

Rai: Alhainen volatilitieetti, luottamus minimoitu

# Vakuus DeFi-ekosysteemille

Stefan C. Ionescu, Ameen Soleimani

toukokuu 2020

**Abstrakti.** Esittelemme hallinnoinnista minimoidun, hajautetun protokollan, joka reagoi automaattisesti markkinavoimiin muuttaakseen alkuperäisen vakuudellisen omaisuuden tavoitearvoa. Protokolla mahdollistaa sen, että kuka tahansa voi hyödyntää kryptoomaisuuttaan ja antaa "refleksiindeksin", joka on vaimennettu versio sen taustalla olevista vakuuksista. Selvitämme, kuinka indeksit voivat olla hyödyllisiä yleismaailmallisina, alhaisen volatilitietin vakuuksina, jotka voivat suojata sen haltijoita sekä muita hajautettuja rahoitusprotokollia äkillisiltä markkinoiden muutoksilta. Esittelemme suunnitelmamme auttaa muita tiimejä lanseeraamaan omia synteettisiä tuotteita hyödyntämällä infrastruktuuriamme. Lopuksi tarjoamme vaihtoehtoja nykyisille oraakkeleille ja hallintorakenteille, joita usein löytyy monista DeFi-protokollista.

## Sisällys

1. Esittely
2. Refleksiindeksien yleiskatsaus
3. Suunnittelufilosofia ja markkinoille pääsyn strategia
4. Rahapolitiikan mekanismit
  - 4.1. Johdatus ohjausteoriaan
  - 4.2. Lunastuskoron palautemekanismi
    - 4.2.1. Komponentit
    - 4.2.2. Skenaariot
    - 4.2.3. Algoritmi
    - 4.2.4. Viritys
  - 4.3. Rahamarkkinoiden asettaja

#### 4.4. Maailmanlaajuinen ratkaisu

### 5. Hallinto

#### 5.1. Aikarajallinen hallinto

#### 5.2. Toimintarajoitettu hallinto

#### 5.3. Hallinto jääkausi

#### 5.4. Ydinalueet, joilla hallintoa tarvitaan

##### 5.4.1. Rajoitettu siirtomoduuli

### 6. Automaattinen järjestelmän sammutus

### 7. Oraakkelit

#### 7.1. Hallinto johti Oraakkeleita

#### 7.2. Oracle Network Medianizer

##### 7.2.1. Oracle Network Backup

### 8. Kassakaapit

#### 8.1. TURVALLINEN elinkaari

### 9. TURVALLINEN selvitystila

#### 9.1. Vakuushuutokauppa

##### 9.1.1. Selvitystilavakuutus

##### 9.1.2. Vakuushuutokaupan parametrit

##### 9.1.3. Vakuutushuutokauppamekanismi

#### 9.2. Velkahuutokauppa

##### 9.2.1. Autonominen velkahuutokaupan parametriasetus

##### 9.2.2. Velkahuutokaupan parametrit 9.2.3. Velkahuutokauppamekanismi

### 10. Protokollamerkit

#### 10.1. Ylijäämähuutokaupat

##### 10.1.1. Ylijäämähuutokaupan parametrit

##### 10.1.2. Ylijäämähuutokauppamekanismi

### 11. Ylijäämäindeksien hallinta

### 12. Ulkopuoliset toimijat

### 13. Osoitettavat markkinat

### 14. Tulevaisuuden tutkimus

### 15. Riskit ja lieventäminen

### 16. Yhteenveto

### 17. Viitteet

### 18. Sanasto

# Johdanto

Raha on yksi tehokkaimmista koordinaatiomekanismeista, jota ihmiskunta käyttää menestyäkseen. Rahan tarjonnan hallinnan etuoikeus on historiallisesti pidetty suvereenin johdon ja finanssieliitin käsissä, samalla kun se on pakotettu tahattomalle suurelle yleisölle. Kun Bitcoin on osoittanut ruohonjuuritason protestin mahdollisuuden ilmentää arvoa varastoivaa hyödykeomaisuutta, Ethereum tarjoaa meille alustan rakentaa omaisuusvakuudellisia synteettisiä instrumentteja, jotka voidaan suojata volatilitteetilta ja joita voidaan käyttää vakuutena tai sidottu viitehintaan. Ja sitä käytetään päivittäisten liiketoimien vaihtovälineenä. Kaikkia valvotaan samojen hajautetun konsensuksen periaatteiden mukaisesti.

Luvaton pääsy Bitcoinin varallisuuden säilyttämiseen ja asianmukaisesti hajautetut synteettiset instrumentit Ethereumissa luovat perustan tulevalle rahoitusvallankumoukselle ja tarjoavat modernin rahoitusjärjestelmän reunamilla oleville keinot koordinoida uuden rakentamista.

Tässä artikkelissa esittelemme viitekehysten refleksiindeksien rakentamiseen. Se on uusi omaisuustyyppi, joka auttaa muita synteettisiä tuotteita kukoistamaan ja muodostaa keskeisen rakennuspalikan koko hajautetun rahoitusalan toiminnalle.

## Refleksiindeksien yleiskatsaus

Refleksiindeksin tarkoituksena ei ole ylläpitää tiettyä sitoumusta, vaan vaimentaa sen vakuuksien volatilitteettia. Indeksien avulla kuka tahansa voi altistua kryptovaluuttamarkkinoille ilman samaa riskiä kuin todellisten kryptovarojen omistaminen. Uskomme, että RAI:sta, ensimmäisestä refleksiindeksistämme, on välitöntä hyötyä muille tiimeille, jotka julkaisevat synteettisiä tuotteita Ethereumissa (esim. MakerDAO:n Multi-Collateral DAI [1], UMA [2], Synthetix [3]), koska se antaa heidän järjestelmilleen vähemmän altistumista epävakait varat, kuten ETH, ja tarjoaa käyttäjille enemmän aikaa poistua positioistaan, jos markkinat muuttuvat merkittävästi.

Refleksiindeksien ymmärtämiseksi voimme verrata niiden lunastushinnan käyttäytymistä vakaan kolikon hintaan.

Lunastushinta on yhden velkayksikön (tai kolikon) arvo järjestelmässä. Se on tarkoitettu käytettäväksi vain sisäisenä kirjanpityökaluna ja se eroaa markkinahinnasta (arvosta, jolla markkinat käyvät kauppaa kolikolla). Jos kyseessä on fiat-selkä

stabiileissa kolikoissa, kuten USDC, järjestelmän ylläpitäjät ilmoittavat, että kuka tahansa voi lunastaa yhden kolikon yhdestä Yhdysvaltain dollarista ja siten näiden kolikoiden lunastushinta on aina yksi. On myös tapauksia kryptoturvalisista stabiileista kolikoista, kuten MakerDAO:n Multi Collateral DAI (MCD), joissa järjestelmä tavoittelee kiinteää dollaria ja siten myös lunastushinta on kiinteä.

Useimmissa tapauksissa vakaan kolikon markkinahinnan ja sen lunastushinnan välillä on ero. Nämä skenaariot luovat arbitraasimahdollisuuksia, joissa kauppiat luovat enemmän kolikoita, jos markkinahinta on lunastushintaa korkeampi, ja he lunastavat vakaat kolikot vakuudeksi (esim. USDC:n tapauksessa USD), jos markkinahinta on alempi kuin lunastushinta.

Reflex-indeksit ovat samanlaisia kuin stablecoins, koska niillä on myös lunastushinta, jonka järjestelmä tavoittelee. Suurin ero heidän tapauksessaan on, että niiden lunastus ei pysy kiinteänä, vaan se on suunniteltu muuttumaan markkinavoimien vaikutuksesta. Osassa 4 selitämme, kuinka indeksin lunastushinta kelluu ja luo uusia arbitraasimahdollisuuksia sen käyttäjille.

