PETH sinkt. Nach dem Upgrade der Maker-Plattform zur Unterstützung mehrerer Sicherheitsarten (Multi-Collateral Dai) wird PETH entfallen und durch ETH und andere neuen Sicherheitsarten ersetzt.

Preisstabilitätsmechanismen

Richtpreis

Der Richtpreis von Dai hat zwei Hauptfunktionen auf der Maker-Plattform: 1) Er wird zur Berechnung des Sicherheiten/Schulden-Verhältnisses eines CDP verwendet, und 2) Er wird zur Bestimmung des Wertes von Sicherheiten verwendet, die Dai-Halter im Falle einer Globalabwicklung erhalten. Der Richtpreis ist zunächst in USD angegeben und beginnt bei 1, was zu einem 1:1 USD Kurs führt.

Leitzins-Feedback-Mechanismus

Im Falle einer schweren Marktschwankung kann der Leitzins-Feedback-Mechanismus (Target Rate Feedback Mechanism, kurz TRFM) aktiviert werden. Die Aktivierung des TRFM löst den fixierten Kurs von Dai, behält aber die gleiche Stückelung bei.

Der TRFM ist der automatische Mechanismus, mit dem das Dai-Stablecoin-System den Leitzins anpasst, um die Markttakteure dazu zu bringen, die Stabilität des Dai-Marktpreises nahe dem Richtpreis zu erhalten. Der Leitzins bestimmt die Veränderung des Richtpreises, so dass er entweder als Anreiz dienen kann, Dai zu halten (wenn der Leitzins positiv ist) oder als Anreiz, Dai zu leihen (wenn der Leitzins negativ ist). Wenn der TRFM nicht aktiv ist, wird der Leitzins auf 0% festgelegt, so dass sich der Richtpreis im Laufe der Zeit nicht ändert und der Dai-Wert fixiert ist. Wenn der TRFM aktiv ist, ändern sich sowohl der Leitzins als auch der Richtpreis dynamisch, um Angebot und Nachfrage von Dai auszugleichen, indem die Anreize für das Generieren und Halten von Dai automatisch angepasst werden. Der Feedback-Mechanismus drückt den Marktpreis von Dai in Richtung des variablen Richtpreises, dämpft dessen Volatilität und stellt Liquidität bei Nachfrageschocks in Echtzeit zur Verfügung.

Wenn der TRFM aktiv ist und der Marktpreis von Dai unter dem Richtpreis liegt, steigt der Leitzins. Dies führt dazu, dass der Richtpreis steigt, was dazu führt, dass die Erzeugung von Dai mit CDPs teurer wird. Gleichzeitig bewirkt der höhere Leitzins, dass das Halten von Dai lukrativer wird, was zu erhöhter Nachfrage nach Dai führt. Die Kombination aus verringertem Angebot und erhöhter Nachfrage führt zu einer Erhöhung des Dai-Marktpreises und drückt ihn wieder in die Nähe des Richtpreises.

Der gleiche Mechanismus funktioniert umgekehrt, wenn der Marktpreis von Dai höher ist als der Richtpreis: Der Leitzins sinkt, was mehr Anreize schafft Dai zu generieren und weniger Anreize bietet, Dai zu halten. Dies führt zu einem Rückgang des Dai-Marktpreises und drückt ihn in die Nähe des Richtpreises.

Dieser Mechanismus ist eine negative Rückkopplungsschleife: Die Abweichung vom Richtpreis in eine Richtung erhöht die Kraft in die entgegengesetzte Richtung.

Sensitivitätsparameter

Der Sensitivitätsparameter des TRFM ist ein Parameter, der das Maß der Leitzinsänderung als Reaktion auf die Abweichung vom Dai-Richtpreis bestimmt. Dadurch wird die Feedbackrate auf die Dimension des Systems abgestimmt. MKR-Wähler können den Sensitivitätsparameter festlegen, aber wenn der TRFM aktiv ist, werden der Richtpreis und der Leitzins durch die Marktentwicklung bestimmt und nicht direkt von MKR-Wählern kontrolliert.

Der Sensitivitätsparameter ist auch das, was zum Ein- und Ausschalten des TRFM verwendet wird. Wenn sowohl der Sensitivitätsparameter als auch der Leitzins Null sind, ist Dai an den aktuellen Richtpreis gebunden.

Globalabwicklung

Die Globalabwicklung ist ein Prozess, der als letzter Ausweg genutzt werden kann, um den Haltern von Dai den Richtpreis kryptographisch zu garantieren. Sie fährt die Maker-Plattform herunter stellt sicher, dass alle Benutzer, sowohl Dai-Halter als auch CDP-Nutzer, den Nettowert der Assets erhalten, auf die sie Anspruch haben. Der Prozess ist vollständig dezentralisiert und nur die MKR-Wähler entscheiden über den Zugriff darauf, um sicherzustellen, dass er nur im Notfall eingesetzt wird. Beispiele für schwere Notfälle sind langfristige Marktirrationalität, Hacking oder Sicherheitsverletzungen und System-Upgrades.

