Rai: Isang Mababang Pagkasumpungin at Pinaliit na Tiwalang Panggarantiya para sa Ekosistema ng DeFi

Stefan C. Ionescu, Ameen Soleimani

Mayo 2020

Buod. Inihahandog namin ang pinaliit at desentralisadong protokol ng pamamahala na kusang tumutugon sa mga puwersa ng merkado upang baguhin ang punteryang halaga ng likas na panggarantiyang asset nito. Ang protokol ay nagbibigay-daan sa sinuman na gamitin ang kanilang mga kryptong asset at mag-isyu ng "indiseng reflex" na isang matamlay na bersyon ng pinagbabatayan nitong panggarantiya. Binabalangkas namin kung paano maaaring maging kapaki-pakinabang ang mga talatuntunan bilang isang unibersal at mababang pagkasumpunging garantiya na maaaring maprotektahan ang mga may hawak nito, pati na rin ang iba pang desentralisadong protokol na pinansyal, mula sa biglaang pagbabago ng merkado. Ipinakita namin ang aming mga plano upang matulungan ang ibang mga koponan na maglunsad ng sarili nilang mga sintetiko sa pamamagitan ng paggamit ng aming imprastraktura. Sa pag-tatapos, nag-alok kami ng mga alternatibo sa kasalukuyang orakulo at mga istruktura ng pamamahala na kadalasang makikita sa mga protokol ng DeFi.

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 walang malay na pangkalahatang publiko. Kung saan ipinakita ng Bitcoin ang potensyal para sa isang katutubong protesta upang magpakita ng store-of-value commodity asset, binibigyan tayo ng Ethereum ng plataporma para bumuo ng suportado ng asset na sintetikong instrumento na maaaring maprotektahan mula sa pagkasumpungin at magamit bilang garantiya, o nakakabit sa isang sanggunian na presyo at gamitin bilang daluyan ng palitan para sa mga pang araw-araw na transaksyon, lahat ay ipinapatupad ng parehong mga prinsipyo ng desentralisadong kasunduan.

Ang walang pahintulot na pag-access sa Bitcoin para sa pag-iimbak ng kayamanan at maayos na desentralisadong instrumentong sintetiko sa Ethereum ay maglalatag ng pundasyon para sa paparating na rebolusyong pinansyal, na nagbibigay sa mga modernong sistemang pinansyal ng paraan upang makipag-ugnayan sa pagbuo ng panibago.

Sa papel na ito, ipinakikilala namin ang isang balangkas para sa pagbuo ng mga indiseng reflex, isang bagong uri ng asset na tutulong sa iba pang mga sintetiko na umunlad at magtatatag ng isang pangunahing building block para sa buong desentralisadong industriya ng pinansyal.

Pangkalahatang-ideya ng Indiseng Reflex

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

Upang maunawaan ang mga indiseng reflex, maaari nating ihambing ang gawi ng kanilang presyo ng pagtubos sa presyo ng isang *stablecoin*.

Ang presyo ng pagtubos ay ang halaga ng isang yunit ng utang (o barya) sa sistema. Ito ay nilalayong gamitin lamang bilang isang panloob na kagamitan sa pananalapi 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 sistema na maaaring kunin ng sinuman ang isang barya para sa isang US dollar at sa gayon ang presyo ng pagtubos para sa mga baryang ito ay palaging isa. Mayroon ding mga kaso ng mga crypto-backed na stablecoin gaya ng Multi Collateral DAI (MCD) ng MakerDAO kung saan tina-target ng sistema ang isang nakapirming marka ng isang US dollar at sa gayon ang presyo ng pagtubos 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 pagtubos nito. Lumilikha ang mga sitwasyong ito ng mga pagkakataon sa arbitrahe kung saan ang mga traders ay gagawa ng mas maraming barya kung ang presyo sa merkado ay mas mataas kaysa sa pagtubos at kukunin nila ang kanilang mga stablecoin para sa kolateral (hal. US dollars sa kaso ng USDC) kung sakaling ang presyo sa merkado ay mas mababa kaysa sa presyo ng pagtubos.

