Il sistema dello stablecoin Dai

Whitepaper

https://makerdao.com/

Del team Maker

Dicembre 2017

Panoramica del sistema dello stablecoin Dai 3

Smart contract per posizioni debitorie collateralizzate 3

Il processo di interazione della CDP 5

Dai monocollateral e multicollateral 5

Pooled Ether (meccanismo temporaneo per il Dai monocollateral) 6

Meccanismi di stabilità del prezzo 6

Prezzo target 6

Meccanismo di feedback del tasso target 6

Parametro di sensibilità 7

Regolamento globale 8

Regolamento globale: i passaggi 8

Gestione del rischio della piattaforma Maker 9

Parametri di rischio 10

Governance del token MKR 11

MKR e Dai multicollateral 12

Liquidazioni automatiche di CDP rischiose 12

Contratto per la fornitura di liquidità (meccanismo temporaneo per il Dai monocollateral) 13

Aste del debito e di collateral (Dai multicollateral) 13

Operatori esterni chiave 14

Keeper 14

Oracoli 14

Regolatori globali 16

Esempi 16

Mercato disponibile 19

Rischi e relativa mitigazione 19

Attacco dannoso di pirateria informatica contro l'infrastruttura degli smart contract 21

Evento del cigno nero in uno o più asset collateral 21

Concorrenza e importanza della facilità d'uso 22

Errori di prezzo, irrazionalità ed eventi imprevisti 22

Insuccesso dell'infrastruttura centralizzata 23

Conclusione 23

Glossario 24

Link 25

Panoramica del sistema dello stablecoin Dai

Gli asset digitali più diffusi come Bitcoin (BTC) ed Ether (ETH) sono troppo volatili per essere utilizzati come valuta quotidiana. Il valore di un bitcoin è spesso soggetto a notevoli fluttuazioni, aumentando o diminuendo fino al 25% in un solo giorno e occasionalmente aumentando di oltre il 300% in un mese.[1].

Lo stablecoin Dai è una criptovaluta garantita da collateral, il cui valore è stabile rispetto al dollaro statunitense. Riteniamo che gli asset digitali stabili come lo stablecoin Dai siano fondamentali per comprendere l'intero potenziale della tecnologia blockchain.

Maker è una piattaforma per smart contract su Ethereum, che garantisce e stabilizza il valore del Dai attraverso un sistema dinamico di CDP (Collateralized Debt Positions: posizioni debitorie collateralizzate), meccanismi di feedback autonomi e operatori esterni debitamente incentivati.

Maker consente a tutti di sfruttare i propri asset Ethereum per generare Dai sulla sua piattaforma. Una volta generato, il Dai può essere utilizzato nello stesso modo di qualsiasi altra criptovaluta, ovvero può essere liberamente inviato ad altri, utilizzato come strumento di pagamento per beni e servizi o conservato a titolo di risparmio a lungo termine. È importante sottolineare che la generazione di Dai crea anche i componenti necessari per un'affidabile piattaforma decentralizzata di negoziazioni a margine.

Smart contract per posizioni debitorie collateralizzate

Chiunque possieda asset collateral può sfruttarli per generare Dai sulla piattaforma Maker attraverso gli esclusivi smart contract noti come posizioni debitorie collateralizzate (CDP). [2]

Le CDP contengono gli asset collateral depositati da un utente e permettono a quest'ultimo di generare Dai. Tuttavia, tale operazione provoca anche la maturazione di un debito. Questo debito blocca efficacemente gli asset collateral depositati nella CDP fino a quando non viene coperto mediante il pagamento di un importo equivalente di Dai. A questo punto, il proprietario può prelevare di nuovo i propri asset collateral. Le CDP attive sono sempre collateralizzate per eccesso, ovvero il valore del collateral è più elevato di quello del debito.

---

[1] David Ernst Hard Problems in Cryptocurrency

[2] https://github.com/makerdao

Il processo di interazione della CDP

- **Passaggio 1. Creazione della CDP e deposito del collateral**
  L'utente della CDP invia in primo luogo una transazione a Maker per creare la CDP, quindi invia un'altra transazione per finanziarla con l'importo e il tipo di collateral che verrà utilizzato per generare Dai. A questo punto, la CDP è considerata collateralizzata.

- **Passaggio 2. Generazione di Dai dalla CDP collateralizzata**
  L'utente della CDP invia quindi una transazione per recuperare l'importo di Dai desiderato dalla CDP; in cambio, la CDP matura un importo equivalente di debito, bloccando l'accesso al collateral finché il debito insoluto non viene pagato.

- **Passaggio 3. Pagamento del debito e della commissione di stabilità**
  Se l'utente vuole recuperare il collateral, deve pagare il debito nella CDP, maggiorato della commissione di stabilità che matura costantemente sul debito nel corso del tempo. La commissione di stabilità può essere pagata solo in MKR. Quando l'utente paga il debito e la commissione di stabilità inviando i Dai e gli MKR necessari alla CDP, questa risulta priva di debito.

- **Passaggio 4. Prelievo del collateral e chiusura della CDP**
  Dopo aver pagato il debito e la commissione di stabilità, l'utente della CDP può liberamente ripristinare nel suo portafoglio i collateral in parte o per intero inviando una transazione a Maker.

