

Dai Stablecoinシステム

ホワイトペーパー

<https://makerdao.com/>

Makerチーム制作

2017年12月

Dai Stablecoinシステムの概要 4

担保付債務ポジションスマートコントラクト 4

CDPインタラクションプロセス 6

単一担保Daiと複数担保Dai 6

プールドイーサ(単一担保Daiの一時的メカニズム) 8

価格安定メカニズム 8

目標価格 8

目標レートフィードバックメカニズム 8

感度パラメーター 10

グローバル決済 11

グローバル決済:具体的な手順 11

Makerプラットフォームのリスク管理 12

リスクパラメーター 13

MKRトークンガバナンス 15

MKRと複数担保Dai 16

リスクのあるCDPの自動清算 16

流動性提供コントラクト(単一担保Daiの一時的メカニズム) 18

債務と担保オークション(複数担保Dai) 18

主要な外部アクター 20

キーパー 20

オラクル 20

グローバルセトラー 22

例 22

対応可能な市場 25

リスクとリスク緩和 25

スマートコントラクトインフラストラクチャに対する悪意のあるハッキング攻撃 27

1つまたは複数の担保資産の予測不能な事象 27

競争と使いやすさの重要性 29
価格エラー、非合理性、想定外の事象 29
中央集権型インフラストラクチャの失敗 30

結論 30

用語集 31

リンク 33

Dai stablecoinシステムの概要

ビットコイン(BTC)とイーサ(ETH)は、日常的に使用する通貨としては変動が大きすぎます。ビットコインは値動きが激しく、1日で25%も乱高下することがあり、ときには1か月で300%以上も上昇します。¹

Dai Stablecoinは担保に裏付けられた仮想通貨で、その価値は米ドルと同程度に安定しています。私たちは、ブロックチェーン技術の可能性を最大限に引き出すためには、Dai Stablecoinのような安定したデジタル資産が不可欠だと考えています。

Makerはイーサリアム上のスマートコントラクトプラットフォームで、Daiの価値を裏付け、安定させます。これは、MakerのもつCDP(Collateralized Debt Positions:担保付債務ポジション)、自律的なフィードバックメカニズム、適切にインセンティブを与えられた外部機関によるダイナミックなシステムによって支えられています。

Makerでは、誰もがイーサリアム資産を活用してMakerプラットフォーム上にDaiを生成できます。いったん生成されたDaiは、他の仮想通貨と同じように使用できます。つまり、他者に自由に送信したり、商品やサービスの決済に使用したり、長期的な貯蓄のために保有したりできます。重要なのは、Daiの生成により、堅牢な分散化信用取引のプラットフォームに必要なコンポーネントも作成されるという点です。

担保付債務ポジションスマートコントラクト

担保資産を持っている人は誰でもそれを活用し、担保付債務ポジションというMaker独自のスマートコントラクトを通じてMakerプラットフォーム上にDaiを生成できます。²

CDPはユーザーが預託した担保資産を保有し、Daiの生成をこのユーザーに許可しますが、生成と同時に債務も発生します。この債務は、あとで等価のDaiの支払いにより返済されるまで、CDP内に預託された担保資産を事実上保護します。返済の時点で、所有者は再び担保を引き出すことができます。有効なCDPは常に過剰担保になり、担保価値が債務価値より高い状態になっています。

¹ David Ernst [Hard Problems in Cryptocurrency](#)

² <https://github.com/makerdao>

CDPインタラクションプロセス

- **ステップ1: CDPを作成して担保を預託する**

CDPユーザーは最初にトランザクションをMakerに送信してCDPを作成し、次にDaiの生成に使用する担保の金額とタイプを別のトランザクションで送信してCDPに資金を調達します。この時点でCDPは担保されていると見なされます。

- **ステップ2: 担保されたCDPからDaiを生成する** 次にCDPユーザーは希望する金額のDaiをCDPから引き出すためのトランザクションを送信します。同時に、等価の債務がCDPに発生し、債務残高が返済されるまでは担保にアクセスできなくなります。

- **ステップ3: 債務を返済して安定化手数料を支払う** ユーザーは、担保を回収したいときにCDPの債務を返済し、時間の経過とともに債務に累積された安定化手数料を支払う必要があります。安定化手数料はMKRでのみ支払うことができます。ユーザーが必要なDaiとMKRをCDPに送信して債務と安定化手数料を支払うと、CDPは完済状態になります。

