Rai: A Low Volatility, Trust Minimized Collateral for the DeFi Ecosystem

Stefan C. Ionescu, Ameen Soleimani

May 2020

Abstract. We present a governance minimized, decentralized protocol that automatically reacts to market forces in order to modify the target value of its native collateralized asset. The protocol allows anyone to leverage their crypto assets and issue a “reflex index” which is a dampened version of its underlying collateral. We outline how indexes can be useful as universal, low volatility collateral which can protect its holders, as well as other decentralized finance protocols, from sudden market shifts. We present our plans to help other teams launch their own synthetics by leveraging our infrastructure. Finally, we offer alternatives to current oracle and governance structures that are often found in many DeFi protocols.

Rai: Isang Mababang Volatility, Pinaliit ang Tiwala

Collateral para sa DeFi Ecosystem

Stefan C. Ionescu, Ameen Soleimani

Mayo 2020

Abstract. Nagpapakita kami ng pinaliit na pamamahala, desentralisadong protocol na awtomatikong tumutugon sa mga puwersa ng merkado upang mabago ang target na halaga ng katutubong collateralized na asset nito. Ang protocol ay nagbibigay-daan sa sinuman na gamitin ang kanilang mga crypto asset at mag-isyu ng "reflex index" na isang dampened na bersyon ng pinagbabatayan nitong collateral. Binabalangkas namin kung paano maaaring maging kapaki-pakinabang ang mga index bilang unibersal, mababang volatility collateral na maaaring maprotektahan ang mga may hawak nito, pati na rin ang iba pang mga desentralisadong protocol sa pananalapi, mula sa biglaang pagbabago sa merkado. Ipinakita namin ang aming mga plano upang matulungan ang ibang mga koponan na maglunsad ng sarili nilang mga synthetics sa pamamagitan ng paggamit ng aming imprastraktura. Sa wakas, nag-aalok kami ng mga alternatibo sa kasalukuyang oracle at mga istruktura ng pamamahala na kadalasang makikita sa maraming DeFi protocol.

Mga nilalaman

4.2. Mekanismo ng Feedback sa Rate ng Redemption

4.2.1. Mga bahagi

4.2.2. Mga sitwasyon

4.2.3. Algorithm

4.2.4. Pag-tune

4.3. Setter ng Money Market

4.4. pandaigdigang settlement

5. Pamamahala

5.1. Time Bounded Governance

5.2. Action Bounded Governance

5..3. Panahon ng Yelo ng Pamamahala

5.4. Mga Pangunahing Lugar Kung Saan Kailangan ang Pamamahala

5.4.1. Restricted Migration Module

6. Awtomatikong Pag-shutdown ng System

7. Orakulo

7.1. Mga Oracle na Pinangunahan ng Pamamahala

7.2. Oracle Network Medianizer

7.2.1. Oracle Network Backup

8. Safe

8.1. LIGTAS na Ikot ng Buhay

9. LIGTAS na Pagpuksa

9.1. Collateral Auction

9.1.1. Seguro sa Pagpuksa

9.1.2. Mga Parameter ng Collateral Auction

9.1.3. Collateral Auction Mechanism

9.2. Utang Auction

9.2.1. Setting ng Parameter ng Autonomous Utang Auction

9.2.2. Mga Parameter ng Utang Auction

9.2.3. Mekanismo ng Utang Auction

panimula

Ang pera ay isa sa pinakamakapangyarihang mekanismo ng koordinasyon na ginagamit ng sangkatauhan upang umunlad. Ang pribilehiyong pangasiwaan ang suplay ng pera ay makasaysayang itinago sa mga kamay ng soberanong pamumuno at ng mga piling tao sa pananalapi habang ipinapataw sa isang hindi sinasadyang pangkalahatang publiko. Kung saan ipinakita ng Bitcoin ang potensyal para sa isang grassroots protest upang magpakita ng store-of-value commodity asset, binibigyan tayo ng Ethereum ng platform para bumuo ng assetbacked synthetic na instrumento na maaaring maprotektahan mula sa pagkasumpungin at magamit bilang collateral, o i-pegged sa isang reference na presyo at ginamit bilang medium-of-exchange para sa mga pangaraw-araw na transaksyon, lahat ay ipinapatupad ng parehong mga prinsipyo ng desentralisadong pinagkasunduan.

Ang walang pahintulot na pag-access sa Bitcoin para sa pag-iimbak ng kayamanan at maayos na desentralisadong sintetikong mga instrumento sa Ethereum ay maglalatag ng pundasyon para sa paparating na rebolusyong pinansyal, na magbibigay sa mga nasa gilid ng modernong sistemang pinansyal ng paraan upang makipag-ugnayan sa pagbuo ng bago.

Sa papel na ito, ipinakilala namin ang isang balangkas para sa pagbuo ng mga reflex index, isang bagong uri ng asset na tutulong sa iba pang mga synthetic na umunlad at magtatatag ng isang pangunahing bloke para sa buong desentralisadong industriya ng pananalapi.

Pangkalahatang-ideya ng Reflex Index

Ang layunin ng isang reflex index ay hindi upang mapanatili ang isang tiyak na peg, ngunit upang palamigin ang pagkasumpungin ng collateral nito. Binibigyang-daan ng mga index ang sinuman na magkaroon ng pagkakalantad sa merkado ng cryptocurrency nang walang kaparehong sukat ng panganib sa paghawak ng aktwal na mga asset ng crypto. Naniniwala kami na ang RAI, ang aming unang reflex index, ay magkakaroon ng agarang gamit para sa iba pang mga koponan na naglalabas ng synthetics sa Ethereum (hal. MakerDAO's Multi-Collateral DAI [1], UMA [2], Synthetix [3]) dahil binibigyan nito ang kanilang mga system ng mas mababang exposure sa mga pabagu-bagong asset gaya ng ETH at nag-aalok ng mga user ng mas maraming oras upang lumabas sa kanilang mga posisyon kung sakaling magkaroon ng makabuluhang pagbabago sa merkado.

Upang maunawaan ang mga reflex index, maaari nating ihambing ang gawi ng presyo ng kanilang redemption sa presyo ng isang stablecoin.

Ang presyo ng pagtubos ay ang halaga ng isang unit ng utang (o barya) sa system. Ito ay nilalayong gamitin lamang bilang isang panloob na tool sa accounting at ito ay iba sa presyo ng merkado (ang halaga kung saan ipinagbibili ng merkado ang barya). Sa kaso ng fiat-backed stablecoins gaya ng USDC, ipinapahayag ng mga operator ng system na maaaring kunin ng sinuman ang isang coin para sa isang US dollar at sa gayon ang presyo ng redemption para sa mga coin na ito ay palaging isa. Mayroon ding mga kaso ng mga crypto-backed na stablecoin tulad ng Multi Collateral DAI (MCD) ng MakerDAO kung saan tina-target ng system ang isang nakapirming peg ng isang US dollar at sa gayon ang presyo ng redemption ay naayos din sa isa

Sa karamihan ng mga kaso, magkakaroon ng pagkakaiba sa pagitan ng presyo sa merkado ng isang stablecoin at sa presyo ng redemption nito. Ang mga sitwasyong ito ay lumilikha ng mga pagkakataon sa arbitrage kung saan ang mga mangangalakal ay gagawa ng mas maraming coin kung ang presyo sa merkado ay mas mataas kaysa sa pagtubos at kanilang kukunin ang kanilang mga stablecoin para sa collateral (hal. US dollars sa kaso ng USDC) kung sakaling ang presyo sa merkado ay mas mababa kaysa sa presyo ng pagtubos.

Ang mga reflex index ay katulad ng mga stablecoin dahil mayroon din silang presyo ng redemption na tina-target ng system. Ang pangunahing pagkakaiba sa kanilang kaso ay ang kanilang pagtubos ay hindi mananatiling maayos, ngunit idinisenyo upang magbago habang naiimpluwensyahan ng mga puwersa ng merkado. Sa Seksyon 4, ipinapaliwanag namin kung paano lumulutang ang presyo ng redemption ng index at lumilikha ng mga bagong pagkakataon sa arbitrage para sa mga user nito.

Disenyo ng Pilosopiya at Go-to-market Strategy

Ang aming pilosopiya sa disenyo ay unahin ang seguridad, katatagan at bilis ng paghahatid.

Ang Multi-Collateral DAI ay ang natural na lugar upang simulan ang pag-ulit sa disenyo ng RAI. Ang system ay na-audit nang husto at pormal na na-verify, mayroon itong kaunting mga panlabas na dependency at nakakalap ng aktibong komunidad ng mga eksperto. Upang mabawasan ang pagsusumikap sa pag-unlad at komunikasyon, gusto lang naming gumawa ng mga pinakasimpleng pagbabago sa orihinal na MCD codebase upang makamit ang aming pagpapatupad.

Kasama sa aming pinakamahahalagang pagbabago ang pagdaragdag ng isang autonomous rate setter, isang Oracle Network Medianizer na isinama sa maraming independiyenteng mga feed ng presyo at isang layer ng minimization ng pamamahala na nilalayong ihiwalay ang system hangga't maaari mula sa interbensyon ng tao

. Ang pinakaunang bersyon ng protocol (Stage 1) ay isasama lamang ang rate setter at iba pang maliliit na pagpapahusay sa pangunahing arkitektura. Kapag napatunayan namin na gumagana ang setter gaya ng inaasahan, mas *ligtas* naming maidaragdag ang oracle medianizer (Stage 2) at ang layer ng minimization ng pamamahala (Stage 3).Mga Mekanismo ng Patakaran sa Monetary

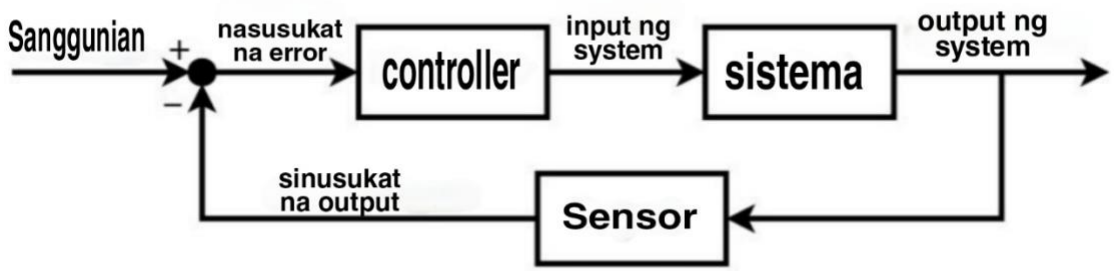
Panimula sa Teorya ng Kontrol

Ang isang karaniwang sistema ng kontrol na pamilyar sa karamihan ng mga tao ay ang shower. Kapag nagsimula ang isang tao sa pagligo, nasa isip nila ang nais na temperatura ng tubig na, sa teorya ng kontrol, ay tinatawag na reference set point.ang Ang tao, na kumikilos bilang controller, patuloy na sinusukat ang temperatura ng daloy ng tubig (na tinatawag na system output)ang aang nd binabago ang bilis kung saan pinihit nila ang knob ng shower batay sa paglihis(opagkakamali) sa pagitan ng nais at kasalukuyang temperatura. Ang bilis ng pagpihit ng knob ay tinatawag na systeminput. Tang Layunin niya na paikutin nang mabilis ang knob para mabilis na maabot ang reference set point, ngunit hindi ganoon kabilis kaysa sa temperatura overshoots. Kung may sistemashocks kung saan biglang nagbabago ang temperatura ng daloy ng

tubig, dapat na mapanatili ng tao ang kasalukuyang temperatura sa pamamagitan ng pag-alam kung gaano kabilis ipihit ang knob bilang tugon sa kaguluhan.

Ang siyentipikong disiplina ng pagpapanatili ng katatagan sa mga dynamic na sistema ay tinatawag na control theory at ito ay nakahanap ng malawak na aplikasyon sa cruise control para sa mga sasakyan, flight navigation, chemical reactors, robotic arm, at industriyal na proseso ng lahat ng uri. Ang algorithm sa pagsasaayos ng kahirapan sa Bitcoin na nagpapanatili ng sampung minutong average na block time, sa kabila ng variable na hashrate, ay isang halimbawa ng isang mission critical control system.