Globalabwicklung: Schritt für Schritt

Schritt 1: Globalabwicklung ist aktiviert.

Wenn genügend Akteure, die von Maker Governance als globale Abwickler benannt wurden, glauben, dass das System einem schweren Angriff ausgesetzt ist, oder wenn ein technisches Upgrades geplant ist, können sie die Globalabwicklung aktivieren. Dadurch wird die Erstellung und Bearbeitung von CDPs gestoppt und der Preisfeed auf einen festen Wert eingefroren, der dann zur Abwicklung anteiliger Ansprüche für alle Benutzer verwendet wird.

Schritt 2: Abwicklung von Ansprüchen im Rahmen der Globalabwicklung

Nach der Aktivierung der Globalabwicklung wird eine gewisse Zeit benötigt, damit die Keeper die anteiligen Ansprüche aller Dai- und CDP-Inhaber auf der Grundlage des festen Preisfeed-Wertes bearbeiten können. Nach Abschluss dieser Verarbeitung können alle Dai- und CDP-Inhaber ihren anteiligen ETH-Betrag mit ihren Dai und CDPs geltend machen.

Schritt 3: Dai- und CDP-Inhaber beanspruchen ihre Sicherheiten

Jeder Dai- und CDP-Inhaber kann eine Claim-Funktion auf der Maker-Plattform aufrufen, um seine Dai- und CDPs direkt gegen einen festen ETH-Betrag einzutauschen, der dem berechneten Wert seines Vermögens entspricht, basierend auf dem Richtpreis von Dai. Wenn z.B. der Richtpreis für Dai 1 US-Dollar beträgt, der ETH/USD-Preis 200 beträgt und ein Benutzer bei aktivierter Globalabwicklung 1000 Dai hält, kann er nach Ablauf der Bearbeitungszeit genau 5 ETH von der Maker-Plattform einfordern. Es gibt keine Frist, bis zu der der endgültige Anspruch geltend gemacht werden muss.

Risikomanagement der Maker-Plattform

Der MKR-Token ermöglicht es deren Inhabern, über die Durchführung der folgenden Risikomanagement-Maßnahmen abzustimmen:

- **Hinzufügen eines neuen CDP-Typs:** Erstellen eines neuen CDP-Typs mit einem individuellen Satz von Risikoparametern. Ein CDP-Typ kann entweder eine neue Art von Sicherheit oder ein neuer Satz von Risikoparametern für eine bestehende Art von Sicherheit sein.
- **Änderung bestehender CDP-Typen:** Änderung der Risikoparameter eines oder mehrerer bestehender CDP-Typen, die bereits hinzugefügt wurden.
- **Änderung des Sensitivitätsparameters:** Ändern der Empfindlichkeit des Leitzins-Feedback-Mechanismus.
- **Änderung des Leitzinses:** Die Governance kann den Leitzins ändern. In der Praxis wird der Leitzins nur in einem bestimmten Fall geändert: Wenn MKR-Wähler den Preis von Dai an das aktuelle Richtpreisniveau koppeln wollen. Dies geschieht immer in Verbindung mit der Änderung des Sensitivitätsparameters. Wenn sowohl der Sensitivitätsparameter als auch die Leitzins auf 0% gesetzt werden, wird der TRFM deaktiviert und der Richtpreis von Dai wird an den aktuellen Wert gekoppelt.
- **Wahl von vertrauenswürdigen Orakeln:** Die Maker-Plattform bezieht ihre Preise für Sicherheiten und den Marktpreis von Dai aus einer dezentralen Orakelinfrastruktur, die aus einer großen Anzahl von einzelnen Orakelknoten besteht. MKR-Wähler bestimmen, wie viele Orakel es gibt und wer diese sind. Bis zu 50 % der Orakel können kompromittiert oder fehlerhaft sein, ohne den sicheren Betrieb des Systems zu gefährden.
- **Änderung der Preisfeed-Sensitivität:** Änderung der Regeln, die die größte Abweichung bestimmen, die die Preisfeeds auf die internen Preise im System bewirken können.
- **Wahl der globalen Abwickler:** Die Globalabwicklung ist ein unverzichtbarer Mechanismus, der es der Maker-Plattform ermöglicht, Angriffe gegen die Orakel oder den Governance-Prozess zu überstehen. Der Governance-Prozess wählt eine bestimmte Anzahl von globalen Abwicklern und bestimmt, wie viele von diesen benötigt werden um die globale Abwicklung zu aktivieren.

Risikoparameter

CDPs haben mehrere Risikoparameter, die ihre Verwendung festlegen. Jeder CDP-Typ hat seinen eigenen, individuellen Satz von Risikoparametern. Die Risikoparameter basieren auf dem Risikoprofil der von diesem CDP-Typ verwendeten Sicherheit. Diese Parameter werden von den MKR-Inhabern direkt durch Abstimmung festgelegt, wobei ein MKR jeweils einer Stimme entspricht.