Dai monocollateral e multicollateral

Al momento del lancio, il Dai supporterà un solo tipo di collateral, il Pooled Ether. Nei successivi 6-12 mesi, è prevista la conversione del Dai monocollateral in Dai multicollateral. La differenza principale è che verranno supportati tutti i tipi di CDP.[3]

---

[3] I meccanismi temporaneamente in essere nel sistema durante la fase monocollateral sono indicati in questo whitepaper

Pooled Ether (meccanismo temporaneo per il Dai monocollateral)

Inizialmente, Pooled Ether (PETH) sarà l'unico tipo di collateral accettato da Maker. Gli utenti che desiderano aprire una CDP e generare Dai durante la prima fase della piattaforma Maker devono prima ottenere un PETH. Questa operazione avviene all'istante e con grande facilità nella blockchain depositando ETH in uno speciale smart contract che riunisce gli ETH di tutti gli utenti e restituisce loro i PETH corrispondenti.

In caso di un improvviso crollo del mercato di ETH, in seguito al quale una CDP risulta contenere un debito più elevato del valore dei suoi collateral, la piattaforma Maker diluisce automaticamente il PETH per ricapitalizzare il sistema. Ciò significa che la rivendicazione proporzionale di ogni PETH diminuisce.

Dopo l'aggiornamento della piattaforma Maker per supportare più tipi di collateral, il PETH sarà rimosso e sostituito dall'ETH insieme agli altri nuovi tipi di collateral.

Meccanismi di stabilità del prezzo

Prezzo target

Il prezzo target del Dai ha due funzioni principali nella piattaforma Maker: è utilizzato per 1) calcolare il rapporto collateral-debito di una CDP e 2) per determinare il valore degli asset collateral che i detentori di Dai ricevono in caso di regolamento globale.

Inizialmente, il prezzo target è denominato in USD e inizia a 1, che si traduce in un tasso di cambio in USD pari a 1:1.

Meccanismo di feedback del tasso target

In caso di grave instabilità del mercato, è possibile attivare il TRFM (Target Rate Feedback Mechanism: meccanismo di feedback del tasso target). Con l'attivazione del TRFM, l'ancoraggio del Dai viene interrotto, ma viene mantenuta la stessa denominazione.

Il TRFM è il meccanismo automatico mediante il quale il sistema dello stablecoin Dai regola il tasso target per fare in modo che le forze del mercato mantengano stabile il prezzo di mercato del Dai su un valore pressoché equivalente al prezzo target. Il tasso target determina la variazione del prezzo target nel tempo, quindi può agire da incentivo a possedere Dai (se è positivo) o a prendere a prestito Dai (se è negativo). Se il TRFM non è attivato, il tasso target è fissato allo 0%; di conseguenza, il prezzo target non cambia nel tempo e il Dai è ancorato.

Se il TRFM è attivato, sia il tasso target che il prezzo target cambiano dinamicamente per bilanciare la domanda e l'offerta di Dai, modificando automaticamente gli incentivi agli utenti per la generazione e il possesso di Dai. Il meccanismo di feedback spinge il prezzo di mercato del Dai verso il prezzo target variabile, attenuandone la volatilità e fornendo liquidità in tempo reale durante gli shock di domanda.

Con il TRFM attivato, se il prezzo di mercato del Dai è inferiore al prezzo target, il tasso target aumenta. Questo provoca l'aumento del prezzo target a un tasso superiore e, di conseguenza, fa sì che la generazione di Dai con CDP risulti più costosa. Allo stesso tempo, il tasso target aumentato provoca l'incremento dei capital gain derivanti dalla detenzione di Dai e un corrispondente aumento della domanda di Dai. Questa combinazione tra minore offerta e maggiore domanda provoca l'aumento del prezzo di mercato del Dai, facendolo nuovamente risalire al livello del prezzo target.

Lo stesso meccanismo ha un effetto contrario se il prezzo di mercato del Dai è più alto del prezzo target: il tasso target diminuisce, provocando un aumento della domanda per la generazione di Dai e una riduzione della stessa per la detenzione. Ne consegue una riduzione del prezzo di mercato del Dai, che viene fatto nuovamente scendere al livello del prezzo target.

Questo meccanismo è un ciclo di feedback negativo: lo scarto rispetto al prezzo target in una direzione aumenta la forza nella direzione opposta.

Parametro di sensibilità

Il parametro di sensibilità del TRFM determina l'entità della variazione del tasso target in risposta allo scarto tra prezzo target e prezzo di mercato del Dai. Il tasso di feedback viene quindi sintonizzato con la scala del sistema. I votanti MKR possono impostare il parametro di sensibilità. Tuttavia, se il TRFM è attivato, il prezzo e il tasso target sono determinati dalle dinamiche del mercato e non sono direttamente controllati dai votanti MKR.

Il parametro di sensibilità è utilizzato anche per attivare o disattivare il TRFM. Se il

parametro di sensibilità e il tasso target sono entrambi pari a zero, il Dai è ancorato al prezzo target corrente.

