Rai: Un collaterale a bassa Volatilità e a Fiducia Minimizzata per l'Ecosistema DeFi

Stefan C. Ionescu, Ameen Soleimani

Maggio 2020

Riassunto. Presentiamo un protocollo decentralizzato a governance minimizzata, il quale reagisce automaticamente ai movimenti del mercato per modificare il valore bersaglio del suo asset collaterale nativo. Il protocollo permette a chiunque di far leva sui propri cryptoasset ed emettere un "indice riflesso", una versione ammortizzata del collaterale sottostante. Delineiamo come gli indici possono essere utilizzati in forma di collaterali universali e a bassa volatilità che possono proteggere i propri titolari, così come altri protocolli finanziari decentralizzati, dai cambi inaspettati del mercato. Presentiamo i nostri piani per aiutare gli altri team a lanciare i propri sintetici facendo leva sulla nostra struttura. Infine, offriamo alternative alle strutture di governance e Oracle attuali che spesso si incontrano in numerosi protocolli DeFi**.**

Indice

Introduzione

Il denaro è uno dei più potenti meccanismi di coordinazione su cui l'umanità fa leva per prosperare. Il privilegio di poter controllare l'offerta monetaria ha risieduto storicamente nelle mani delle leadership sovrane e delle élite finanziarie e imposto sulla popolazione generale inconsapevole di ciò. Mentre il Bitcoin ha dimostrato il suo potenziale rivendicativo di base manifestandosi come un attivo di riserva di valore, Ethereum ci offre una piattaforma per costruire strumenti sintetici garantiti da risorse che possono essere protetti dalla volatilità e usati come collaterali, o ancorati a un prezzo di riferimento e usato come mezzo di scambio per transazioni giornaliere, tutto ciò possibile grazie agli stessi principi di consenso decentralizzato.

L'accesso senza restrizioni a Bitcoin per immagazzinare ricchezza e strumenti sintetici adeguatamente decentralizzati in Ethereum getterà le basi per la prossima rivoluzione finanziaria, fornendo a coloro che si trovano ai margini del moderno sistema finanziario i mezzi per coordinarsi intorno alla costruzione del nuovo sistema.

In questo documento, presentiamo una struttura per la costruzione di indici riflessi, un nuovo tipo di asset che aiuterà altri sintetici a sviluppare e stabilire un pilastro chiave per l'intero settore finanziario decentralizzato.

Descrizione Generale dell'Indice Riflesso

Lo scopo di un indice riflesso non è quello di mantenere una parità specifica, ma di attutire la volatilità del suo collaterale. Gli indici consentono a chiunque di aumentare la propria esposizione al mercato delle criptovalute senza lo stesso rischio di detenere risorse crittografiche reali. Riteniamo che RAI, il nostro primo indice riflesso, sarà di immediato utilizzo per altri computer che emettono materiali sintetici su Ethereum (ad esempio, Multi-Collateral DAI [1] di MakerDAO, UMA [2], Synthetix [3]) perché fornisce meno l'esposizione ad attività volatili come ETH e offre agli utenti più tempo per uscire dalle loro posizioni in caso di un cambiamento significativo nel mercato.

Per comprendere gli indici riflessi, possiamo confrontare l'andamento del suo prezzo di scambio con quello del prezzo di una moneta stabile (stablecoin).

Il prezzo di rimborso è il valore di un'unità di debito (o valuta) nel sistema. È destinato ad essere utilizzato solo come strumento contabile interno ed è diverso dal prezzo di mercato (il valore al quale il mercato negozia la valuta). Nel caso di stablecoin fiat come USDC, gli operatori di sistema dichiarano che chiunque può scambiare una moneta con un dollaro USA e quindi il prezzo di cambio di queste monete è sempre uno. Ci sono anche casi di stablecoin garantiti da criptovaluta, come Multi-collateral DAI (MCD) di

MakerDAO, in cui il sistema mira a una parità fissa di un dollaro USA e quindi anche il prezzo di scambio è fissato a uno.

Nella maggior parte dei casi, ci sarà una differenza tra il prezzo di mercato della stablecoin e il suo prezzo di scambio. Questi scenari creano opportunità di arbitraggio in cui i trader creeranno più monete se il prezzo di mercato è superiore al prezzo di scambio e scambieranno le loro stablecoin con garanzie (ad esempio, dollari USA nel caso di USDC) nel caso in cui il prezzo di mercato sia inferiore prezzo di scambio.

Gli indici riflessi sono simili alle stablecoin in quanto hanno anche un prezzo di rimborso che è preso di mira dal sistema. La differenza principale nel suo caso è che il suo rimborso non rimarrà fisso, ma è progettato per cambiare mentre è influenzato dalle forze di mercato. Nella Sezione 4 spieghiamo come il prezzo di rimborso di un indice fluttui e crei nuove opportunità di arbitraggio per i suoi utenti.

Filosofia del Design e Strategia di Commercio

La nostra filosofia di design è dare la priorità a sicurezza, stabilità e velocità di consegna.
La moneta multi-collaterale DAI è stata il punto di partenza naturale per iniziare a iterare il design RAI. Il sistema è stato controllato e verificato formalmente, ha dipendenze esterne minime e ha riunito una comunità attiva di esperti. Al fine di ridurre al minimo lo sforzo dello sviluppo e della comunicazione, desideriamo apportare solo le modifiche più semplici dal codice base MCD originale per ottenere la nostra implementazione.

Le nostre modifiche più significative includono l'introduzione di un fissatore di tariffe autonomo, un mediatore di rete di Oracle integrato con molte fonti di prezzo indipendenti e un livello di minimizzazione della governance inteso a isolare il sistema il più possibile dall'intervento umano.

La prima versione del protocollo (Fase 1) includerà solo il fissatore di tassi e altri miglioramenti minori all'architettura di base. Una volta dimostrato che il fissatore funziona come previsto, possiamo aggiungere in modo più sicuro il mediatore Oracle (Fase 2) e il livello di minimizzazione della governance (Fase 3).