## Suunnittelufilosofia ja markkinoille pääsyn strategia

Suunnittelufilosofiamme on asettaa etusijalle turvallisuus, vakaus ja toimitusnopeus.

Multi-Collateral DAI oli luonnollinen paikka aloittaa RAI:n suunnittelun iterointi. Järjestelmä on vahvasti auditoitu ja muodollisesti verifioitu, sillä on vähäisiä ulkoisia riippuvuuksia ja se on kerännyt aktiivisen asiantuntijayhteisön. Minimoidaksemme kehitys- ja viestintäponnistelut haluamme tehdä vain yksinkertaisimmat muutokset alkuperäiseen MCD-koodikantaan toteutuksemme saavuttamiseksi.

Tärkeimpiä muutoksiamme ovat autonomisen hintojen asettajan lisääminen, Oracle Network Medianizer, joka on integroitu moniin riippumattomiin hintasyötteisiin, ja hallinnan minimointikerros, jonka tarkoituksena on eristää järjestelmä mahdollisimman paljon ihmisen puuttumisesta.

Protokollan ensimmäinen versio (vaihe 1) sisältää vain nopeuden asettajan ja muita pieniä parannuksia ydinarkkitehtuuriin. Kun olemme todistaneet, että asettaja toimii odotetusti, voimme turvallisemmin lisätä oraakkelin medianisaattorin (vaihe 2) ja hallinnan minimointikerroksen (vaihe 3).

## Rahapolitiikan mekanismit

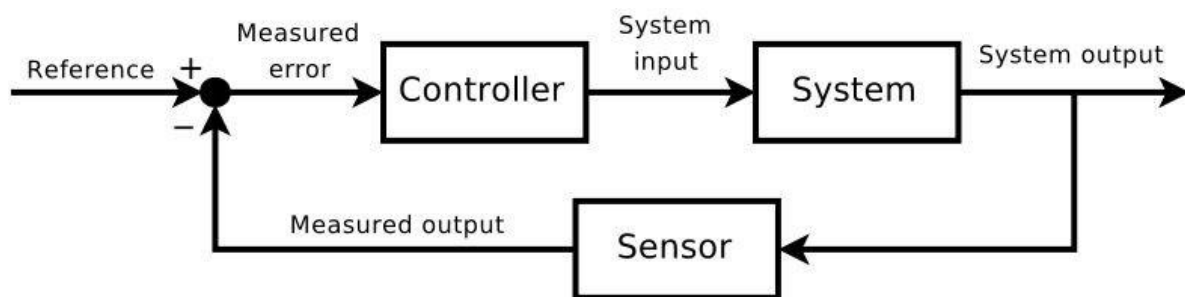
### Johdatus ohjausteoriaan

Yksi yleinen ohjausjärjestelmä, jonka useimmat ihmiset tuntevat, on suihku. Kun joku aloittaa suihkun, hänellä on mielessään haluttu veden lämpötila, jota säätöteoriassa kutsutaan referenssiasetuspiste. Henkilö, joka toimii ohjain, mittaa jatkuvasti veden menolämpötilaa (jota kutsutaan järjestelmäksi ulostulo) ja nd muuttaa nopeutta, jolla he kääntävät suihkun nuppia poikkeama(taivirhe) halutun ja nykyisen lämpötilan välillä. Nopeutta, jolla nuppia käännetään, kutsutaan järjestelmäksisyöttö. Tavoitteena on kiertää nuppia tarpeeksi

nopeasti, jotta viiteasetuspiste saavutetaan nopeasti, mutta ei niin nopeasti, että lämpötila nousee ylikäytökseen. Jos järjestelmiä on tarkkailtava veden menolämpötila muuttuu äkillisesti, henkilön pitäisi pystyä ylläpitämään nykyistä lämpötilaa tietäen, kuinka nopeasti nuppia on käännettävä vastena häiriöön.

Tieteellistä tieteenalaa dynaamisten järjestelmien vakauden ylläpitämisestä kutsutaan ohjausteoriaksi, ja se on löytänyt laajan sovelluksen autojen vakionopeudensäätimessä, lennon navigoinnissa, kemiallisissa reaktoreissa, robottiaseissa ja kaikenlaisissa teollisissa prosesseissa. Bitcoinin vaikeusasteen säätöalgoritmi, joka säilyttää kymmenen minuutin keskimääräisen lohkoajan vaihtelevasta hashratesta huolimatta, on esimerkki tehtäväkriittisestä ohjausjärjestelmästä.

Useimmissa nykyaikaisissa ohjausjärjestelmissä algoritminen ohjain on tyypillisesti upotettu prosessiin ja sille annetaan ohjaus järjestelmän tulon (esim. auton kaasupoljin) sen päivittämiseksi automaattisesti järjestelmän lähdön (esim. auton nopeus) ja asetusarvon (esim. vakionopeudensäätimen nopeus) välisten poikkeamien perusteella. ).



Yleisin algoritmiohjaintyyppi on PID-säädin. Yli 95 % teollisista sovelluksista ja monista biologisista järjestelmistä käyttää PID-elementtejä ohjaus [4]. PID-säädin määrittää lähtönsä matemaattisen kaavan, jossa on kolme osaa:

Ohjaimen lähtö = suhteellinen termi + integraalitermi + johdannaistermi

Suhteellinen termi on se rekisterinpitäjän osa, joka on suoraan suhteellinen poikkeamaan. Jos poikkeama on suuri ja positiivinen (esim. vakionopeudensäätimen nopeuden asetusarvo on paljon suurempi kuin auton nykyinen nopeus), suhteellinen vaste on suuri ja positiivinen (esim. kaasupoljin laskee).

Integral Term on ohjaimen osa, joka ottaa huomioon, kuinka kauan poikkeama on jatkunut. Se määritetään ottamalla kiinteä poikkeamasta ajan myötä ja sitä käytetään ensisijaisesti poistamaan vakaa tilan virhe. Se keraantyy reagoimaan pieniin, vaikkakin pysyviin poikkeamiin asetusarvosta (esim. vakionopeudensäätimen asetusarvo on ollut muutaman minuutin ajan 1 mph korkeampi kuin auton nopeus).

Johdannainen termi on ohjaimen osa, joka ottaa huomioon, kuinka nopeasti poikkeama kasvaa tai pienenee. Se määritetään ottamalla johdannainen poikkeamasta ja nopeuttaa säätimen vastetta poikkeaman kasvaessa (esim. nopeutta, jos vakionopeudensäätimen asetusarvo on korkeampi kuin auton nopeus ja auto alkaa hidastaa). Se auttaa myös vähentämään ylitystä hidastamalla säätimen vastetta poikkeaman pienentyessä (esim. helpottaa kaasua, kun auton nopeus alkaa lähestyä vakionopeudensäätimen asetuspistettä).

Näiden kolmen osan yhdistelmä, joista jokainen voidaan virittää itsenäisesti, antaa PID-säätimille suuren joustavuuden hallita monenlaisia ohjausjärjestelmän sovelluksia.

PID-säätimet toimivat parhaiten järjestelmissä, jotka sallivat jonkinasteisen viiveen vasteajassa sekä mahdollisen ylityksen ja värähtelyn asetusarvon ympärillä, kun järjestelmä yrittää vakauttaa itsensä. Reflex-indeksijärjestelmät, kuten RAI, sopivat hyvin tämän tyyppisiin skenaarioihin, joissa PID-säätimet voivat muuttaa niiden lunastushintoja.