Regolamento globale

Il regolamento globale è un processo che può essere utilizzato come ultima risorsa per garantire crittograficamente il prezzo target ai detentori di Dai. Chiude e "scioglie" di comune accordo la piattaforma Maker garantendo che tutti gli utenti, sia i detentori di Dai sia gli utenti di CDP, ricevano il valore netto degli asset a cui hanno diritto. Il processo è completamente decentralizzato e i votanti MKR ne regolano l'accesso per garantire che venga utilizzato solo in caso di gravi emergenze, ad esempio irrazionalità del mercato a lungo termine, pirateria informatica o violazioni della sicurezza e upgrade di sistema.

Regolamento globale: i passaggi

- **Passaggio 1. Il regolamento globale viene attivato**
  Se un numero sufficiente di operatori designati dalla governance di Maker come regolatori globali ritiene che il sistema sia soggetto a un grave attacco o se un regolamento globale viene pianificato come parte di un upgrade tecnico, è possibile attivare la funzione Regolamento globale. In tal modo, la creazione e la manipolazione di CDP si arrestano e il price feed viene congelato a un valore fisso, che viene successivamente utilizzato per elaborare le rivendicazioni proporzionali per tutti gli utenti.

- **Passaggio 2. Le rivendicazioni in caso di regolamento globale vengono elaborate**
  Dopo l'attivazione del regolamento globale, è necessario lasciar trascorrere un periodo di tempo per consentire ai keeper di elaborare le rivendicazioni proporzionali di tutti i detentori di Dai e CDP in base al valore di feed fissato. Dopo l'elaborazione, tutti i detentori di Dai e CDP potranno rivendicare un importo fisso di ETH con i propri Dai e CDP.

- **Passaggio 3. I detentori di Dai e CDP rivendicano il collateral insieme ai Dai e alle CDP**

  Ogni detentore di Dai e CDP può richiamare una funzione di rivendicazione sulla piattaforma Maker per scambiare i propri Dai e CDP direttamente per un importo fisso di ETH corrispondente al valore calcolato dei propri asset in base al prezzo target del Dai.

g. Nel caso in cui il prezzo target del Dai sia di 1 dollaro USA e il prezzo ETH/dollaro USA sia di 200, se un utente detiene 1000 Dai quando il regolamento globale viene attivato, dopo il periodo di elaborazione potrà richiedere esattamente 5 ETH alla piattaforma Maker. Non esiste un limite di tempo per effettuare la rivendicazione finale.

Gestione del rischio della piattaforma Maker

Il token MKR consente ai detentori di votare per eseguire le seguenti azioni di gestione del rischio:

- **Aggiunta di un nuovo tipo di CDP:** creazione di un nuovo tipo di CDP con un insieme univoco di parametri di rischio. Un tipo di CDP può essere un nuovo tipo di collateral o un nuovo insieme di parametri di rischio per un tipo di collateral esistente.

- **Modifica dei tipi di CDP esistenti:** modifica dei parametri di rischio di uno o più tipi di CDP esistenti che sono stati già aggiunti.

- **Modifica del parametro di sensibilità:** modifica della sensibilità del meccanismo di feedback del tasso target.

- **Modifica del tasso target:** l'amministrazione può modificare il tasso target. In pratica, la modifica del tasso target avviene solo in una specifica circostanza, ovvero quando i votanti MKR vogliono ancorare il prezzo del Dai al suo attuale prezzo target. Questa operazione avviene sempre insieme alla modifica del parametro di sensibilità. Impostando su 0% sia il parametro di sensibilità sia il tasso target, il TRFM viene disabilitato e il prezzo target del Dai viene ancorato al suo valore corrente.

- **Scelta dell'insieme di oracoli attendibili:** la piattaforma Maker ricava i prezzi interni per i collaterali e il prezzo di mercato del Dai da un'infrastruttura di oracoli decentralizzata, composta da un vasto insieme di singoli nodi di oracoli. I votanti MKR controllano il numero di nodi presenti nell'insieme di oracoli attendibili e l'identità dei nodi. Fino a metà degli oracoli possono essere compromessi o malfunzionanti senza causare un'interruzione del funzionamento continuo e sicuro del sistema.

- **Modifica della sensibilità del price feed:** modifica delle regole che determinano la maggiore variazione che i price feed possono provocare sui valori dei prezzi interni nel sistema.

- **Scelta dell'insieme di regolatori globali:** il regolamento globale è un meccanismo fondamentale che consente alla piattaforma Maker di difendersi dagli attacchi contro gli oracoli o il processo di governance. Il processo di governance sceglie un insieme di regolatori globali e ne determina il numero necessario per attivare il regolamento globale.

Parametri di rischio

Le CDP hanno più parametri di rischio che determinano il modo in cui possono essere utilizzate. Ogni tipo di CDP ha il proprio insieme univoco di parametri di rischio e questi sono determinati in base al profilo di rischio del collateral utilizzato dal tipo di CDP. Questi parametri sono direttamente controllati dai detentori di MKR attraverso il voto (ogni MKR conferisce al suo detentore un diritto di voto).

I parametri di rischio fondamentali per le CDP sono:

- **Tetto di debito:** è l'importo massimo di debito che può essere creato da un singolo tipo di CDP. Una volta che una CDP di un determinato tipo ha creato un debito sufficiente, risulta impossibile crearne altro, a meno che non vengano chiuse CDP esistenti. Il tetto di debito è utilizzato per garantire una sufficiente diversificazione del portafoglio di collateral.