Die zentralen Risikoparameter für CDPs sind:

Schuldenobergrenze: Die Schuldenobergrenze ist der maximale Schuldenbetrag, der durch einen einzigen CDP-Typ entstehen darf. Sobald ein bestimmter CDP-Typ die Schuldenobergrenze erreicht hat, ist es unmöglich, weitere Schulden zu machen, es sei denn, bestehende CDPs werden geschlossen. Die Schuldenobergrenze wird verwendet, um eine ausreichende Diversifikation des Sicherheitsportfolios zu gewährleisten.

Liquidationsverhältnis: Das Liquidationsverhältnis ist das Verhältnis von Sicherheiten zu Schulden eines CDP ab dem eine Liquidation droht. Ein niedriges Liquidationsverhältnis bedeutet, dass die MKR-Wähler eine niedrige Volatilität der Sicherheiten erwarten, während ein hohes Liquidationsverhältnis eine hohe erwartete Volatilität bedeutet.

Stabilitätsgebühr: Die Stabilitätsgebühr ist eine Gebühr, die von jedem CDP bezahlt wird. Es handelt sich um einen jährlichen Zins, der auf die bestehenden Schulden des CDP angerechnet wird und vom CDP-Nutzer zu zahlen ist. Die Stabilitätsgebühr wird in Dai angegeben, kann aber nur mit dem MKR-Token bezahlt werden. Der zu zahlende MKR-Betrag wird auf der Grundlage eines Preisfeed des MKR-Marktpreises berechnet. Bei Bezahlung wird der MKR verbrannt und somit unwiderruflich aus dem System entfernt.

Liquidationsrate: Die Liquidationsrate wird verwendet, um den maximalen Dai-Betrag aus einer Liquidationsauktion, der verwendet wird, um MKR aufzukaufen und zu verbrennen, zu bestimmen. Dabei werden überschüssige Sicherheiten an den CDP-Inhaber zurückgegeben. Die Liquidationsrate wird verwendet, um die Ineffizienzen des Liquidationsmechanismus abzudecken. Während der Phase des Single-Collateral Dai wird die Liquidationsrate zum Kauf und zum Verbrennen von PETH verwendet, was dem Verhältnis PETH zu ETH zugutekommt.

MKR Token Governance

Neben der Zahlung der Stabilitätsgebühr für aktive CDPs spielt der MKR-Token eine wichtige Rolle bei der Verwaltung der Maker-Plattform.

Die Governance erfolgt auf Systemebene durch die Wahl eines aktiven Antrags (Active Proposal) durch die MKR-Wähler. Der aktive Antrag ist ein Smart Contract, der durch MKR-Abstimmung Root-Zugriff erhalten hat, und damit die internen Governance-Variablen der Maker-Plattform ändern kann. Anträge können in zwei Formen eingereicht werden: Einzelmaßnahmen-Anträge (Single Action Proposal Contracts, kurz SAPC) und delegierende Anträge (Delegating Proposal Contracts, kurz DPC).

SAPCs sind Anträge, die nur einmal nach Erhalt des Root-Zugriffs ausgeführt werden können und deren Änderungen sofort auf die internen Governance-Variablen der Maker-Plattform angewendet werden. Nach der einmaligen Ausführung löscht sich der SAPC selbst und kann nicht mehr verwendet werden. Diese Art von Antrag wird in der ersten Phase des Systems verwendet, da er nicht sehr kompliziert in der Anwendung, aber weniger flexibel ist.

DPCs sind Anträge, die ihren Root-Zugriff kontinuierlich durch eine im DPC kodierte Governance-Logik auf zweiter Ebene nutzen. Die Governance-Logik zweiter Ebene kann relativ einfach sein, wie z.B. die Definition eines Protokolls für die wöchentliche Abstimmung über aktualisierte Risikoparameter. Sie kann auch fortgeschrittenere Logik implementieren, wie z.B. Beschränkungen des Umfangs der Governance-Aktionen innerhalb definierter Zeiträume, oder sogar einige oder alle ihrer Berechtigungen an einen oder mehrere DPCs dritter Ebene mit oder ohne Einschränkungen weitergeben.

Jedes Ethereum-Konto kann Anträge dieser Art erstellen. MKR-Wähler können dann mit ihren MKR-Token für einen oder mehrere Anträge abstimmen. Der Antrag mit der höchsten Gesamtzahl an Stimmen wird dann als aktiver Antrag ausgewählt.

MKR und Multi-Collateral Dai

Nach dem Upgrade auf Multi-Collateral Dai wird MKR eine noch wichtigere Rolle im Dai-Stablecoin-System einnehmen, da es PETH als Rekapitalisierungsressource ersetzen wird. Wenn CDPs aufgrund von Markteinbrüchen unterbesichert werden, wird MKR automatisch verwässert und verkauft, um genügend Mittel für die Rekapitalisierung des Systems aufzubringen.