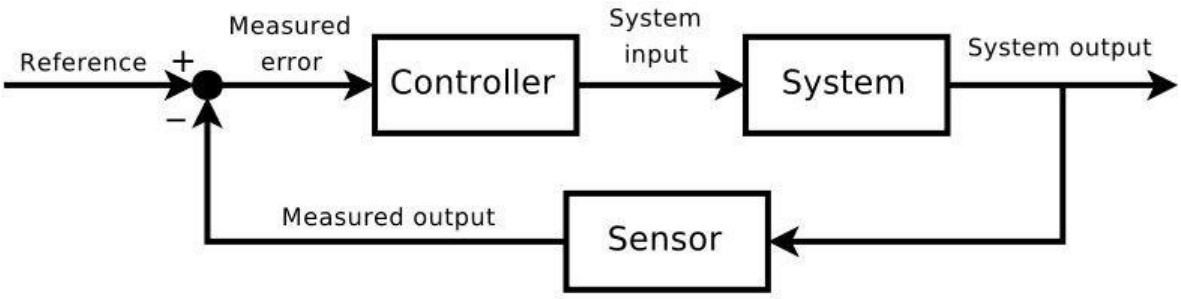
Meccanismi della Politica Monetaria

Introduzione alla Teoria del Controllo

Un sistema di controllo comune che la maggior parte delle persone conosce è la doccia. Quando qualcuno fa la doccia, ha in mente una temperatura dell'acqua desiderata che, nella teoria del controllo, è chiamata *punto di riferimento*. La persona, che funge da controller, misura continuamente la temperatura del flusso d'acqua (che viene chiamata *uscita* dell'impianto) e modifica la velocità di rotazione della maniglia della doccia a seconda della *deviazione* (o *errore*) tra la temperatura desiderata e quello attuale. La velocità alla quale viene girata la maniglia è chiamata input di sistema. L'obiettivo è ruotare la maniglia abbastanza velocemente da raggiungere rapidamente il punto di riferimento, ma non così velocemente da *superare* la temperatura desiderata. Se si verificano *shock* nel sistema in cui la temperatura del flusso d'acqua cambia improvvisamente, la persona dovrebbe essere in grado di mantenere la temperatura corrente sapendo quanto velocemente ruotare la maniglia in risposta al disturbo.

La disciplina scientifica preposta al mantenimento della stabilità nei sistemi dinamici si chiama Teoria del Controllo e ha trovato ampia applicazione nel cruise control per automobili, navigazione aerea, reattori chimici, bracci robotici e processi industriali di ogni tipo. L'algoritmo di impostazione della difficoltà di Bitcoin che mantiene il tempo medio dei blocchi a dieci minuti, nonostante un tasso di hash variabile, è un esempio di un sistema di controllo mission-critical.

Nella maggior parte dei sistemi di controllo moderni, generalmente un *controller algoritmico* è integrato nel processo e ha il controllo su un input di sistema (ad esempio, il pedale dell'acceleratore di un'auto) per aggiornarlo automaticamente in base alle deviazioni tra l'uscita del sistema (ad esempio, la velocità di un'auto) e il punto di riferimento (ad esempio, la velocità del cruise control).



Il tipo più comune di controller algoritmico è il controller PID. Oltre il 95% delle applicazioni industriali e un'ampia gamma di sistemi biologici utilizzano elementi di

controllo PID [4]. Un controller PID utilizza una formula matematica in tre parti per determinare il suo output:

Uscita controller = termine proporzionale + termine integrale + termine derivativo

Il termine proporzionale è la parte del controller che è direttamente proporzionale alla deviazione. Se la deviazione è ampia e positiva (ad esempio, il punto di regolazione della velocità del controllo automatico della velocità è molto più alto della velocità attuale dell'auto), la risposta proporzionale sarà ampia e positiva (ad esempio, premendo il pedale dell'acceleratore).

Il termine integrale è la parte del controller che tiene conto della durata di una deviazione. Viene determinato eseguendo l'integrale della deviazione nel tempo e viene utilizzato principalmente per eliminare l'errore di stato stazionario. Si accumula per rispondere a piccole, ma persistenti, deviazioni dal punto di riferimento (ad esempio, il punto di riferimento del controllo automatico della velocità è stato di 1 mph (1,60934 km/h) superiore alla velocità dell'auto per alcuni minuti).

Il termine derivato è la parte del controller che tiene conto della velocità con cui la deviazione cresce o si contrae. Si determina prendendo la derivata della deviazione e serve ad accelerare la risposta del controller quando la deviazione è in aumento (es. accelerare se il punto di riferimento del cruise control è maggiore della velocità dell'auto e l'auto inizia a rallentare). Aiuta anche a ridurre l'overshoot rallentando la risposta del guidatore quando la deriva si riduce (ad es. Decelerando l'acceleratore quando la velocità dell'auto inizia ad avvicinarsi al punto di regolazione del controllo della velocità di crociera).

La combinazione di queste tre parti, ciascuna delle quali può essere regolata indipendentemente, offre ai controller PID una grande flessibilità per gestire un'ampia varietà di applicazioni del sistema di controllo.

I controller PID funzionano meglio nei sistemi che consentono un certo ritardo nel tempo di risposta, nonché la possibilità di overshoot e oscillazioni intorno al punto di riferimento quando il sistema cerca di stabilizzarsi. I sistemi di indice riflesso come RAI sono adatti a questo tipo di scenario in cui i controller PID possono modificare i loro prezzi di permuta.
In generale, è stato recentemente scoperto che molte delle attuali regole di politica monetaria della banca centrale (ad esempio la regola di Taylor) sono in realtà approssimazioni dei controller PID [5].

Meccanismo di Feedback del tasso di rimborso

Il meccanismo di feedback del tasso di rimborso è la parte del sistema incaricata di modificare il prezzo di rimborso dell'indice riflesso. Per capire come funziona, dobbiamo prima descrivere perché il sistema necessita di un meccanismo di feedback invece di usare il controllo manuale e in seguito qual è l'output del sistema.