Sa karamihan ng mga modernong sistema ng kontrol ang isangalgorithmic angcontroller ay karaniwang naka-embed sa proseso at binibigyan ito ng kontrol sa isang input ng system (hal. gas pedal ng kotse) upang awtomatikong i-update ito batay sa mga paglihis sa pagitan ng output ng system (hal. bilis ng kotse) at ang setpoint (hal. ang bilis ng cruise control).



Ang pinakakaraniwang uri ng algorithmic controller ay angPID controller.ang Higit sa 95% ng mga pangindustriyang aplikasyon at malawak na hanay ng mga biological system ay gumagamit ng mga elemento ng PID kontrol [4]. Gumagamit ang PID controller ng mathematical formula na may tatlong bahagi para matukoy ang output nito:

Output ng Controller = Proporsyonal na Termino + Integral Term + Derivative Term

Ang Proporsyonal na Term ay ang bahagi ng controller na direktang proporsyonalsa paglihis. Kung ang paglihis ay malaki at positibo (hal. ang cruise control speed setpoint ay malayong mas mataas kaysa sa kasalukuyang bilis ng sasakyan) ang proporsyonal na tugon ay magiging malaki at positibo (eg sa sahig ang gas pedal).

Ang Integral Term ay ang bahagi ng controller na isinasaalang-alang kung gaano katagal nananatili ang isang paglihis. Natutukoy ito sa pamamagitan ng pagkuha ngintegral ng paglihis sa paglipas ng panahon at ito ay pangunahing ginagamit upang maalissteady state error. Nag-iipon ito upang tumugon sa maliliit, kahit na patuloy na mga paglihis mula sa setpoint (hal. ang cruise control setpoint ay 1 mph na mas mataas kaysa sa bilis ng kotse sa loob ng ilang minuto).

Ang Derivative Term ay ang bahagi ng controller na isinasaalang-alang kung gaano kabilis lumalaki o lumiliit ang deviation. Natutukoy ito sa pamamagitan ng pagkuha ngderivative ng deviation at nagsisilbing pabilisin ang tugon ng controller kapag lumalaki ang deviation (hal. pabilisin kung ang setpoint ng cruise control ay mas mataas kaysa sa bilis ng sasakyan at nagsimulang bumagal ang sasakyan). Nakakatulong din ito na bawasan ang overshoot sa pamamagitan ng pagdedecelerate sa tugon ng controller kapag lumiliit ang deviation (hal., paghinaan ang gas habang ang bilis ng sasakyan ay nagsisimulang lumapit sa cruise control setpoint).

Ang kumbinasyon ng tatlong bahaging ito, na ang bawat isa ay maaaring independiyenteng tune, ay nagbibigay sa mga PID controller ng mahusay na kakayahang umangkop sa pamamahala ng isang malawak na iba't ibang mga application ng control system.

Pinakamahusay na gumagana ang mga PID controller sa mga system na nagbibigay-daan sa ilang antas ng lag sa oras ng pagtugon pati na rin ang posibilidad ng overshoot at oscillation sa paligid ng setpoint habang sinusubukan ng system na patatagin ang sarili nito. Ang mga reflex index system tulad ng RAI ay angkop para sa ganitong uri ng senaryo kung saan ang kanilang mga presyo ng redemption ay maaaring baguhin ng mga PID controller.

Sa pangkalahatan, natuklasan kamakailan na marami sa kasalukuyang mga panuntunan sa patakaran sa pananalapi ng sentral na bangko (hal. Taylor Rule) ay aktwal na mga pagtatantya ng PID mga controller [5].

Mekanismo ng Feedback sa Rate ng Redemption

Ang Redemption Rate Feedback Mechanism ay ang bahagi ng system na namamahala sa pagbabago ng presyo ng redemption ng reflex index. Upang maunawaan kung paano ito gumagana, kailangan muna nating ilarawan kung bakit kailangan ng system ng mekanismo ng feedback kumpara sa paggamit ng manu-manong kontrol at kung ano ang output ng mekanismo.

Mga Bahagi ng Mekanismo ng Feedback

Sa teorya, posibleng direktang manipulahin ang presyo ng redemption ng reflex index (inilalarawan sa Seksyon 2) upang maimpluwensyahan ang mga user ng index at sa huli ay mabago ang presyo ng market ng index. Sa pagsasagawa, ang pamamaraang ito ay hindi magkakaroon ng nais na epekto sa mga kalahok sa system. Mula sa pananaw ng isang SAFE holder, kung isang beses lang tumaas ang presyo ng redemption, maaari silang tumanggap ng mas mataas na presyo sa bawat unit ng utang, makuha ang pagkalugi mula sa nabawasang ratio ng collateralization at mapanatili ang kanilang posisyon. Kung, gayunpaman, inaasahan nilang patuloy na tataas ang presyo ng pagtubos sa paglipas ng panahon, malamang na mas hilig nilang

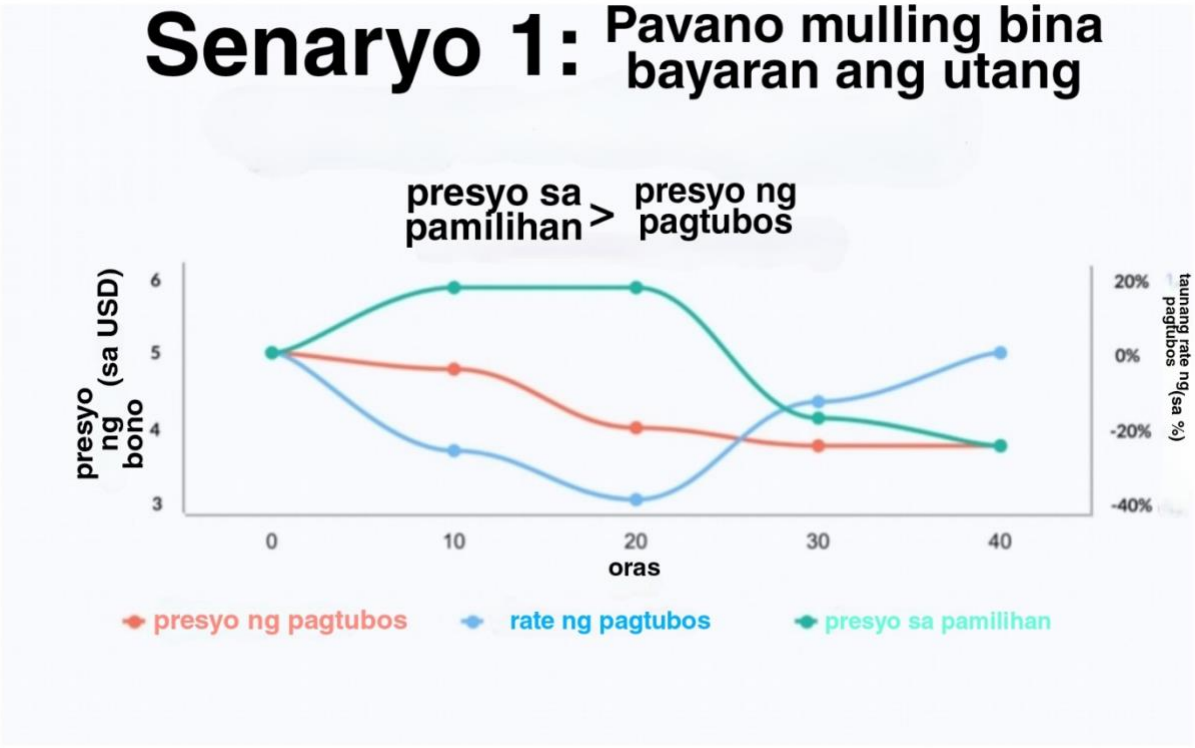
maiwasan ang inaasahang pagkawala sa hinaharap at sa gayon ay pipiliin nilang bayaran ang kanilang utang at isara ang kanilang mga posisyon.

Inaasahan namin na ang mga kalahok ng reflex index system ay hindi direktang tutugon sa mga pagbabago sa presyo ng pagtubos, ngunit sa halip ay tumugon sa rate ng pagbabago ng presyo ng pagtubos na tinatawag natingrate ng pagtubos. Ang rate ng pagtubos ay itinakda ng isangmekanismo ng feedback na ang pamamahala ay maaaring maayos o payagan na maging ganap na awtomatiko.

Mga Sitwasyon ng Mekanismo ng Feedback

Alalahanin na ang mekanismo ng feedback ay naglalayong mapanatili ang ekwilibriyo sa pagitan ng presyo ng pagtubos at ng presyo sa merkado sa pamamagitan ng paggamit ng rate ng pagtubos upang kontrahin ang mga pagbabago sa mga puwersa ng pamilihan. Upang makamit ito, ang rate ng pagtubos ay kinakalkula upang ito ay sumasalungat sa paglihis sa pagitan ng mga presyo ng merkado at pagtubos.

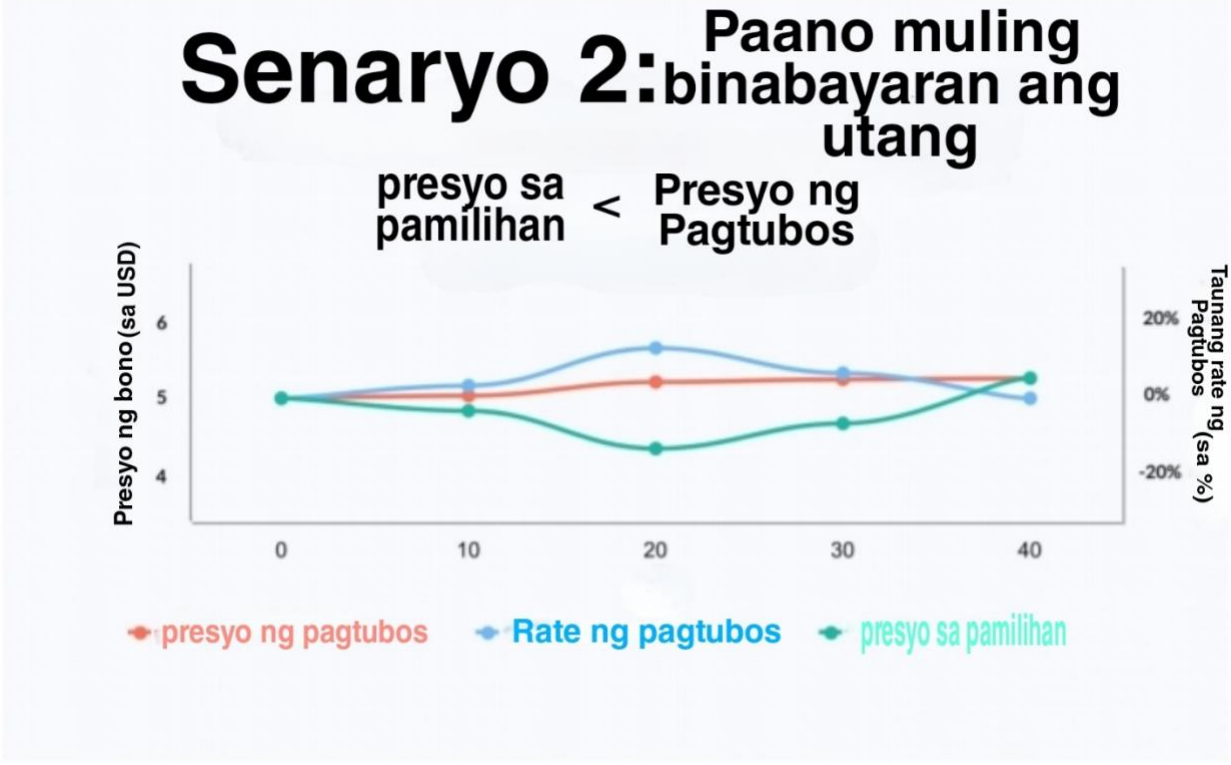
Sa unang senaryo sa ibaba, kung ang presyo ng merkado ng index ay mas mataas kaysa sa presyo ng pagtubos nito, kakalkulahin ng mekanismo ang isang negatibong rate na magsisimulang bawasan ang presyo ng pagtubos, kaya gagawing mas mura ang utang ng system



Ang pag-asa sa pagbaba ng presyo ng redemption ay malamang na mapahina ang loob ng mga tao na humawak ng mga index at mahikayat ang mga may hawak ng SAFE na bumuo ng mas maraming utang (kahit na hindi nagbabago ang presyo ng collateral) na pagkatapos ay ibinebenta sa merkado, sa gayon ay binabalanse ang supply at demand. Tandaan na ito ang perpektong senaryo kung saan mabilis na nagre-react ang mga may hawak ng index bilang tugon sa mekanismo ng feedback. Sa pagsasagawa (at lalo na sa mga unang araw pagkatapos ng paglulunsad) inaasahan namin ang isang lag sa pagitan ng kickoff ng mekanismo at mga aktwal na resulta na makikita sa halaga ng utang na ibinigay at pagkatapos ay sa presyo ng merkado.