Yleisemmin on äskettäin havaittu, että monet keskuspankin nykyisistä rahapolitiikan säännöistä (esim. Taylorin sääntö) ovat itse asiassa PID:n likiarvoja.

ohjaimet [5].

## Lunastuskoron palautemekanismi

Redemption Rate Feedback Mechanism on järjestelmäkomponentti, joka vastaa refleksiindeksin lunastushinnan muuttamisesta. Ymmärtääksemme, miten se toimii, meidän on ensin kuvattava, miksi järjestelmä tarvitsee palautemekanismin manuaalisen ohjauksen sijaan ja mikä mekanismin lähtö on.

### Palautemekanismin osat

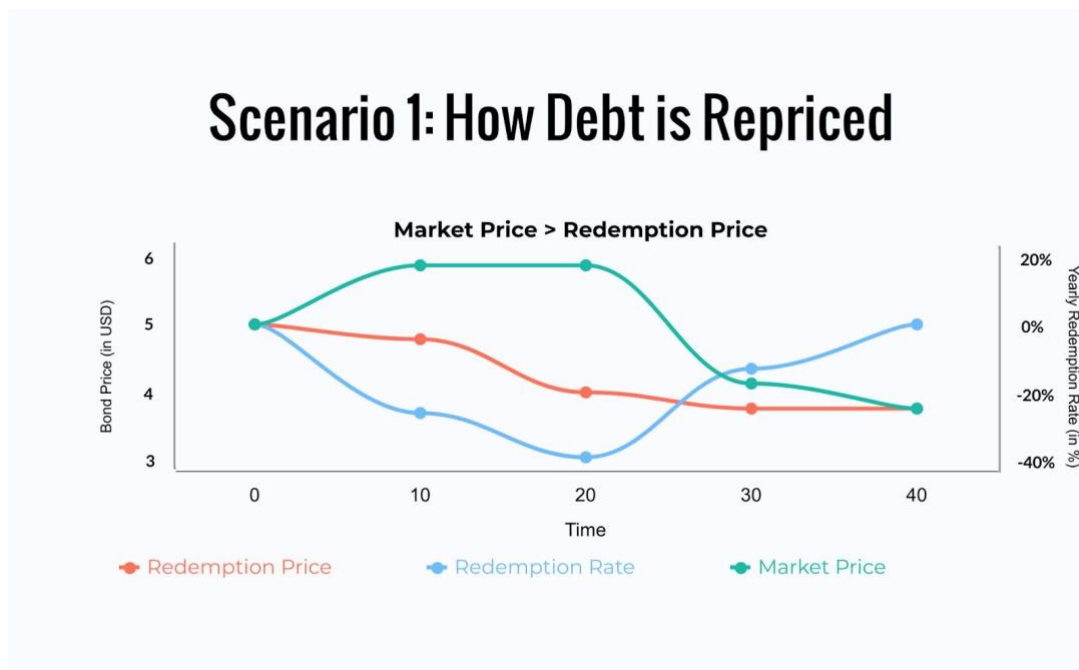
Teoriassa olisi mahdollista manipuloida suoraan refleksiindeksin lunastushintaa (kuvattu kohdassa 2) indeksin käyttäjiin vaikuttamiseksi ja lopulta indeksin markkinahinnan muuttamiseksi. Käytännössä tällä menetelmällä ei olisi toivottua vaikutusta järjestelmän osallistujiin. SAFEn haltijan näkökulmasta, jos lunastushintaa korotetaan vain kerran, hän saattaa hyväksyä korkeamman hinnan velkayksikköä kohden, omaksua alentuneen vakuussuhteen tappion ja säilyttää asemansa. Jos he kuitenkin odottavat lunastushinnan nousevan edelleen ajan mittaan, he olisivat todennäköisesti taipuvaisempia välttämään odotettuja tulevia tappioita ja päättäisivät siten maksaa velkansa takaisin ja sulkea positoidensa.

Odotamme, että refleksiindeksijärjestelmän osallistajat eivät reagoi suoraan lunastushinnan muutoksiin, vaan sen sijaan lunastushinnan muutosprosentti jota me kutsummelunastusprosentti. Lunastuskoron määrää palautemekanismi että hallinto voi hienosäätää tai sallia sen täysin automatisoinnin.

## Palautemekanismin skenaariot

Muista, että palautemekanismi pyrkii ylläpitämään tasapainoa lunastushinnan ja markkinahinnan välillä käyttämällä lunastuskurssia estämään markkinavoimien muutoksia. Tämän saavuttamiseksi lunastuskorko lasketaan siten, että se vastustaa markkina- ja lunastushintojen välistä poikkeamaa.

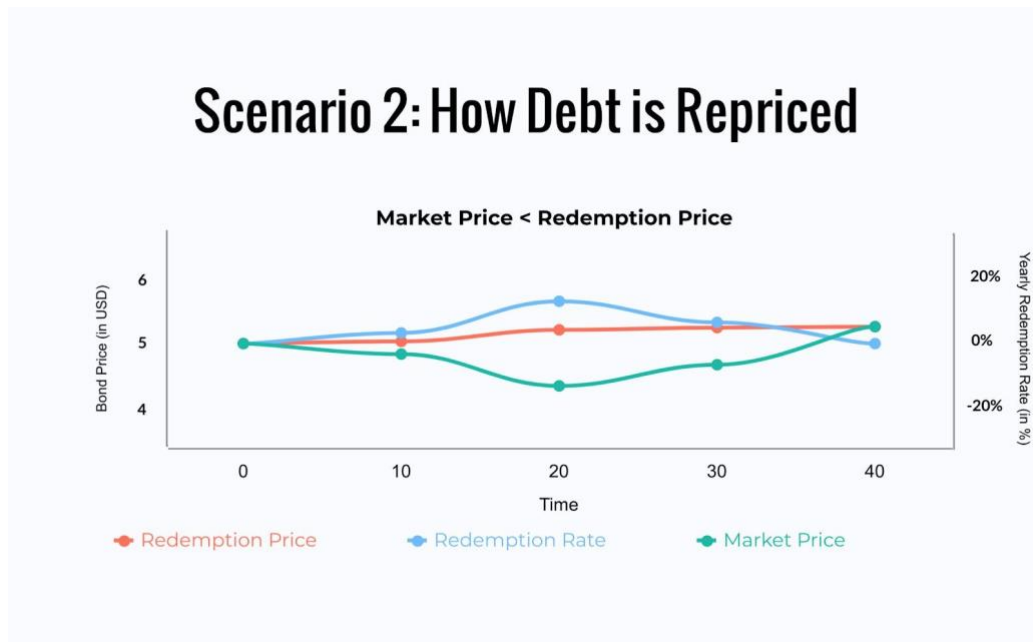
Alla olevassa ensimmäisessä skenaariossa, jos indeksin markkinahinta on korkeampi kuin sen lunastushinta, mekanismi laskee negatiivisen koron, joka alkaa laskea lunastushintaa, mikä tekee järjestelmän velasta halvempaa.



Lunastushinnan laskeva odotus saa ihmiset luopumaan indeksien pitämisestä ja rohkaisee SAFE-haltijoita luomaan lisää velkaa (vaikka vakuuden hinta ei muuttuisi), joka sitten myydään markkinoilla, mikä tasapainottaa kysynnän ja tarjonnan. Huomaa, että tämä on ihanteellinen skenaario, jossa indeksin haltijat reagoivat nopeasti palautemekanismiin. Käytännössä (ja erityisesti julkaisun alkupäivinä) odotamme viivettä mekanismin käynnistymisen ja todellisten tulosten välillä liikkeeseen lasketun velan määrässä ja myöhemmin markkinahinnassa.