Automatische Liquidation von riskanten CDPs

Um sicherzustellen, dass immer genügend Sicherheiten im System vorhanden sind, um den Wert aller ausstehenden Schulden (entsprechend dem Richtpreis) zu decken, kann ein CDP liquidiert werden, wenn es als zu riskant eingestuft wird. Die Maker-Plattform bestimmt, wann ein CDP liquidiert werden soll, indem sie dessen Liquidationsverhältnis mit dem aktuellen Verhältnis von Sicherheiten zu Schulden des CDP vergleicht.

Jeder CDP-Typ hat seine eigenes, individuelles Liquidationsverhältnis, die von MKR-Wählern bestimmt und auf der Grundlage des Risikoprofils der jeweiligen Sicherheit dieses CDP-Typs festgelegt wird.

Die Liquidation tritt ein, wenn ein CDP sein Liquidationsverhältnis erreicht. Die Maker-Plattform übernimmt automatisch die Sicherheiten des CDP und veräußert diese anschließend. Für das Single-Collateral Dai gibt es einen vorübergehenden Mechanismus, den sogenannten Liquidity Providing Contract. Für den Multi-Collateral Dai wird ein Auktionsmechanismus verwendet werden.

Liquidity Providing Contract (Temporärer Mechanismus für Single-Collateral Dai)

Während der Phase des Single-Collateral Dai ist der Liquidity Providing Contract der Mechanismus für die Liquidation: ein Smart Contract, der direkt mit Ethereumnutzern und -haltern gemäß des Preisfeeds des Systems handelt.

Wenn ein CDP liquidiert wird, wird es sofort vom System gekauft. Der CDP-Eigentümer erhält den Wert der verbleibenden Sicherheiten abzüglich Schulden, Stabilitätsgebühr und Liquidationsrate.

Die PETH-Sicherheiten werden im Liquidity Providing Contract zum Verkauf angeboten, und die Keeper können die PETH automatisch gegen Zahlung von Dai erwerben. Alle auf diese Weise bezahlten Dai werden sofort aus dem Bestand genommen, bis ein Betrag in Höhe der CDP-Schuld entfernt wurde. Wenn ein Dai über die Schuldenunterdeckung hinaus bezahlt wird, wird der Überschuss an Dai verwendet, um PETH vom Markt zu kaufen und zu verbrennen, was das Verhältnis PETH/ETH positiv verändert. Dies führt zu einem Nettogewinn für PETH-Halter.

Wenn der PETH-Verkauf zunächst nicht genügend Dai aufbringt, um den gesamten Schuldenstand zu decken, wird kontinuierlich mehr PETH geschaffen und verkauft. Das so geschaffene PETH verändert das Verhältnis PETH/ETH negativ, was dazu führt, dass die PETH-Halter einen Wertverlust erleiden.

Schulden- und Sicherheitenauktionen (Multi-Collateral Dai)

Während einer Liquidation kauft die Maker-Plattform die Sicherheiten eines CDP und verkauft sie anschließend in einer automatischen Auktion. Dieser Auktionsmechanismus ermöglicht es dem System, CDPs auch dann abzuwickeln, wenn Preisinformationen nicht verfügbar sind.

Um die Sicherheiten des CDP zu übernehmen, damit sie verkauft werden können, muss das System zunächst genügend Dai aufbringen, um die Schulden des CDP zu decken. Dies wird als Schuldenauktion bezeichnet und funktioniert, indem das Angebot des MKR-Tokens verwässert und an Bieter in einem Auktionsverfahren verkauft wird.

Parallel dazu werden die Sicherheiten des CDP in einer Sicherheitenauktion verkauft, bei der alle Erlöse (in Dai angegeben) bis zum CDP-Schuldenbetrag zuzüglich der Liquidationsrate (ein durch MKR-Votum festgelegter Risikoparameter) verwendet werden, um MKR zu kaufen und aus dem Angebot zu ziehen.

Dies wirkt der MKR-Verwässerung, die während der Schuldenauktion stattgefunden hat, direkt entgegen. Wenn genug Dai geboten wird, um die CDP-Schuld plus Liquidationsrate vollständig zu decken, schaltet die Sicherheitenauktion auf einen Reverse-Auktionsverfahren um und versucht, so wenig Sicherheiten wie möglich zu verkaufen - alle verbleibenden Sicherheiten werden an den ursprünglichen Eigentümer des CDP zurückgegeben.

Wichtige externe Akteure

Zusätzlich zu ihrer Smart Contract Infrastruktur ist die Maker Platform auf bestimmte externe Akteure angewiesen, um ihren Betrieb zu gewährleisten. Keeper sind externe Akteure, die die wirtschaftlichen Anreize der Maker-Plattform nutzen. Orakel und globale Abwickler sind externe Akteure mit besonderen Berechtigungen die ihnen von den MKR-Wählern zugewiesen wurden.