Sa kabilang banda, sa pangalawang senaryo, kung ang presyo ng merkado ng index ay mas mababa kaysa sa presyo ng pagtubos, ang rate ay magiging positibo at magsisimulang palitan ang lahat ng utang upang ito ay maging mas mahal.

Habang nagiging mas mahal ang utang, bumababa ang mga ratio ng collateralization ng lahat ng SAFE (kaya nabibigyang-insentibo ang mga tagalikha ng SAFE na bayaran ang kanilang utang) at nagsisimulang mag-hoard ang mga user ng mga index na may inaasahang tataas ang halaga ng mga ito.



Mekanismo ng Feedback Algorithm

Sa sumusunod na senaryo, ipinapalagay namin na ang protocol ay gumagamit ng proportional-integral na controller para kalkulahin ang rate ng redemption:

● Ang reflex index ay inilunsad na may arbitrary na presyo ng redemption na 'rand'

● Sa ilang mga punto, ang presyo ng merkado ng index ay tumataas mula sa 'rand' hanggang 'rand' + x. Matapos basahin ng mekanismo ng feedback ang bagong presyo sa merkado, kinakalkula nito ang isang proporsyonal na terminop,ang na sa kasong ito ay -1 * (('rand' + x) / 'rand'). Negatibo ang proporsyonal upang bawasan ang presyo ng redemption at muling palitan ang mga index upang maging mas mura ang mga ito

● Pagkatapos kalkulahin ang proporsyonal, tutukuyin ng mekanismo ang integral termi sa pamamagitan ng pagdaragdag ng lahat ng mga nakaraang paglihis mula sa hulingdeviationInterval segundo

● Binubuo ng mekanismo ang proporsyonal at integral at kinakalkula ang bawat segundong rate ng pagtubos r na dahan-dahang nagsisimulang bumaba sa presyo ng pagtubos. Habang napagtanto ng mga SAFE creator na maaari silang makabuo ng mas maraming utang, dadagsain nila ang merkado ng mas maraming index

● pagkataposn segundo, nakita ng mekanismo na ang paglihis sa pagitan ng merkado at mga presyo ng pagtubos ay bale-wala (sa ilalim ng isang tinukoy na parameter ingay). Sa puntong ito, itinatakda ng algorithm ang r sa zero at pinapanatili ang presyo ng redemption kung nasaan ito

Sa pagsasagawa, ang algorithm ay magiging mas matatag at gagawa kami ng ilang mga variable na hindi nababago (hal.ingay parameter,deviationInterval) o magkakaroon ng mahigpit na mga hangganan sa kung ano ang maaaring baguhin ng pamamahala.

Pag-tune ng Mekanismo ng Feedback

Ang pinakamahalaga sa wastong paggana ng sistema ng reflex index ay ang pag-tune ng mga parameter ng algorithmic controller. Ang hindi tamang parameterization ay maaaring magresulta sa pagiging masyadong mabagal ng system upang makamit ang katatagan, napakalaking overshoot, o sa pangkalahatan ay hindi matatag sa harap ng mga panlabas na shocks.

Ang proseso ng pag-tune para sa isang PID controller ay karaniwang nagsasangkot ng pagpapatakbo ng live na system, pagsasaayos ng mga parameter ng pag-tune, at pag-obserba sa tugon ng system, na kadalasang sinasadyang nagpapakilala ng mga pagkabigla sa daan. Dahil sa

kahirapan at panganib sa pananalapi ng pagsasaayos ng mga parameter ng isang live na reflex index system, plano naming gamitin ang pagmomodelo at simulation ng computer hangga't maaari upang itakda ang mga paunang parameter, ngunit papayagan din ang pamamahala na i-update ang mga parameter ng pag-tune kung may karagdagang data mula sa produksyon. ipinapakita ang mga ito na sub-optimal.

Setter ng Money Market

Sa RAI, pinaplano naming panatilihing naayos o nilimitahan ang rate ng paghiram (nalalapat ang rate ng interes kapag bumubuo ng mga index) at babaguhin lamang ang presyo ng pagtubos, kaya pinapaliit ang pagiging kumplikadong kasangkot sa pagmomodelo ng mekanismo ng feedback. Ang rate ng paghiram sa aming kaso ay katumbas ng spread sa pagitan ng stability fee at DSR sa Multi-Col-lateral DAI.

Kahit na plano naming panatilihing nakapirmi ang rate ng paghiram, posibleng baguhin ito kasama ng presyo ng redemption gamit ang money market setter. Binabago ng money market ang rate ng paghiram at ang presyo ng redemption sa paraang nagbibigay-insentibo sa mga SAFE creator na bumuo ng mas marami o mas kaunting utang. Kung ang presyo sa merkado ng isang index ay mas mataas sa redemption, ang parehong mga rate ay magsisimulang bumaba, samantalang kung ito ay mas mababa sa redemption, ang tataas ang mga rate.

Pandaigdigang settlement

Ang pandaigdigang settlement ay isang paraan ng huling paraan na ginagamit upang magarantiya ang presyo ng pagtubos sa lahat ng may hawak ng reflex index. Nilalayon nitong payagan ang mga may hawak ng reflex index at SAFE creator na kunin ang collateral ng system sa netong halaga nito (dami ng mga index sa bawat uri ng collateral, ayon sa pinakabagong presyo ng redemption). Kahit sino ay maaaring mag-trigger ng settlement pagkatapos magsunog ng isang tiyak na halaga ng mga protocol token.

Ang settlement ay may tatlong pangunahing yugto:

- **Trigger** : na-trigger ang settlement, hindi na makakagawa ang mga user ng mga SAFE, ang lahat ng collateral price feed at ang redemption price ay frozen at naitala
- Proseso: iproseso ang lahat ng natitirang auction
- **I-claim** : bawat may hawak ng reflex index at SAFE creator ay maaaring mag-claim ng nakapirming halaga ng anumang collateral ng system batay sa huling naitalang presyo ng redemption ng index

Pamamahala

Ang karamihan sa mga parameter ay hindi mababago at ang panloob na smart contract mechanics ay hindi maaupgrade maliban kung ang mga may hawak ng token ng pamamahala ay mag-deploy ng isang ganap na bagong sistema. Pinili namin ang diskarteng ito dahil maaari naming alisin ang meta-game kung saan sinusubukan ng mga tao na impluwensyahan ang proseso ng pamamahala para sa kanilang sariling kapakinabangan, kaya nakakasira ng tiwala sa system. Itinatag namin ang wastong operasyon ng protocol nang hindi masyadong naniniwala sa mga tao (ang "bitcoin effect") para ma-maximize namin ang social scalability at mabawasan ang mga panganib para sa iba pang developer na gustong gumamit ng RAI bilang pangunahing imprastraktura sa sarili nilang mga proyekto. Para sa ilang mga parameter na maaaring baguhin, iminumungkahi namin ang pagdaragdag ng isang Restricted Governance Module na sinadya upang maantala o itali ang lahat ng posibleng pagbabago sa system. Bukod dito, ipinakita namin ang Governance Ice Age, isang registry ng mga pahintulot na maaaring mag-lock ng ilang bahagi ng system mula sa labas ng kontrol pagkatapos lumipas ang ilang mga deadline.

Time Bounded Governance

Ang Time Bounded Governance ay ang unang bahagi ng Restricted Governance Module. Nagpapataw ito ng mga pagkaantala sa oras sa pagitan ng mga pagbabagong inilapat sa parehong parameter. Ang isang halimbawa ay ang posibilidad na baguhin ang mga address ng mga orakulo na ginamit sa Oracle Network Medianizer (Seksyon 6.2) pagkatapos ng hindi bababa sa T sang lumipas na ang mga econ mula noong huling pagbabago sa oracle

Action Bounded Governance

Ang pangalawang bahagi sa Restricted Governance Module ay Action Bounded Governance. Ang bawat napapamahalaang parameter ay may mga limitasyon sa kung anong mga halaga ang maaari itong itakda at kung gaano ito maaaring magbago sa isang tiyak na tagal ng panahon. Ang mga kapansin-pansing halimbawa ay ang mga unang bersyon ng Redemption Rate Feedback Mechanism (Seksyon 4.2) kung saan ang mga may hawak ng token ng pamamahala ay magagawang maayos.

Panahon ng Yelo ng Pamamahala

a Ang Ice Age ay isang hindi nababagong smart contract na nagpapataw ng mga deadline sa pagbabago ng mga partikular na parameter ng system at sa pag-upgrade ng protocol. Maaari itong gamitin sa kaso kung saan gustong matiyak ng pamamahala na maaayos nila ang mga bug bago i-lock ang sarili nitong protocol at itanggi ang interbensyon sa labas. Ang Ice Age ay magbe-verify kung ang isang pagbabago ay pinahihintulutan sa pamamagitan ng pagsuri sa pangalan ng parameter at sa address ng apektadong kontrata laban sa isang registry ng mga deadline. Kung lumipas na ang deadline, babalik ang tawag.

Maaaring maantala ng Pamamahala ang Panahon ng Yelo nang ilang beses kung may makikitang mga bug malapit sa petsa kung kailan dapat magsimulang i-lock ang sarili nitong protocol. Halimbawa, ang Panahon ng Yelo ay maaari lamang maantala ng tatlong beses, bawat oras sa loob ng isang buwan, upang ang mga bagong ipinatupad na pagaayos ng bug ay masuri nang maayos.