Toisaalta skenaariossa kaksi, jos indeksin markkinahinta on alempi kuin lunastushinta, korko muuttuu positiiviseksi ja alkaa hinnoitella uudelleen koko velkaa niin, että se tulee kalliimmaksi.

Kun velka tulee kalliimmaksi, kaikkien SAFE:iden vakuussuhteet laskevat (täten SAFE:n luojia kannustetaan maksamaan takaisin velkansa) ja käyttäjät alkavat hamstrata indeksejä odottaen niiden arvon nousevan.



## Palautemekanismin algoritmi

Seuraavassa skenaariossa oletetaan, että protokolla käyttää suhteellista integraaliohjainta lunastussuhteen laskemiseen:

- Refleksiindeksi käynnistetään mielivaltaisella lunastushinnalla "rand"
- Jossain vaiheessa indeksin markkinahinta nousee "randista" arvoon "rand" + x. Kun palautemekanismi lukee uuden markkinahinnan, se laskee suhteellisen termin, joka tässä tapauksessa on  $-1 * ((\text{'rand'} + x) / \text{'rand'})$ . Suhteellinen on negatiivinen lunastushinnan alentamiseksi ja puolestaan indeksien uudelleenhinnoitteluksi siten, että ne tulevat halvemmiksi
- Suhteellisen laskemisen jälkeen mekanismi määrittää integraaliterminminä lisäämällä kaikki aiemmat poikkeamat edellisestäpoikkeamavälisekuntia



- Mekanismi summaa suhteellisen ja integraalin ja laskee sekuntikohtaisen lunastusprosentinrjoka alkaa hitaasti laskea lunastushintaa. Kun SAFEn tekijät ymmärtävät, että he voivat saada lisää velkaa, he tulvivat markkinoille lisää indeksejä
- jälkeenn sekuntia, mekanismi havaitsee, että markkina- ja lunastushinnan välinen poikkeama on mitätön (tietyn parametrin alla melua). Tässä vaiheessa algoritmi asettaa r:n nollaan ja pitää lunastushinnan siellä, missä se on

Käytännössä algoritmi tulee olemaan robustimpi ja joko teemme joistakin muuttujista muuttumattomia (esim.meluaparametri,poikkeamaväli) tai siinä on tiukat rajat sille, mitä hallinto voi muuttaa.

## Palautemekanismin viritys

Äärimmäisen tärkeää refleksiindeksijärjestelmän moitteettoman toiminnan kannalta on algoritmisen ohjaimen parametrien viritys. Virheellinen parametointi voi johtaa siihen, että järjestelmä on liian hidas saavuttamaan vakautta, ylittämään massiivisesti tai olemaan yleisesti epävakaa ulkoisten iskujen edessä.

PID-säätimen vitysprosessiin kuuluu tyypillisesti reaaliaikaisen järjestelmän käyttäminen, vitysparemetrien säätäminen ja järjestelmän vasteen tarkkailu, usein tarkoituksellisesti aiheuttamalla iskuja matkan varrella. Kun otetaan huomioon live-refleksiindeksijärjestelmän parametrien säätämisen vaikeus ja taloudellinen riski, aiomme hyödyntää tietokonemallinnusta ja simulointia mahdollisimman paljon alkuparametrien asettamiseksi, mutta sallimme myös hallinnon päivittää vitysparemetrit, jos tuotannosta saadaan lisätietoa. osoittaa, että ne eivät ole optimaalisia.

## Rahamarkkinoiden asettaja

RAI:ssa aiomme pitää lainakoron (indeksejä luotaessa käytetty korko) kiinteänä tai rajoitettuna ja vain muokata lunastushintaa, mikä minimoi palautemekanismin mallintamisen monimutkaisuuden. Meidän tapauksessamme lainakorko on yhtä suuri kuin vakauspalkkion ja DSR:n välinen ero Multi-Collateral DAI:ssa.

Vaikka aiomme pitää lainakoron kiinteänä, sitä on mahdollista muuttaa lunastushinnan rinnalla rahamarkkinoiden asettajalla. Rahamarkkinat muuttavat lainakorkoa ja lunastushintaa tavalla, joka kannustaa SAFE:n tekijöitä luomaan enemmän tai vähemmän velkaa. Jos indeksin markkinahinta on lunastuksen yläpuolella, molemmat korot alkavat laskea, kun taas jos se on lunastuksen alapuolella,

hinnat nousevat.

Globaali selvitys on viimeinen keino, jolla taataan lunastushinta kaikille refleksi-indeksin haltijoille. Se on tarkoitettu antamaan sekä refleksiindeksin haltijat että SAFE:n luoja lunastaa järjestelmävakuudet sen nettoarvolla (indeksien määrä kutakin vakuustyyppiä kohti viimeisimmän lunastushinnan mukaan). Kuka tahansa voi käynnistää selvityksen poltettuaan tietyn määrän protokollatunnuksia.

Sovittelussa on kolme päävaihetta:

- **Laukaista** : selvitys käynnistyy, käyttäjät eivät voi enää luoda kassakaappeja, kaikki vakuuksien hintasyötteet ja lunastushinta jäädytetään ja kirjataan
- **Prosessi** : käsittelee kaikki käynnissä olevat huutokaupat
- **Väite** : jokainen refleksi-indeksin haltija ja SAFEn luoja voi vaatia kiinteän määrän mistä tahansa järjestelmävakuudesta indeksin viimeisimmän kirjatun lunastushinnan perusteella

## Hallinto

Suurin osa parametreista on muuttumattomia, ja sisäinen älykäs sopimusmekaniikka ei ole päivitettävissä, elleivät hallintotunnuksen haltijat ota käyttöön täysin uutta järjestelmää. Valitsimme tämän strategian, koska voimme eliminoida metapelin, jossa ihmiset yrittävät vaikuttaa hallintoprosessiin omaksi edukseen, mikä vahingoittaa luottamusta järjestelmään. Varmistamme protokollan oikean toiminnan luottamatta liikaa ihmisiin ("bitcoin-ilmio"), jotta maksimoimme sosiaalisen skaalautuvuuden ja minimoimme riskit muille kehittäjille, jotka haluavat käyttää RAI:ta ydininfrastruktuurina omissa projekteissaan.

Niille muutamille parametreille, joita voidaan muuttaa, ehdotamme rajoitetun hallinnan moduulin lisäämistä, jonka tarkoituksena on viivyttää tai rajoittaa kaikkia mahdollisia järjestelmän muutoksia. Lisäksi esittelemme Governance Ice Age -käyttöoikeusrekisterin, joka voi lukita osan järjestelmän osista ulkopuolelta tiettyjen määräaikojen umpeuduttua.

## Aikarajallinen hallinto

Aikarajallinen hallinto on rajoitetun hallinnon moduulin ensimmäinen osa. Se asettaa aikaviiveet samaan parametriin tehtyjen muutosten välillä. Esimerkkinä on mahdollisuus muuttaa Oracle Network Medianizerissa (osio 6.2) käytettyjen

oraakkeliin osoitteita vähintään Ts sekuntia on kulunut viimeisestä oraakkeliinmuutoksesta.

## Toimintarajoitettu hallinto

Rajoitetun hallinnon moduulin toinen osa on Action Bounded Governance. Jokaisella säädettävällä parametrilla on rajat sille, mihin arvoihin se voidaan asettaa ja kuinka paljon se voi muuttua tietyn ajanjakson aikana. Merkittäviä esimerkkejä ovat Lunastuskoron palautemekanismin (osio 4.2) alkuperäiset versiot, joita hallintotunnuksen haltijat voivat hienosäätää.