- **ステップ4: 担保を回収してCDPを閉じる** 債務と安定化手数料の支払いを完了すると、CDPユーザーは、トランザクションをMakerに送信することにより、担保の全部または一部を自分のウォレットに自由に返すことができます。

単一担保Daiと複数担保Dai

Daiで当初使えるのは、プールドイーサという1種類の担保のみです。その後6~12か月で、単一担保Daiを複数担保Daiにアップグレードする予定です。主な違いは、任意の数のCDPタイプを使用できることです。³

³単一担保の段階で一時的に使用されるメカニズムは、このホワイトペーパーで印が付いています

プールドイーサ(単一担保Daiの一時的メカニズム)

当初は、プールドイーサ(PETH)が、Makerで受け入れられる唯一の担保タイプです。Makerプラットフォームの第1段階の間にCDPを開設してDaiを生成したいユーザーは、まずPETHを入手する必要があります。これは、全ユーザーのETHをプールし、それに対応するPETHを返す特別なスマートコントラクトにETHを預託することにより、ブロックチェーンで即時に簡単に行えます。

ETHに突然の市場暴落があり、CDPが担保の価値よりも大きな債務を抱えてしまった場合、MakerプラットフォームではPETHが自動的に希釈され、システムで資本再編成が行われます。このため、PETHあたりの相対的請求が下がることとなります。

Makerプラットフォームがアップグレードされて複数タイプの担保が利用可能になると、PETHは抹消され、ETHやその他の新しいタイプの担保がその代わりになります。

価格安定メカニズム

目標価格

MakerプラットフォームにおいてDaiの目標価格には、1)CDPの担保債務比率の計算に使用する、2)グローバル決済でDai保有者が受け取る担保資産の価値を決定するために使用する、という2つの主要な役割があります。

目標価格は当初は米ドル建てで、1から始まり、1:1 USDソフトペッグで換算されます。

目標レートフィードバックメカニズム

市場が非常に不安定になった場合、目標レートフィードバックメカニズム(TRFM: Target Rate Feedback Mechanism)が作動することがあります。TRFMが作動すると、Daiの固定ペッグは外されますが、額面金額は維持されます。

TRFMは、Dai Stablecoinシステムが目標レートを調整する自動メカニズムで、市場力を使ってDai市場価格が目標価格付近で安定するようにします。目標レートは時間の経過にもなう目標価格の変化を決定するため、Daiの保有(目標レートがプラスの場合)またDaiの借入(目標レートがマイナスの場合)のインセンティブとして作用します。TRFM が作動していないときは目標レートが0%に固定されるため、時間が経過しても目標価格は変化せず、Daiはペッグされています。

TRFMが作動すると、目標レートと目標価格の両方が動的に変化し、Daiの生成と保有によるユーザーのインセンティブが自動的に調整されて、Daiの需給バランスが均衡されます。フィードバックメカニズムにより、変動する目標価格に向けてDaiの市場価格を誘導して変動性を弱め、需要ショック中のリアルタイムの流動性を提供します。

TRFMの作動中、Daiの市場価格が目標価格を下回ると、目標レートが上がります。これにより、目標価格がより高いレートへと上昇し、CDPでのDAI生成がより高額になります。同時に、上昇した目標レートは、Daiの保有によるキャピタルゲインを増加させるため、それに連動してDaiの需要が増加します。Daiの供給が減り需要が増すと、Daiの市場価格が上昇し、目標価格に戻るよう誘導されます。

Dai市場価格が目標価格を上回った場合は、同じメカニズムが反対方向に働きます。つまり目標レートが下がり、Dai生成の需要が増加し、Dai保有の需要が減少します。これにより、Daiの市場価格が下がり、目標価格に向かって押し下げられます。

このメカニズムはネガティブフィードバックループです。目標価格から一方方向に剥離すると、逆方向の力が強まります。

感度パラメーター

TRFMの感度パラメーターは、Dai目標/市場価格の偏差に呼応する目標レートの変化の影響度を決定するパラメーターです。これにより、フィードバックのレートが、システムのスケールに合わせて調整されます。MKR有権者は感度パラメーターを設定できますが、TRFMの作動中は、目標価格と目標レートは市場ダイナミクスによって決定され、MKR有権者は直接コントロールできなくなります。感度パラメーターは、TRFMの作動または解放にも使用されます。感度パラメーターと目標レートが両方とも0の場合、Daiは現在の目標価格にペッグされます。