Mga Pangunahing Lugar Kung Saan Kailangan ang Pamamahala

Naiisip namin ang apat na lugar kung saan maaaring kailanganin ang pamamahala, lalo na sa mga unang bersyon ng balangkas na ito:

- **Pagdaragdag ng mga bagong uri ng collateral** : Ang RAI ay susuportahan lamang ng ETH, ngunit ang iba pang mga index ay susuportahan ng maraming uri ng collateral at magagawa ng pamamahala upang pag-iba-ibahin ang panganib sa paglipas ng panahon

- **Pagbabago ng mga panlabas na dependency** : ang mga orakulo at DEX kung saan nakasalalay ang system ay maaaring ma-upgrade. Maaaring ituro ng pamamahala ang system sa mga mas bagong dependency upang patuloy itong gumana nang maayos

- **Fine-tuning rate setters** : Ang mga maagang tagakontrol ng patakaran sa pananalapi ay magkakaroon ng mga parameter na maaaring baguhin sa loob ng makatwirang mga hangganan (tulad ng inilalarawan ng Action and Time Bounded Governance)

- **Paglipat sa pagitan ng mga bersyon ng system**: sa ilang mga kaso, ang pamamahala ay maaaring mag-deploy ng isang bagong system, bigyan ito ng pahintulot na mag-print ng mga protocol token at bawiin ang pahintulot na ito mula sa isang lumang system. Isinasagawa ang paglipat na ito sa tulong ng Restricted Migration Module na nakabalangkas sa ibaba

pinigilan ang Module ng paglipat

Ang sumusunod ay isang simpleng mekanismo para sa paglipat sa pagitan ng mga bersyon ng system:

- Mayroong isang migration registry na sumusubaybay kung gaano karaming iba't ibang mga system ang sinasaklaw ng parehong protocol token at kung aling mga system ang maaaring tanggihan ng pahintulot na mag-print ng mga protocol token sa isang auction sa utang

● Sa tuwing magde-deploy ang pamamahala ng bagong bersyon ng system, isusumite nila ang address ng kontrata sa auction sa utang ng system sa rehistro ng paglilipat. Kailangan ding tukuyin ng pamamahala kung mapipigilan nila ang system sa pag-print ng mga token ng protocol. Gayundin, maaaring sabihin ng pamamahala, anumang oras, na ang isang sistema ay palaging makakapag-print ng mga token at sa gayon ay hindi na ito malilipat mula sa

● Mayroong panahon ng cooldown sa pagitan ng pagmumungkahi ng isang bagong system at pagwithdraw ng mga pahintulot mula sa isang luma

● Maaaring mag-set up ng isang opsyonal na kontrata upang awtomatiko nitong isara ang isang lumang sistema pagkatapos nitong tanggihan ang mga pahintulot sa pag-print

Ang migration module ay maaaring isama sa isang Ice Age na awtomatikong nagbibigay ng pahintulot sa mga partikular na system na palaging makapag-print ng mga token.

Awtomatikong Pag-shutdown ng System

May mga kaso na awtomatikong matutukoy ng system at bilang resulta ay nag-trigger ng pag-aayos nang mag-isa, nang hindi kinakailangang mag-burn ng mga protocol token :

● **Matinding Pagkaantala sa Feed ng Presyo** : nakita ng system na ang isa o higit pa sa mga collateral o index price feed ay hindi na-update sa mahabang panahon

● **System Migration** : isa itong opsyonal na kontrata na maaaring mag-shut down ng protocol pagkatapos lumipas ang panahon ng cooldown mula sa sandaling binawi ng pamamahala ang kakayahan ng mekanismo ng auction ng utang na mag-print ng mga protocol token (Restricted Migration Module, Seksyon 5.4.1)

● **Pare-parehong Paglihis sa Presyo ng Market** : nakita ng system na ang presyo ng merkado ng index ay naging x% nalihis ng mahabang panahon kumpara sa presyo ng redemption

Magagawang i-upgrade ng Pamamahala ang mga autonomous na shutdown module na ito habang nililimitahan pa rin o hanggang sa magsimulang i-lock ng Ice Age ang ilang bahagi ng system.

Mga safe

Upang makabuo ng mga index, sinuman ay maaaring magdeposito at gumamit ng kanilang crypto collateral sa loob ng Safes. Habang binuksan ang isang SAFE, magpapatuloy ito sa pag-iipon ng utang ayon sa rate ng paghiram ng nakadeposito na collateral. Habang binabayaran ng SAFE creator ang kanilang utang, mas marami na silang ma-withdraw ng kanilang naka-lock na collateral.

LIGTAS na Ikot ng Buhay

Mayroong apat na pangunahing hakbang na kailangan para sa paglikha ng mga reflex index at kasunod na pagbabayad ng utang ng SAFE:

- Magdeposito ng collateral sa SAFE Kailangan muna ng user na lumikha ng bagong SAFE at magdeposito ng collateral dito.

- Bumuo ng mga index na sinusuportahan ng collateral ng SAFE

Tinutukoy ng user kung gaano karaming mga index ang gusto nilang buuin. Lumilikha ang system ng pantay na halaga ng utang na nagsisimulang maipon ayon sa rate ng paghiram ng collateral.

- Bayaran ang LIGTAS na utang Kapag gustong bawiin ng SAFE creator ang kanilang collateral, kailangan nilang bayaran ang kanilang paunang utang kasama ang naipon na interes.

- Mag-withdraw ng collatera

Pagkatapos mabayaran ng user ang ilan o lahat ng kanilang utang, pinapayagan silang bawiin ang kanilang collateral.

LIGTAS na Pagpuksa

Upang mapanatiling solvent ang system at masakop ang halaga ng buong natitirang utang, maaaring maliquidate ang bawat SAFE kung sakaling ang collateralization ratio nito ay bumaba sa ilalim ng isang tiyak na threshold. Kahit sino ay maaaring mag-trigger ng liquidation, kung saan kukumpiskahin ng system ang collateral ng SAFE at ibebenta ito sa isang collateral auction.

Seguro sa Pagpuksa

Sa isang bersyon ng system, maaaring magkaroon ng opsyon ang mga SAFE creator na pumili ng gatilyo para kapag naliquidate ang kanilang mga SAFE. Ang mga nag-trigger ay mga

matalinong kontrata na awtomatikong nagdaragdag ng higit pang collateral sa isang LIGTAS at posibleng i-save ito mula sa pagpuksa. Ang mga halimbawa ng mga nagtrigger ay mga kontrata na nagbebenta ng mga maiikling posisyon o kontrata na nakikipag-ugnayan sa mga protocol ng insurance gaya ng Nexus Mutual [6].

Ang isa pang paraan upang maprotektahan ang mga SAFE ay ang pagdaragdag ng dalawang magkaibang mga threshold ng collateralization: ligtas atpanganib.ang Maaaring makabuo ng utang ang mga user ng SAFE hanggang sa maabot nila ang ligtas na threshold (na mas mataas kaysa sa panganib) at ma-liquidate lang sila kapag ang collateralization ng SAFE ay mas mababa sa threshold ng panganib.

Mga Collateral na Auction

Para magsimula ng collateral auction, kailangang gumamit ang system ng variable na tinatawag likidasyonDami upang matukoy ang halaga ng utang na sasakupin ng bawat auction at ang katumbas na halaga ng collateral na ibebenta. Aparusa sa pagpuksa ay ilalapat sa bawat auction na SAFE.

Mga Parameter ng Collateral Auction

Pangalan ng Parameter	Paglalarawan
minimumBid	Minimum na halaga ng mga barya na kailangan iaalok sa isang bid
diskwento	Diskwento kung saan ibinebenta ang collateral

lowerCollateralMedianDeviation	Max lower bound deviation na maaaring magkaroon ng collateral median kumpara sa ang presyo ng oracle
upperCollateralMedianDeviation	Max upper bound deviation na maaaring magkaroon ng collateral median kumpara sa ang presyo ng oracle
lowerSystemCoinMedianDeviation	Max lower bound deviation na maaaring magkaroon ng system coin oracle price feed kumpara sa system coin oracle presyo
upperSystemCoinMedianDeviation	Max upper bound deviation na maaaring magkaroon ng collateral median kumpara sa ang sistema ng coin oracle na presyo
minSystemCoinMedianDeviation	Min deviation para sa system coin median na resulta kumpara sa presyo ng pagtubos upang kunin ang median sa account

Collateral Auction mechanism

Ang fixed discount auction ay isang direktang paraan (kumpara sa mga English auction) para maglagay ng collateral para sa pagbebenta kapalit ng system coins na ginamit para bayaran ang masamang utang. Kinakailangan lamang ng mga bidder na payagan ang auction house na ilipat ang kanilang safeEngine.coinBalance at pagkatapos ay maaaring tumawag bumiliCollateral system coins para sa collateral na ibinebenta nang may diskwento kumpara sa pinakahuling naitala nitong presyo sa merkado

Maaari ding suriin ng mga bidder ang halaga ng collateral na makukuha nila mula sa isang partikular na auction sa pamamagitan ng pagtawag getCollateralBought o makakuha ng TinatayangCollateralBili . Tandaan na Ang getCollateralBought ay hindi minarkahan bilang view dahil

binabasa nito (at ina-update din) ang redemptionPrice mula sa oracle relayer samantalang makakuha ng TinatayangCollateralBili gumagamit ng hulingReadRedemptionPrice .

Mga Auction sa Utang

Sa senaryo kung saan hindi masakop ng collateral auction ang lahat ng masamang utang sa isang SAFE at kung ang system ay walang anumang labis na reserba, sinuman ay maaaring mag-trigger ng isang auction sa utang. Ang mga auction ng utang ay sinadya upang gumawa ng higit pang mga protocol token (Seksyon 10) at ibenta ang mga ito para sa mga index na maaaring magpawalang-bisa sa natitirang masamang utang ng system.

Upang makapagsimula ng isang auction sa utang, kailangang gumamit ang system ng dalawang parameter:

- initialDebtAuctionAmount : ang paunang halaga ng mga token ng protocol sa mint pagkatapos ng auction
- utangAuctionBidSize : ang paunang laki ng bid (kung gaano karaming mga index ang dapat ialok sa ipagpalit sainitialDebtAuctionAmount mga token ng protocol)

Setting ng Parameter ng Autonomous Utang Auction

Ang paunang halaga ng mga protocol na token na na-minted sa isang auction ng utang ay maaaring itakda sa pamamagitan ng boto sa pamamahala o maaari itong awtomatikong ayusin ng system. Ang isang awtomatikong bersyon ay kailangang isama sa mga orakulo (Seksyon 6) kung saan babasahin ng system ang protocol token at reflex index na mga presyo sa merkado. Itatakda ng system ang paunang halaga ng mga token ng protocol (initialDebtAuctionAmount) na gagawin para sa utangAuctionBidSize mga index. anginitialDebtAuctionAmountmaaaring

itakda sa isang diskwento kumpara sa aktwal na presyo ng merkado ng PROTOCOL/INDEX upang ma-incentivize ang pag-bid .

Mga Parameter ng Utang Auction

Pangalan ng Parameter	Paglalarawan
amountSoldIncrease	Pagtaas sa dami ng protocol mga token na gagawa para sa pareho dami ng mga index
Pagbaba ng bid	Ang susunod na minimum na pagbaba ng bid sa tinatanggap na halaga ng mga token ng protocol para sa ang parehong dami ng mga index
bidDuration	Gaano katagal ang pag-bid pagkatapos ng bago naisumite ang bid (sa mga segundo)
kabuuangAuctionLength	Kabuuang haba ng auction (sa mga segundo)
Nagsimula ang mga auction	Ilang auction ang nagsimula hanggang ngayon

Mekanismo ng Utang Auction

Taliwas sa mga collateral na auction, ang mga auction sa utang ay mayroon lamang isang yugto:

lowerSoldAmount(uint id, uint amountToBuy, uint bid) : bawasan ang halaga ng tinanggap ang tinanggap ang mga protocol na token kapalit ng isang nakapirming halaga ng mga index.

Ang auction ay magsisimulang muli kung wala itong mga bid na inilagay. Sa tuwing magre-restart ito, magaalok ang system ng mas maraming protocol token para sa parehong dami ng mga index. Ang bagong halaga ng token ng protocol ay kinakalkula bilanghulingTokenAmount *amountSoldIncrease / 100. Pagkatapos mag-ayos ang auction, ang system ay mag-mint ng mga token para sa pinakamataas na bidder .

Mga Token ng Protocol

Gaya ng inilarawan sa mga naunang seksyon, ang bawat protocol ay kailangang protektahan ng isang token na na-minted sa pamamagitan ng mga auction sa utang. Bukod sa proteksyon, ang token ay gagamitin para pamahalaan ang ilang bahagi ng system. Gayundin, ang supply ng protocol token ay untiunting mababawasan sa paggamit ng mga surplus na auction. Ang halaga ng surplus na kailangang maipon sa system bago i-auction ang mga karagdagang pondo ay tinatawag na surplusBuffer at ito ay awtomatikong inaayos bilang isang porsyento ng kabuuang utang na ibinigay.

Pondo ng Seguro

Bukod sa protocol token, ang pamamahala ay maaaring lumikha ng isang insurance fund na nagtataglay ng malawak na hanay ng mga hindi nauugnay na asset at maaaring magamit bilang backstop para sa mga auction sa utang.