## Hallinto jääkausi

Ice Age on muuttumaton älykäs sopimus, joka asettaa määraaikoja tiettyjen järjestelmäparametrien muuttamiselle ja protokollan päivittämiselle. Sitä voidaan käyttää tapauksissa, joissa hallinto haluaa varmistaa, että he voivat korjata virheet ennen kuin protokolla lukitsee itsensä ja estää ulkopuolisen puuttumisen. Ice Age tarkistaa, onko muutos sallittu, tarkistamalla parametrin nimen ja vaikutuksen kohteena olevan sopimuksen osoitteen määraaikojen rekisteristä. Jos määraaika on umpeutunut, puhelu palaa.

Hallinto saattaa viivyttää jääkautta tietyn määrän kertoja, jos vikoja löydetään lähellä päivämäärää, jolloin protokollan pitäisi alkaa lukita itseään. Esimerkiksi Ice Agea voidaan lykätä vain kolme kertaa, joka kerta kuukauden ajan, jotta äskettäin käyttöön otetut virhekorjaukset testataan kunnolla.

## Ydinalueet, joilla hallintoa tarvitaan

Näemme neljä aluetta, joilla hallintoa saatetaan tarvita, erityisesti tämän kehyksen varhaisissa versioissa:

- **Uusien vakuustyyppien lisääminen** : RAI:ta tukee vain ETH, mutta muiden indeksien taustalla on useita vakuuksia, ja hallinto voi hajauttaa riskiä ajan mittaan
- **Ulkoisten riippuvuuksien muuttaminen** : Oraakkelit ja DEX:t, joista järjestelmä riippuu, voidaan päivittää. Hallinto voi osoittaa järjestelmän uudemmille riippuvuuksille, jotta se voi jatkaa toimintaansa kunnolla

- **Hienosäätökorkoasetukset** : varhaisilla rahapolitiikan valvojiilla on parametreja, joita voidaan muuttaa kohtuullisissa rajoissa (kuten Action and Time Bounded Governance kuvailee)
- **Siirtyminen järjestelmäversioiden välillä**: joissakin tapauksissa hallinto voi ottaa käyttöön uuden järjestelmän, antaa sille luvan tulostaa protokollatunnuksia ja poistaa tämän luvan vanhasta järjestelmästä. Tämä siirto suoritetaan alla kuvatun Restricted Migration Module -moduulin avulla **Rajoitettu siirtomoduuli**

Seuraava on yksinkertainen mekanismi siirtymiseen järjestelmäversioiden välillä:

- Käytössä on siirtorekisteri, joka seuraa kuinka monta eri järjestelmää sama protokollatunnus kattaa ja miltä järjestelmästä voidaan evätä lupa tulostaa protokollatunnisteita velkahuutokaupassa.
- Aina kun hallinto ottaa käyttöön uuden järjestelmäversion, he lähettävät järjestelmän velkahuutokauppasopimuksen osoitteen siirtorekisteriin. Hallinnon on myös määritettävä, pystyvätkö he koskaan estämään järjestelmää tulostamasta protokollatunnuksia. Hallinto voi myös milloin tahansa sanoa, että yksi järjestelmä pystyy aina tulostamaan tunnuksia, joten sitä ei koskaan siirretä
- Uuden järjestelmän ehdottamisen ja vanhan järjestelmän lupien peruuttamisen välillä on jäähtymisjakso
- Valinnainen sopimus voidaan määrittää niin, että se sammuttaa automaattisesti vanhan järjestelmän, kun siltä evätään tulostusoikeudet

Migraatiomoduuili voidaan yhdistää Ice Ageen, joka antaa tietyille järjestelmille automaattisesti luvan tulostaa aina rahakkeita.  
Automaattinen järjestelmän sammutus

Joissakin tapauksissa järjestelmä voi havaita automaattisesti ja laukaista selvityksen ilman tarvetta polttaa protokollatunnuksia:

- **Vakavat hintasyötteen viivästykset** : järjestelmä havaitsee, että yhtä tai useampaa vakuus- tai indeksihintasyötteistä ei ole päivitetty pitkään aikaan

- **Järjestelmän siirto** : tämä on valinnainen sopimus, joka voi sulkea protokollan sen jälkeen, kun jäähdytysjakso on kulunut siitä hetkestä, kun hallinto poistaa velkahuutokauppamekanismilta mahdollisuuden tulostaa protokollatunnuksia (rajoitettu siirtomoduuli, osio 5.4.1)
- **Yhdenmukainen markkinahinnan poikkeama** : järjestelmä havaitsee, että indeksin markkinahinta on ollut  $x\%$  poikkesi pitkään lunastushintaan verrattuna

Hallinto pystyy päivittämään näitä autonomisia sammutusmoduuleja, vaikka ne ovat edelleen rajoitettuja tai kunnes jääkausi alkaa lukita joitakin järjestelmän osia.

## Oraakkelit

Järjestelmän on luettava hintasyötteitä kolmella pääasiallisella omaisuustyyppillä: indeksi, protokollatunnus ja jokainen sallittujen luetteloon lisätty vakuustyyppi. Hintasyötteitä voivat tarjota hallintojohtoiset oraakkelit tai jo perustetut oraakkeliverkostot.

## Hallinto johti Oraakkeleita

Hallintotunnuksen haltijat tai protokollan käynnistänyt ydintiimi voivat tehdä yhteistyötä muiden tahojen kanssa, jotka keräävät useita hintasyötteitä ketjun ulkopuolelta ja lähettävät sitten yhden tapahtuman älykkäälle sopimukselle, joka medianisoi kaikki datapisteet.

Tämä lähestymistapa mahdollistaa enemmän joustavuutta oraakkelin infrastruktuurin päivittämisessä ja muuttamisessa, vaikka se tuleekin luottamattomuuden kustannuksella.

## Oracle Network Medianizer

Oracle-verkkomedianisaattori on älykäs sopimus, joka lukee hinnat useista lähteistä, joita hallinto ei suoraan hallitse (esim. Uniswap V2 -pooli indeksivakuustyyppin ja muiden stabiilien kolikoiden välillä) ja medianisoi sitten kaikki tulokset. ONM toimii seuraavasti:

- Sopimuksemme pitää kirjaa sallittujen listalla olevista oraakkeliverkoista, joihin se voi soittaa pyytääkseen vakuushintoja. Sopimus rahoitetaan osalla järjestelmän kertyneestä ylijäämästä (käyttämällä Ylijäämäkassaa, kohta 11). Jokainen oraakkeliverkko hyväksyy maksuna tiettyjä tokeneita, joten sopimuksemme pitää kirjaa myös kunkin pyynnön vähimmäismäärästä ja tokenien tyypistä.

- Uuden hintasyötteen työntämiseksi järjestelmään kaikki oraakkelit on kutsuttava etukäteen. Oraakkelille soittaessa sopimus vaihtaa ensin joitakin vakausmaksuja jollakin oraakkelin hyväksymästä rahakkeesta. Kun oraakkeli on kutsuttu, sopimus merkitsee kutsun "päteväksi" tai "epäkelpoiseksi". Jos kutsu on virheellinen, tiettyä viallista oraakkelia ei voida kutsua uudelleen ennen kuin kaikki muut on kutsuttu ja sopimus tarkistaa, onko kelvollinen enemmistö. Kelvollinen oraakkeli puhelu ei saa palata, ja sen on haettava hinta, joka on julkaistu ketjussa joskus viime msekuntia. "Hae" tarkoittaa eri asioita kunkin oraakkeli tyyppin mukaan:

☐ Vetopohjaisista oraakkeleista, joista saamme tuloksen heti, sopimuksemme on maksettava maksu ja noudettava hinta suoraan

☐ Työntöpohjaisista oraakkeleista sopimuksemme maksaa maksun, soittaa oraakkelille ja odottaa tietyn ajann ennen kuin soitat uudelleen oraakkelille saadakseen pyydetyn hinnan

- Jokainen oraakkelin tulos tallennetaan taulukkoon. Kun jokainen sallittujen luetteloon merkitty oraakkeli on kutsuttu ja jos taulukossa on tarpeeksi kelvollisia datapisteitä muodostamaan enemmistön (esim. sopimus sai kelvollista dataa 3/5 oraakkeleilta), tulokset lajitellaan ja sopimus valitsee mediaanin.