Componenti del meccanismo di feedback

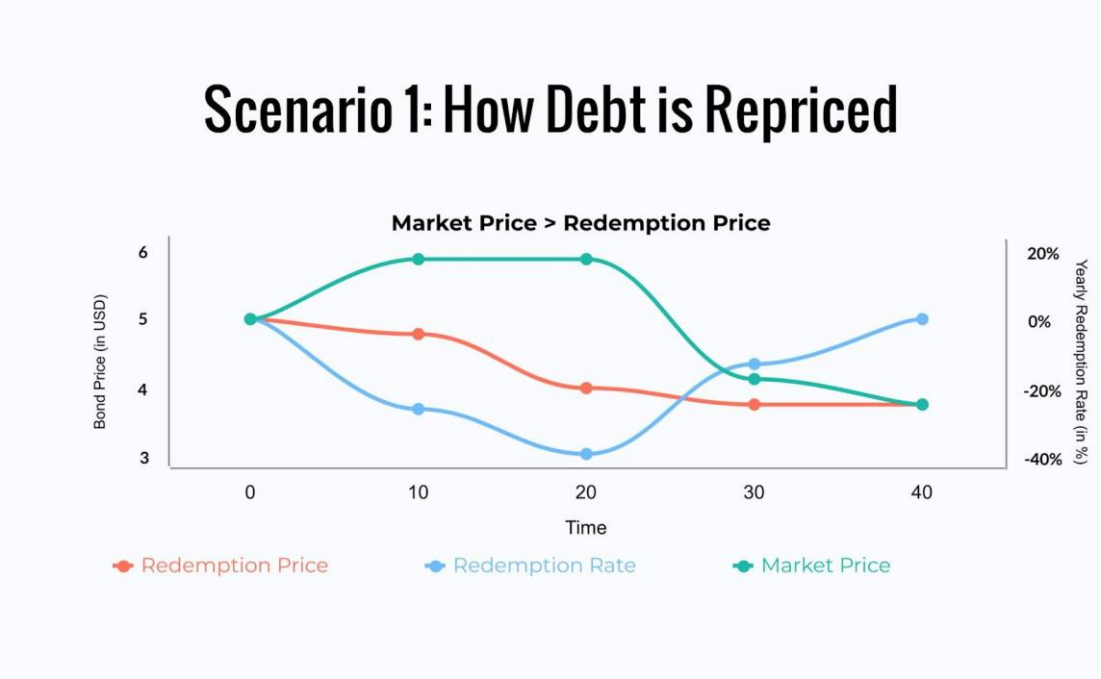
In teoria, sarebbe possibile manipolare direttamente il prezzo di rimborso dell'indice riflesso (descritto nel Capitolo 2) per influenzare gli utenti dell'indice e, in ultima analisi, alterare il prezzo di mercato dell'indice. In pratica, questo metodo non avrebbe l'effetto desiderato sui partecipanti del sistema. Dal punto di vista di un investitore in SAFE (Accordo Semplificato per l'Equità Futura), se il prezzo di rimborso aumenta una sola volta, potrebbe accettare un prezzo più alto per unità di debito, assorbire la perdita da una riduzione del rapporto di garanzia e mantenere la sua posizione. Se invece si aspettano che il prezzo di rimborso continui a crescere nel tempo, probabilmente saranno più propensi ad evitare perdite future prevedibili e quindi sceglieranno di cancellare il loro debito e chiudere le loro posizioni.

Ci aspettiamo che i partecipanti al sistema dell'indice riflesso non rispondano direttamente alle variazioni del prezzo di rimborso, ma rispondano invece al tasso di variazione del prezzo di rimborso che chiamiamo tasso di rimborso. Il tasso di rimborso è fissato tramite un meccanismo di feedback che la governance può regolare o consentire di essere completamente automatizzato.

Scenari del meccanismo di feedback

Bisogna ricordare che lo scopo del meccanismo di feedback è mantenere l'equilibrio tra il prezzo di rimborso e il prezzo di mercato utilizzando il tasso di rimborso per contrastare i cambiamenti nelle forze di mercato. Per ottenere ciò, il tasso di rimborso viene calcolato in modo da contrastare lo scostamento tra il prezzo di mercato e il prezzo di rimborso.

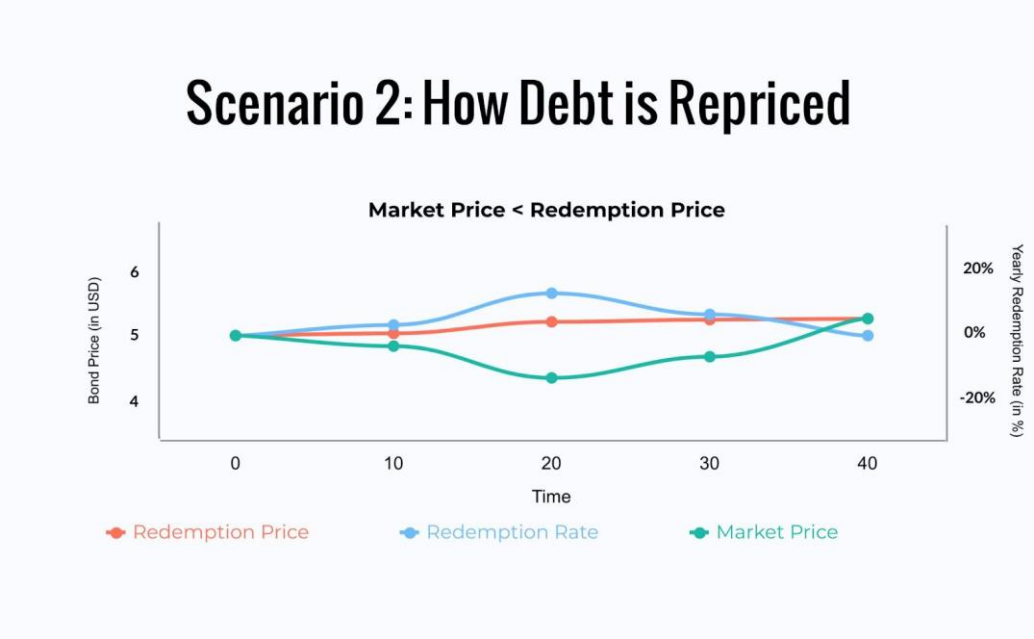
Nel primo scenario seguente, se il prezzo di mercato dell'indice è superiore al suo prezzo di rimborso, il meccanismo calcolerà un tasso negativo che inizierà a diminuire il prezzo di rimborso, abbassando così il debito del sistema.



L'aspettativa di un prezzo di rimborso decrescente probabilmente dissuaderà le persone dal detenere indici e incoraggerà i detentori di SAFE a generare più debito (anche se il prezzo del collaterale non cambia) che viene poi venduto sul mercato, bilanciando così offerta e domanda. Si noti che questo è lo scenario ideale in cui i titolari di indici reagiscono rapidamente in risposta al meccanismo di feedback. In pratica (e soprattutto nei primi giorni dopo il lancio), ci aspettiamo uno sfasamento tra l'avvio del meccanismo e gli effettivi risultati osservati nell'ammontare del debito emesso e successivamente nel prezzo di mercato.

D'altra parte, nel secondo scenario, se il prezzo di mercato dell'indice è inferiore al prezzo di rimborso, il tasso diventa positivo e il prezzo di tutto il debito inizia a essere ricalcolato in modo tale da diventare più costoso.