Keeper

Ein Keeper ist ein unabhängiger (meist automatisierter) Akteur, der durch Gewinnmöglichkeiten motiviert wird, zu dezentralen Systemen beizutragen. Im Kontext des Dai-Stablecoin-Systems beteiligen sich Keeper bei der Liquidation von CDPs an den Schulden- und Sicherheitenauktionen.

Keeper handeln Dai zudem rund um den Richtpreis. Keeper verkaufen Dai, wenn der Marktpreis über dem Richtpreis liegt und kaufen Dai, wenn der Marktpreis unter dem Richtpreis liegt, um von der erwarteten langfristigen Angleichung an den Richtpreis zu profitieren.

Orakel

Die Maker-Plattform benötigt Echtzeitinformationen über den Marktpreis der als Sicherheiten in CDPs verwendeten Vermögenswerte, um zu wissen, wann Liquidationen ausgelöst werden müssen. Die Maker-Plattform benötigt außerdem Informationen über den Marktpreis von Dai und dessen Abweichung vom Richtpreis, um den Leitzins bei aktiven TRFM anzupassen. Die MKR-Wähler wählen eine Reihe von vertrauenswürdigen Orakeln, um diese Informationen über Ethereum-Transaktionen an die Maker-Plattform weiterzugeben. Um das System vor einem Angreifer (der die Kontrolle über die Mehrheit der Orakel erlangt) oder Absprachen zu schützen, gibt es eine globale Variable, die die

maximale erlaubte Änderung des Preisfeeds bestimmt. Diese Variable wird als Preisfeed-Sensitivitätsparameter bezeichnet.

Ein Beispiel für die Funktionsweise des Preisfeed-Sensitivitätsparameters: Wenn der Preisfeed-Sensitivitätsparameter als "5% in 15 Minuten" definiert ist, darf sich der Preisfeed innerhalb eines Zeitraums von 15 Minuten nicht mehr als 5% ändern, eine Änderung von 15% würde 45 Minuten dauern. Diese Einschränkung stellt sicher, dass genügend Zeit bleibt, um eine globale Abwicklung auszulösen, falls ein Angreifer die Kontrolle über einen Großteil der Orakel erlangt.

Globale Abwickler

Globale Abwickler sind ähnlich wie PreisFeed-Orakel externe Akteure und bilden die letzte Verteidigungslinie für das Dai-Stablecoin-System im Falle eines Angriffs. Die Gruppe der globalen Abwickler, die von den MKR-Wählern ausgewählt wurden, haben die Befugnis, eine globale Abwicklung auszulösen. Abgesehen von dieser Befugnis haben diese Akteure keinen zusätzlichen besonderen Zugang oder Kontrolle innerhalb des Systems.

Beispiele

Das Dai-Stablecoin-System kann von jedermann ohne Einschränkungen oder Anmeldeverfahren genutzt werden.

- **Beispiel 1:** Bob braucht einen Kredit, also beschließt er, 100 Dai zu generieren. Er steckt ETH im Wert von deutlich mehr als 100 Dai in ein CDP und erzeugt daraus 100 Dai. Die 100 Dai werden sofort auf sein Ethereum-Konto überwiesen. Unter der Annahme, dass die Stabilitätsgebühr 1% pro Jahr beträgt, muss Bob 101 Dai zur Deckung des CDP aufbringen, wenn er beschließt, seine ETH ein Jahr später wieder abzurufen.

Einer der wichtigsten Anwendungsfälle von CDPs ist der Margenhandel.

- **Beispiel 2:** Bob möchte bei ETH/Dai long gehen, also generiert er 100 USD an Dai, indem er 150 USD an ETH an ein CDP sendet. Dann kauft er mit seinem neu generierten Dai weitere 100 USD an ETH und erhält damit ein Nettopositionswert von 1,66x ETH/USD. Mit den 100 USD an ETH, die er durch den Verkauf des Dai erhalten hat, kann er tun, was er will. Die ursprünglichen ETH-Sicherheiten (150 USD wert) bleiben im CDP gesperrt, bis die Schulden plus die Stabilitätsgebühr gedeckt sind.

Obwohl CDPs nicht untereinander vertauschbar sind, ist das Eigentum an einem CDP übertragbar. Dies ermöglicht den Einsatz von CDPs in Smart Contracts, die komplexere Methoden der Dai-Generierung anwenden (z.B. mit mehr als einem Akteur).