- Saako sopimus enemmistön tai ei, oraakkelin tulosten joukko tyhjennetään ja sopimusta on odotettava p sekuntia ennen kuin aloitat koko prosessin alusta

## Oracle Network Backup

Hallinto voi lisätä varaoraakkelivaihtoehtoon, joka alkaa nostaa hintoja järjestelmään, jos medianaattori ei löydä suurinta osaa kelvollisista oraakkeliverkoista useita kertoja peräkkäin.

Varavaihtoehto on asetettava, kun medianizer otetaan käyttöön, koska sitä ei voi muuttaa jälkikäteen. Lisäksi erillisellä sopimuksella voidaan valvoa, jos varmuuskopio on korvannut mediaanimekanismin liian kauan, ja sammuttaa protokollan automaattisesti.

Kassakaapit

Indeksien luomiseksi kuka tahansa voi tallettaa ja hyödyntää kryptovakuustaan kassakaapeissa. Kun SAFE avataan, se jatkaa velan kertymistä talletetun

vakuuden lainakoron mukaisesti. Kun SAFEn luoja maksaa takaisin velkansa, he voivat nostaa yhä enemmän lukittuja vakuuksiaan.

#### TURVALLINEN elinkaari

Refleksiindeksien luomiseen ja sen jälkeen SAFEn velan takaisinmaksuun tarvitaan neljä päävaihetta:

- Talleta vakuudet kassakaappiin

Käyttäjän on ensin luotava uusi SAFE ja talletettava siihen vakuus.

- Luo indeksejä SAFE:n vakuuksilla

Käyttäjä määrittää kuinka monta indeksiä hän haluaa luoda.

Järjestelmä luo saman verran velkaa, joka alkaa kertyä vakuuden lainakoron mukaan.

- Maksa takaisin TURVALLINEN velka

Kun SAFEn luoja haluaa nostaa vakuuksiensa, hänen on maksettava takaisin alkuperäinen velkansa ja kertyneet korot.

- Nosta vakuudet

Kun käyttäjä on maksanut takaisin osan tai kaikki velkansa, hän voi nostaa vakuuksiensa.

#### TURVALLINEN selvitystila

Jotta järjestelmä pysyisi maksukykyisenä ja kattaisi koko velan arvon, jokainen SAFE voidaan likvidoida, jos sen vakuussuhde laskee tietyn kynnyksen alle. Kuka tahansa voi käynnistää selvitystilan, jolloin järjestelmä takavarikoi kassakaapin vakuudet ja myy sen pois vakuushuutokauppa.

### Selvitystilavakuutus

Yhdessä järjestelmän versiossa SAFEn tekijöillä voi olla mahdollisuus valita laukaista kun heidän kassakaappinsa likvidoidaan. Triggerit ovat älykkäitä sopimuksia, jotka lisäävät automaattisesti lisää vakuuksia SAFE:hen ja mahdollisesti säästävät sen selvitystilaan. Esimerkkejä laukaisimista ovat sopimukset, jotka myyvät lyhyitä positioita tai sopimukset, jotka kommunikoivat vakuutusprotokollien, kuten Nexus Mutual [6], kanssa.

Toinen tapa suojata SAFE:ita on lisätä kaksi erilaista vakuuskynnystä: turvallinen jariski. SAFE-käyttäjät voivat luoda velkaa, kunnes saavuttavat turvallisen kynnyksen (joka on suurempi kuin riski), ja heidät realisoidaan vain, kun SAFE:n vakuudet alittavat riskirajan.

## Vakuutushuutokaupat

Vakuushuutokaupan aloittamiseksi järjestelmän on käytettävä muuttujaa nimeltä likvidaatio Määrä jokaisessa huutokaupassa katettavan velan määrän ja sitä vastaavan myytävien vakuuksien määrittämiseksi. Alikvidaatiosakko sovelletaan jokaiseen huutokaupattavaan SAFE:iin.

## Vakuushuutokaupan parametrit

Parametrin nimi	Kuvaus
minimiBid	Tarvittava vähimmäismäärä kolikoita tarjotaan yhdessä tarjouksessa
alennus	Alennus, jolla vakuus myydään
alempiCollateralMediaanipoikkeama	Suurin alarajapoikkeama, johon vakuuden mediaanilla voi olla verrattuna oraakkelin hinta
ylempiCollateralMediaanipoikkeama	Suurin ylärajan poikkeama, johon vakuuden mediaani voi olla verrattuna oraakkelin hinta
LowSystemCoinMedianDeviation	Suurin alarajapoikkeama, joka järjestelmäkolikon oraakkelin hintasyötteellä voi olla verrattuna järjestelmän kolikon oraakkeliin hinta
yläjärjestelmäCoinMedianDeviation	Suurin ylärajan poikkeama, johon vakuuden mediaani voi olla verrattuna järjestelmän kolikon oraakkelin hinta
minSystemCoinMedianDeviation	Järjestelmäkolikon vähimmäispoikkeama mediaanitulos verrattuna lunastushintaan, jotta voidaan ottaa mediaani huomioon

## Vakuutushuutokauppamekanismi

Kiinteän alennushuutokauppa on suoraviivainen tapa (verrattuna englantilaisiin huutokauppoihin) saattaa vakuudet myyntiin vastineeksi luottotappioiden maksamiseen



käytetyistä järjestelmäkolikoista. Tarjoajien on vain sallittava huutokauppakamarin siirtää omat `safeEngine.coinBalance` ja voi sitten soittaa `ostaa vakuuksia vaihtaakseen` ne järjestelmäkolikot vakuuksille, jotka myydään alennuksella viimeisimpään markkinahintaan verrattuna.

Tarjoajat voivat myös tarkistaa tietystä huutokaupasta saamiensa vakuuksien määrän soittamalla `getCollateralBought` tai. Ota `getApproximateCollateralBought` huomioon, että `getCollateralBought` ei ole merkitty näkymäksi, koska se lukee (ja myös päivittää) `lunastushinta oraakkelivälitteestä`, kun taas `getApproximateCollateralBought` käyttää `lastReadRedemptionPrice`.

## Velkahuutokaupat

Skenaariossa, jossa vakuushuutokauppa ei voi kattaa kaikkia SAFE:n luottotappioita ja jos järjestelmässä ei ole ylimääräisiä varauksia, kuka tahansa voi käynnistää velkahuutokaupan.

Velkahuutokauppojen tarkoituksena on lyödä lisää protokollatokeneita (kohta 10) ja myydä niitä indekseillä, jotka voivat mitätöidä järjestelmän jäljellä olevat luottotappiot.