グローバル決済

グローバル決済は、目標価格をDaiの保有者に暗号的に保証する最後の手段として使用できるプロセスです。Makerプラットフォームをシャットダウンし、適切に巻き戻して、Dai保有者とCDPユーザーの両方を含むすべてのユーザーが、自身が持つ資産の正味値を受け取れるようにします。プロセスは完全に分散化されており、重大な緊急事態の場合にのみこのプロセスが実施されるようにMKR有権者がグローバル決済へのアクセスを制御します。重大な緊急事態の例としては、長期にわたって市場が不合理な動きをする場合や、ハッキングやセキュリティ侵害、システムアップグレードなどが挙げられます。

グローバル決済:具体的な手順

● ステップ1: グローバル決済が発動される

Makerガバナンスがグローバルセトラーとして指定したアクターのうち十分な人数が、システムが重大な攻撃を受けていると判断した場合、また技術的アップグレードの一環としてグローバル決済がスケジュールされている場合に、グローバル決済機能を発動できます。これにより、CDPの作成と操作が停止し、価格フィードが固定値で凍結されます。この固定値が全ユーザーの相対的請求に使用されます。

● ステップ2: グローバル決済請求が処理される

グローバル決済が発動された後、キーパーが固定フィード値に基づいてDaiとCDPの全保有者による相対的申請を処理するまでに、しばらく時間がかかります。この処理が完了すると、Daiの全保有者とCDPの全保有者は、各自が保有するDaiとCDPに応じて固定金額のETHを申請できるようになります。

● ステップ3: DaiとCDPの保有者がDaiとCDPで担保を請求する

DaiとCDPの各保有者はMakerプラットフォームの請求機能呼び出して、保有するDaiとCDPを、Daiの目標価格に基づいて算出された資産価値に相当する固定額のETHと交換できます。

Daiの目標値が1米ドルの場合、ETH/USD価格は200です。グローバル決済が発動されたときにユーザーが1000 Daiを保有している場合、ユーザーはプロセス期間後にMakerプラットフォームに5ETHちょうどを請求できます。請求に期限は設けられていません。

Makerプラットフォームのリスク管理

MKRトークン保有者は、リスク管理のための以下のアクションの実施に投票できます。

- **新規CDPタイプの追加:** リスクパラメーターの一意のセットをもつ新規CDPタイプを作成します。CDPタイプには、新しい担保タイプか既存の担保タイプのリスクパラメーターの新しいセットを使用できます。
- **既存CDPタイプの変更:** すでに追加されている1つまたは複数の既存CDPタイプのリスクパラメーターを変更します。
- **感度パラメーターの変更:** 目標レートフィードバックメカニズムの感度を変更します。
- **目標レートの変更:** カバランスで目標レートを変更できます。実際には、目標レートの変更は、MKR有権者がDaiの価格を現在の目標価格にペッグしたいときなど、特殊な状況でのみ行われます。これは、常に感度パラメーターの変更と同時に行われます。感度パラメーターと目標レートを両方とも0%に設定すると、TRFMは無効になり、Daiの目標価格は現在の値にペッグされた状態になります。
- **信頼されるオラクルのセットの選択:** Makerプラットフォームでは、さまざまなセットの個別オラクルノードからなる分散型オラクルインフラストラクチャから、担保の内部価格とDaiの市場価格を導出します。MKR有権者は、信頼されるオラクルのセットに含まれるノードの数と、これらのノードが誰であるかを管理します。最大でオラクルの半分に侵害や動作異常があったとしても、システムの継続的な安全動作が中断されることはありません。
- **価格フィード感度の変更:** 価格フィードがシステム内の内部価格値に影響を与える最大の変化を決定するルールを変更します。
- **グローバルセトラーの選択:** グローバル決済は、オラクルまたはガバナンスプロセスへの攻撃からMakerプラットフォームを守るための非常に重要なメカニズムです。ガバナンスプロセスでは、グローバルセトラーのセットを選択し、グローバル決済の発動に必要なセトラーの数を決定します。

リスクパラメーター

担保で保証された債務ポジションには、その使用方法を強制する複数のリスクパラメーターがあります。各CDPタイプには独自のリスクパラメーターセットがあり、これらのパラメーターは、各CDPタイプで使用される担保のリスクプロファイルに基づいて決定されます。これらのパラメーターは、MKR保有者が投票を通じて直接管理します。MKR保有者にはMKR1単位につき1票の投票権が与えられます。

CDPの主要なリスクパラメーター:

- **債務上限:** 債務上限は、単一タイプのCDPで作成できる債務の最大限度額です。あるタイプのCDPによって十分な債務が作成されると、既存のCDPを閉鎖しない限り、それ以上の債務を作成できなくなります。債務上限は、担保ポートフォリオの十分な分散を確保するために使用されます。
- **清算比率:** 清算比率は、CDPが清算に対して脆弱になる担保債務の比率です。清算比率が低いと、MKR有権者は担保の価格変動が低くなると予測し、清算比率が高い場合は変動が高くなると予測します。
- **安定化手数料:** 安定化手数料はすべてのCDPが支払う手数料です。CDPの既存の債務に基づき計算される年率パーセントで、CDPユーザが支払います。安定化手数料はDai建てですが、MKRトークンでしか支払えません。支払うMKRの金額は、MKR市場価格の価格フィードに基づき計算されます。支払いが行われるとMKRは焼却され、供給から永久に抹消されます。
- **ペナルティ比率:** ペナルティ比率は、MKRを購入して供給から消す清算オークションから調達するDaiの最大金額の決定に使用されます。超過分の担保は、清算前からCDPを所有していたCDPユーザーに返還されます。ペナルティ比率は、清算メカニズムの非効率性を補うために使われます。単一担保Daiの段階では、清算ペナルティはPETHの購入と焼却に使われ、これによりPETH:ETH比が改善されます。

MKRトークンガバナンス

MKRトークンは、有効なCDPに課される安定化手数料の支払いに加えて、Makerプラットフォームのガバナンスにおいて重要な役割を担います。

ガバナンスは、MKR有権者によるアクティブ提案への投票を通じて、システムレベルで行われます。アクティブ提案は、MKR投票によりMakerプラットフォームの内部ガバナンス変数を変更するためのルートアクセス権を獲得できるスマートコントラクトで

ます。提案には、シングルアクション提案コントラクト(SAPC)と委任提案コントラクト(DPC)の2つの形式があります。

シングルアクション提案コントラクトは、ルートアクセス権の取得後に一度だけ実行できる提案です。実行後は、Makerプラットフォームの内部ガバナンス変数への変更がただちに適用されます。一度限りの実行後、SAPCは自身を削除し、再使用できなくなります。このタイプの提案はシステムの第一段階で使用され、使用方法は複雑ではありませんが、柔軟性に欠けます。

委任提案コントラクトは、DPC内でコード化された第2層ガバナンスロジックを通じて、継続的にルートアクセス権を使用する提案です。第2層ガバナンスロジックは比較的単純で、更新されたリスクパラメーターについて毎週投票を開催するプロトコルの定義などがあります。また、所定期間中のガバナンスアクションの影響度に対する制約など、より高度なロジックを実装することもできます。さらに、第3層の1つまたは複数のDPCにそのパーミッションの一部または全部を、制約あり、または制約なしで委譲することも可能です。

どのイーサリアム口座でも、有効な提案スマートコントラクトをデプロイできます。次にMKR有権者は自分のMKRトークンを使用して、アクティブ提案として選出したい1つまたは複数の提案に対して承認投票を行えます。MKR有権者からの総承認得票数が最も多いスマートコントラクトが、アクティブ提案として選出されます。

MKRと複数担保Dai

複数担保Daiへのアップグレード後、MKRは資本再構成リソースとしてPETHに取って代わることにより、Dai Stablecoinシステムでより大きな役割を担うようになります。市場崩壊によりCDPが過小担保になった場合、MKRの供給は自動的に希釈されて売却され、システムの資本再構成に十分な資金が調達されます。

リスクのあるCDPの自動清算

(目標価格に基づく)全発行済債務の価値をカバーする十分な担保が常にシステム内に確保されるように、CDPのリスクが高くなりすぎたと判断される場合には清算できます。Makerプラットフォームでは、清算比率とCDPの現在の担保債務比率とを比較することにより、CDPをいつ清算するかを決定します。

各CDPタイプには独自の清算比率があり、MKR有権者により管理され、そのCDPタイプの特定の担保資産のリスクプロファイルに基づいて設定されます。

清算は、CDPが清算比率に達した時点で行われます。Makerプラットフォームでは、その CDPの担保が自動的に購入され、その後売却されます。単一担保Daiには、流動性提供コントラクトという一時的なメカニズムがあります。複数担保Daiでは、オークションメカニズムが使用されます。

流動性提供コントラクト(単一担保Daiの一時的メカニズム)