Man mano che il debito diventa più costoso, i rapporti di collateralizzazione di tutti i SAFE diminuiscono (quindi, i creatori di SAFE sono incentivati a ripagare il loro debito) e gli utenti iniziano ad accumulare rapporti nell'aspettativa che aumenteranno di valore.



Algoritmi del meccanismo di feedback

Nel seguente scenario, si presume che il protocollo utilizzi un controller proporzionale-integrale per calcolare il tasso di rimborso:

- L'indice riflesso viene lanciato con un prezzo di rimborso arbitrario e "casuale".

- Ad un certo punto, il prezzo di mercato dell'indice sale da "casuale" a "casuale" + x.
  Dopo che il meccanismo di feedback ha letto il nuovo prezzo di mercato, calcola un termine proporzionale *p*, che in questo caso è -1 * (('casuale' + x) / 'casuale'). La parte proporzionale è negativa per abbassare il prezzo di rimborso e allo stesso tempo ricalcolare gli indici in modo che diventino più economici.

- Dopo aver calcolato il termine proporzionale, il meccanismo determinerà il termine integrale sommando tutte le deviazioni passate negli ultimi *deviationInterval* secondi.

- Il meccanismo aggiunge le parti proporzionale e integrale e calcola un tasso di rimborso al secondo *r* che inizia lentamente a diminuire il prezzo di rimborso. Man mano che i creatori di SAFE si rendono conto che possono generare più debito, inonderanno il mercato con più indici.

- Dopo n secondi, il meccanismo rileva che la deviazione tra il prezzo di mercato e il prezzo di rimborso è trascurabile (sotto uno specifico parametro *noise*). A questo punto, l'algoritmo imposta r a zero e mantiene il prezzo di rimborso dov'è.

In pratica, l'algoritmo sarà più robusto e o renderemo immutabili alcune variabili (ad esempio il parametro *noise*, *deviationInterval*) oppure ci saranno limiti stretti su ciò che la governance può cambiare.

Regolazione del meccanismo di feedback

Di cruciale importanza per il corretto funzionamento del sistema dell'indice riflesso è la regolazione dei parametri del controller algoritmico. Una parametrizzazione inadeguata potrebbe far sì che il sistema sia troppo lento per raggiungere la stabilità, eccessivamente eccitato o generalmente instabile agli shock esterni.

Il processo di messa a punto per un controller PID generalmente comporta l'esecuzione del sistema in tempo reale, la regolazione dei parametri di regolazione e l'osservazione della risposta del sistema, spesso introducendo intenzionalmente degli shock durante il processo. Data la difficoltà e il rischio finanziario implicati nel modificare i parametri di un sistema di indice dei riflessi in tempo reale, intendiamo sfruttare il più possibile la modellazione e la simulazione al computer per stabilire i parametri iniziali, ma consentirà anche alla governance di aggiornare i parametri se i dati ottenuti dalla produzione mostrano che sono sub-ottimali.

Fissatore del mercato monetario

In RAI, il nostro piano è di mantenere il tasso di interesse (il tasso di interesse applicato durante la generazione degli indici) fisso o limitato e modificare solo il prezzo di rimborso, riducendo così al minimo la complessità legata alla modellazione del meccanismo di feedback. Nel nostro caso, il tasso di interesse è pari al differenziale tra la commissione di stabilità e il DSR nel DAI Multi-Collateral.

Sebbene il nostro piano sia di mantenere fisso il tasso di interesse, è possibile modificarlo insieme al prezzo di rimborso utilizzando un fissatore del mercato monetario. Il mercato monetario modifica il tasso di interesse e il prezzo di rimborso in un modo che incentiva i creatori di SAFE a generare più o meno debito. Se il prezzo di mercato di un indice è superiore al rendimento, entrambi i tassi inizieranno a diminuire, mentre se è inferiore al rimborso, i tassi aumenteranno.

Liquidazione Globale

La liquidazione globale è un metodo di ultima istanza utilizzato per garantire un prezzo di rimborso a tutti i possessori di indici riflessi. Ha lo scopo di consentire sia ai detentori di indici riflessivi che ai creatori di SAFE di riscattare le garanzie del sistema al loro

valore netto (numero di indici per ogni tipo di garanzia, in base all'ultimo prezzo di rimborso). Chiunque può attivare il regolamento dopo aver bruciato un certo numero di token di protocollo.

La liquidazione possiede tre fasi principali:

- **Innesco**: viene attivata la liquidazione, gli utenti non possono più creare SAFE, tutti i prezzi per i collaterali e il prezzo di rimborso vengono congelati e registrati

- **Processo**: condurre tutte le aste in sospeso

- **Rivendicazione**: tutti i creatori di SAFE e i titolari di indici riflessi possono richiedere un importo fisso di qualsiasi garanzia nel sistema in base all'ultimo prezzo di rimborso registrato dell'indice.

Governance

La stragrande maggioranza dei parametri sarà immutabile e la meccanica interna dello smart contract non potrà essere aggiornata a meno che i detentori di token di governance non implementino un sistema completamente nuovo. Abbiamo scelto questa strategia perché in questo modo possiamo eliminare il metagioco in cui alcune persone cercano di influenzare il processo di governance a proprio vantaggio, danneggiando così la fiducia nel sistema. Stabiliamo il corretto funzionamento del protocollo senza riporre troppa fiducia negli esseri umani (l'"effetto Bitcoin") per massimizzare la scalabilità sociale e ridurre al minimo i rischi per altri sviluppatori che vorranno utilizzare RAI come infrastruttura centrale nei propri progetti.

Per i pochi parametri modificabili, proponiamo l'aggiunta di un modulo di governance ristretto destinato a ritardare o limitare tutte le possibili modifiche del sistema. Inoltre, introduciamo un'era glaciale della governance, un registro dei permessi che può bloccare parti del sistema dal controllo esterno dopo che sono trascorse determinate scadenze.

Governance delimitata nel tempo

La governance limitata nel tempo è il primo componente del modulo di governance limitata. Stabilisce ritardi temporanei tra le modifiche applicate allo stesso parametro. Un esempio è la possibilità di modificare gli indirizzi degli Oracle utilizzati in Oracle Network Mediator (Sezione 6.2) dopo che sono trascorsi almeno T secondi dall'ultima modifica dell'Oracle.

Governance delimitata dall’azione

La seconda componente del Modulo di Governance Ristretta è la governance ad azioni limitate. Ogni parametro governabile ha dei limiti sui valori che possono essere impostati e su quanto possono cambiare in un certo periodo di tempo. Esempi notevoli sono le versioni iniziali del meccanismo di feedback del tasso di rimborso (Sezione 4.2) che i titolari di token governativi potranno modificare.