- **Beispiel 3:** Alice und Bob arbeiten mit Hilfe eines Ethereum OTC-Contracts zusammen, um durch ETH gesicherte Dai im Wert von 100 USD zu erstellen. Alice steuert ETH im Wert von 50 USD bei, während Bob 100 USD beiträgt. Der OTC-Vertrag verwendet diese Mittel und schafft ein CDP, wodurch Dai im Wert von 100 USD generiert werden. Die neu generierten Dai werden automatisch an Bob gesendet. Aus Bobs Sicht kauft er Dai im Wert von 100 USD, indem er den Gegenwert an der ETH bezahlt. Der Vertrag überträgt dann das Eigentum an

dem CDP auf Alice. Sie hat am Ende Verpflichtungen im Wert von 100 USD (auf Dai lautend) und Sicherheiten von 150 USD (auf ETH lautend). Da sie mit nur 50 USD an ETH anfang, hat sie nun eine 3x Hebelwirkung auf ETH/USD.

Liquidationen stellen sicher, dass das System im Falle eines Preissturzes der Sicherheiten, die einen CDP-Typ absichern, automatisch in der Lage ist, CDPs zu schließen, die zu riskant werden. Dadurch wird sichergestellt, dass das ausstehende Dai-Volumen vollständig besichert bleibt.

- **Beispiel 4:** Nehmen wir an, es gibt einen Ether-CDP mit einem Liquidationsverhältnis von 145%, einer Liquidationsrate von 105% und einem Sicherheiten-/Schulden-Verhältnis von 150%. Der Etherpreis stürzt nun um 10% gegenüber dem Richtpreis ab, so dass das Sicherheiten-/Schuldenverhältnis des CDP auf ~135% fällt. Da es unter das Liquidationsverhältnis fällt, können Händler die Liquidation auslösen und mit Dai ein Gebot für den Kauf von MKR in der Schuldenauktion abgeben. Gleichzeitig können Händler mit Dai ein Gebot abgeben, um die Sicherheiten im Wert von ~135 Dai in der Sicherheitenauktion zu kaufen. Sobald mindestens 105 Dai auf die Ether-Sicherheiten geboten werden, bieten Händler rückwärts, um die geringste Menge an Sicherheiten für 105 Dai zu nehmen. Alle verbleibenden Sicherheiten werden an den CDP-Eigentümer zurückgegeben.

Erreichbarer Markt

Wie in der Einleitung erwähnt, ist eine preisstabile Kryptowährung eine Grundvoraussetzung für die meisten dezentralen Anwendungen. Damit ist das Marktpotenzial für Dai mindestens so groß wie das der gesamten Blockchain-Branche. Nachfolgend finden Sie eine kurze, nicht vollständige Liste einiger der unmittelbaren Märkte (sowohl für die Blockchain als auch für weitere Branchen) für das Dai-Stablecoin-System in seiner Eigenschaft als preisstabile Kryptowährung und seinem Anwendungsbereich als dezentrale Margenhandelsplattform:

Prognosemärkte & Glücksspiel: Wenn man eine unabhängige Prognose machen will, sollte man das Risiko nicht dadurch erhöhen, dass man die Wette mit einer volatilen Kryptowährung abschließt. Langzeitwetten werden besonders dann unrentabel, wenn der Nutzer auch auf den zukünftigen Preis der volatilen Währung setzen muss, mit der die Wette abgeschlossen wurde. Stattdessen wird eine preisstabile Kryptowährung wie Dai die erste Wahl für Prognosemarkt- und Glücksspielnutzer sein.

Finanzmärkte; Hedging, Derivate, Hebel: CDPs ermöglichen einen Leverage-Handel ohne Eintrittshürden. Dai wird außerdem als stabile und zuverlässige Sicherheit in Smart Contracts für Derivate, wie Optionen oder CFDs, nützlich sein.

Handelsbelege, grenzüberschreitende Transaktionen und Rücküberweisungen: Durch die Vermeidung von Wechselkursvolatilität und den Wegfall von Intermediären können Transaktionskosten im internationalen Handel durch den Einsatz von Dai deutlich reduziert werden.

Transparente Buchhaltungssysteme: Wohltätigkeitsorganisationen, NGOs und Regierungen werden durch die Nutzung von Dai Effizienzsteigerungen und ein geringeres Maß an Korruption erzielen.

Risiken und ihre Minimierung

Die Entwicklung, Bereitstellung und der Betrieb der Maker-Plattform birgt viele potenzielle Risiken. Es ist wichtig, dass die Maker-Community alle notwendigen Schritte unternimmt, um diese Risiken zu minimieren. Die folgende Liste enthält einige der identifizierten Risiken und die jeweils dazugehörigen Abwehrmaßnahmen:

Hackangriff auf die Smart Contract Infrastruktur

Das größte Risiko für das System in seiner Anfangsphase ist, dass ein Hacker einen Schwachpunkt in den eingesetzten Smart Contracts findet und damit das System knackt oder bestiehlt, bevor die Schwachstelle behoben werden kann. Im schlimmsten Fall könnten alle dezentralen digitalen Werte, die als Sicherheiten in der Maker-Plattform gehalten werden, wie Ether (ETH) oder Augur Reputation (REP), ohne Chance auf Rückgewinnung gestohlen werden. Der Teil des Sicherheitenportfolios, der nicht dezentralisiert ist, wie z.B. die Digix Gold IOU's, würde in einem solchen Fall nicht gestohlen werden. Diese könnten durch eine Hintertür zentral eingefroren und kontrolliert werden.