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

Disenyo ng Pilosopiya at Puntahang-merkado na estratehiya

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 pagpapabuti sa disenyo ng RAI. Ang sistema ay na-audit nang husto at pormal na napatunayan, mayroon itong kaunting mga panlabas na dependensya 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 codebase ng MCD upang makamit ang aming implementasyon.

Kasama sa aming pinakamahahalagang pagbabago ang pagdaragdag ng isang awtomatikong pagtatakda ng singil, isang Tagapamagitan sa Network ng Orakulo na

isinama sa mga malayang balitaan ng presyo at isang patong ng mababang pamamahala na nilalayong ihiwalay ang sistema hangga't maaari mula sa pakikialam ng tao.

Ang pinakaunang bersyon ng protokol (Unang Yugto) ay kasama lang ang pagtatakda ng singil (rate setter) at iba pang maliliit na pag-aayos sa pangunahing arkitektura. Kapag napatunayan namin na gumagana ang pagtatakda gaya ng inaasahan, mas ligtas naming maidaragdag ang Tagapamagitan ng Orakulo (Pangalawang Yugto) at ang patong o layer ng mababang pamamahala (Pangatlong Yugto).

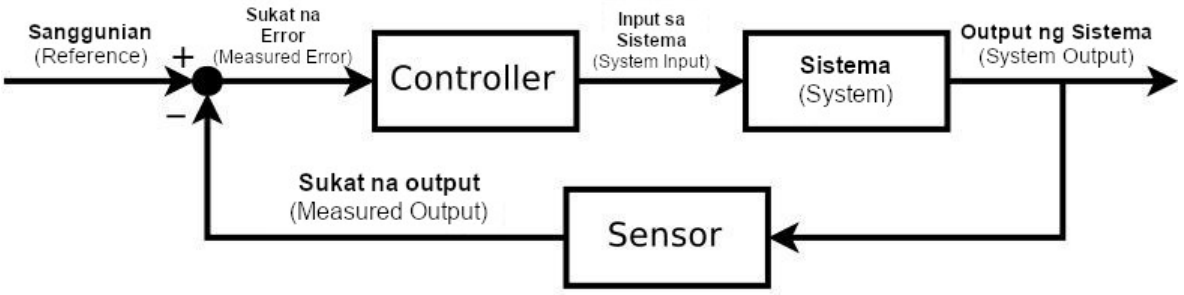
Mga Mekanismo ng Patakaran sa Salapi

Panimula sa Teorya ng Kontrol

Ang isang karaniwang sistema ng kontrol na pamilyar sa karamihan ng mga tao ay ang shower. Kapag ang isang tao ay nag shower, nasa isip nila ang nais na temperatura ng tubig na, sa teorya ng kontrol, ay tinatawag na *punto ng takdang reperensya*. Ang tao, na kumikilos bilang *magsusupil*, patuloy na sinusukat ang temperatura ng daloy ng tubig (na tinatawag na *output* ng sistema) at binabago ang bilis kung saan pinipihit nila ang pihihtan ng shower batay sa paglihis (*pagkakamali*) sa pagitan ng nais at kasalukuyang temperatura. Ang bilis ng pagpihit ng pihitan ay tinatawag na *input* ng sistema. Ang layunin niya na paikutin nang mabilis ang knob para mabilis na maabot ang punto ng takdang reperensya, ngunit hindi ganoon kabilis para *sumobra ang* temperatura. Kung may *biglaang pagbabago* sa sistema ukol sa temperatura ng daloy ng tubig, Kayang panatiliin ng tao ang kasalukuyang temperatura sa pamamagitan ng pag-alam kung gaano kabilis ipihit ang pihitan bilang pagtugon sa biglaang pagbabago.