Era Glaciale della Governance

L'era glaciale è uno smart contract immutabile che impone scadenze per la modifica di parametri di sistema specifici e l'aggiornamento del protocollo. Può essere utilizzato nel caso in cui la governance voglia assicurarsi di poter correggere i bug prima che il protocollo si blocchi e blocchi l'intervento esterno. L'era glaciale verificherà se una modifica è consentita, verificando il nome del parametro e l'indirizzo del contratto interessato con un record di scadenze. Se il termine è scaduto, la richiesta verrà annullata.

La governance può ritardare l'era glaciale un numero fisso di volte se vengono rilevati bug in prossimità della data in cui il protocollo dovrebbe iniziare a bloccarsi. Ad esempio, l'era glaciale può essere ritardata solo tre volte, ogni volta per un mese, in modo che le nuove correzioni di bug implementate possano essere adeguatamente testate.

Aree principali in cui la Governance è necessaria

Individuiamo quattro aree in cui potrebbe essere necessaria la governance, specialmente nelle prime versioni di questo framework:

- **Aggiungere nuovi tipi di garanzie collaterali**: RAI sarà supportata solo da ETH, ma altri indici saranno supportati da diversi tipi di garanzie collaterali e la governance sarà in grado di diversificare il rischio nel tempo.

- **Modificare le dipendenze esterne**: gli Oracle e il DEX da cui dipende il sistema possono essere aggiornati. La governance può concentrare il sistema sulle dipendenze più recenti in modo che continui a funzionare correttamente

- **Ottimizzare del configuratore di tassi**: i primi driver di politica monetaria avranno parametri che possono essere modificati entro limiti ragionevoli (come descritto in Governance Delimitata dall’Azione e nel Tempo)

- **Migrare tra le versioni del sistema**: in alcuni casi, la governance potrebbe implementare un nuovo sistema, concedere l'autorizzazione a stampare i token di protocollo e rimuovere questa autorizzazione dal vecchio sistema. Questa migrazione viene eseguita con l'aiuto del modulo di migrazione ristretta descritto di seguito

Modulo di Migrazione Ristretta

Quello che segue è un semplice meccanismo per la migrazione tra le versioni del sistema:

- Esiste un registro di migrazione che tiene traccia di quanti sistemi diversi sono coperti dallo stesso token di protocollo e a quali sistemi può essere negata l'autorizzazione per stampare token di protocollo in un'asta del debito.

- Ogni volta che la governance implementa una nuova versione del sistema, invia l'indirizzo del contratto di asta del debito del sistema al registro della migrazione. La governance deve anche specificare se sarà mai in grado di impedire al sistema di stampare token di protocollo. Inoltre, la governance può, in qualsiasi momento, affermare che un sistema sarà sempre in grado di stampare token e quindi non migrerà mai da lì

- C'è un periodo di transizione tra la proposta di un nuovo sistema e il ritiro dei permessi da uno vecchio.

- È possibile configurare un contratto opzionale per arrestare automaticamente un sistema precedente dopo che le autorizzazioni di stampa sono state negate.

Il modulo di migrazione può essere combinato con un'era glaciale che concede automaticamente a sistemi specifici il permesso di poter stampare token in ogni momento.

Spegnimento Automatico del Sistema

Ci sono casi in cui il sistema può rilevare automaticamente e, di conseguenza, attivare il regolamento da solo, senza la necessità di masterizzare i token del protocollo:

- **Gravi ritardi nel feed di prezzo**: il sistema rileva che uno o più feed di prezzo del collaterale o dell'indice non sono stati aggiornati da molto tempo

- **Migrazione del sistema**: si tratta di un contratto opzionale che può chiudere il protocollo dopo che è trascorso un periodo di transizione dal momento in cui la governance revoca la capacità del meccanismo dell'asta del debito di stampare i token del protocollo (modulo di migrazione ristretta, Sezione 5.4.1)

- **Scostamento costante dal prezzo di mercato**: il sistema rileva che il prezzo di mercato dell'indice si è discostato di x% per troppo tempo rispetto al prezzo di rimborso

La Governance sarà in grado di aggiornare questi moduli di spegnimento autonomo finché sono ancora limitati o fino a quando l'era glaciale non inizierà a bloccare alcune parti del sistema.

Oracle

Esistono tre tipi principali di risorse per le quali il sistema deve leggere i feed di prezzo: l'indice, il token di protocollo e tutti i tipi di garanzia autorizzata. Le fonti dei prezzi possono essere fornite da Oracle guidati dalla governance o da reti Oracle consolidate.

Oracle gestiti dalla Governance

I titolari di token di governance o il core team che ha lanciato il protocollo possono collaborare con altre entità che raccolgono più fonti di prezzo fuori catena e quindi inviare una singola transazione a uno smart contract che calcola la mediana di tutti i punti dati.

Questo approccio consente una maggiore flessibilità per aggiornare e modificare l'infrastruttura Oracle, anche a scapito di una mancanza di fiducia.

Mediatore della Rete di Oracle

Un Oracle Network Mediator è uno smart contract che legge i prezzi da più fonti non direttamente controllate dalla governance (ad esempio un pool Uniswap V2 tra un tipo di garanzia sull’indice e altre stablecoin) e quindi fa la media di tutti i risultati. MRO

funziona come segue:

- Il nostro contratto tiene traccia delle reti Oracle autorizzate che puoi chiamare per richiedere il prezzo del collaterale. Il contratto è finanziato con parte del surplus accumulato dal sistema (utilizzando Surplus Treasury, Sezione 11). Ogni rete Oracle accetta token specifici come pagamento, quindi il nostro contratto tiene traccia anche dell'importo minimo e del tipo di token richiesti per ogni richiesta.

- Per inserire un nuovo feed di prezzo nel sistema, è necessario richiederlo in anticipo a tutti gli Oracle. Quando si chiama un Oracle, il contratto scambia prima alcune commissioni di stabilità con uno dei gettoni accettati dall'Oracle. Dopo aver chiamato l'Oracle, il contratto etichetta la richiesta come "valida" o "non valida". Se una richiesta non è valida, non può essere richiesta nuovamente allo specifico Oracle difettoso fino a quando tutti gli altri non vengono richiesti e il contratto verifica se esiste una maggioranza valida. Una richiesta Oracle valida non deve essere annullata e deve recuperare un prezzo che è stato pubblicato sulla catena negli ultimi *m* secondi. "Recuperare" significa cose diverse a seconda di ogni tipo di Oracle:

    - Per gli Oracle basati su *pull*, di cui possiamo ottenere un risultato immediato, il nostro contratto deve pagare una commissione e ottenere direttamente il prezzo.