単一担保Dai段階の間、清算のためのメカニズムは流動性提供コントラクトです。これは、システムの価格フィードに応じてイーサリアムのユーザーおよびキーパーと直接取引するスマートコントラクトです。

清算されたCDPはただちにシステムによって取得されます。CDPの所有者は、残りの担保から債務、安定化手数料、および清算ペナルティを差し引いた金額を受け取ります。

PETH担保は流動性提供コントラクトで売却できるように設定されており、キーパーは、Daiを支払うことによりPETHをアトミックに購入できます。この方法で支払われたDaiはすべて直ちにDai供給から抹消され、CDP債務と等価の金額が抹消されるまでこれが継続されます。Daiが債務不足を超えて支払われる場合、市場からPETHを購入して焼却するために、超過分のDaiが使用されます。これにより、ETHとPETHの比率が有利に変更され、PETH所有者の正味利益につながります。

PETHの売却が最初の段階で債務不足全体をカバーするための十分なDaiに達しない場合、より多くのPETHが継続的に作成されて売却されます。この方法で新しいPETHが作成されると、ETHとPETHの比率が不利に変更され、PETH所有者の利益が減ります。

債務と担保オークション(複数担保Dai)

清算中、Makerプラットフォームでは、CDPの担保が購入され、その後自動オークションで売却されます。このオークションメカニズムにより、価格情報がないときにも、システムでCDPを決済できます。

CDPの担保を販売できるように取得するには、まず、システムでCDPの債務をカバーするための十分なDaiを調達する必要があります。これは、債務オークションと呼ばれ、

MKRトークンの供給を希薄化し、オークション形式で入札者に売却することで機能します。

同時に、CDPの担保は担保オークションで売却されます。ここでは、最大でCDP債務金額と清算ペナルティ(MKR投票によって決定されたリスク要因)の合計に相当するすべての収益(Dai建て)が使用され、すべてのMKRを購入して供給から消します。これは、債務オークション中に発生したMKR希薄化の影響を直接的に弱めます。CDP債務と清算ペナルティの合計を完全にカバーするだけの十分な価格がDaiに付いた場合、担保オークションはリバースオークションに切り替わり、できる限り売却する担保を少なくしようとします。残りの担保はCDPの元の所有者に返却されます。

主要な外部アクター

スマートコントラクトインフラストラクチャのほかに、Makerプラットフォームは、特定の外部アクターに頼って、運用を管理します。キーパーは、Makerプラットフォームで提供される経済的インセンティブを利用する外部アクターです。オラクルとグローバルセトラーは、MKR有権者によって割り当てられたシステムで特別な権限を有する外部アクターです。

キーパー

キーパーは独立した(通常は自動の)アクターであり、分散システムに貢献する利益機械によってインセンティブを受け取ります。Dai Stablecoinシステムのコンテキストでは、CDPが清算されるときに、キーパーが債務オークションと担保オークションに参加します。

また、キーパーは、目標価格周辺でDaiを取引します。キーパーは、市場価格が目標価格より高いときにDaiを売却し、市場価格が目標価格より低いときにDaiを購入し、目標価格に対する想定長期コンバージェンスから利益を得ます。

オラクル

Makerプラットフォームは、清算をトリガーするときを知るために、CDPの担保として使用される資産の市場価格に関するリアルタイム情報を必要とします。また、TRFMが関係する場合、目標レートを調整するために、Daiの市場価格と目標価格からの偏差に関する情報も必要とします。MKR有権者は信頼するオラクルのグループを選択し、イーサリアム取引を通して、この情報をMakerプラットフォームに投入します。

大多数のオラクルを支配する攻撃者と、他の形式の衝突からシステムを保護するために、価

価格フィードの価値に対してシステムが許容する最大限の変更を決めるためのグローバル変数
があります。この変数は、価格フィード感度パラメーターと呼ばれます。

価格フィード感度パラメーターの使用例としては、価格フィード感度パラメーターを「15分で5%」と定義した場合、1回の15分間における価格フィードの変更が5%以下に制限されるため、15%の変更には45分かかります。この制限は、攻撃者が大多数のオラクルを支配する場合に、グローバル決済をトリガーするために十分な時間が確保されることを保証します。

グローバルセトラー

グローバルセトラーは、価格フィードオラクルに似た外部アクターであり、攻撃の際は Dai Stablecoinシステムの最終防衛線となります。MKR有権者によって選択されたグローバルセトラーのグループには、グローバル決済をトリガーする権限があります。この権限以外、これらのアクターには、システム内での追加の特別なアクセスまたはコントロールは一切ありません。

