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 kanilang sariling 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 matatagpuan sa maraming DeFi protocol.

Mga nilalaman

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 pamunuan 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. Lumilikha ang mga sitwasyong ito 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 redemption at kukunin nila 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 pinakamahalagang 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

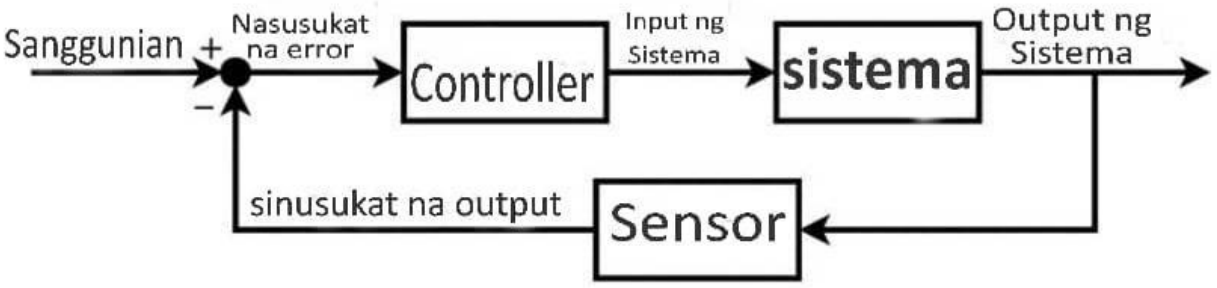
Panimula sa Teorya ng Kontrol

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 alisinsteady 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.

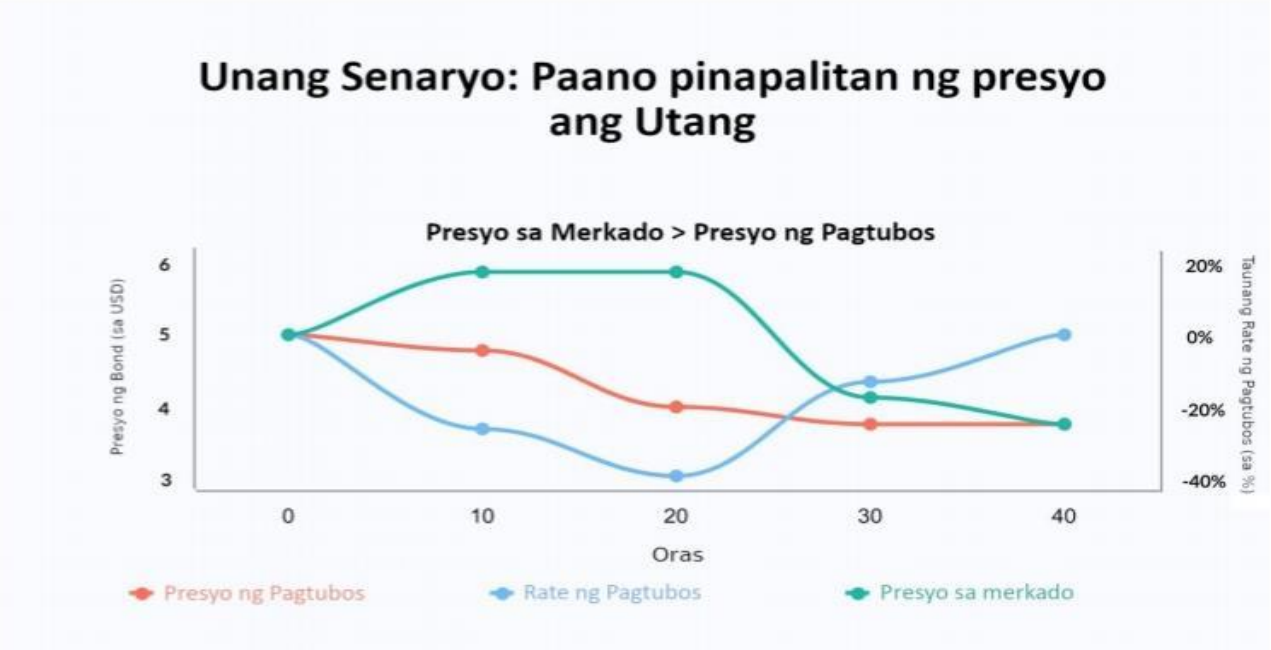
Sa pangkalahatan, natuklasan kamakailan na marami sa kasalukuyang mga panuntunan sa patakaran sa pananalapi ng sentral na bangko (hal. Taylor Rule) ay aktwal na mga pagtatantya ng PID mga controller [5].