Velkahuutokaupan aloittamiseksi järjestelmän on käytettävä kahta parametria:

- `originalDebtAuctionAmount` : lyötyjen protokollamerkkien alkuperäinen määrä huutokaupan jälkeen
- `velkaAuctionBidSize` : alkuperäinen tarjouksen koko (kuinka monessa indeksissä on tarjottava vaihtaa vastaan `originalDebtAuctionAmount` protokollatunnukset)

## Itsenäisen velkahuutokaupan parametriasetus

Velkahuutokaupassa lyötyjen protokollamerkkien alkuperäinen määrä voidaan asettaa joko hallintoäänestyksellä tai järjestelmä voi säätää sitä automaattisesti. Automaattinen versio olisi integroitava oraakkeleihin (kohta 6), josta järjestelmä lukisi protokollatunnuksen ja refleksiindeksin markkinahinnat. Tämän jälkeen järjestelmä asettaisi protokollatunnusteiden alkuperäisen määrän ( `originalDebtAuctionAmount` ), joka lyödään hintaan `velkaAuctionBidSize` indeksiin. `originalDebtAuctionAmount` voidaan asettaa alennukseen verrattuna todelliseen PÖYTÄKIRJA/INDEKSI-markkinahintaan tarjousten kannustamiseksi.

## Velkahuutokaupan parametrit

Parametrin nimi	Kuvaus
	Protokollan määrän lisääminen

määräSoldNouse	rahakkeita lyödään samaa varten indeksien määrä
tarjousPienennä	Seuraavan tarjouksen vähimmäislasku protokollatunnusten hyväksytyssä määrässä saman verran indeksejä
tarjouksen kesto	Kuinka kauan tarjous kestää uuden jälkeen tarjous on jätetty (sekunneissa)
TotalAuctionLength	Huutokaupan kokonaiskesto (sekunteina)
huutokaupat alkaneet	Kuinka monta huutokauppaa on alkanut asti nyt

## Velkahuutokauppamekanismi

Toisin kuin vakuushuutokaupoissa, velkahuutokaupoissa on vain yksi vaihe:

```
: pienentääSoldAmount(uint-tunnus, uint-ostettava summa, uint-hinta) vähennä määrää
                                                                protokollatunnukset
```

hyväksytään vastineeksi kiinteästä määrästä indeksejä.

Huutokauppa aloitetaan uudelleen, jos sille ei ole tehty tarjouksia. Joka kerta kun se käynnistyy uudelleen, järjestelmä tarjoaa lisää protokollatunnuksia samalle määrälle indeksejä. Uuden protokollan tunnuksen määrä lasketaan viimeinen TokenAmount \*määräSoldNouse / 100. Huutokaupan ratkettua järjestelmä lyö rahakkeita eniten tarjoavalle.

## Protokollamerkit

Kuten aiemmissa osissa kuvattiin, jokainen protokolla on suojattava velkahuutokaupoissa lyödyllä tunnuksella. Suojauksen lisäksi merkkiä käytetään muutamien järjestelmän komponenttien hallitsemiseen. Myös protokollamerkkien tarjontaa vähennetään asteittain käyttämällä ylijäämahuutokauppoja. Ylijäämän määrää, jonka on kerryttävä järjestelmään ennen kuin ylimääräiset varat huutokaupataan, kutsutaan ylijäämäpuskuri ja se mukautuu automaattisesti prosenttiosuutena liikkeeseen lasketusta kokonaisvelasta.

## Vakuutusrahasto

Protokollamerkin lisäksi hallinto voi luoda vakuutusrahaston, jolla on laaja valikoima korreloimattomia varoja ja jota voidaan käyttää velkahuutokauppojen suojana.

## Ylijäämähuutokaupat

Ylijäämähuutokaupat myyvät järjestelmään kertyneet vakaumaksut protokollatunnuksista, jotka sitten poltetaan.

### Ylijäämähuutokaupan parametrit

Parametrin nimi	Kuvaus
bidNosta	Minimikorotus seuraavassa tarjouksessa
tarjouksen kesto	Kuinka kauan huutokauppa kestää uuden jälkeen tarjous on jätetty (sekunneissa)
TotalAuctionLength	Huutokaupan kokonaiskesto (sekunteina)
huutokaupat alkaneet	Kuinka monta huutokauppaa on alkanut asti nyt

### Ylijäämähuutokauppamekanismi

Ylijäämähuutokaupoissa on yksi vaihe: `nostaBidSize(uint-tunnus, uint-ostettava summa, uint-hinta)` : kuka tahansa voi tarjota suuremman summan protokollatokeneita samalle määrälle indeksejä (yliäämä). Jokaisen uuden tarjouksen on oltava suurempi tai yhtä suuri kuin viimeinen tarjous\*bidNosta/100. Huutokauppa päättyy maksimiajan jälkeen TotalAuctionLength sekuntia tai sen jälkeentarjouksen kestosekuntia on kulunut viimeisimmästä tarjouksesta, eikä uusia tarjouksia ole tällä välin jätetty.

Huutokauppa alkaa uudelleen, jos sillä ei ole tarjouksia. Toisaalta, jos huutokaupassa on vähintään yksi tarjous, järjestelmä tarjoaa yliäämän eniten tarjoavalle ja polttaa sitten kaikki kerätyt protokollamerkit.

## Ylijäämäindeksien hallinta

Joka kerta kun käyttäjä luo indeksejä ja luo implisiittisesti velkaa, järjestelmä alkaa soveltaa lainakorkoa käyttäjän SAFE:hen. Kertyneet korot yhdistetään kahteen eri älykkääseen sopimukseen:

- Thekirjanpitomoottorikäytetään velan (9.2 jakso) ja yliäämän (jakso 10.1) huutokaupat

- The ylijäämäinen kassa käytetään rahoittamaan ydininfrastruktuurin komponentteja ja kannustamaan ulkopuolisia toimijoita ylläpitämään järjestelmää

Ylijäämärahasto vastaa kolmen järjestelmän ydinosan rahoituksesta:

- Oracle-moduuli (osio 6). Riippuen siitä, kuinka oraakkeli on rakentunut, valtiovarainministeriö joko maksaa hallinnointivaltuutetuille, ketjun ulkopuolisille oraakkeleille tai se maksaa puheluista oraakkeliverkkoihin. Kassa voidaan myös perustaa maksamaan kaasua käyttäneille osoitteille soittamaan oraakkelille ja päivittämään se
- Joissakin tapauksissa itsenäisiä tiimejä, jotka ylläpitävät järjestelmää. Esimerkkejä ovat tiimit, jotka sallivat uusia vakuustyypppejä tai hienosäätävät järjestelmän koron asettajaa (osio 4.2).

Rahasto voidaan perustaa siten, että osa ylijäämäsaajista evätään automaattisesti jatkossa ja toiset voivat tulla tilalle.

Ulkopuoliset näyttelijät

Järjestelmä on riippuvainen ulkoisista toimijoista toimiakseen kunnolla. Näitä toimijoita kannustetaan taloudellisesti osallistumaan esimerkiksi huutokauppoihin, globaaleihin selvitysten käsittelyyn, markkinatakaukseen ja hintasyötteiden päivittämiseen järjestelmän kunnon ylläpitämiseksi.

Tarjoamme alustavat käyttöliittymät ja automaattiset komentosarjat, jotta mahdollisimman monet ihmiset voivat pitää protokollan suojattuna.

Osoitteelliset markkinat

Näemme RAI:n hyödyllisenä kahdella pääalueella:

- **Portfolion monipuolistaminen** : sijoittajat käyttävät RAI:ta saadakseen vaimennetun altistuksen ETH:n kaltaiselle omaisuudelle ilman koko riskiä eetterin omistamisesta.
- **Synteettisten omaisuuserien vakuudet** : RAI voi tarjota protokollille, kuten UMA, MakerDAO ja Synthetix pienemmän altistumisen kryptomarkkinoille ja antaa käyttäjille enemmän aikaa poistua positioistaan sellaisissa skenaarioissa kuin musta torstai

## Tulevaisuuden tutkimus

Työntääksemme hajautetun rahan rajoja ja tuodaksemme lisää innovaatioita hajautettuun rahoitukseen jatkamme vaihtoehtojen etsimistä ydinalueilta, kuten hallinnon minimointi- ja likvidaatiomekanismit.