Mga Sobra na Auction

Ang mga surplus na auction ay nagbebenta ng mga stability fee na naipon sa system para sa mga protocol na token na sinusunog.

Mga Surplus na Parameter ng Auction

Pangalan ng Parameter	Paglalarawan
Pagtaas ng bid	Minimum na pagtaas sa susunod na bid
bidDuration	Gaano katagal ang auction pagkatapos ng bago naisumite ang bid (sa mga segundo)
kabuuangAuctionLength	Kabuuang haba ng auction (sa mga segundo)
Nagsimula ang mga auction	Ilang auction ang nagsimula hanggang ngayon

Mekanismo ng Sobra sa Auction

Ang mga surplus na auction ay may isang yugto:

IncreaseBidSize(uint id, uint amountToBuy, uint bid) : **kahit sino ay maaaring mag-bid ng mas mataas na halaga ng mga token ng protocol para sa parehong dami ng mga index (surplus). Ang bawat bagong bid ay kailangang mas mataas kaysa o katumbas nglastBid *Pagtaas ng bid / 100. Ang auction ay magtatapos pagkatapos ng maximum kabuuangAuctionLength segundo o pagkataposbidDuration ilang segundo na ang lumipas mula noong pinakahuling bid at walang bagong bid na naisumite sa ngayon.**

Magsisimula muli ang isang auction kung wala itong mga bid. Sa kabilang banda, kung ang auction ay may hindi bababa sa isang bid, iaalok ng system ang sobra sa pinakamataas na bidder at pagkatapos ay susunugin ang lahat ng nakalap na protocol token.

Pamamahala ng Surplus Indexes

Sa bawat oras na ang isang user ay bubuo ng mga index at hindi malinaw na lumilikha ng utang, ang system ay magsisimulang maglapat ng rate ng paghiram sa LIGTAS ng user. Ang naipon na interes ay pinagsama-sama sa dalawang magkaibang smart contract:

- Angmakina ng accountingginamit upang magpalitaw ng utang (Seksyon 9.2) at labis (Seksyon 10.1) mga auction
- Ang labis na treasury ginagamit upang pondohan ang mga pangunahing bahagi ng imprastraktura at hikayatin ang mga panlabas na aktor na mapanatili ang sistema

Ang sobrang treasury ang namamahala sa pagpopondo ng tatlong pangunahing bahagi ng system:

- Oracle module (Seksyon 6). Depende sa kung paano nakabalangkas ang isang orakulo, ang treasury ay maaaring magbabayad ng pamamahala na naka-whitelist, off-chain na mga orakulo o nagbabayad ito para sa mga tawag patungo sa mga network ng oracle. Ang treasury ay maaari ding i-set up upang bayaran ang mga address na gumastos ng gas upang tumawag sa isang orakulo at i-update ito
- Sa ilang mga kaso, ang mga independiyenteng koponan na nagpapanatili ng system. Ang mga halimbawa ay ang mga team na nag-whitelist ng mga bagong uri ng collateral o nag-fine tune ng rate setter ng system (Seksyon 4.2)

Maaaring i-set up ang treasury upang ang ilang mga surplus na tatanggap ay awtomatikong tanggihan ng pondo sa hinaharap at ang iba ay maaaring pumalit sa kanila.

Panlabas na Aktor

ng sistema ay nakasalalay sa mga panlabas na aktor upang gumana nang maayos. Ang mga aktor na ito ay insentibo sa ekonomiya na lumahok sa mga lugar tulad ng mga auction, pagpoproseso ng pandaigdigang settlement, paggawa ng merkado at pag-update ng mga feed ng presyo upang mapanatili ang kalusugan ng system.

Magbibigay kami ng mga paunang user interface at mga automated na script para paganahin ang pinakamaraming tao hangga't maaari na panatilihing secure ang protocol.

Maa-address na Market

Nakikita namin ang RAI bilang kapaki-pakinabang sa dalawang pangunahing lugar:

- **Pag-iiba-iba ng portfolio** : ginagamit ng mga mamumuhunan ang RAI para magkaroon ng dampened exposure sa isang asset tulad ng ETH nang walang buong panganib na aktwal na humawak ng ether

- **Collateral para sa mga sintetikong asset** : Maaaring mag-alok ang RAI sa mga protocol gaya ng UMA, MakerDAO at Synthetix ng mas mababang pagkakalantad sa crypto market at bigyan ang mga user ng mas maraming oras na umalis sa kanilang mga posisyon sa kaso ng mga sitwasyon tulad ng Black Thursday mula Marso 2020 kung kailan milyon-milyong dolyar na halaga ng mga asset ng crypto ay naliquidate

Pananaliksik sa Hinaharap

Upang itulak ang mga hangganan ng desentralisadong pera at magdala ng karagdagang pagbabago sa desentralisadong pananalapi, patuloy kaming maghahanap ng mga alternatibo sa mga pangunahing lugar tulad ng pagliit ng pamamahala at mga mekanismo ng pagpuksa.

Gusto muna naming maglatag ng batayan para sa mga pamantayan sa hinaharap sa paligid ng mga protocol na nagkukulong sa kanilang sarili mula sa labas ng kontrol at para sa mga tunay na "money robot" na umaangkop bilang tugon sa mga puwersa ng merkado. Pagkatapos, inaanyayahan namin ang komunidad ng Ethereum na makipagdebate at magdisenyo ng mga pagpapabuti sa paligid ng aming mga panukala na may partikular na pagtuon sa mga collateral at auction sa utang.

Mga Panganib at Pagbabawas

Mayroong ilang mga panganib na kasangkot sa pagbuo at paglulunsad ng isang reflex index, pati na rin ang mga kasunod na sistema na binuo sa itaas:

- **Mga bug ng matalinong kontrata** : ang pinakamalaking panganib na idinudulot sa system ay ang posibilidad ng isang bug na nagpapahintulot sa sinuman na kunin ang lahat ng collateral o i-lock ang protocol sa isang estado na hindi nito mabawi. Plano naming suriin ang aming code ng maraming mananaliksik sa seguridad at ilunsad ang system sa isang testnet bago kami mangako na i-deploy ito sa produksyon

- **Kabiguan ng Oracle** : magsasama-sama kami ng mga feed mula sa maraming network ng oracle at magkakaroon ng mahigpit na mga panuntunan para sa pag-upgrade ng isang orakulo lamang sa isang pagkakataon upang ang malisyosong pamamahala ay hindi madaling makapagpasok ng mga maling presyo

- **Collateral black swan na mga kaganapan** : may panganib na magkaroon ng kaganapan sa black swan sa pinagbabatayan na collateral na maaaring magresulta sa mataas na halaga ng mga na-liquidate na SAFE. Maaaring hindi masakop ng mga liquidation ang buong hindi pa nababayarang masamang utang at sa gayon ay patuloy na babaguhin ng system ang sobrang buffer nito upang masakop ang isang disenteng halaga ng inilabas na utang at makatiis ng mga shock sa merkado

- **Mga parameter ng hindi wastong rate setter** : ang mga mekanismo ng autonomous na feedback ay lubos na pang-eksperimento at maaaring hindi kumilos nang eksakto tulad ng hinuhulaan namin sa mga simulation. Plano naming payagan ang pamamahala na ayusin ang bahaging ito (habang nasa hangganan pa rin) upang maiwasan ang mga hindi inaasahang sitwasyon

- **Pagkabigong i-bootstrap ang isang malusog na liquidator market** : ang mga liquidator ay mahahalagang aktor na tinitiyak na ang lahat ng inilabas na utang ay sakop ng collateral. Plano naming lumikha ng mga interface at mga automated na script upang ang pinakamaraming tao hangga't maaari ay maaaring lumahok sa pagpapanatiling secure ng system.

Buod

Nagmungkahi kami ng protocol na unti-unting nagla-lock sa sarili mula sa kontrol ng tao at naglalabas ng mababang volatility, collateralized asset na tinatawag na reflex index. Una naming ipinakita ang autonomous na mekanismo na nilalayong impluwensyahan ang presyo ng merkado ng index at pagkatapos ay inilarawan kung paano maaaring limitahan ng ilang matalinong kontrata ang kapangyarihan ng mga may hawak ng token sa system. Nag-outline kami ng self-sustaining scheme para sa medianizing price feed mula sa maraming independiyenteng oracle network at pagkatapos ay tinapos sa pamamagitan ng paglalahad ng pangkalahatang mekanismo para sa pag-minting ng mga index at pag-liquidate sa mga SAFE.

Mga sanggunian

[1] "Ang Maker Protocol: Multi Collateral Dai (MCD) System ng MakerDAO", https:// 2YL5S6j

[2] “UMA: Isang Desentralisadong Platform ng Kontrata sa Pinansyal”, https://

[3] Synthetix Litepaper,https:// bit.ly/ 2SNHxZO bit.ly/ 2Wgx7E1

[4] KJ Åström , RM Murray, “Mga Sistema ng Feedback: Isang Panimula para sa mga Siyentipiko at Inhinyero”, anghttps:// bit.ly/ bit.ly/ 3bHwnMC

[5] RJ Hawkins, JK Speakes, DE Hamilton, "Monetary Policy at PID Control", https:// 2TeQZFO

[6] H. Karp, R. Melbardis, “Isang peer-to-peer discretionary mutual sa Ethereum blockchain”, https:// bit.ly/ 3du8TMy

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

Talasalitaan

Reflex index : isang collateralized na asset na nagpapahina sa pagkasumpungin ng pinagbabatayan nito

RAI: ang aming unang reflex index

Presyo ng Pagtubos: ang presyo na gustong magkaroon ng index ang system. Nagbabago ito, naiimpluwensyahan ng isang rate ng pagtubos (kinakalkula ng RRFM), kung sakaling ang presyo sa merkado ay hindi malapit dito. Nilayong impluwensyahan ang mga SAFE creator na bumuo ng higit pa o magbayad ng ilan sa kanilang utang

Rate ng Pahiram : taunang rate ng interes na inilalapat sa lahat ng SAFE na may natitirang utang

Redemption Rate Feedback Mechanism (RRFM) : isang autonomous na mekanismo na nagkukumpara sa merkado at mga presyo ng redemption ng isang reflex index at pagkatapos ay kinukuwenta ang isang rate ng pagtubos na dahan-dahang nakakaimpluwensya sa mga SAFE creator na makabuo ng mas marami o mas kaunting utang (at tuwirang sumusubok na bawasan ang paglihis ng presyo sa merkado/pagtubos)

Money Market Setter (MMS) : isang mekanismong katulad ng RRFM na kumukuha ng maraming monetary levers nang sabay-sabay. Sa kaso ng mga reflex index, binabago nito ang parehong rate ng paghiram at ang presyo ng pagtubos

Oracle Network Medianizer (ONM) : isang matalinong kontrata na kumukuha ng mga presyo mula sa maraming mga network ng oracle (na hindi kontrolado ng pamamahala) at pinapagitnaan ang mga ito kung ang karamihan (hal. 3 sa 5) ay nagbalik ng resulta nang hindi ibinabato

Restricted Governance Module (RGM): isang hanay ng mga matalinong kontrata na nagbubuklod sa kapangyarihang taglay ng mga may hawak ng mga token ng pamamahala sa system. Ito ay maaaring magpatupad ng mga pagkaantala sa oras o nililimitahan ang mga posibilidad na ang pamamahala ay kailangang magtakda ng ilang partikular na parameter

Panahon ng Yelo ng Pamamahala : hindi nababagong kontrata na nagla-lock sa karamihan ng mga bahagi ng isang protocol mula sa interbensyon sa labas pagkatapos lumipas ang isang tiyak na deadline

Accounting Engine : bahagi ng system na nag-trigger ng utang at mga surplus na auction. Sinusubaybayan din nito ang halaga ng kasalukuyang auction na utang, hindi naaaksyunan na masamang utang at ang sobrang buffer

Labis na Buffer : halaga ng interes na maiipon at itago sa system. Anumang interes na naipon sa itaas ng threshold na ito ay ibebenta sa mga surplus na auction na nagsusunog ng mga token ng protocol .