- **Rapporto di liquidazione:** si tratta del rapporto collateral-debito al quale una CDP diventa vulnerabile alla liquidazione. Un rapporto di liquidazione basso indica che i votanti MKR prevedono una ridotta volatilità del prezzo del collateral, mentre un rapporto di liquidazione alto fa prevedere un'elevata volatilità.

- **Commissione di stabilità:** è un onere pagato da ogni CDP. È una percentuale annua di rendimento calcolata sul debito esistente della CDP e deve essere pagata dall'utente della CDP. La commissione di stabilità è denominata in Dai, ma può essere pagata solo utilizzando il token MKR. L'importo di MKR che deve essere pagato è calcolato in base a un price feed del prezzo di mercato dell'MKR. Quando viene pagato, l'importo di MKR viene bruciato e quindi rimosso definitivamente dall'offerta.

- **Rapporto di penale:** è utilizzato per determinare l'importo massimo di Dai ricavato da un'asta di liquidazione utilizzata per acquistare e rimuovere tutti gli MKR dall'offerta e il cui risultato è la restituzione dei collateral in eccesso all'utente della CDP che la possedeva prima della sua liquidazione. Il rapporto di penale è utilizzato per coprire l'inefficienza del meccanismo di liquidazione. Durante la fase del Dai monocollateral, la penale di liquidazione viene utilizzata per acquistare e bruciare PETH, producendo un effetto positivo sul rapporto PETH-ETH.

Governance del token MKR

Oltre al pagamento della commissione di stabilità sulle CDP attive, il token MKR gioca un ruolo importante nella governance della piattaforma Maker.

La governance avviene a livello di sistema attraverso l'elezione di una proposta attiva da parte dei votanti MKR. La proposta attiva è lo smart contract autorizzato dal voto MKR per ottenere accesso root per la modifica delle variabili di governance interne della piattaforma Maker.
Le proposte possono essere di due tipi: Single Action Proposal Contract [SAPC] e Delegating Proposal Contract [DPC].

I Single Action Proposal Contract sono proposte che possono essere eseguite solo una volta dopo l'ottenimento dell'accesso root e, dopo l'esecuzione, le sue modifiche vengono applicate immediatamente alle variabili di governance interne della piattaforma Maker. Dopo l'esecuzione una tantum, il SAPC si autoelimina e non può essere riutilizzato. Questo tipo di proposta viene utilizzato durante le prime fasi del sistema, in quanto è relativamente semplice, ma meno flessibile.

I Delegating Proposal Contract sono proposte che utilizzano continuamente l'accesso root attraverso la logica di governance di secondo livello codificata all'interno della DPC. La logica di governance di secondo livello può essere relativamente semplice, ad esempio definire un protocollo per procedere a una votazione settimanale sui parametri di rischio aggiornati. Inoltre, può implementare una logica più avanzata, come restrizioni sull'entità

delle azioni di governance in periodi di tempo definiti, o persino delegare ulteriormente alcune o tutte le autorizzazioni a una o più DPC di terzo livello con o senza restrizioni.

Ogni account Ethereum può distribuire smart contract di proposta validi. I votanti MKR possono quindi utilizzare i token MKR per esprimere voti di approvazione per una o più proposte che vogliono scegliere come attive. Lo smart contract con il più alto numero totale di voti di approvazione da parte dei votanti MKR viene scelto come proposta attiva.

MKR e Dai multicollateral

Dopo l'upgrade al Dai multicollateral, MKR avrà un ruolo più significativo nel sistema dello stablecoin Dai sostituendo il PETH come risorsa di ricapitalizzazione. Quando le CDP risultano sottocollateralizzate a causa di tracolli del mercato, l'offerta di MKR viene automaticamente diluita e venduta per raccogliere fondi sufficienti alla ricapitalizzazione del sistema.

Liquidazioni automatiche di CDP rischiose

Per garantire la presenza costante di collateral sufficienti nel sistema a copertura del valore complessivo del debito insoluto (conformemente al prezzo target), una CDP può essere liquidata se è ritenuta rischiosa. La piattaforma Maker determina quando liquidare una CDP confrontando il rapporto di liquidazione con il suo rapporto collateral-debito corrente.

Ogni tipo di CDP ha il proprio rapporto di liquidazione univoco che è controllato dai votanti MKR e stabilito in base al profilo di rischio del particolare asset collateral del tipo di CDP.

La liquidazione avviene quando una CDP raggiunge il proprio rapporto di liquidazione. La piattaforma Maker acquista automaticamente il collateral della CDP e successivamente lo rivende. Per il Dai monocollateral esiste un meccanismo temporaneo noto come Contratto per la fornitura di liquidità. Per il Dai multicollateral verrà utilizzato un meccanismo di asta.

Contratto per la fornitura di liquidità (meccanismo temporaneo per il Dai monocollateral)

Durante la fase del Dai monocollateral, il meccanismo per la liquidazione è un Contratto per la fornitura di liquidità, ovvero uno smart contract che negozia direttamente con gli utenti e i keeper Ethereum in base al price feed del sistema.

Quando viene liquidata, una CDP viene immediatamente acquisita dal sistema. Il proprietario della CDP riceve il valore del collateral residuo meno il debito, la commissione di stabilità e la penale di liquidazione.