例

Dai Stablecoinシステムは、制限や登録処理がなく、誰でも使用できます。

- **例1:** ボブは融資が必要であるため、100 Daiを発行することを決めました。そこで、100 Daiを大幅に超える価値に相当するETHをCDPに固定し、それを使用して、100 Daiを発行します。100 Daiは即時に彼のイーサリアムアカウントに直接送信されます。安定化手数料を年1%とすると、ボブが1年後にETHを取り戻すときは、CDPをカバーするために101 Daiが必要になります。

CDPの主な使用例の1つは、CDPユーザーによるマージン取引です。

- **例2:** ボブは、ETH/Daiペアのロング取引でマージンを得ようと考えています。このため、150米ドル相当のETHをCDPに入れ、100米ドル相当のDaiを発行します。その後、新しく発行されたDaiを使用して、別の100米ドル相当のETHを購入します。これで、正味1.66倍のETH/USDのエクスポージャーとなります。ボブは、Daiの売却で得た100米ドル相当のETHは自由に使うことができますが、元のETH担保(150米ドル相当)は、債務と安定化手数料を補えるまでCDPに固定されます。

CDPは相互に代替可能ではありませんが、CDPの所有権は移転可能です。これにより、より複雑なDai発行方法を実行するスマートコントラクトでCDPを使用できます(複数のアクターの関与など)。

● **例3:** アリスとボブは共同でイーサリアムOTCコントラクトを使用し、ETHで裏付けられた100米ドル相当のDaiを発行します。アリスは50米ドル相当のETH、ボブは100米ドル相当のETHを拠出します。OTCコントラクトは資金を取得してCDPを作成することで、100米ドル相当のDaiを発行します。新しく発行されたDaiは自動的にボブに送信されます。ボブの視点からは、ETHで等価を支払うことで、100米ドル相当のDaiを購入しています。その後、コントラクトはCDPの所有権をアリスに移転します。アリスは最終的に100米ドル相当の債務(Dai建て)と150米ドル相当の担保(ETH建て)を引き受けます。アリスはわずか50米ドル相当のETHで開始したため、現在、ロングEHT/USDで3倍のレバレッジがかかっています。

清算により、CDPタイプを裏付けする担保の価格暴落の際に、システムが自動的に危険が高すぎるCDPの取引を終了することができます。これにより、市場のDai供給がすべて確実に担保で保証されます。

● **例4:** 清算レートが145%、ペナルティレートが105%のイーサリアムCDPタイプと、担保と債務の比率が150%のイーサリアムCDPがあるとします。現在、イーサリアム価格は目標価格から10%下落し、CDPの担保と債務の比率が135%にまで落ちています。清算レートを下回っているため、トレーダーは清算をトリガーし、債務オークションでMKRを購入するために、Daiの売りを開始できます。同時に、トレーダーは、担保オークションで最大135 Dai相当の担保を購入するために、Daiの売りを開始できます。イーサリアム担保で最低105 Daiの売り注文が出されているため、トレーダーは、途転で最低105 Daiの担保を取得します。残りの担保はCDP所有者に返却されます。

対応可能な市場

導入部で説明したように、暗号通貨と価格安定化は、ほとんどの分散アプリケーションにとって基本的な要件です。このため、Daiの潜在市場は、少なくとも、ブロックチェーン業界全体の市場と同じ規模です。次に、価格安定化を備えた暗号通貨としての立場でDai Stablecoinシステムの一部の直接市場(ブロックチェーンおよび広い業界の両方)の簡潔な網羅的ではない一覧、分散マージントレードプラットフォームとしての使用例を示します。

● **金融市場、ヘッジ、デリバティブ、レバレッジ:** また、CDPIは自由なレバレッジ取引を可能にします。Daiは、オプションやCFDなどのカスタムデリバティブスマートコントラクトにおける安定性と信頼性のある担保としても役立ちます。

● **マーチャント受領、国際取引、国際送金:** Daiを使用すると、外国為替の変動を軽減し、仲介者がいないため、国際取引の取引コストを大幅に削減できます。

- **透明な会計システム:** 慈善事業、NGO、政府は、Daiを使用することで、効率化と腐敗レベルの低減を実現できます。

リスクとリスク緩和

Makerプラットフォームの開発の成功、開発、および運用には多数の潜在的なリスクがあります。Makerコミュニティがあらゆる必要な手順を実施して、このようなリスクを軽減することが重要です。次の一覧は、特定されたリスクの一部と、それに対応するリスク軽減のための計画です。