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

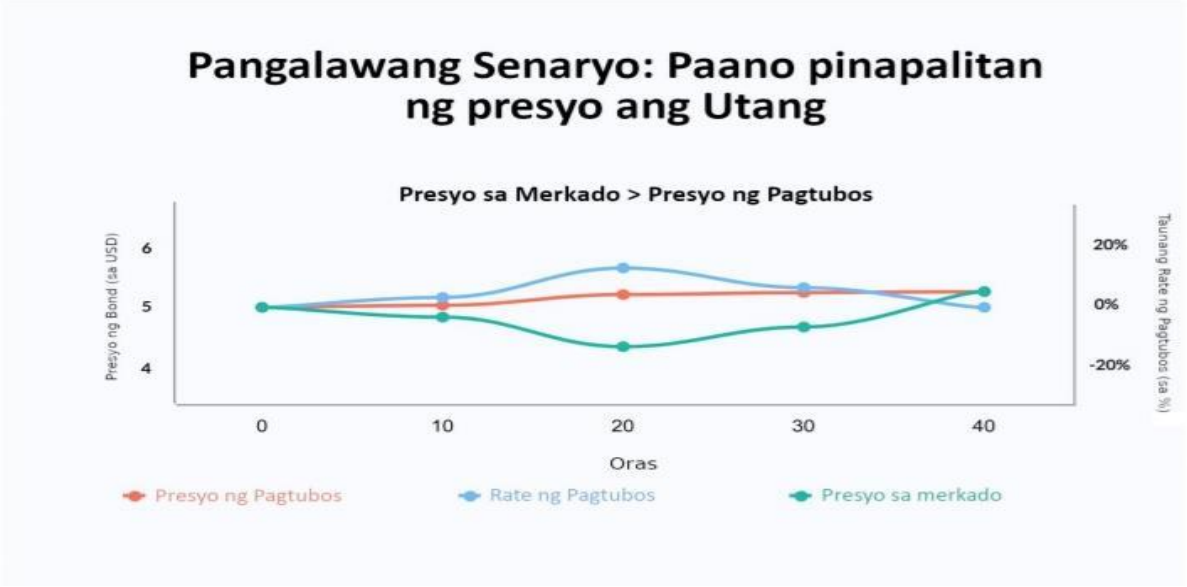
Alalahanin na ang mekanismo ng feedback ay naglalayong mapanatili ang ekwilibriyo sa pagitan ng presyo ng pagtubos at ng presyo sa merkado sa pamamagitan ng paggamit ng rate ng pagtubos upang kontrahin ang mga pagbabago sa mga puwersa ng pamilihan. Upang makamit ito, ang rate ng pagtubos ay kinakalkula 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 pagtubos 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 proporsyonal na termino p,ang na sa kasong ito ay -1 * (('rand' + x) / 'rand'). Ang proporsyonal ay negatibo upang bawasan ang presyo ng redemption at muling palitan ang mga index upang maging mas mura ang mga ito

- Pagkatapos kalkulahin ang proporsyonal, matutukoy 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 ang 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-Collateral DAI.

Kahit na plano naming panatilihing maayos 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 pagtubos, ang parehong mga rate ay magsisimulang bumaba, samantalang kung ito ay mas mababa sa pagtubos, ang

tataas ang mga rate.

Global 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

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

Restricted Migration Module

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 bagong system at pagwithdraw ng mga pahintulot mula sa luma

- Maaaring mag-set up ng isang opsyonal na kontrata upang awtomatiko nitong isara ang isang lumang system 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% matagal na lumihis kumpara sa redemption price

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 Orakulo

May tatlong pangunahing uri ng asset na kailangang basahin ng system ang mga feed ng presyo: ang index, ang protocol token at ang bawat naka-whitelist na uri ng collateral. Ang mga feed ng presyo ay maaaring ibigay ng mga oracle na pinangungunahan ng pamamahala o ng mga naitatag nang oracle network.

Mga Oracle na Pinangunahan ng Pamamahala

Ang mga may hawak ng token ng pamamahala o ang pangunahing team na naglunsad ng protocol ay maaaring makipagsosyo sa iba pang mga entity na kumukuha ng maraming mga feed ng presyo sa labas ng chain at pagkatapos ay magsumite ng isang transaksyon sa isang matalinong kontrata na nagpapagitna sa lahat ng mga punto ng data.

Ang diskarte na ito ay nagbibigay-daan para sa higit na kakayahang umangkop sa pag-upgrade at pagpapalit ng oracle na imprastraktura kahit na ito ay dumating sa kapinsalaan ng kawalan ng tiwala.