Abwehrmaßnahme: Smart Contract Sicherheit und andere bewährte Sicherheitspraktiken haben bei der Entwicklung von Dai seither absolute höchste Priorität. Die Codebasis wurde bereits drei unabhängigen Sicherheitsüberprüfungen durch die besten Sicherheitsfachkräfte der Blockchain-Industrie unterzogen.

Langfristig kann das Risiko, gehackt zu werden, durch eine formale Verifikation des Codes theoretisch fast vollständig reduziert werden. Formale Verifikation bedeutet, mathematisch zu beweisen, dass der Code genau das tut, was er tun soll. Obwohl die vollständige formale Verifikation ein sehr langfristiges Ziel ist, wurden bereits umfangreiche Arbeiten durchgeführt, einschließlich einer vollständigen Referenzimplementierung des Dai-Stablecoin-Systems in der funktionalen Programmiersprache Haskell. Diese Implementierung dient als Ausgangspunkt für komplexere Formalisierungen, welche derzeit aktiv erforscht und entwickelt werden.

Schwarzer Schwan

Ein weiteres großes Risiko ist ein potenzielles Schwarzer-Schwan-Ereignis der Sicherheiten (Collateral Assets), die für CDP verwendet werden. Dies könnte entweder in der Anfangsphase des Dai-Stablecoin-Systems geschehen, bevor MKR robust genug ist, um inflationäre Verwässerungen zu verkraften, oder nachdem das Dai-Stablecoin-System ein breiteres Portfolio an Sicherheiten unterstützt.

Abwehrmaßnahme: In der Anfangsphase kann nur ETH als Sicherheit für CDPs verwendet werden, wobei die Schuldenobergrenze zunächst beschränkt ist und im Laufe der Zeit allmählich zunimmt.

Wettbewerber und Benutzerfreundlichkeit

Wie bereits erwähnt, arbeiten große Mengen Geld und Fachwissen an preisstabilen Kryptowährungen. Aufgrund seiner "echten Dezentralisierung" ist das Dai-Stablecoin-System das bei weitem komplexeste Modell in der Blockchain-Branche. Ein potenzielles Risiko ist eine Tendenz unter den Benutzern von Kryptowährungen, die Ideale der Dezentralisierung gegen die Einfachheit und Vermarktbarkeit von zentralisierten digitalen Assets auszutauschen.

Abwehrmaßnahme: Wir erwarten, dass Dai für einen normalen Kryptowährungsnutzer sehr einfach zu bedienen sein wird. Dai ist ein Ethereum-Token, der dem ERC-20-Standard entspricht und ist im gesamten Ökosystem mit hoher Liquidität verfügbar. Dai wurde so konzipiert, dass der Normalverbraucher die zugrundeliegende Mechanik des Systems nicht verstehen muss, um es nutzen zu können.

Die Komplexität des Dai-Stablecoin-Systems muss in erster Linie von Keepern und Kapitalanlagegesellschaften verstanden werden, die das Dai-Stablecoin-System für den Margenhandel nutzen wollen. Diese Benutzergruppen haben genügend Ressourcen, um sich selbst einzuarbeiten, vorausgesetzt, es gibt eine umfassende und klare Dokumentation aller Aspekte der Mechanik des Systems. Die Maker-Community wird dafür sorgen, dass dies der Fall ist.

Preisfehler, Irrationalität und unvorhersehbare Ereignisse

Eine Reihe von unvorhergesehenen Ereignissen kann auftreten, wie z.B. ein Problem mit dem Preisfeed der Orakel oder irrationale Marktdynamiken, die über einen längeren Zeitraum zu Schwankungen im Wert von Dai führen. Wenn das Vertrauen in das System verloren geht, könnten die TRFM-Anpassungen oder die MKR-Verwässerung extreme Werte erreichen, dem Markt aber trotzdem nicht genügend Liquidität und Stabilität liefern.

Abwehrmaßnahme: Die Maker Community muss einen ausreichend großen Kapitalpool schaffen, um als Markthalter zu agieren, damit Rationalität und Markteffizienz maximiert werden können und das Dai-Angebot ohne größere Marktschocks stetig wachsen kann.

Ausfall der zentralen Infrastruktur

In der Anfangsphase spielt das Maker-Team eine wichtige Rolle bei der Entwicklung und Steuerung der Maker-Plattform: Budgetplanung, Rekrutierung neuer Entwickler, Suche nach Partnerschaften und institutionellen Nutzern sowie die Zusammenarbeit mit Regulierungsbehörden und anderen wichtigen externen Interessensgruppen. Sollte das Maker-Team in irgendeiner Weise (ohne einen geeigneten Backup-Plan) scheitern - aus rechtlichen Gründen oder aufgrund interner Probleme mit dem Management - könnte die Zukunft von Maker gefährdet sein.