Il collateral PETH viene messo in vendita nel Contratto per la fornitura di liquidità e i keeper possono automaticamente acquistare il PETH pagando in Dai. Tutti i Dai pagati in questo modo vengono immediatamente eliminati dall'offerta di Dai finché non viene rimosso un importo pari al debito CDP. Se vengono pagati Dai in eccesso rispetto all'ammanco di debito, tali Dai eccedenti vengono utilizzati per acquistare PETH dal mercato e bruciarli, modificando positivamente il rapporto ETH-PETH. Questo provoca un aumento del valore netto per i detentori di PETH.

Se con la vendita di PETH non si raccoglie inizialmente un quantitativo sufficiente di Dai per coprire l'intero ammanco di debito, altri PETH vengono continuamente creati e venduti. I nuovi PETH creati in questo modo modificano negativamente il rapporto ETH-PETH, con la conseguente perdita di valore per i detentori di PETH.

Aste del debito e di collateral (Dai multicollateral)

Durante la liquidazione, la piattaforma Maker acquista il collateral di una CDP e successivamente lo rivende in un'asta automatica. Questo meccanismo di asta consente al sistema di pagare le CDP anche quando le informazioni di prezzo non sono disponibili.

Per acquisire il collateral della CDP in modo da poterlo vendere, il sistema deve prima raccogliere Dai a sufficienza per coprire il debito della CDP. Questo sistema è noto come asta del debito e consiste nella diluizione dell'offerta del token MKR e nella sua vendita agli offerenti in formato di asta.

Parallelamente, il collateral della CDP viene venduto in un'asta di collateral, in cui tutti i ricavi (anch'essi denominati in Dai) fino al raggiungimento dell'importo del debito della CDP maggiorato di una penale di liquidazione (un parametro di rischio determinato mediante il voto MKR) vengono utilizzati per acquistare MKR e rimuoverli dall'offerta. Questo meccanismo neutralizza direttamente la diluizione di MKR verificatasi durante l'asta del debito. Se vengono offerti Dai a sufficienza per coprire completamente il debito della CDP maggiorato della penale di liquidazione, l'asta di collateral si trasforma in un meccanismo di asta inversa e tenta di vendere meno collateral possibili (tutti i collateral residui vengono restituiti al proprietario originale della CDP).

Operatori esterni chiave

Oltre che sull'infrastruttura di smart contract, la piattaforma Maker si basa su alcuni operatori esterni per la gestione delle operazioni. I keeper sono operatori esterni che usufruiscono degli incentivi economici presentati dalla piattaforma Maker. Gli oracoli e i regolatori globali sono operatori esterni con autorizzazioni speciali nel sistema assegnate loro dai votanti MKR.

Keeper

Un keeper è un operatore indipendente (solitamente automatico), incentivato da opportunità di profitto a contribuire a sistemi decentralizzati. Nel contesto del sistema dello stablecoin Dai, i keeper partecipano alle aste del debito e alle aste di collateral quando le CDP vengono liquidate.

I keeper inoltre scambiano Dai all'incirca al prezzo target. I keeper vendono Dai quando il prezzo di mercato è più alto del prezzo target e li acquistano quando il prezzo di mercato è più basso del prezzo target, per usufruire della convergenza a lungo termine prevista verso il prezzo target.

Oracoli

La piattaforma Maker richiede informazioni in tempo reale sul prezzo di mercato degli asset utilizzati come collateral nelle CDP per sapere quando attivare le liquidazioni. Inoltre, necessita di informazioni sul prezzo di mercato del Dai e sul relativo scarto rispetto al prezzo target per rettificare il tasso target quando il TRFM è attivato. I votanti MKR scelgono un insieme di oracoli attendibili per fornire queste informazioni alla piattaforma Maker attraverso transazioni Ethereum.

Per proteggere il sistema da aggressori che acquisiscono il controllo della maggior parte degli oracoli e da altre forme di collusione, esiste una variabile globale che determina la variazione massima del valore del price feed ammessa dal sistema. Tale variabile è nota come parametro di sensibilità del price feed.

Ecco un esempio del suo funzionamento: se il parametro di sensibilità del price feed è definito come "5% in 15 minuti", i price feed non possono cambiare di più del 5% in un periodo di 15 minuti e una variazione pari a ~15% richiederebbe 45 minuti. Questa restrizione garantisce un tempo sufficiente per l'attivazione di un regolamento globale nel caso in cui un aggressore acquisisca il controllo sulla maggioranza degli oracoli.

Regolatori globali

I regolatori globali sono operatori esterni simili agli oracoli del price feed e sono l'ultima linea di difesa per il sistema dello stablecoin Dai in caso di attacco. L'insieme di regolatori globali, selezionato dai votanti MKR, ha l'autorità di attivare il regolamento globale. Indipendentemente da ciò, tali operatori non possiedono alcun accesso o controllo speciale aggiuntivo all'interno del sistema.

Esempi

Il sistema dello stablecoin Dai può essere utilizzato da chiunque senza restrizioni o procedura di registrazione.