Ang siyentipikong disiplina sa pagpapanatili ng katatagan sa mga pabago-bagong sistema ay tinatawag na teorya ng kontrol at ito ay nakahanap ng malawak na aplikasyon sa paglalayag ng kontrol para sa mga sasakyan, himpapawid na paglalayag, kemikal na reaktor, robotic arm, at industriyal na proseso ng lahat ng uri. Ang algoritmo sa pagsasaayos ng kahirapan sa Bitcoin na nagpapanatili ng karaniwang sampung minutong na block time, sa kabila ng pabago-bagong hashrate, ay isang halimbawa ng isang *mission critical control sistema*.

Sa karamihan ng mga modernong sistema ng kontrol ang isang *algorithmic controller* ay karaniwang naka-kabit sa proseso at binibigyan ito ng kontrol sa isang input ng sistema (hal. Pedal ng gas ng kotse) upang kusang mabago ito batay sa mga paglihis sa pagitan ng resulta ng sistema(hal. bilis ng kotse) at ang takdang punto (hal. Bilis ng cruise control).



Ang pinaka-karaniwang uri ng algorithmic controller ay ang *PID controller*. Higit sa 95% ng

mga pang-industriyang aplikasyon at malawak na hanay ng mga sistemang biyolohikal ay gumagamit ng mga elemento ng PID na kontrol [4]. Gumagamit ang PID controller ng matematikong pormula na may tatlong bahagi para matukoy ang resulta nito:

Controller Output = Proportional Term + Integral Term + Derivative Term

Ang *Proportional Term* ay ang bahagi ng controller na direktang *proporsyonal* sa paglihis (deviation). Kung ang paglihis ay malaki at positibo (hal. ang setpoint sa cruise control ay mas mataas kaysa sa kasalukuyang bilis ng sasakyan) ang proporsyonal na tugon ay magiging malaki at positibo (hal. Todong pedal ng gas).

Ang *Integral Term* ay ang bahagi ng controller na isinasaalang-alang kung gaano katagal nananatili ang isang paglihis (deviation). Natutukoy ito sa pamamagitan ng pagkuha ng *integral* ng paglihis sa paglipas ng panahon at ito ay pangunahing ginagamit upang maalis ang *steady state error*. Nag-iipon ito upang tumugon sa maliliit, kahit na patuloy ang mga paglihis mula sa setpoint (hal. ang setpoint ng kontrol ng bilis 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 paglihis (deviation). Natutukoy ito sa pamamagitan ng pagkuha ng *derivative* ng paglihis at nagsisilbing pabilisin ang tugon ng controller kapag lumalaki ang paglihis (hal., pabilisin ang takbo kung mas mataas ang setpoint ng cruise control kaysa sa bilis ng sasakyan at nagsimulang bumagal ang sasakyan). Nakatutulong din itong bawasan ang pag-sobra o *overshoot* sa pamamagitan ng pagbabawas ng bilis ng tugon ng controller kapag lumiliit ang paglihis (hal., bagalan ang pagtakbo habang ang bilis ng sasakyan ay nagsisimulang lumapit sa takdang punto ng cruise control).

Ang kombinasyon ng tatlong bahaging ito, na ang bawat isa ay maaaring na mai-tune, ay nagbibigay sa mga PID controller ng mahusay na kakayahang umangkop sa pangangasiwa ng isang malawak na iba't ibang mga aplikasyon ng sistemang kontrol.

Pinakamahusay na gumagana ang mga PID controller sa mga sistema na nagbibigay-daan sa ilang antas ng pagkaantala sa oras ng pagtugon pati na rin ang posibilidad ng pagsobra at osilasyon sa paligid ng takdang punto habang sinusubukan ng sistema na patatagin ang sarili nito. Ang mga indiseng reflex sistema tulad ng RAI ay angkop para sa ganitong uri ng senaryo kung saan ang kanilang mga presyo ng pagtubos ay maaaring baguhin ng mga PID controller.

Sa pangkalahatan, kamakailang natuklasan na marami sa kasalukuyang mga patakaran sa pananalapi ng bangko sentral (hal. Taylor Rule) ay aktwal na pagtatantya ng mga PID

controller [5].