    - Per gli Oracle basati su *push*, il nostro contratto paga la quota, chiama l'Oracle e devi attendere un determinato periodo di tempo *n* prima di chiamare nuovamente l'Oracle per ottenere il prezzo richiesto

- Ogni risultato di un Oracle viene memorizzato in una matrice. Dopo aver chiamato ogni Oracle sulla whitelist e se la matrice ha abbastanza punti dati validi per formare la maggioranza (ad esempio il contratto ha ricevuto dati validi da 3/5 degli Oracle), i risultati vengono ordinati e il contratto seleziona il valore medio.

- Indipendentemente dal fatto che il contratto trovi la maggioranza o meno, la matrice con i risultati Oracle viene cancellata e il contratto deve attendere *p* secondi prima di riavviare l'intero processo.

Backup della Rete di Oracle

La governance può aggiungere un'opzione di backup Oracle che inizia a far aumentare

i prezzi nel sistema se il broker non riesce a trovare le reti Oracle più valide più volte di seguito.

L'opzione di backup deve essere configurata quando viene distribuito il mediatore, poiché non può essere modificata in seguito. Inoltre, un contratto separato può monitorare se il backup ha sostituito il meccanismo di mediazione per troppo tempo e chiudere automaticamente il protocollo.

SAFE

Per generare indici, chiunque può depositare e sfruttare la propria garanzia crittografica all'interno di un SAFE (Accordo Semplificato per l'Equità Futura). Durante l'apertura di un SAFE, il debito continuerà ad accumularsi in base al tasso di interesse della garanzia depositata. Man mano che il creatore SAFE ripaga il suo debito, sarà in grado di ritirare sempre di più la sua garanzia bloccata.

Ciclo Vitale del SAFE

Ci sono quattro passaggi principali necessari per creare indici riflessi e successivamente ripagare il debito SAFE:

- Depositare il collaterale nel SAFE
  L'utente deve prima creare un nuovo SAFE e depositare su di esso la garanzia.

- Generare indici supportati dal collaterale del SAFE
  L'utente specifica quanti indici vuole generare. Il sistema crea una quantità uguale di debito che inizia ad accumularsi in base al tasso di indebitamento della garanzia.

- Ripagare il debito del SAFE
  Quando i creatori del SAFE vogliono ritirare la garanzia, devono pagare l'interesse iniziale più l'interesse maturato.

- Ritirare il collaterale
  Dopo che l'utente ha pagato una parte o tutto il suo debito, può ritirare la sua garanzia.

Liquidazione del SAFE

Per mantenere la solvibilità del sistema e coprire il valore del debito totale in essere,

ogni SAFE può essere liquidato nel caso in cui il rapporto di collateralizzazione scenda al di sotto di una certa soglia. Chiunque può attivare una liquidazione, nel qual caso il sistema confischerà la garanzia SAFE e la venderà a un'asta collaterale.

Asta di Collaterali

In una versione del sistema, i creatori di SAFE hanno la possibilità di scegliere un trigger per quando il loro SAFE viene cancellato. I trigger sono smart contract che aggiungono automaticamente più garanzie su un SAFE e potenzialmente lo salvano dalla liquidazione. Esempi di trigger sono contratti che vendono posizioni corte o contratti che comunicano con protocolli assicurativi come Nexus Mutual [6].

Un altro metodo per proteggere SAFE è l'aggiunta di due diverse soglie di garanzia: *assicurazione* e *rischio*. Gli utenti SAFE possono generare debito fino a raggiungere la soglia di sicurezza (che è maggiore del rischio) e vengono liquidati solo quando la garanzia SAFE scende al di sotto della soglia di rischio.

Assicurazione di Liquidazione

Per avviare un'asta collaterale, il sistema deve utilizzare una variabile chiamata *liquidationQuantity* per determinare l'importo del debito che sarà coperto in ciascuna asta e l'importo corrispondente della garanzia collaterale che verrà venduta. A ogni SAFE messo all'asta verrà applicata una *multa di liquidazione*.

Parametri dell’Asta di Collaterali

Nome del Parametro	Descrizione
minimumBid	Numero minimo di monete da offrire in un’offerta
discount	Sconto al quale viene venduto il collaterale
lowerCollateralMedianDeviation	Deviazione massima del limite inferiore che la mediana della garanzia può avere rispetto al prezzo Oracle
upperCollateralMedianDeviation	Deviazione massima del limite superiore che la mediana della garanzia può avere rispetto al prezzo Oracle

lowerSystemCoinMedianDeviation	Deviazione massima dal limite inferiore che il feed del prezzo Oracle della moneta del sistema può confrontare con il prezzo Oracle della moneta del sistema
upperSystemCoinMedianDeviation	Deviazione massima del limite superiore che la mediana della garanzia può avere rispetto al prezzo Oracle della valuta di sistema
minSystemCoinMedianDeviation	Deviazione minima per il risultato della mediana della valuta di sistema rispetto al prezzo di rimborso per tenere conto della mediana

Meccanismo dell'Asta di Collaterali

L'asta a sconto fisso è un modo semplice (rispetto alle aste in inglese) per mettere in vendita garanzie collaterali in cambio delle valute di sistema utilizzate per saldare i crediti inesigibili. Gli offerenti dovrebbero consentire solo alla casa d'aste di trasferire il proprio *safeEngine.coinBalance* e quindi chiamare *buyCollateral* per scambiare le monete nel proprio sistema con garanzie vendute a uno sconto rispetto all'ultimo prezzo di mercato registrato.

Gli offerenti possono anche esaminare la quantità di garanzie che possono ottenere da un'asta specifica chiamando *getCollateralBought* o *getApproximateCollateralBought*. Nota che *getCollateralBought* non è contrassegnato come visibile perché legge (e aggiorna anche) il *redemptionPrice* del mittente Oracle, mentre *getApproximateCollateralBought* utilizza *lastReadRedemptionPrice*.

Aste di Debiti

Nello scenario in cui un'asta collaterale non può coprire tutti i crediti inesigibili in un SAFE e se il sistema non dispone di riserve in eccesso, chiunque può attivare un'asta del debito.
Le aste di debito hanno lo scopo di coniare più token di protocollo (Sezione 10) e di venderli per indici che possono cancellare il debito inesigibile rimanente dal sistema.