- **Esempio 1.** Carlo ha bisogno di un prestito, quindi decide di generare 100 Dai. Blocca un importo di ETH di valore molto superiore rispetto a 100 Dai in una CDP e lo utilizza per generare 100 Dai. I 100 Dai vengono subito inviati direttamente al suo account Ethereum. Supponendo che la commissione di stabilità sia dell'1% all'anno, Carlo avrà bisogno di 101 Dai per coprire la CDP se decide di recuperare i suoi ETH un anno dopo.

Uno dei principali casi di utilizzo delle CDP è la negoziazione a margine da parte di utenti delle CDP.

- **Esempio 2.** Carlo vuole effettuare operazioni di trading a margine con posizione lunga sulla coppia di valute ETH/Dai, quindi genera Dai per un valore pari a 100 USD registrando ETH in una CDP per un valore pari a 150 USD. Successivamente, acquista altri ETH per un valore pari a 100 USD con i Dai appena generati, ottenendo un'esposizione ETH/USD netta di 1,66 volte. Può disporre come desidera dei 100 USD di ETH ottenuti vendendo i Dai. Il collateral ETH originale (di valore pari a 150 USD) rimane bloccato nella CDP finché il debito maggiorato della commissione di stabilità non viene coperto.

Sebbene le CDP non siano reciprocamente fungibili, la loro proprietà è trasferibile. Questo consente alle CDP di essere utilizzate negli smart contract che adottano metodi più complessi di generazione di Dai (ad esempio quelli che coinvolgono più di un operatore).

- **Esempio 3.** Alice e Carlo collaborano utilizzando un contratto OTC Ethereum per emettere Dai per un valore pari a 100 USD garantiti da ETH. Alice e Carlo contribuiscono con un importo di ETH rispettivamente pari a 50 USD e 100 USD. Il contratto OTC acquisisce i fondi e crea una CDP, generando Dai per un valore pari a 100 USD. I Dai appena generati vengono automaticamente inviati a Carlo. Carlo, dal suo punto di vista, acquista Dai per un valore pari a 100 USD pagando il valore equivalente in ETH. Il contratto trasferisce quindi la proprietà della CDP ad Alice. Alice si ritrova con un debito di importo pari a 100 USD (denominato in Dai) e un collateral di importo pari a 150 USD (denominato in ETH). Poiché ha iniziato con soli 50 USD di ETH, ora ha una posizione a leva lunga tripla per la coppia di valute ETH/USD.

Le liquidazioni garantiscono che, in caso di crollo del prezzo del collateral a garanzia di un tipo di CDP, il sistema riesca automaticamente a chiudere le CDP diventate troppo rischiose. Questo meccanismo garantisce che l'offerta in sospeso di Dai rimanga completamente collateralizzata.

- **Esempio 4.** Supponiamo di avere un tipo di CDP Ether con un rapporto di liquidazione del 145%, un rapporto di penale del 105% e una CDP Ether con un rapporto collateral-debito del 150%. Il prezzo Ether crolla verso il prezzo target per una percentuale pari al 10%, provocando un calo a ~135% del rapporto collateral-debito della CDP. Poiché tale rapporto scende al di sotto del rapporto di liquidazione, i trader possono attivarne la liquidazione e iniziare a fare offerte in Dai per acquistare MKR nell'asta del debito. Contemporaneamente, i trader possono iniziare a fare offerte in Dai per acquistare i ~135 Dai in collateral nella relativa asta. Quando sono stati offerti almeno 105 Dai per il collateral Ether, i trader invertono l'offerta per ottenere il minore importo di collateral per 105 Dai. Qualsiasi collateral rimanente viene restituito al proprietario della CDP.

Mercato disponibile

Come accennato nell'introduzione, una criptovaluta con stabilità di prezzo è un requisito fondamentale per la maggior parte delle applicazioni decentralizzate. Pertanto, il mercato potenziale per i Dai è vasto almeno quanto quello dell'intero settore delle blockchain. Riportiamo di seguito un breve elenco non esaustivo di alcuni dei mercati immediati (sia nel settore delle blockchain che nel settore in senso lato) per il sistema dello stablecoin Dai in qualità di criptovaluta con stabilità di prezzo e utilizzo come piattaforma decentralizzata di trading a margine.

- **Mercati predittivi e applicazioni di gioco d'azzardo:** quando si effettua una previsione indipendente, è normale non voler aumentare il rischio piazzando la scommessa con una criptovaluta volatile. Le scommesse a lungo termine diventano particolarmente irrealizzabili se l'utente deve anche scommettere sul prezzo futuro dell'asset volatile utilizzato per piazzare la scommessa. Una criptovaluta con stabilità di prezzo come il Dai, invece, sarà la scelta più ovvia per gli utenti dei mercati predittivi e del gioco d'azzardo.

- **Mercati finanziari, hedging, derivati, leva finanziaria:** le CDP consentono lo svolgimento del trading permissionless con leva finanziaria. I Dai sono utili anche come collateral stabile e affidabile negli smart contract derivati personalizzati, come opzioni o CFD.

- **Ricevute commerciante, transazioni transfrontaliere e rimesse:** la mitigazione della volatilità dei cambi esteri e la mancanza di intermediari indicano che i costi delle transazioni del commercio internazionale possono essere notevolmente ridotti utilizzando il Dai.

- **Sistemi contabili trasparenti:** organizzazioni di beneficienza, ONG e amministrazioni pubbliche registreranno un aumento dell'efficienza e minori livelli di corruzione utilizzando il Dai.