Mekanismo ng Katugunan sa Singil ng Pagtubos

Ang mekanismo ng katugunan sa singil ng pagtubos ay ang bahagi ng sistema na namamahala sa pagbabago ng presyo ng pagtubos ng indiseng reflex. Upang maunawaan kung paano ito gumagana, kailangan muna nating ilarawan kung bakit kailangan ng sistema ng mekanismo ng feedback kumpara sa paggamit ng manu-manong kontrol at kung ano ang output ng mekanismo.

Mga Bahagi ng Mekanismo ng Katugunan

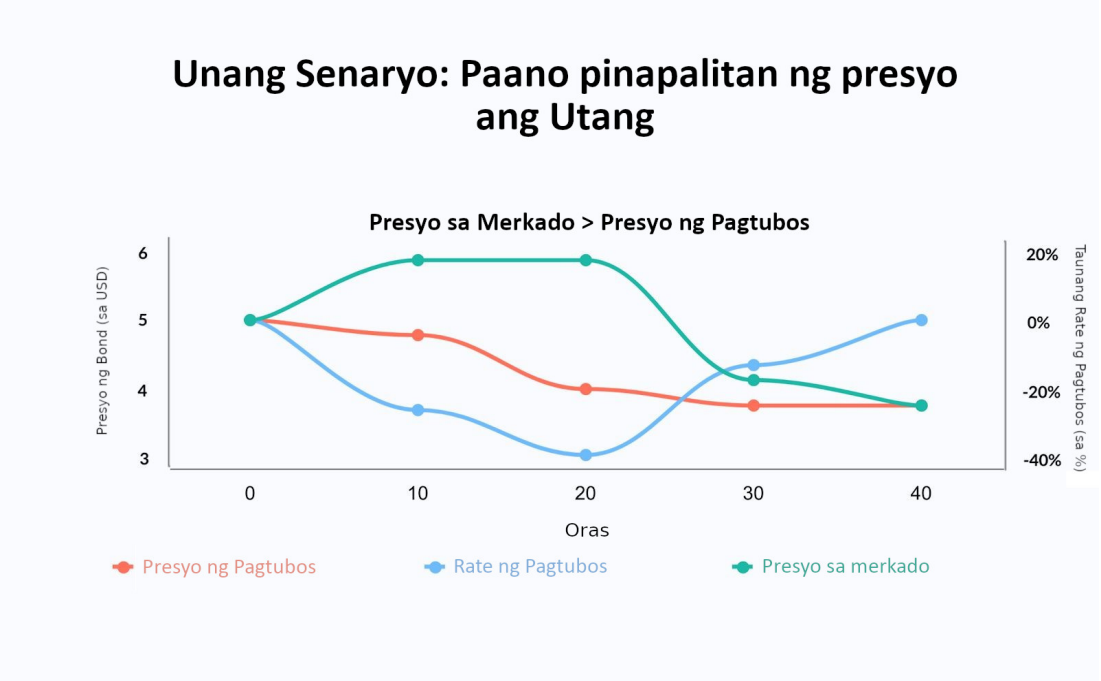
Sa teorya, posibleng direktang manipulahin ang presyo ng pagtubos ng indiseng reflex (inilalarawan sa Seksyon 2) upang maimpluwensyahan ang mga gumagamit ng indise at sa huli ay baguhin ang presyo ng merkado ng indise. Sa pagsasagawa, ang pamamaraang ito ay hindi magkakaroon ng nais na epekto sa mga kalahok sa sistema. Mula sa pananaw ng isang may hawak ng SAFE , kung isang beses lang tumaas ang presyo ng pagtubos, maaari silang tumanggap ng mas mataas na presyo sa bawat unit ng utang, makuha ang pagkalugi mula sa pinababang proposyon ng panggarantiya at mapanatili ang kanilang posisyon. Kung, gayunpaman, inaasahan nilang patuloy na tataas ang presyo ng pagtubos sa paglipas ng panahon, malamang na mas gusto nilang maiwasan ang inaasahang pagkalugi 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 sistema ng indiseng reflex ay hindi direktang tutugon sa mga pagbabago sa presyo ng pagtubos, ngunit sa halip ay tutugon sa *pagbabago ng singil sa presyo ng pagtubos* na tinatawag nating *presyo ng pagtubos*. Ang singil sa pagtubos ay itinatakda ng isang *mekanismo ng katugunan* na ang pamamahala ay maaaring maisaayos (fine-tune) o payagan na maging ganap na awtomatikong pamamahala.