スマートコントラクトインフラストラクチャに対する悪意のあるハッキング攻撃

早い段階でのシステムに対する最大のリスクは、展開されたスマートコントラクトのセキュリティの突破口を見つけ、それを悪用して、脆弱性が修正される前にシステムに侵入したり窃盗を行う悪意のあるプログラマーのリスクです。最悪の場合、イーサ(ETH)やオーカーレピュテーション(REP)などのMakerプラットフォームで担保として維持されているすべての分散デジタル資産が盗まれ、回復の可能性がない場合があります。Digix Gold IOUなどの分散されていない担保ポートフォリオの一部は、中央バックドアを通して凍結および支配できる場合でも、盗まれることはありません。

軽減策: スマートコントラクトセキュリティおよびセキュリティのベストプラクティスは、初期段階からDaia開発における絶対的に最高優先課題です。コードベースは、すでに、ブロックチェーン業界の最高のセキュリティ研究者の一部による3つの独立したセキュリティ監査を受けています。

非常に長期的には、コードの正式な検証によって、ハッキングされるリスクが理論的にはほぼ完全に軽減できます。つまり、コードの動作が想定と正確に一致することを数学的に証明します。完全な正式検証は非常に長期的な目標ですが、機能プログラミング言語HaskellにおけるDai Stablecoinシステムの完全参照実装など、それに向けた主要な

作業はすでに完了しています。これは、現在積極的な研究開発が行われているより高度な形式化に向けた足がかりです。

1つまたは複数の担保資産の予測不能な事象

影響度の大きいもう1つのリスクは、Daiで使用される担保に対する潜在的な予測不能の事象です。これは、Dai Stablecoinシステムの初期段階で、MKRがインフレの希薄化を支えられるだけの堅牢性を備える前や、Dai Stablecoinシステムが担保の多様なポートフォリオをサポートした後に発生する可能性があります。

軽減策: CDP担保は初期段階ではETHに制限され、当初は債務上限が制限され、経時的に徐々に引き上げられます。

競争と使いやすさの重要性

前述のとおり、価格安定化を備えた暗号通貨には、多大な資金と頭脳が投入されています。「真の分散化」を実現するため、Dai Stablecoinシステムはブロックチェーン業界が目指している最も複雑なモデルです。リスクとしては、暗号通貨ユーザー間の移動が認知されています。つまり、分散化の概念が中央集権型のデジタル資産の簡素化とマーケティングにすり替えられることです。

軽減策: 私たちは、標準の暗号通貨ユーザーにとって、Daiが非常に使いやすい通貨であることを想定しています。Daiは、ERC-20に準拠した標準イーサリアムトークンで、エコシステム全体ですぐに使用できる高い流動性を備えています。Daiは、一般的なユーザーが使用するために、システム基盤の機構を理解する必要がないように設計されています。

Dai Stablecoinシステムの複雑さは、主に、マージン取引でDai Stablecoinシステムを使用するキーパーと資本投資会社によって理解される必要があります。このような種類のユーザーは、システムの機構のすべての要素に関する豊富かつ明確なドキュメントが存在する限り、導入するための十分なリソースを有しています。Makerコミュニティはこれが該

当することを保証します。

価格エラー、非合理性、想定外の事象

オラクルからの価格フィードの問題や、Dai価格の長期の変動を引き起こす非合理的な市場ダイナミクスなど、想定外の事象が多数発生する可能性があります。システムの信頼が失われた場合、まだ市場に十分な流動性と安定性がもたらされていないうちに、TRFM調整 またはMKR希薄化が究極レベルに達する可能性があります。

軽減策: Makerコミュニティは、合理性と市場効率を最大化し、大きな市場ショックを引き起こさずに、Dai供給を一定のペースで成長させるために、市場のキーパーとして機能する十分に大きい資本プールにインセンティブを与える必要があります。

中央集権型インフラストラクチャの失敗

Makerチームは、初期段階で、Makerプラットフォームの開発とガバナンスにおける重要な役割を担います。これには、費用の予算管理、新しい開発者の採用、パートナーシップおよび機関ユーザーを探すこと、規制当局や他の主要な外部関係者との連携などがあります。法的な理由や経営者との内部的な問題などにより、Makerチームがこうした役割のいくつかを遂行できなかった場合、適切なバックアップ計画がないと、Makerの将来がリスクにさらされる可能性があります。