Oracle Network Medianizer

Ang oracle network medianizer ay isang matalinong kontrata na nagbabasa ng mga presyo mula sa maraming pinagmumulan na hindi direktang kinokontrol ng pamamahala (hal. Uniswap V2 pool sa pagitan ng index collateral type at iba pang stablecoin) at pagkatapos ay medianize ang lahat ng resulta. Gumagana ang ONM tulad ng sumusunod:

- Sinusubaybayan ng aming kontrata ang mga naka-whitelist na network ng oracle na maaari nitong tawagan upang humiling ng mga collateral na presyo. Ang kontrata ay pinondohan ng bahagi ng labis na naipon ng system (gamit ang Surplus Treasury, Seksyon 11). Ang bawat oracle network ay tumatanggap ng mga partikular na token bilang bayad kaya sinusubaybayan din ng aming kontrata ang pinakamababang halaga at ang uri ng mga token na kailangan para sa bawat kahilingan

- Upang itulak ang isang bagong feed ng presyo sa system, ang lahat ng mga orakulo ay kailangang tawagan muna. Kapag tumatawag ng oracle, pinapalitan muna ng kontrata ang ilang stability fee sa isa sa mga tinatanggap na token ng oracle. Pagkatapos tawagin ang isang orakulo, tina-tag ng kontrata ang tawag bilang "wasto" o "di-wasto". Kung ang isang tawag ay hindi wasto, ang tiyak na may sira na orakulo ay hindi maaaring tawaging muli hanggang sa ang lahat ng iba pa ay tinatawag na at ang kontrata ay nagsusuri kung mayroong isang wastong mayorya. Ang isang wastong tawag sa oracle ay hindi dapat bumalik at dapat itong makuha ang isang presyo na nai-post sa chain minsan sa huling m segundo. Ang ibig sabihin ng "Retrieve" ay iba't ibang bagay depende sa bawat uri ng orakulo:

    - Para sa mga pull based oracle, kung saan makakakuha tayo kaagad ng resulta, kailangang magbayad ang ating kontrata ng bayad at direktang kunin ang presyo

    - Para sa mga push based na oracle, ang aming kontrata ang nagbabayad ng bayad, tumawag sa oracle at kailangang maghintay ng partikular na tagal ng panahon n bago tumawag muli sa orakulo upang makuha ang hinihiling na presyo

- Ang bawat resulta ng orakulo ay nai-save sa isang array. Pagkatapos tawagin ang bawat naka-whitelist na oracle at kung ang array ay may sapat na valid na data point para makabuo ng mayorya (hal. ang kontrata ay nakatanggap ng valid na data mula sa 3/5 oracles), ang mga resulta ay pinagbubukod-bukod at pinipili ng kontrata ang median

- Nakahanap man ng mayorya ang kontrata o hindi, ang array na may mga resulta ng oracle ay na-clear at ang kontrata ay kailangang maghintay p segundo bago simulan muli ang buong proseso

Oracle Network Backup

Maaaring magdagdag ang pamamahala ng backup na opsyon sa oracle na magsisimulang mag-push ng mga presyo sa system kung hindi mahanap ng medianizer ang karamihan ng wastong mga network ng oracle nang maraming beses nang magkakasunod.

Ang backup na opsyon ay dapat itakda kapag ang medianizer ay na-deploy dahil hindi na ito mababago pagkatapos. Higit pa rito, maaaring masubaybayan ng isang hiwalay na kontrata kung masyadong matagal na pinapalitan ng backup ang mekanismo ng medianization at awtomatikong isinara ang protocol.

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 silang maa-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 magsisimulang 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 collateral

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 SAFE at potensyal na 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 para protektahan 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 upang ipagpalit ang kanilang 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 TinatayangCollateralBinili . 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 TinatayangCollateralBinili 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

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

: bawasanlowerSoldAmount(uint id, uint amountToBuy, uint bid) ang halaga ng 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:

: kahit sino ayincreaseBidSize(uint id, uint amountToBuy, uint bid) 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 surplus treasury ay namamahala sa pagpopondo ng tatlong pangunahing bahagi ng system:

- Oracle module (Seksyon 6). Depende sa kung paano nakaayos 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

Ang 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://bit.ly/2YL5S6j

[2] “UMA: Isang Desentralisadong Platform ng Kontrata sa Pinansyal”, https://bit.ly/2Wgx7E1

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

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

[5] RJ Hawkins, JK Speakes, DE Hamilton, "Monetary Policy at PID Control", https://bit.ly/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", https://bit.ly/3dqzNEU

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)