Mga Sitwasyon ng Mekanismo ng Katugunan

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

Sa unang senaryo sa ibaba, kung ang presyo ng merkado ng indise ay mas mataas kaysa sa presyo ng pagtubos nito, kakalkulahin ng mekanismo ang isang negatibong rate na magsisimulang bawasan ang presyo ng pagtubos, gayumpaman mas mura ang utang ng sistema.

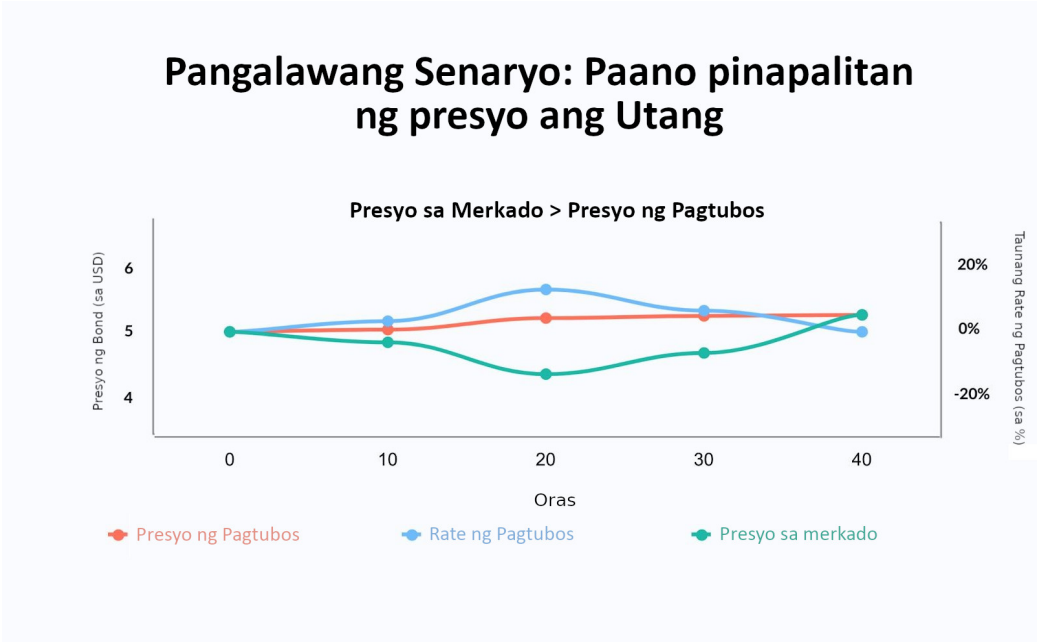


Ang inaasahan sa isang bumababa na presyo ng pagtubos ay malamang na pahinain ang loob ng mga tao na humawak ng mga indise at mahikayat ang mga may hawak ng SAFE na bumuo ng mas maraming utang (kahit na ang presyo ng panggarantiya ay hindi nagbabago) na pagkatapos ay ibinebenta sa merkado, dahilan para mabalanse ang suplay at demand. Tandaan na ito ang perpektong senaryo kung saan mabilis na nagre-react ang mga may hawak ng indise bilang tugon sa mekanismo ng katugunan. Sa pagsasagawa (at lalo na sa mga unang araw pagkatapos ng paglulunsad) inaasahan namin ang isang lag sa pagitan ng pagsisimula ng mekanismo at mga aktwal na resulta na makikita sa halaga ng utang na ibinigay at pagtapos sa presyo ng merkado.

Sa kabilang banda, sa pangalawang senaryo, kapag ang presyo ng merkado ng indise 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 proporsyon ng panggarantiya ng lahat ng SAFE (kaya nabibigyang-insentibo ang mga tagalikha ng SAFE

na bayaran ang kanilang utang) at nagsisimulang mag-imbak ang mga gumagamit ng mga indise na may inaasahang pagtaas sa halaga ng mga ito.