Per avviare un'asta del debito, il sistema deve utilizzare due parametri:

- initialDebtAuctionAmount: la quantità iniziale di token di protocollo da coniare

dopo l'asta

- debtAuctionBidSize: la dimensione dell'offerta iniziale (quanti indici dovrebbero essere offerti in cambio di token di protocollo *initialDebtAuctionAmount*)

Stabilimento Autonomo dei Parametri dell'Asta del Debito

La quantità iniziale di token di protocollo coniati in un'asta del debito può essere impostata da un voto di governance o può essere regolata automaticamente dal sistema. Dovrebbe essere integrata una versione automatizzata con Oracle (Sezione 6) dalla quale il sistema legga il token del protocollo e i prezzi di mercato degli indici riflessi. Il sistema imposterà quindi il numero iniziale di token di protocollo (*initialDebtAuctionAmount*) che verrebbero coniati per gli indici *debtAuctionBidSize*. *initialDebtAuctionAmount* può essere impostato con uno sconto rispetto al prezzo di mercato effettivo del PROTOCOLLO / INDICE per incentivare le offerte.

Parametri dell'Asta del Debito

Nome del Parametro	Descrizione
amountSoldIncrease	Aumento del numero di gettoni protocollo da coniare per lo stesso numero di indici.
bidDecrease	Riduzione minima per l'offerta successiva del numero accettato di token di protocollo per lo stesso numero di indici
bidDuration	Quanto dura l'offerta dopo che è stata presentata una nuova offerta (in secondi)
totalAuctionLength	Durata totale dell'asta (in secondi)
auctionsStarted	Quante aste sono iniziate finora

Meccanismo dell'Asta del Debito

A differenza delle aste collaterali, le aste del debito hanno solo una fase:

decreaseSoldAmount(uint id, uint amountToBuy, uint bid: diminuisce il numero di token di protocollo accettati in cambio di un numero fisso di indici.

L'asta riprenderà se non sono state fatte offerte. Ogni volta che si riavvia, il sistema offrirà più token di protocollo per lo stesso numero di indici. L'importo del nuovo token del protocollo viene calcolato come *lastTokenAmount * amountSoldIncrease / 100*. Dopo che l'asta è stata risolta, il sistema emetterà gettoni al miglior offerente.

Token di Protocollo

Come descritto nelle sezioni precedenti, ogni protocollo dovrà essere protetto da un token coniato tramite aste di debito. Oltre alla protezione, il token verrà utilizzato per controllare alcuni componenti del sistema. Inoltre, l'offerta di token di protocollo verrà gradualmente ridotta con l'uso di aste di eccedenze. L'importo del surplus che deve accumularsi nel sistema prima che i fondi aggiuntivi vengano messi all'asta è chiamato *surplusBuffer* e viene automaticamente adeguato come percentuale del debito totale emesso.

Fondo Assicurativo

Oltre al token del protocollo, la governance può creare un fondo assicurativo che contiene un'ampia gamma di attività non correlate e che può essere utilizzato come supporto per le aste del debito.

Aste di Eccedenze

Le aste di eccedenze vendono commissioni di stabilità accumulate nel sistema per i token di protocollo che vengono poi bruciati.

Parametri dell'Asta di Eccedenze

Nome del Parametro	Descrizione
bidIncrease	Aumento minimo dell'offerta successiva
bidDuration	Quanto dura l'asta dopo che è stata presentata una nuova offerta (in secondi)
totalAuctionLength	Durata totale dell'asta (in secondi)
auctionsStarted	Quante aste sono iniziate finora

Meccanismi dell’Asta di Eccedenze

Le aste di eccedenze hanno un’unica fase:
`increaseBidSize(uint id, uint amountToBuy, uint bid)`: chiunque può offrire un numero maggiore di token di protocollo per lo stesso numero di indici (surplus). Ogni nuova offerta deve essere maggiore o uguale a *lastBid * bidIncrease* / 100. L'asta terminerà dopo che sono trascorsi i secondi massimi di *totalAuctionLength* o dopo che sono trascorsi i secondi di *bidDuration* dall'ultima offerta e non sono state presentate nuove offerte durante questo tempo.

Un'asta riprenderà se non ha offerte. D'altra parte, se l'asta ha almeno un'offerta, il sistema offrirà il surplus al miglior offerente e quindi brucerà tutti i token di protocollo raccolti.

Gestione degli Indici di Eccedenze

Ogni volta che un utente genera indici e allo stesso tempo crea implicitamente un debito, il sistema inizia ad applicare un tasso di indebitamento all'utente SAFE. L'interesse maturato è raggruppato in due diversi smart contract:

- L’*accounting engine* utilizzato per attivare le aste del debito (Sezione 9.2) e le eccedenze (Sezione 10.1).
- Il *surplus treasury* utilizzato per finanziare i componenti di base dell'infrastruttura e incentivare gli attori esterni a mantenere il sistema

L'eccedenza di cassa è responsabile del finanziamento di tre componenti fondamentali del sistema:

- Modulo Oracle (Sezione 6). A seconda di come è strutturato un Oracle, la tesoreria paga per gli Oracle off-chain dalla whitelist di governance o paga per le petizioni alle reti di Oracle. La tesoreria può anche essere configurata per pagare gli indirizzi che hanno speso il gas per chiamare un Oracle e aggiornarlo.

- In alcuni casi, team indipendenti che mantengono il sistema. Alcuni esempi sono i team che inseriscono nella whitelist nuovi tipi di garanzie collaterali o modificano il fissatore del tasso del sistema (Sezione 4.2).

La tesoreria può essere configurata in modo che ad alcuni beneficiari in eccesso venga automaticamente negato il finanziamento in futuro e altri possano prendere il loro posto.

Attori Esterni

Il sistema dipende da attori esterni per funzionare correttamente. Questi attori sono economicamente incentivati a partecipare ad aree come le aste, il processo di regolamento globale, la creazione del mercato e gli aggiornamenti dei prezzi per mantenere la salute del sistema.

Forniremo interfacce utente iniziali e script automatizzati per consentire a quante più persone possibile di mantenere il protocollo protetto.

Mercato Obiettivo

Vediamo che la RAI è utile in due aree principali:

- **Diversificazione del portfolio:** Gli investitori utilizzano RAI per ridurre l'esposizione a un asset come ETH senza tutto il rischio di detenere effettivamente ether

- **Collateral per asset sintetici:** RAI può offrire protocolli come UMA, MakerDAO e Synthetix una minore esposizione al mercato delle criptovalute e dare agli utenti più tempo per uscire dalle loro posizioni nel caso di scenari come il Black Thursday a marzo 2020 quando furono liquidati milioni di dollari nelle risorse crittografiche.