Labis na Treasury : kontrata na nagbibigay ng pahintulot sa iba't ibang mga module ng system na bawiin ang naipon na interes (hal. ONM para sa mga tawag sa oracle)

Contents

Introduction

Money is one of the most powerful coordination mechanisms humanity leverages in order to thrive. The privilege of managing the money supply has historically been kept in the hands of sovereign leadership and the financial elite while being imposed upon an unwitting general public. Where Bitcoin has demonstrated the potential for a grassroots protest to manifest a store-of-value commodity asset, Ethereum gives us a platform to build asset-backed synthetic instruments that can be protected from volatility and used as collateral, or pegged to a reference price and used as a medium-of-exchange for daily transactions, all enforced by the same principles of decentralized consensus.

Permissionless access to Bitcoin for storing wealth and properly decentralized synthetic instruments on Ethereum will lay the foundation for the upcoming financial revolution, providing those at the fringes of the modern financial system the means to coordinate around building the new one.

In this paper, we introduce a framework for building reflex indexes, a new asset type which will help other synthetics flourish and will establish a key building block for the entire decentralized finance industry.

Overview of Reflex Indexes

A reflex index's purpose is not to maintain a specific peg, but to dampen the volatility of its collateral. Indexes allow anyone to gain exposure to the cryptocurrency market without the same scale of risk as holding actual crypto assets. We believe RAI, our first reflex index, will have immediate utility for other teams issuing synthetics on Ethereum (e.g MakerDAO's Multi-Collateral DAI [1], UMA [2], Synthetix [3]) because it gives their systems a lower exposure to volatile assets such as ETH and offers users more time to exit their positions in case of a significant market shift.

In order to understand reflex indexes, we can compare the behaviour of their redemption price to that of a stablecoin's price.

The redemption price is the value of one debt unit (or coin) in the system. It is meant to be used only as an internal accounting tool and it is different from the market price (the value that the market is trading the coin at). In the case of fiat-backed

stablecoins such as USDC, the system operators declare that anyone can redeem one coin for one US dollar and thus the redemption price for these coins is always one. There are also cases of crypto-backed stablecoins such as MakerDAO's Multi Collateral DAI (MCD) where the system targets a fixed peg of one US dollar and thus the redemption price is also fixed at one.

In most cases, there will be a difference between the market price of a stablecoin and its redemption price. These scenarios create arbitrage opportunities where traders will create more coins if the market price is higher than redemption and they will redeem their stablecoins for collateral (e.g US dollars in the case of USDC) in case the market price is lower than the redemption price.

Reflex indexes are similar to stablecoins because they also have a redemption price that the system targets. The main difference in their case is that their redemption will not remain fixed, but is designed to change while being influenced by market forces. In Section 4 we explain how an index's redemption price floats and creates new arbitrage opportunities for its users.

Design Philosophy and Go-to-market Strategy

Our design philosophy is to prioritize security, stability and speed of delivery.

Multi-Collateral DAI was the natural place to start iterating on RAI's design. The system has been heavily audited and formally verified, it has minimal external dependencies and it gathered an active community of experts. To minimize development and communications effort, we want to make only the simplest changes to the original MCD codebase in order to achieve our implementation.

Our most important modifications include the addition of an autonomous rate setter, an Oracle Network Medianizer which is integrated with many independent price feeds and a governance minimization layer meant to isolate the system as much as possible from human intervention.

The very first version of the protocol (Stage 1) will only include the rate setter and other minor improvements in the core architecture. Once we prove that the setter works as expected, we can more safely add the oracle medianizer (Stage 2) and the governance minimization layer (Stage 3).

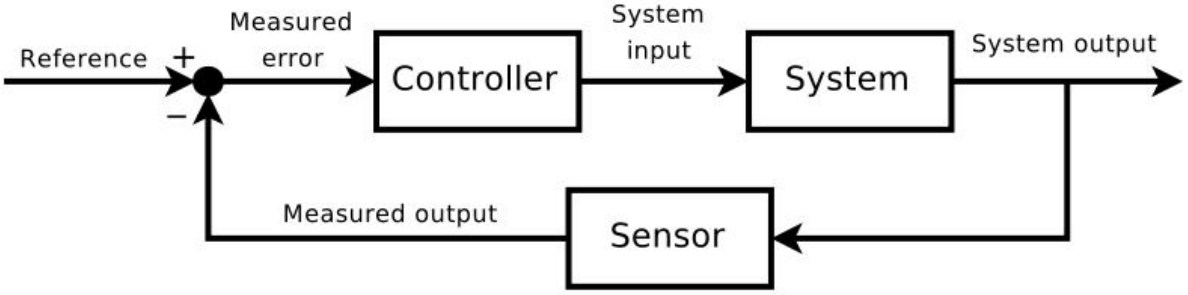
Monetary Policy Mechanisms

Introduction to Control Theory

One common control system that most people are familiar with is the shower. When someone starts a shower, they have a desired water temperature in mind which, in control theory, is called the *reference set point*. The person, acting as the *controller*, continuously measures the water flow temperature (which is called the system *output*) and modifies the speed at which they turn the shower's knob based on the *deviation* (or *error*) between the desired and the current temperature. The speed at which the knob is turned is called the system *input.* The objective is to turn the knob fast enough as to reach the reference set point quickly, but not so fast that the temperature *overshoots*. If there are system *shocks* where the water flow temperature suddenly changes, the person should be able to maintain the current temperature by knowing how fast to turn the knob in response to the disturbance.

The scientific discipline of maintaining stability in dynamic systems is called control theory and it has found broad application in cruise control for cars, flight navigation, chemical reactors, robotic arms, and industrial processes of all kinds. The Bitcoin difficulty adjustment algorithm which maintains the ten minute average block time, despite a variable hashrate, is an example of a mission critical control system.

In most modern control systems an *algorithmic controller* is typically embedded in the process and it is given control over a system input (e.g. a car's gas pedal) in order to automatically update it based on deviations between the system output (e.g. a car's speed) and the setpoint (e.g. the cruise control speed).



The most common type of algorithmic controller is the *PID controller*. Over 95% of industrial applications and a wide range of biological systems employ elements of PID

control [4]. A PID controller uses a mathematical formula with three parts to determine its output:

Controller Output = Proportional Term + Integral Term + Derivative Term

The Proportional Term is the part of the controller which is directly *proportional* to the deviation. If the deviation is large and positive (e.g. the cruise control speed setpoint is far higher than the car's current speed) the proportional response will be large and positive (e.g. floor the gas pedal).

The Integral Term is the part of the controller which takes into account how long a deviation has persisted. It is determined by taking the *integral* of the deviation over time and it is primarily used to eliminate *steady state error*. It accumulates in order to respond to small, albeit persistent deviations from the setpoint (e.g. the cruise control setpoint has been 1 mph higher than the car's speed for a few minutes).

The Derivative Term is the part of the controller which takes into account how fast the deviation is growing or shrinking. It is determined by taking the *derivative* of the deviation and serves to accelerate the controller response when the deviation is growing (e.g. speed up if the cruise control setpoint is higher than the car's speed and the car starts to slow down). It also helps reduce overshoot by decelerating the controller response when the deviation is shrinking (e.g. ease up on the gas as the car's speed starts to approach the cruise control setpoint).

The combination of these three parts, each of which can be independently tuned, gives PID controllers great flexibility at managing a wide variety of control system applications.

PID controllers work best in systems that allow some degree of lag in the response time as well as the possibility of overshoot and oscillation around the setpoint as the system attempts to stabilize itself. Reflex index systems like RAI are well suited for this type of scenario where their redemption prices can be changed by PID controllers.

More generally, it has recently been discovered that many of the current central bank monetary policy rules (e.g. the Taylor Rule) are actually approximations of PID

controllers [5].

Redemption Rate Feedback Mechanism

The Redemption Rate Feedback Mechanism is the system component in charge of changing a reflex index's redemption price. In order to understand how it works, we first need to describe why the system needs a feedback mechanism as opposed to using manual control and what the mechanism's output is.

Feedback Mechanism Components

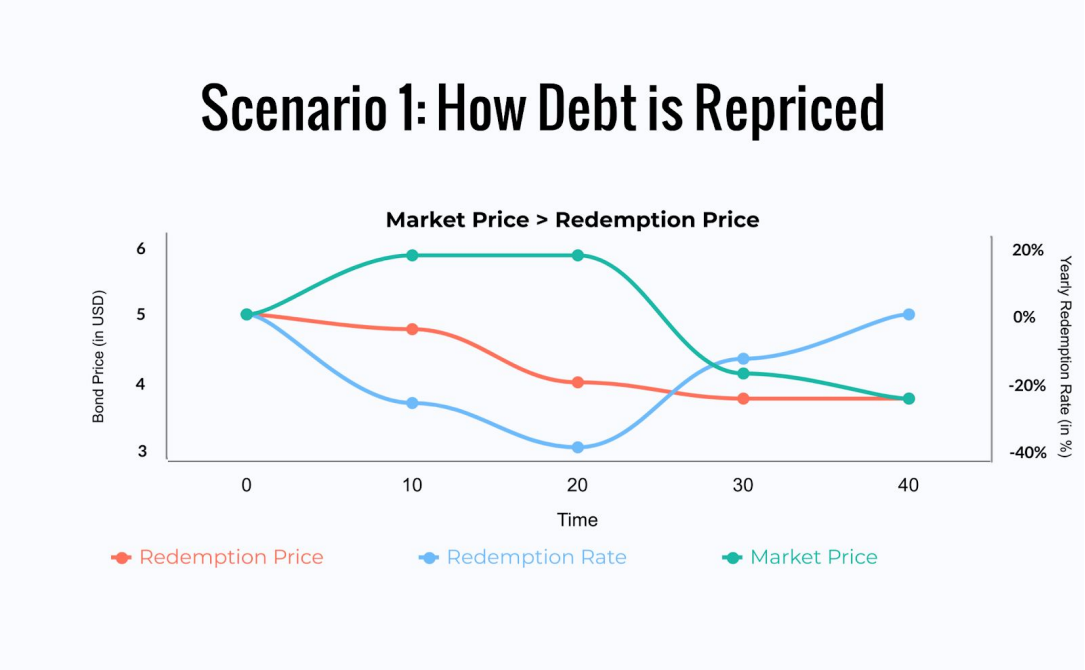
In theory, it would be possible to directly manipulate the reflex index's redemption price (described in Section 2) in order to influence index users and ultimately change the index's market price. In practice, this method would not have the desired effect on system participants. From the perspective of a SAFE holder, if the redemption price is increased only once, they might accept a higher price per debt unit, absorb the loss from a decreased collateralization ratio and maintain their position. If, however, they expect the redemption price to continue to increase over time, they would likely be more inclined to avoid expected future loss and thus choose to pay back their debt and close their positions.

We expect reflex index system participants not to respond directly to changes in the redemption price, but instead respond to the *rate of change of the redemption price* which we call the *redemption rate*. The redemption rate is set by a *feedback mechanism* that governance can fine-tune or allow to be fully automated.

Feedback Mechanism Scenarios

Recall that the feedback mechanism aims to maintain equilibrium between the redemption price and the market price by using the redemption rate to counter shifts in market forces. To achieve this, the redemption rate is calculated so that it opposes the deviation between market and redemption prices.