Mekanismo ng Algoritmo sa Katugunan

Sa sumusunod na senaryo, ipinapalagay natin na ang protokol ay gumagamit ng proportional-integral na magsusupil para kalkulahin ang singil ng pagtubos:

- Ang indiseng reflex ay inilunsad na may arbitraryong presyo ng pagtubos na 'rand'
- Sa ilang punto, ang presyo ng merkado ng indise ay tumataas 'rand' sa 'rand' + x. Pagkatapos basahin ng mekanismo ng katugunan ang bagong presyo sa merkado, kinakalkula nito ang proportional term *p*, kung saan sa kasong ito ay -1 * (('rand' + x) / 'rand'). Negatibo ang proportional upang bawasan ang presyo ng pagtubos at muling palitan ang presyo ng mga indise upang maging mas mura ang mga ito
- Pagkatapos kalkulahin ang *proportional*, matutukoy ng mekanismo ang integral term *i* sa pamamagitan ng pagdaragdag ng lahat ng mga nakaraang paglihis mula sa huling segundo ng *deviationInterval*
- Binubuo ng mekanismo ang proportional at integral at kinakalkula ang bawat segundong singil ng pagtubos *r* na dahan-dahang nagsisimulang bumaba sa presyo ng pagtubos. Habang napagtatanto ng mga lumikha ng SAFE na maaari silang makabuo ng mas malaking utang, dadagsain nila ang merkado ng mas maraming indise

- pagkatapos ng *n* segundo, nakita ng mekanismo na ang paglihis sa pagitan ng merkado at mga presyo ng pagtubos ay pwedeng bale-walain (sa ilalim ng isang tinutukoy na parametrong *ingay*). Sa puntong ito, itinatakda ng algoritmo ang *r* sa zero at pinapanatili ang presyo ng pagtubos kung nasaan ito

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

Pag-sasaayos ng Mekanismo ng Katugunan

Ang pinakamahalaga sa wastong pag-papagana ng sistema ng indiseng reflex ay ang pag-sasayos ng mga parametro ng algorithmic controller. Ang hindi paglalagay ng tamang parametro ay maaaring magresulta sa pagiging mabagal ng sistema upang makamit ang katatagan, malakihang pagsobra, o sa pangkalahatan ay hindi pagiging matatag sa mga panlabas na problema.

Ang proseso ng pag-sasaayos para sa isang PID controller ay karaniwang nagsasangkot ng pagpapatakbo ng live na sistema, pagsusubok sa mga parametro ng pagsasaayos, at pag-oobserba sa tugon ng sistema, madalas na sadyang nagpapalitaw ng mga problema sa daan. Dahil sa kahirapan at pinansyal na panganib ng pagsasaayos ng mga parametro ng isang live na indiseng reflex sistema, plano naming gamitin ang pagmomodelo at simulasyon ng kompyuter hangga't maaari upang itakda ang mga inisyal na parametro, ngunit papayagan din ang namamahala na baguhin ang mga parametro ng pagsasaayos kung may karagdagang datos mula sa produksyon kung ang mga ito ay sub-optimal.

Setter ng Pamihilan ng Pera

Sa RAI, pinaplano naming panatilihing nakapirmi o limitado ang singil ng paghiram o *borrowing rate* (nalalapat na singil ng interes kapag bumubuo ng mga indise) at nababago lamang ang presyo ng pagtubos, dahilan para mabawasan ang pagiging kumplikado sa pagmomodelo ng mekanismo ng feedback. Ang rate ng paghiram sa aming kaso ay katumbas ng pagkalat sa pagitan ng bayad sa katatagan (stability fee) at DSR sa Multi-Collateral DAI.