Ricerche Future

Per espandere i confini del denaro decentralizzato e portare più innovazione nella finanza decentralizzata, continueremo a cercare alternative in aree fondamentali come la minimizzazione della governance e dei meccanismi di regolamento.

In primo luogo, vogliamo gettare le basi per standard futuri attorno a protocolli che si bloccano dal controllo esterno e per veri "robot monetari" che si adattano in risposta alle forze di mercato. Successivamente, abbiamo invitato la comunità di Ethereum a discutere e progettare miglioramenti attorno alle nostre proposte con un focus specifico sulle aste di garanzie e debito.

Rischi e Mitigazione

Ci sono diversi rischi coinvolti nello sviluppo e nel lancio di un indice riflesso, così come

i sistemi a valle che sono costruiti sopra un livello:

- **Errori nello smart contract:** il rischio maggiore presentato dal sistema è la possibilità di un errore che consenta a chiunque di estrarre tutte le garanzie o bloccare il protocollo in uno stato dal quale non può essere recuperato. Prevediamo che più ricercatori di sicurezza esaminino il nostro codice e rilascino il sistema su una testnet prima di impegnarsi a implementarlo in produzione.

- Bug Oracle: aggiungeremo feed da più reti Oracle e ci saranno regole rigide per aggiornare solo un Oracle alla volta, in modo che la governance dannosa non possa introdurre facilmente prezzi falsi.

- **Eventi collaterali del cigno nero:** esiste il rischio di un evento collaterale del cigno nero che può comportare la liquidazione di una grande quantità di SAFE. Gli insediamenti potrebbero non essere in grado di coprire tutto il debito inesigibile, e quindi il sistema cambierà continuamente il suo cuscinetto in eccesso per coprire una discreta quantità di debito emesso e resistere agli shock di mercato.

- **Parametri di impostazione della frequenza inadeguati:** i meccanismi di feedback autonomo sono altamente sperimentali e potrebbero non comportarsi esattamente come previsto durante le simulazioni. Prevediamo di consentire alla governance di adeguare questa componente (pur rimanendo vincolata) per evitare scenari imprevisti

- **Impossibilità nell'avviare un mercato sano dei liquidatori:** i liquidatori sono attori fondamentali che garantiscono che tutto il debito emesso sia coperto da garanzie. Abbiamo in programma di creare interfacce e script automatizzati in modo che quante più persone possibile possano partecipare alla protezione del sistema.

Riassunto

Abbiamo proposto un protocollo che si isola progressivamente dal controllo umano ed emette un asset garantito a bassa volatilità chiamato indice riflesso. Per prima cosa introduciamo il meccanismo autonomo inteso a influenzare il prezzo di mercato dell'indice e poi descriviamo come vari smart contract possono limitare il potere che i possessori di token hanno sul sistema. Descriviamo uno schema autosufficiente per mediare i feed di prezzo di più reti Oracle indipendenti e, infine, concludiamo presentando la procedura generale per il conio degli indici e il regolamento SAFE.

Riferimenti Bibliografici

[1] "The Maker Protocol: MakerDAO's Multi Collateral Dai (MCD) System", https://bit.ly/2YL5S6j

[2] "UMA: A Decentralized Financial Contract Platform", https://bit.ly/2Wgx7E1

[3] Synthetix Litepaper, https://bit.ly/2SNHxZO

[4] K.J. Åström, R.M. Murray, "Feedback Systems: An Introduction for Scientists and Engineers", https://bit.ly/3bHwnMC

[5] R.J. Hawkins, J.K. Speakes, D.E. Hamilton, "Monetary Policy and PID Control", https://bit.ly/2TeQZFO

[6] H. Karp, R. Melbardis, "A peer-to-peer discretionary mutual on the Ethereum blockchain", https://bit.ly/3du8TMy

[7] H. Adams, N. Zinsmeister, D. Robinson, "Uniswap V2 Core",https://bit.ly/3dqzNEU

Glossario

Indice Riflesso: un asset garantito che smorza la volatilità del sottostante

RAI: il nostro primo indice riflesso

Prezzo di Rimborso: il prezzo che il sistema vuole che l'indice abbia. Cambia, influenzato dal tasso di rimborso (calcolato da RRFM), nel caso in cui il prezzo di mercato non sia vicino ad esso. Intende influenzare i creatori di SAFE per generare di più o ripagare parte del tuo debito.

Tasso di Debito: tasso di interesse annuo applicato a tutti i SAFE che hanno debiti in sospeso

Meccanismo di Feedback del Tasso di Rimborso (RRFM): un meccanismo autonomo che confronta i prezzi di mercato e di rimborso di un indice riflesso e quindi calcola un tasso di rimborso che influenza lentamente i creatori di SAFE a generare più o meno debito (e cerca implicitamente di ridurre al minimo il prezzo di mercato / rimborso deviazione)

Fissatore del Mercato Monetario (MMS): un meccanismo simile a RRFM che aziona più leve monetarie contemporaneamente. Nel caso degli indici riflessi, modifica sia il tasso di interesse passivo che il prezzo di rimborso.

Mediatore della Rete di Oracle: uno smart contract che estrae i prezzi da più reti Oracle (che non sono controllate dalla governance) e le media se la maggioranza (ad esempio 3 su 5) ha restituito un risultato inedito

Modulo di Governance Ristretta: un insieme di smart contract che collegano il potere che i detentori di token di governance hanno sul sistema. Implica ritardi nel tempo o limita le possibilità per la governance di stabilire determinati parametri.

Era Glaciale della Governance: contratto immutabile che blocca la maggior parte dei componenti di un protocollo dall'intervento esterno dopo che è trascorso un limite di tempo specificato.

Accounting Engine: componente del sistema che attiva le aste di debito e surplus. Tiene traccia anche dell'ammontare del debito attualmente venduto all'asta, del debito inesigibile non trattato e del buffer in eccesso.

Surplus buffer: importo degli interessi da maturare e mantenere nel sistema. Qualsiasi

interesse maturato al di sopra di questa soglia viene venduto in aste in eccesso che bruciano token di protocollo

Surplus Treasury: contratto che dà il permesso a diversi moduli del sistema di ritirare gli interessi maturati (es. ONM per richieste Oracle)