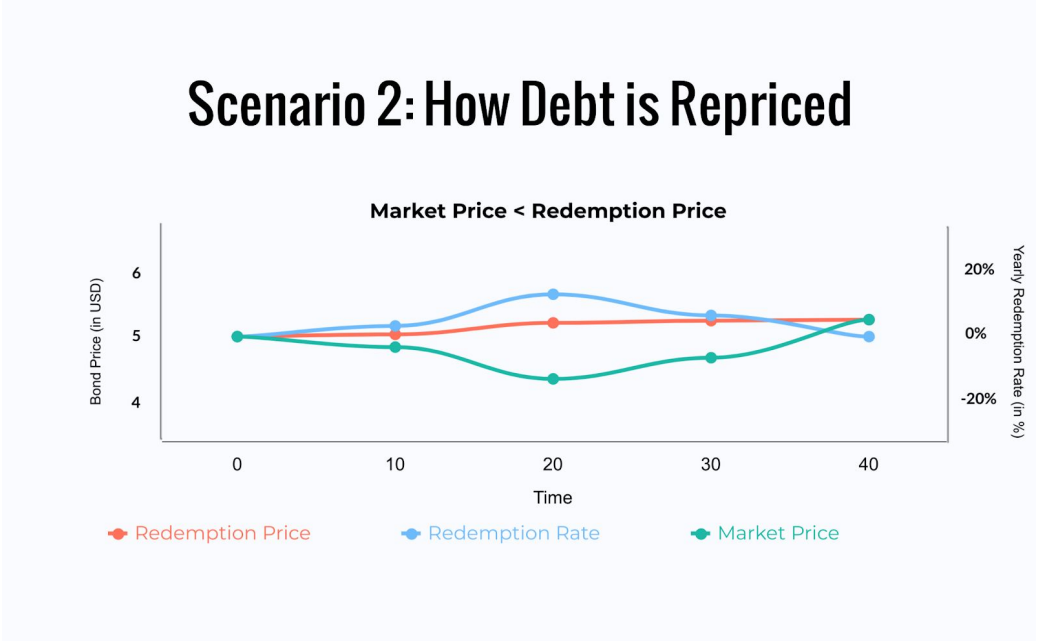
In the first scenario below, if the index's market price is higher than its redemption price, the mechanism will calculate a negative rate which will start to decrease the redemption price, thus making the system's debt cheaper.



The expectation of a decreasing redemption price will likely discourage people from holding indexes and encourage SAFE holders to generate more debt (even if the collateral price does not change) which is then sold on the market, thus balancing out supply and demand. Note that this is the ideal scenario where index holders react quickly in response to the feedback mechanism. In practice (and especially in the early days post launch) we expect a lag between the mechanism's kickoff and actual results seen in the amount of debt issued and subsequently in the market price.

On the other hand, in scenario two, if the index's market price is lower than the redemption price, the rate becomes positive and starts to reprice all the debt so that it becomes more expensive.

As debt becomes more expensive, the collateralization ratios of all SAFEs go down (thus SAFE creators are incentivized to pay back their debt) and users start to hoard indexes with the expectation that they will increase in value.



Feedback Mechanism Algorithm

In the following scenario, we assume that the protocol uses a proportional-integral controller to calculate the redemption rate:

- The reflex index is launched with an arbitrary redemption price ‘rand’
- At some point, the index’s market price rises from ‘rand’ to ’rand’ + x. After the feedback mechanism reads the new market price, it calculates a proportional term *p*, which in this case is -1 * ((‘rand’ + x) / ‘rand’). The proportional is negative in order to decrease the redemption price and in turn reprice the indexes so that they become cheaper
- After calculating the proportional, the mechanism will determine the integral term *i* by adding all the past deviations from the last *deviationInterval* seconds
- The mechanism sums the proportional and the integral and calculates a per-second redemption rate *r* that slowly starts to decrease the redemption price. As SAFE creators realize they can generate more debt, they will flood the market with more indexes

- After *n* seconds, the mechanism detects that the deviation between the market and redemption prices is negligible (under a specified parameter *noise*). At this point, the algorithm sets r to zero and keeps the redemption price where it is

In practice, the algorithm will be more robust and we will either make some variables immutable (e.g the *noise* parameter, *deviationInterval*) or there will be strict bounds over what governance can change.

Feedback Mechanism Tuning

Of the utmost importance to the proper functioning of the reflex index system is the tuning of the algorithmic controller parameters. Improper parameterization could result in the system being too slow to achieve stability, massively overshooting, or being generally unstable in the face of external shocks.

The tuning process for a PID controller typically involves running the live system, tweaking the tuning parameters, and observing the system's response, often purposefully introducing shocks along the way. Given the difficulty and financial risk of tweaking the parameters of a live reflex index system, we plan to leverage computer modeling and simulation as much as possible to set the initial parameters, but will also allow governance to update the tuning parameters if additional data from production shows them to be sub-optimal.

Money Market Setter

In RAI, we plan to keep the borrowing rate (interest rate applied when generating indexes) fixed or capped and only modify the redemption price, thus minimizing the complexity involved in modelling the feedback mechanism. The borrowing rate in our case is equal to the spread between the stability fee and DSR in Multi-Collateral DAI.

Even though we plan to keep the borrowing rate fixed, it is possible to change it alongside the redemption price using a money market setter. The money market changes the borrowing rate and the redemption price in a way that incentivizes SAFE creators to generate more or less debt. If an index's market price is above redemption, both rates will start to decrease, whereas if it is below redemption, the

rates will increase.

Global Settlement

Global settlement is a method of last resort used to guarantee the redemption price to all reflex index holders. It is meant to allow both reflex index holders and SAFE creators to redeem system collateral at its net value (amount of indexes per each collateral type, according to the latest redemption price). Anyone can trigger settlement after burning a certain amount of protocol tokens.

Settlement has three main phases:

- **Trigger**: settlement is triggered, users cannot create SAFEs anymore, all collateral price feeds and the redemption price are frozen and recorded
- **Process**: process all outstanding auctions
- **Claim**: every reflex index holder and SAFE creator can claim a fixed amount of any system collateral based on the index's last recorded redemption price

Governance

The vast majority of parameters will be immutable and the inner smart contract mechanics will not be upgradeable unless governance token holders deploy an entirely new system. We chose this strategy because we can eliminate the meta-game where people try to influence the governance process for their own benefit, thus damaging trust in the system. We establish the proper operation of the protocol without putting too much faith in humans (the "bitcoin effect") so that we maximize social scalability and minimize the risks for other developers who will want to use RAI as core infrastructure in their own projects.

For the few parameters that can be changed, we propose the addition of a Restricted Governance Module meant to delay or bound all possible system modifications. Moreover, we present Governance Ice Age, a permissions registry that can lock some parts of the system from outside control after certain deadlines have passed.

Time Bounded Governance

Time Bounded Governance is the first component of the Restricted Governance Module. It imposes time delays between changes applied to the same parameter. An example is the possibility to change the addresses of the oracles used in the Oracle Network Medianizer (Section 6.2) after at least *T* seconds have passed since the last oracle modification.

Action Bounded Governance

The second component in the Restricted Governance Module is Action Bounded Governance. Every governable parameter has limits on what values it can be set to and how much it can change over a certain period of time. Notable examples are the initial versions of the Redemption Rate Feedback Mechanism (Section 4.2) which governance token holders will be able fine-tune.

Governance Ice Age

The Ice Age is an immutable smart contract that imposes deadlines on changing specific system parameters and on upgrading the protocol. It can be used in the case where governance wants to make sure they can fix bugs before the protocol locks itself and denies outside intervention. Ice Age will verify if a change is permitted by checking the parameter's name and the affected contract's address against a registry of deadlines. If the deadline has passed, the call will revert.

Governance may be able to delay Ice Age a fixed number of times if bugs are found close to the date when the protocol should start to lock itself. For example, Ice Age can only be delayed three times, each time for one month, so that the newly implemented bug fixes are tested properly.

Core Areas Where Governance Is Needed

We envision four areas where governance might be needed, especially in the early versions of this framework:

- **Adding new collateral types**: RAI will be backed only by ETH, but other indexes will be backed by multiple collateral types and governance will be able

to diversify risk over time

- **Changing external dependencies**: oracles and DEXs that the system depends on can be upgraded. Governance can point the system to newer dependencies in order for it to continue functioning properly

- **Fine-tuning rate setters**: early monetary policy controllers will have parameters that can be changed within reasonable bounds (as described by Action and Time Bounded Governance)

- **Migrating between system versions**: in some cases, governance can deploy a new system, give it permission to print protocol tokens and withdraw this permission from an old system. This migration is performed with the help of the Restricted Migration Module outlined below

Restricted Migration Module

The following is a simple mechanism for migrating between system versions:

- There is a migration registry that keeps track of how many different systems the same protocol token covers and which systems can be denied the permission to print protocol tokens in a debt auction

- Every time governance deploys a new system version, they submit the address of the system's debt auction contract in the migration registry. Governance also needs to specify if they will ever be able to stop the system from printing protocol tokens. Also, governance can, at any time, say that one system will always be able to print tokens and thus it will never be migrated from

- There is a cooldown period between proposing a new system and withdrawing permissions from an old one

- An optional contract can be set up so that it automatically shuts down an old system after it is denied printing permissions

The migration module can be combined with an Ice Age that automatically gives specific systems the permission to always be able to print tokens.

Automatic System Shutdown

There are cases that the system can automatically detect and as a result trigger settlement by itself, without the need to burn protocol tokens:

- **Severe Price Feed Delays**: the system detects that one or more of the collateral or index price feeds have not been updated in a long time

- **System Migration**: this is an optional contract that can shut down the protocol after a cooldown period passes from the moment when governance withdraws the ability of the debt auction mechanism to print protocol tokens (Restricted Migration Module, Section 5.4.1)

- **Consistent Market Price Deviation**: the system detects that the index's market price has been *x%* deviated for a long time compared to the redemption price

Governance will be able to upgrade these autonomous shutdown modules while still being bounded or until the Ice Age starts to lock some parts of the system.

Oracles

There are three main asset types that the system needs to read price feeds for: the index, the protocol token and every whitelisted collateral type. The price feeds can be provided by governance led oracles or by already established oracle networks.

Governance Led Oracles

Governance token holders or the core team that launched the protocol can partner with other entities who gather multiple price feeds off-chain and then submit a single transaction to a smart contract that medianizes all data points.

This approach allows for more flexibility on upgrading and changing the oracle infrastructure although it comes at the expense of trustlessness.

Oracle Network Medianizer

An oracle network medianizer is a smart contract that reads prices from multiple sources which are not directly controlled by governance (e.g Uniswap V2 pool between an index collateral type and other stablecoins) and then medianizes all the results. ONM works as follows:

- Our contract keeps track of whitelisted oracle networks it can call in order to request collateral prices. The contract is funded by part of the surplus the system accrues (using the Surplus Treasury, Section 11). Each oracle network accepts specific tokens as payment so our contract also keeps track of the minimum amount and the type of tokens needed for each request

- In order to push a new price feed in the system, all the oracles need to be called beforehand. When calling an oracle, the contract first swaps some stability fees with one of the oracle's accepted tokens. After an oracle is called, the contract tags the call as "valid" or "invalid". If a call is invalid, the specific faulty oracle cannot be called again until all the other ones are called and the contract checks if there is a valid majority. A valid oracle call must not revert and it must retrieve a price that has been posted on-chain sometime in the last *m* seconds. "Retrieve" means different things depending on each oracle type:

    - For pull based oracles, from which we can get a result right away, our contract needs to pay a fee and directly fetch the price

    - For push based oracles, our contract pays the fee, calls the oracle and needs to wait a specific period of time *n* before calling the oracle again in order to get the requested price

- Every oracle result is saved in an array. After every whitelisted oracle is called and if the array has enough valid data points to form a majority (e.g the contract received valid data from 3/5 oracles), the results are sorted and the contract chooses the median

- Whether the contract finds a majority or not, the array with oracle results is cleared and the contract will need to wait *p* seconds before starting the entire process all over again

Oracle Network Backup

Governance can add a backup oracle option that starts to push prices in the system if the medianizer cannot find a majority of valid oracle networks several times in a row.

The backup option must be set when the medianizer is deployed as it cannot be changed afterwards. Furthermore, a separate contract can monitor if the backup has been replacing the medianization mechanism for too long and automatically shut down the protocol.

Safes

In order to generate indexes, anyone can deposit and leverage their crypto collateral inside Safes. While a SAFE is opened, it will continue accruing debt according to the deposited collateral's borrowing rate. As the SAFE creator pays back their debt, they will be able to withdraw more and more of their locked collateral.