Rischi e relativa mitigazione

Lo sviluppo, l'implementazione e il funzionamento della piattaforma Maker presentano molti rischi potenziali. È fondamentale che la community di Maker adotti tutti le misure necessarie per attenuare tali rischi. Di seguito è riportato un elenco di alcuni dei rischi identificati e del relativo piano di mitigazione.

Attacco dannoso di pirateria informatica contro l'infrastruttura degli smart contract

Il maggiore rischio per il sistema nelle sue fasi iniziali è rappresentato da un programmatore malintenzionato che individua un exploit negli smart contract implementati e lo utilizza per danneggiare il sistema o rubare da esso prima che la vulnerabilità possa essere corretta. Nel peggiore dei casi, tutti gli asset digitali decentralizzati detenuti come collateral nella piattaforma Maker, come Ether (ETH) o Augur Reputation (REP), potrebbero essere rubati senza possibilità di ripristino. *La parte non decentralizzata del portafoglio di collateral, come gli IOU Digix Gold, non verrebbe rubata in casi di questo tipo, in quanto può essere congelata e controllata attraverso una backdoor centralizzata.*

Mitigazione: le pratiche di sicurezza e migliore sicurezza relative agli smart contract sono state la massima priorità nello sviluppo del Dai fin dagli inizi. La codebase è già stata sottoposta a tre ispezioni di sicurezza indipendenti da parte di alcuni dei migliori enti di ricerca sulla sicurezza nel settore delle blockchain.

Nel lunghissimo periodo, il rischio di attacchi di pirateria informatica può teoricamente essere quasi del tutto attenuato attraverso la verifica formale del codice. Ciò significa dimostrare matematicamente che il codice svolge esattamente la funzione prevista. Sebbene la verifica formale completa sia un obiettivo a lunghissimo termine, sono già stati effettuati considerevoli interventi in tal senso, compresa un'implementazione di riferimento completa del sistema dello stablecoin Dai nel linguaggio di programmazione funzionale Haskell, che funge da trampolino verso formalizzazioni più sofisticate al momento in fase di ricerca attiva e sviluppo.

Evento del cigno nero in uno o più asset collateral

Un altro rischio ad alto impatto è rappresentato da un potenziale evento del cigno nero sul collateral utilizzato per il Dai. Questo può verificarsi nelle prime fasi del sistema dello stablecoin Dai, prima che l'MKR sia abbastanza solido da supportare le diluizioni inflazionistiche, oppure quando il sistema dello stablecoin Dai supporterà un portafoglio diversificato di collateral.

Mitigazione: nelle prime fasi, il collateral CDP sarà limitato all'ETH, con il tetto di debito inizialmente limitato e gradualmente in aumento nel tempo.

Concorrenza e importanza della facilità d'uso

Come precedentemente accennato, per una criptovaluta con stabilità di prezzo entrano in gioco grandi quantitativi di denaro e notevoli capacità intellettive. Poiché è caratterizzato da una "vera decentralizzazione", il sistema dello stablecoin Dai è di gran lunga il modello più complesso contemplato nel settore delle blockchain. Un rischio percepito è una tendenza tra gli utenti delle criptovalute a scambiare gli ideali di decentralizzazione con la semplicità e il marketing degli asset digitali centralizzati.

Mitigazione: si prevede che il Dai sia molto facile da utilizzare per un normale utente di criptovalute. Il Dai sarà un normale token Ethereum conforme allo standard ERC20 e sarà prontamente disponibile con elevata liquidità in tutto l'ecosistema. Il Dai è stato concepito in modo tale che, per essere utilizzato, l'utente medio non sia tenuto a capire i meccanismi sottostanti del sistema.

Le complessità del sistema dello stablecoin Dai dovranno essere comprese in primo luogo dai keeper e dalle società di investimento di capitali che lo utilizzano per il trading a margine. Questi tipi di utenti hanno risorse sufficienti per iniziare a utilizzare il sistema autonomamente, a condizione che esista una ricca e chiara documentazione su ogni aspetto del suo funzionamento. La community di Maker dovrà garantire questo aspetto.

Errori di prezzo, irrazionalità ed eventi imprevisti

Potrebbero verificarsi vari eventi imprevisti, ad esempio problemi con il price feed degli oracoli, o dinamiche irrazionali del mercato che causano una variazione del valore del Dai per un periodo di tempo prolungato. Se il sistema perde fiducia, le rettifiche del TRFM o persino la diluizione dell'MKR potrebbero raggiungere livelli estremi, pur continuando a non apportare liquidità e stabilità sufficienti al mercato.

Mitigazione: la community di Maker dovrà incentivare una riserva di capitale sufficientemente elevata per agire in qualità di keeper del mercato al fine di massimizzare la razionalità e l'efficienza del mercato e consentire all'offerta di Dai di aumentare a un ritmo costante senza grandi shock del mercato.

Insuccesso dell'infrastruttura centralizzata

Il team Maker ricopre un ruolo di primo piano nello sviluppo e nella governance della piattaforma Maker nelle sue prime fasi: definizione del budget di spesa, assunzione di nuovi sviluppatori, ricerca di partnership e utenti istituzionali e relazioni con gli enti di controllo e altri stakeholder esterni importanti. Qualora il team Maker fallisca in alcuni dei suoi incarichi, per motivi legali o a causa di problemi interni di gestione, il futuro di Maker potrebbe essere a rischio senza un adeguato piano di emergenza.