Ensinnäkin haluamme luoda pohjan tuleville standardeille, jotka liittyvät protokollien ympärille, jotka lukitsevat itsensä ulkopuoliselta hallitukselta, ja todellisille "raharoboteille", jotka mukautuvat markkinavoimiin. Tämän jälkeen kutsumme Ethereum-yhteisön keskustelemaan ja suunnittelemaan parannuksia ehdotuksiimme keskittyen erityisesti vakuus- ja velkahuutokauppoihin.

## Riskit ja lieventäminen

Refleksiindeksin sekä myöhempien päälle rakennettujen järjestelmien kehittämiseen ja käynnistämiseen liittyy useita riskejä:

- **Älykkäät sopimusvirheet** : suurin järjestelmälle aiheutuva riski on virheen mahdollisuus, joka antaa kenen tahansa poimia kaikki vakuudet tai lukitsee protokollan tilaan, josta se ei voi toipua. Suunnittelemme, että useat tietoturvatutkijat tarkistavat koodimme ja julkaisemme järjestelmän testiverkkoon ennen kuin sitoudumme ottamaan sen käyttöön tuotannossa
- **Oracle vika** : yhdistämme syötteitä useista oraakkeliiverkoista ja vain yhden oraakkelin päivittämiseksi tulee tiukat säännöt kerrallaan, jotta haitallinen hallinto ei voi helposti ottaa käyttöön vääriä hintoja
- **Mukana olevat musta joutsentapahtumat** : taustalla oleviin vakuuksiin on olemassa musta joutsentapahtuman riski, joka voi johtaa suureen määrään likvidoitavia kassakaappeja. Likvidaatiot eivät välttämättä pysty kattamaan koko luottotappiota, joten järjestelmä muuttaa jatkuvasti ylijäämäpuskuriaan kattaakseen kohtuullisen määrän liikkeeseen laskettua velkaa ja kestääkseen markkinasokkeja.
- **Virheelliset nopeuden asettimen parametrit** : autonomiset takaisinkytkentämekanismit ovat erittäin kokeellisia eivätkä välttämättä toimi täsmälleen kuten ennustamme simulaatioiden aikana. Aiomme antaa hallinnon hienosäätää tätä komponenttia (samalla kun se on edelleen rajoitettu) odottamattomien skenaarioiden välttämiseksi

## ● **Epäonnistuminen terveiden selvitysmiesmarkkinoiden käynnistämisessä** : Selvittäjät ovat tärkeitä

toimijoita, jotka varmistavat, että kaikki liikkeeseen lasketut velat on katettu vakuuksilla.

Suunnittelemme luovamme käyttöliittymiä ja automatisoituja skriptejä, jotta mahdollisimman monet ihmiset voivat osallistua järjestelmän turvallisuuteen.

## Yhteenveto

Olemme ehdottaneet protokollaa, joka asteittain lukitsee itsensä ihmisen hallinnasta ja antaa alhaisen volatilitiitin, vakuudellisen omaisuuden, jota kutsutaan refleksiindeksiksi. Esittelimme ensin itsenäisen mekanismin, jolla on tarkoitus vaikuttaa indeksin markkinahintaan, ja sitten kuvailimme, kuinka useat älykkäät sopimukset voivat rajoittaa merkinhaltijoiden valtaa järjestelmään. Esittelimme omavaraisen järjestelmän useiden riippumattomien oraakkeliverkostojen hintasyötteiden mediaanisoimiseksi ja esittelimme lopuksi yleisen mekanismin indeksien lyömiseen ja SAFE:iden likvidoimiseen.

# Viitteet

- [1] "Maker Protocol: MakerDAO's Multi Collateral Dai (MCD) System", <https://bit.ly/2YL5S6j>
- [2] "UMA: Hajautettu rahoitussopimusjärjestelmä", <https://bit.ly/2Wgx7E1>
- [3] Synthetix Litepaper, <https://bit.ly/2SNHxZO>
- [4] KJ Åström, RM Murray, Feedback Systems: An Introduction for Scientists and Engineers, <https://bit.ly/3bHwnMC>
- [5] RJ Hawkins, JK Speakes, DE Hamilton, "Moetary Policy and PID Control", <https://bit.ly/2TeQZFO>
- [6] H. Karp, R. Melbardis, "Peer-to-peer harkinnanvarainen keskinäinen Ethereumlohkoketjussa", <https://bit.ly/3du8TMy>
- [7] H. Adams, N. Zinsmeister, D. Robinson, "Uniswap V2 Core", <https://bit.ly/3dqzNEU>

## Sanasto

**Refleksiindeksi** : vakuudellinen omaisuususerä, joka vaimentaa kohde-etuuden volatilitteettia

**RAI** : ensimmäinen refleksiindeksimme

**Lunastushinta** : hinta, jonka järjestelmä haluaa indeksillä olevan. Se muuttuu lunastuskurssin (laskeman  $RRFM:n$ ) vaikutuksesta, jos markkinahinta ei ole lähellä sitä. Tarkoituksena on vaikuttaa SAFEn sisällöntuottajiin tuottamaan enemmän tai maksamaan takaisin osan veloistaan

**Lainakorko** : vuotuinen korko, jota sovelletaan kaikkiin SAFE:ihin, joilla on velkaa

**Lunastuskoron palautemekanismi (RRFM)** : itsenäinen mekanismi, joka vertaa refleksiindeksin markkina- ja lunastushintoja ja laskee sitten lunastusprosentin, joka hitaasti vaikuttaa SAFE:n luojiin luomaan enemmän tai vähemmän velkaa (ja implisiittisesti yrittää minimoida markkina-/lunastushinnan poikkeaman)

**Rahamarkkinoiden asettaja (MMS)** : RRFM:n kaltainen mekanismi, joka vetää useita rahavipuja kerralla. Refleksiindeksien tapauksessa se muuttaa sekä lainakorkoa että lunastushintaa

**Oracle Network Medianizer (ONM)** : älykäs sopimus, joka hakee hinnat useista oraakkeli-verkoista (jotka eivät ole hallinnon hallinnassa) ja medianisoivat ne, jos enemmistö (esim. 3 viidestä) palautti tuloksen heittämättä

**Rajoitettu hallintomoduuli (RGM)**: joukko älykkäitä sopimuksia, jotka rajoittavat hallinnointitokenien haltijoiden valtaa järjestelmään. Se joko pakottaa aikaviiveet tai rajoittaa mahdollisuuksia, joita hallinnon on asetettava tiettyjä parametreja

**Hallinto jääkausi** : muuttumaton sopimus, joka lukitsee useimmat protokollan komponentit ulkopuoliselta puuttumiselta tietyn määräajan jälkeen

**Kirjanpito moottori** : järjestelmäkomponentti, joka käynnistää velka- ja ylijäämähuutokaupat. Se myös pitää kirjaa tällä hetkellä huutokaupattujen velkojen, toimittamattomien luottotappioiden ja ylijäämäpuskurin määrästä

**Ylimääräinen puskur** : koron määrä, joka kertyy ja säilytetään järjestelmässä. Kaikenlaista kiinnostusta tämän kynnyksen yli kertyneet myydään ylijäämähuutokaupoissa, jotka polttavat protokollatunnuksia

**Ylijäämä valtiovarainministeriö** : sopimus, joka antaa eri järjestelmämoduuleille luvan nostaa kertynyttä korkoa (esim. ONM oracle-puheluille)