SAFE Lifecycle

There are four main steps needed for creating reflex indexes and subsequently paying back a SAFE's debt:

- Deposit collateral in the SAFE

  The user first needs to create a new SAFE and deposit collateral in it.

- Generate indexes backed by the SAFE's collateral

  The user specifies how many indexes they want to generate. The system creates an equal amount of debt that starts to accrue according to the collateral's borrowing rate.

- Pay back the SAFE debt

  When the SAFE creator wants to withdraw their collateral, they have to pay back their initial debt plus the accrued interest.

- Withdraw collateral

After the user pays back some or all of their debt, they are allowed to withdraw their collateral.

SAFE Liquidation

In order to keep the system solvent and cover the value of the entire outstanding debt, each SAFE can be liquidated in case its collateralization ratio falls under a certain threshold. Anyone can trigger a liquidation, in which case the system will confiscate the SAFE's collateral and sell it off in a *collateral auction*.

Liquidation Insurance

In one version of the system, SAFE creators can have the option to choose a *trigger* for when their SAFEs get liquidated. Triggers are smart contracts that automatically add more collateral in a SAFE and potentially save it from liquidation. Examples of triggers are contracts that sell short positions or contracts that communicate with insurance protocols such as Nexus Mutual [6].

Another method to protect SAFEs is the addition of two different collateralization thresholds: *safe* and *risk*. SAFE users can generate debt until they hit the safe threshold (which is higher than risk) and they only get liquidated when the SAFE's collateralization goes below the risk threshold.

Collateral Auctions

To start a collateral auction, the system needs to use a variable called *liquidationQuantity* in order to determine the amount of debt to be covered by every auction and the corresponding amount of collateral to be sold. A *liquidation penalty* will be applied to every auctioned SAFE.

Collateral Auction Parameters

Parameter Name	Description
minimumBid	Minimum amount of coins that need to be offered in one bid
discount	Discount at which collateral is being sold

lowerCollateralMedianDeviation	Max lower bound deviation that the collateral median can have compared to the oracle price
upperCollateralMedianDeviation	Max upper bound deviation that the collateral median can have compared to the oracle price
lowerSystemCoinMedianDeviation	Max lower bound deviation that the system coin oracle price feed can have compared to the system coin oracle price
upperSystemCoinMedianDeviation	Max upper bound deviation that the collateral median can have compared to the system coin oracle price
minSystemCoinMedianDeviation	Min deviation for the system coin median result compared to the redemption price in order to take the median into account

Collateral Auction Mechanism

The fixed discount auction is a straightforward way (compared to English auctions) to put collateral up for sale in exchange for system coins used to settle bad debt. Bidders are only required to allow the auction house to transfer their `safeEngine.coinBalance` and can then call `buyCollateral` in order to exchange their system coins for collateral which is sold at a discount compared to its latest recorded market price.

Bidders can also review the amount of collateral they can get from a specific auction by calling `getCollateralBought` or `getApproximateCollateralBought`. Note that `getCollateralBought` is not marked as view because it reads (and also updates) the `redemptionPrice` from the oracle relayer whereas `getApproximateCollateralBought` uses the `lastReadRedemptionPrice`.

Debt Auctions

In the scenario where a collateral auction cannot cover all the bad debt in a SAFE and if the system does not have any surplus reserves, anyone can trigger a debt auction.

Debt auctions are meant to mint more protocol tokens (Section 10) and sell them for indexes that can nullify the system's remaining bad debt.

In order to start a debt auction, the system needs to use two parameters:

- initialDebtAuctionAmount: the initial amount of protocol tokens to mint post-auction
- debtAuctionBidSize: the initial bid size (how many indexes must be offered in exchange for *initialDebtAuctionAmount* protocol tokens)

Autonomous Debt Auction Parameter Setting

The initial amount of protocol tokens minted in a debt auction can either be set through a governance vote or it can be automatically adjusted by the system. An automated version would need to be integrated with oracles (Section 6) from which the system would read the protocol token and reflex index market prices. The system would then set the initial amount of protocol tokens (*initialDebtAuctionAmount*) that will be minted for *debtAuctionBidSize* indexes. *initialDebtAuctionAmount* can be set at a discount compared to the actual PROTOCOL/INDEX market price in order to incentivize bidding.

Debt Auction Parameters

Parameter Name	Description
amountSoldIncrease	Increase in the amount of protocol tokens to be minted for the same amount of indexes
bidDecrease	Next bid's minimum decrease in the accepted amount of protocol tokens for the same amount of indexes
bidDuration	How long the bidding lasts after a new bid is submitted (in seconds)
totalAuctionLength	Total length of the auction (in seconds)
auctionsStarted	How many auctions have started until now

Debt Auction Mechanism

As opposed to collateral auctions, debt auctions only have one stage:

`decreaseSoldAmount(uint id, uint amountToBuy, uint bid)`: decrease the amount of protocol tokens accepted in exchange for a fixed amount of indexes.

The auction will be restarted if it has no bids placed. Every time it restarts, the system will offer more protocol tokens for the same amount of indexes. The new protocol token amount is calculated as *lastTokenAmount* * *amountSoldIncrease* / 100. After the auction settles, the system will mint tokens for the highest bidder.

Protocol Tokens

As described in earlier sections, each protocol will need to be protected by a token that is minted through debt auctions. Apart from protection, the token will be used to govern a few system components. Also, the protocol token supply will gradually be reduced with the use of surplus auctions. The amount of surplus that needs to accrue in the system before extra funds are auctioned is called the *surplusBuffer* and it is automatically adjusted as a percentage of the total debt issued.

Insurance Fund

Apart from the protocol token, governance can create an insurance fund that holds a wide array of uncorrelated assets and which can be used as a backstop for debt auctions.

Surplus Auctions

Surplus auctions sell stability fees accrued in the system for protocol tokens that are then burned.

Surplus Auction Parameters

Parameter Name	Description
bidIncrease	Minimum increase in the next bid
bidDuration	How long the auction lasts after a new bid is submitted (in seconds)
totalAuctionLength	Total length of the auction (in seconds)
auctionsStarted	How many auctions have started until now

Surplus Auction Mechanism

Surplus auctions have a single stage:

`increaseBidSize(uint id, uint amountToBuy, uint bid)`: anyone can bid a higher amount of protocol tokens for the same amount of indexes (surplus). Every new bid needs to be higher than or equal to *lastBid* * *bidIncrease* / 100. The auction will end after maximum *totalAuctionLength* seconds or after *bidDuration* seconds have passed since the latest bid and no new bids have been submitted in the meantime.

An auction will restart if it has no bids. On the other hand, if the auction has at least one bid, the system will offer the surplus to the highest bidder and will then burn all the gathered protocol tokens.

Surplus Indexes Management

Every time a user generates indexes and implicitly creates debt, the system starts applying a borrowing rate to the user's SAFE. The accrued interest is pooled in two different smart contracts:

- The *accounting engine* used to trigger debt (Section 9.2) and surplus (Section 10.1) auctions
- The *surplus treasury* used to fund core infrastructure components and incentivize external actors to maintain the system

The surplus treasury is in charge of funding three core system components:

- Oracle module (Section 6). Depending on how an oracle is structured, the treasury either pays governance whitelisted, off-chain oracles or it pays for calls toward oracle networks. The treasury can also be set up to pay the addresses that spent gas to call an oracle and update it

- In some cases, independent teams that maintain the system. Examples are teams who whitelist new collateral types or fine tune the system's rate setter (Section 4.2)

The treasury can be set up so that some surplus recipients will automatically be denied funding in the future and others can take their place.

External Actors

The system depends on external actors in order to function properly. These actors are economically incentivized to participate in areas such as auctions, global settlement processing, market making and updating price feeds in order to maintain the system's health.

We will provide initial user interfaces and automated scripts to enable as many people as possible to keep the protocol secure.

Addressable Market

We see RAI as being useful in two main areas:

- **Portfolio diversification**: investors use RAI to get dampened exposure to an asset like ETH without the whole risk of actually holding ether

- **Collateral for synthetic assets**: RAI can offer protocols such as UMA, MakerDAO and Synthetix a lower exposure to the crypto market and give users more time to exit their positions in the case of scenarios such as Black Thursday from March 2020 when millions of dollars worth of crypto assets were liquidated

Future Research

To push the boundaries of decentralized money and bring further innovation in decentralized finance, we will continue to look for alternatives in core areas such as governance minimization and liquidation mechanisms.

We first want to lay the groundwork for future standards around protocols that lock themselves from outside control and for true “money robots” which adapt in response to market forces. Afterwards, we invite the Ethereum community to debate and design improvements around our proposals with a specific focus on collateral and debt auctions.

Risks and Mitigation

There are several risks involved in developing and launching a reflex index, as well as subsequent systems that are built on top:

- **Smart contract bugs**: the greatest risk posed to the system is the possibility of a bug that allows anyone to extract all the collateral or locks the protocol in a state it cannot recover from. We plan to have our code reviewed by multiple security researchers and launch the system on a testnet before we commit to deploying it in production

- **Oracle failure**: we will aggregate feeds from multiple oracle networks and there will be strict rules in place for upgrading only one oracle at a time so that malicious governance cannot easily introduce false prices

- **Collateral black swan events**: there is the risk of a black swan event in the underlying collateral which can result in a high amount of liquidated SAFEs. Liquidations may not be able to cover the entire outstanding bad debt and so the system will continuously change its surplus buffer in order to cover a decent amount of issued debt and withstand market shocks

- **Improper rate setter parameters**: autonomous feedback mechanisms are highly experimental and may not behave exactly like we predict during simulations. We plan to allow governance to fine-tune this component (while still being bounded) in order to avoid unexpected scenarios

- **Failure to bootstrap a healthy liquidator market**: liquidators are vital actors that make sure all issued debt is covered by collateral. We plan to create interfaces and automated scripts so that as many people as possible can participate in keeping the system secure.

Summary

We have proposed a protocol that progressively locks itself from human control and issues a low volatility, collateralized asset called a reflex index. We first presented the autonomous mechanism meant to influence the index's market price and then described how several smart contracts can limit the power that token holders have over the system. We outlined a self-sustaining scheme for medianizing price feeds from multiple independent oracle networks and then finished by presenting the general mechanism for minting indexes and liquidating SAFEs.

References

[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

Glossary

Reflex index: a collateralized asset that dampens the volatility of its underlying

RAI: our first reflex index

Redemption Price: the price that the system wants the index to have. It changes, influenced by a redemption rate (computed by RRFM), in case the market price is not close to it. Meant to influence SAFE creators to generate more or pay back some of their debt

Borrowing Rate: annual interest rate applied to all SAFEs that have outstanding debt

Redemption Rate Feedback Mechanism (RRFM): an autonomous mechanism which compares the market and redemption prices of a reflex index and then computes a redemption rate that slowly influences SAFE creators to generate more or less debt (and implicitly tries to minimize the market/redemption price deviation)

Money Market Setter (MMS): a mechanism similar to RRFM which pulls multiple monetary levers at once. In the case of reflex indexes, it modifies both the borrowing rate and the redemption price

Oracle Network Medianizer (ONM): a smart contract that pulls prices from multiple oracle networks (which are not controlled by governance) and medianizes them if a majority (e.g 3 out of 5) returned a result without throwing

Restricted Governance Module (RGM): a set of smart contracts that bound the power that governance tokens holders have over the system. It either enforces time delays or limits the possibilities that governance has to set certain parameters

Governance Ice Age: immutable contract that locks most components of a protocol from outside intervention after a certain deadline has passed

Accounting Engine: system component which triggers debt and surplus auctions. It also keeps track of the amount of currently auctioned debt, unactioned bad debt and the surplus buffer

Surplus Buffer: amount of interest to accrue and keep in the system. Any interest

accrued above this threshold gets sold in surplus auctions that burn protocol tokens

Surplus Treasury: contract that gives permission to different system modules to withdraw accrued interest (e.g ONM for oracle calls)