Abwehrmaßnahme: Die Maker-Community existiert auch als dezentrale Gegenpartei zum Maker-Team. Sie ist ein loser Zusammenschluss unabhängiger Akteure, die alle durch den Besitz des MKR-Tokens verbunden sind. Das gibt ihnen einen starken Anreiz, den Erfolg der Maker-Plattform voranzutreiben. In den frühen Phasen der Verteilung von MKR wurde sehr darauf geachtet, dass die wichtigsten Entwickler einen bedeutenden MKR-Anteil erhalten. Für den Fall, dass das Maker-Team nicht mehr in der Lage ist, die Entwicklung der Maker-Plattform effektiv zu leiten, werden einzelne MKR-Inhaber dazu angehalten, Entwickler zu fördern (oder einfach selbst zu entwickeln), um ihre Investitionen zu schützen.

Fazit

Das Dai-Stablecoin-System wurde entwickelt, um das zentrale Problem des wertstabilen Handels im Ethereum-Ökosystem und der gesamten Blockchainökonomie zu lösen. Wir glauben, dass der Mechanismus, durch den Dai geschaffen, verwaltet und aus dem Markt genommen wird, zusammen mit dem direkten Risikomanagement der MKR-Inhaber es eigennützig handelnden Keepern ermöglicht, die Preisstabilität von Dai effizient aufrechtzuerhalten. Die Gründungsmitglieder der Maker-Community haben einen sorgfältigen Governance-Fahrplan erstellt, der den Bedürfnissen einer agilen Entwicklung auf kurze Sicht gerecht wird, aber auch mit den Idealen der Dezentralisierung langfristig vereinbar ist. Der Entwicklungsplan ist sehr ambitioniert aber verantwortungsbewusst und fokussiert sich auf eine flächendeckende Nutzung von Dai.

Glossar

- **Collateralized Debt Position (CDP):** Ein Smart Contract, dessen Nutzer einen Vermögenswert (Dai) erhalten, der als Schuldtitel mit einem Zinssatz fungiert. Der CDP-Nutzer hat Sicherheiten hinterlegt, die den Wert des Dai-Kredits übersteigen, um seine Schuldenposition zu sichern.
- **Dai:** Die preisstabile Kryptowährung, die der Tauschwert im Dai-Stablecoin-System ist. Es handelt sich um einen Ethereum-Standard-Token, der dem ERC20-Standard entspricht.
- **Schuldenauktion:** Die Rückwärtsauktion, bei der MKR für Dai verkauft wird, um Notfall-Schulden zu decken, wenn ein CDP unterbesichert wird.
- **Sicherheitenauktion:** Die Auktion, bei der Sicherheiten von einem in Liquidation befindlichen CDP verkauft werden. Sie soll der Deckung der Schulden des CDP Vorrang geben und dem CDP-Eigentümer den bestmöglichen Preis für die Rückerstattung seiner überschüssigen Sicherheiten bieten.
- **Dai Stiftung:** Ein dezentrales Team von Smart Contract Entwicklern, das die erfolgreiche Realisierung der Maker Plattform zum Ziel hat.
- **Keeper:** Unabhängige Akteure, die Dai, CDPs und/oder MKR handeln; Dai generieren oder CDPs schließen und nach Arbitragemöglichkeiten im Dai-Stablecoin-System suchen. Dadurch tragen die Keeper dazu bei, die Marktrationalität und Preisstabilität von Dai zu erhalten.
- **MKR:** Der ERC20-Token, der von den MKR-Wählern für Abstimmungen verwendet wird. Er dient auch als Absicherung bei insolventen CDPs.
- **MKR-Wähler:** MKR-Inhaber, die das Risikomanagement des Dai Stablecoin-Systems aktiv gestalten, indem sie über die Risikoparameter abstimmen.
- **Maker:** Der Name der dezentralen autonomen Organisation (DAO), die sich aus der technischen Infrastruktur der Maker Plattform und der Community der MKR-Wähler zusammensetzt.
- **Orakel:** Ethereum Accounts (entweder Smart Contracts oder Benutzer), die auserwählt wurden Preisinformationen für verschiedene Komponenten der Maker Plattform liefern.
- **Risikoparameter:** Die Variablen, die u.a. bestimmen, wann die Maker-Plattform ein CDP automatisch als zu riskant einstuft, so dass die Keeper es dann liquidieren können.
- **Sensitivitätsparameter:** Die Variable, die bestimmt, wie stark das Dai-Stablecoin-System den Leitzins automatisch ändert kann, als Reaktion auf Preisschwankungen am Dai-Markt.
- **Leitzins-Feedback-Mechanismus (TRFM):** Der automatische Mechanismus, mit dem das Dai-Stablecoin-System den Leitzins anpasst, um die Marktteilnehmer dazu zu bringen, den Dai-Preis stabil und möglichst nah am Richtpreis zu halten.