Mitigazione: l'obiettivo della community di Maker è parzialmente quello di fungere da controparte decentralizzata del team Maker. Si tratta di un insieme di operatori indipendenti, tutti accomunati dalla detenzione del token MKR, che fornisce loro un forte incentivo a contribuire al successo della piattaforma Maker. Durante le prime fasi della distribuzione di MKR, è stata prestata grande attenzione affinché gli sviluppatori più importanti ricevessero una partecipazione significativa in MKR. Qualora il team Maker non sia più in grado di guidare lo sviluppo della piattaforma Maker, i singoli detentori di MKR saranno incentivati a sovvenzionare gli sviluppatori (o semplicemente a svolgere loro stessi l'attività di sviluppo) nel tentativo di tutelare il loro investimento.

Conclusione

Il sistema dello stablecoin Dai è stato pensato per risolvere il grave problema dello scambio stabile di valore nell'ecosistema Ethereum e nella più ampia economia delle blockchain. Riteniamo che il meccanismo mediante il quale il Dai viene creato, scambiato e ritirato, unitamente al ruolo diretto di gestione del rischio dei detentori di MKR, consenta ai keeper interessati di mantenere efficacemente la stabilità del prezzo del Dai nel tempo. I fondatori della community di Maker hanno creato una roadmap di governance prudente adeguata alle esigenze di uno sviluppo agile nel breve periodo, ma anche coerente con gli ideali di decentralizzazione nel tempo. La roadmap di sviluppo è aggressiva e focalizzata sull'adozione diffusa del Dai in maniera responsabile.

Glossario

- **CDP (Collateralized Debt Position: posizione debitoria collateralizzata).** uno smart contract i cui utenti ricevono un asset (Dai), che funge efficacemente da strumento di debito con un tasso di interesse. L'utente della CDP ha registrato collateral in eccesso rispetto al valore del prestito per garantire la sua posizione debitoria.

- **Dai:** la criptovaluta con stabilità di prezzo, asset di scambio nel sistema dello stablecoin Dai. È un normale token Ethereum conforme allo standard ERC20.

- **Asta del debito:** l'asta inversa che vende MKR per Dai al fine di coprire il debito di emergenza quando una CDP diventa sottocollateralizzata.

- **Asta del collateral:** l'asta che vende il collateral da una CDP sottoposta a liquidazione. È pensata per privilegiare la copertura del debito di proprietà della CDP e, in secondo luogo, per offrire al proprietario della CDP il prezzo migliore possibile per il rimborso del collateral in eccesso.

- **La fondazione Dai:** un team decentralizzato di sviluppatori di smart contract dedicati allo sviluppo e al lancio della piattaforma Maker.

- **Keeper:** operatori economici indipendenti che effettuano operazioni di trading in Dai, CDP e/o MKR, creano Dai o chiudono CDP ed effettuano arbitraggio nel sistema dello stablecoin Dai. Di conseguenza, i keeper contribuiscono a mantenere la stabilità del prezzo e la razionalità del mercato del Dai.

- **MKR:** il token ERC20 utilizzato dai votanti MKR per esercitare il voto. Funge anche da scudo in caso di CDP insolventi.

- **Votanti MKR:** detentori di MKR che gestiscono attivamente il rischio del sistema dello stablecoin Dai esprimendo un voto sui parametri di rischio.

- **Maker:** nome dell'organizzazione autonoma decentralizzata costituita dall'infrastruttura tecnica della piattaforma Maker e dalla community di votanti MKR.

- **Oracoli:** account Ethereum (contratti o utenti) selezionati per fornire price feed in vari componenti della piattaforma Maker.

- **Parametri di rischio:** le variabili che determinano (tra gli altri fattori) i casi in cui la piattaforma Maker giudica automaticamente una CDP come rischiosa, consentendo ai keeper di liquidarla.

- **Parametro di sensibilità:** la variabile che determina il livello di aggressività con cui il sistema dello stablecoin Dai modifica automaticamente il tasso target in risposta agli scarti del prezzo di mercato del Dai.

- **TRFM (Target Rate Feedback Mechanism: meccanismo di feedback del tasso target):** meccanismo automatico mediante il quale il sistema dello stablecoin Dai regola il tasso target per fare in modo che le forze del mercato mantengano stabile il prezzo di mercato del Dai su un valore pressoché equivalente al prezzo target.

Link

- **Chat:** https://chat.makerdao.com/: piattaforma principale di interazione della community

- **Forum:** https://forum.makerdao.com/: per dibattiti e proposte

- **Subreddit:** https://reddit.com/r/makerdao/: sito migliore per consultare le ultime notizie e i link più aggiornati

- **GitHub:** https://github.com/makerdao/: repository del codice Maker pubblico

- **TeamSpeak:** https://ts.makerdao.com/: per conference call di governance

- **SoundCloud:** https://soundcloud.com/makerdao/: registrazioni dei meeting di governance

- **Oasis:** https://oasisdex.com/: cambio decentralizzato di MKR e Dai

- **Sai:** https://sai.makerdao.com/: stablecoin sperimentale