軽減策: Makerコミュニティはある意味で、Makerチームの分散された取引相手として機能するために存在しています。このコミュニティは、MKRトークンを保有することで一致する個々のアクターたちの緩い集団であり、Makerプラットフォームの成功のために強力なインセンティブを与えています。MKRの初期段階では、最も重要なコア開発者が確実に大きいMKR報酬を受け取れるように細心の注意が払われました。MakerチームがMakerプラットフォームの開発を効果的に主導できない場合には、投資を保護するために、個別のMKR所有者が開発者に資金を提供する(あるいは自身で開発を行う)ためにインセンティブを与えられます。

結論

Dai Stablecoinシステムは、イーサリアムエコシステムおよびより広範囲なブロックチェーン経済における価値の安定した取引に関連する重要な問題を解決するために設計されました。私たちは、Daiの発行、取引、回収を行うメカニズムと、MKR所有者の直接的なリスク管理により、私利的なキーパーが経時的に効率的な方法でDaiの価格安定化を維持できると考えています。Makerコミュニティの創始者は、短期的にはアジャイル開発のニーズに適し、経時的には分散化の概念にも適合する賢明なガバナンスロードマップを策定しました。この開発ロードマップは、積極的で、信頼できる方法でDaiを広く普及することに焦点を当てています。

用語集

- **担保付債務ポジション(CDP):** ユーザーが資産(Dai)を受け取るスマートコントラクト。金利によって債務を効果的に運用します。CDPユーザーは、債務状況を保証するために、融資の金額を超過した担保を支払います。
- **Dai:** Dai Stablecoinシステムで資産として取引される、価格安定化を備えた暗号通貨。ERC20標準に準拠した標準イーサリアムトークンです。
- **債務オークション:** CDPの担保が不足したときに、緊急の債務を埋め合わせるために、DaiのためにMKRを売却するリバースオークション。
- **担保オークション:** 清算中のCDPから担保を売却するオークション。CDPが所有する債務埋め合わせの優先順位を決定し、超過した担保の返金の際にCDP所有者に可能な限り最高価格を提供するために設計されています。
- **Dai Foundation:** Makerプラットフォームの開発と立ち上げの成功に注力したスマートコントラクト開発者の分散チーム。

- **キーパー:** Dai、CDP、MKRを取引する独立した経済アクター。Daiの発行、CDPの決済を行い、Dai Stablecoinシステムで裁定取引を求めます。結果として、キーパーは、Dai市場の合理性と価格安定化を維持することを支援します。
- **MKR:** 投票の際にMKR有権者によって使用されるERC20トークン。また、CDPが支払い不能になった場合に、バックストップとしても機能します。
- **MKR有権者:** リスクパラメーターに投票することで、Dai Stablecoinシステムのリスクを積極的に管理するMKR所有者。
- **Maker:** Makerプラットフォームの技術的インフラストラクチャとMKR有権者のコミュニティから構成される、自律分散型組織の名前。
- **オラクル:** Makerプラットフォームのさまざまなコンポーネントに価格フィードを提供するために選択されたイーサリアムアカウント(コントラクトまたはユーザー)。
- **リスクパラメーター:** 特にMakerプラットフォームが自動的にCDPにリスクがあるかと判定するときを決定し、キーパーが清算できるようにする変数。
- **感度パラメーター:** Dai Stablecoinシステムがどの程度積極的にDai市場価格偏差に対して目標価格を自動的に変更するかを決定する変数。
- **目標レートフィードバックメカニズム(TRFM):** Dai Stablecoinシステムが目標レートを調整する自動メカニズムで、市場力を使ってDai市場価格が目標価格付近で安定するようにします。

リンク

- **チャット:** <https://chat.makerdao.com/> — コミュニティ対話のための主要なプラットフォーム
- **フォーラム:** <https://forum.makerdao.com/> — 議論と提案
- **Subreddit:** <https://reddit.com/r/makerdao/> — 最新のニュースとリンク
- **GitHub:** <https://github.com/makerdao/> — 公開Makerコードのリポジトリ

- **TeamSpeak:** <https://ts.makerdao.com/> — ガバナンス会議のカンファレンスコール
- **SoundCloud:** <https://soundcloud.com/makerdao/> — ガバナンス会議の録音音
- **Oasis:** <https://oasisdex.com/> — MKRおよびDaiの分散取引
- **Sai:** <https://sai.makerdao.com/> — 実験用Stablecoin