Kahit na plano naming panatilihing nakapirmi ang singil ng paghiram, posibleng baguhin ito kasama ng presyo ng pagtubos gamit ang setter ng pamilihan ng pera. Binabago ng pamihilan ng pera ang rate ng paghiram at ang presyo ng redemption sa paraang nag-uudyok sa mga lumikha ng SAFE na bumuo ng mas marami o mas kaunting utang. Kung

ang presyo sa merkado ng isang indise 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 Pamayanan

Ang pandaigdigang settlement ay isang paraan ng huling paraan na ginagamit upang magarantiya ang presyo ng pagtubos sa lahat ng may hawak ng indiseng reflex. Nilalayon nitong payagan ang mga may hawak ng indiseng reflex at SAFE creator na kunin ang collateral ng sistema sa netong halaga nito (dami ng mga indise 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 gumagamit ng mga SAFE, lahat ng feed ng presyo ng panggarantiya at ang presyo ng pagtubos ay naka-tigil at nakatala

- **Proseso**: iproseso ang lahat ng natitirang subasta

- **Pag-angkin** : bawat may hawak ng indiseng reflex at lumikha ng SAFE ay maaaring mag-angkin ng nakapirming halaga ng anumang panggarantiya ng sistema batay sa huling naitalang presyo ng pagtubos ng indise

Pamamahala

Ang karamihan sa mga parametro ay hindi nababago at ang panloob na mekanika ng matalinong kontrata (smart contracts) ay hindi maa-upgrade maliban kung ang mga may hawak ng token ng pamamahala ay mag-patayo 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, dahilan para masira ang tiwala sa sistema. Itinatag namin ang wastong operasyon ng protokol nang hindi masyadong naniniwala sa mga tao (ang “epektong bitcoin”) para mapalaki namin ng labis ang sosyal na 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 parametro na maaaring baguhin, ipinapanukala namin ang pagdaragdag ng isang Modyul ng Pinaghihigpitang Migrasyon na sinadya upang maantala o itali ang lahat ng posibleng pagbabago sa sistema. Bukod dito, inihahandog namin ang Pamamahalang Kapanahunan ng Kalamigan, isang talaan ng mga pahintulot na maaaring i-kandado ang ilang bahagi ng sistema mula sa labas ng kontrol pagkatapos lumipas ang ilang mga huling araw o oras.

Pamamahalang Nakatali sa Oras

Ang Pamamahalang Nakatali sa Oras ay ang unang bahagi ng Modyul ng Pinaghihigpitang Pamamahala. Nagpapataw ito ng mga pagkaantala sa oras sa pagitan ng mga pagbabagong inilapat sa parehong parametro. Ang isang halimbawa ay ang posibilidad na baguhin ang mga address ng mga orakulo na ginamit sa Tagapamagitan sa Network ng Orakulo (Seksyon 6.2) pagkatapos ng hindi bababa sa *T* na oras ang lumipas mula noong huling pagbabago sa orakulo.

Pamamahalang Nakatali sa Aksyon

Ang pangalawang bahagi sa Modyul ng Pinaghihigpitang Pamamahala ay Pamamahalang Nakatali sa Aksyon. Ang bawat napapamahalaang parametro ay may mga limitasyon sa kung anong mga halaga ang maaaring itakda at kung gaano ito maaaring magbago sa isang partikular na yugto ng panahon. Ang mga kapansin-pansing halimbawa ay ang mga unang bersyon ng Mekanismo ng Katugunan sa Singil ng Pagtubos (Seksyon 4.2) kung saan ang mga may hawak ng token ng pamamahala ay magagawang mag-saayos.

Pamamahalang Panahon ng Kalamigan

Ang Panahon ng Kalamigan ay isang hindi nababagong matalinong na nagpapataw ng mga huling araw o oras sa pagbabago ng mga partikular na parametro ng sistema at sa pag-upgrade ng protokol. Maaari itong gamitin sa kaso kung saan gustong tiyakin ng pamamahala na maaayos nila ang mga problema (bug) bago i-lock ang sarili nitong protokol at tanggihan ang interbensyon sa labas. Be-beripikahin ng Panahon ng Kalamigan kung pinahihintulutan ang isang pagbabago sa pamamagitan ng pagsuri sa pangalan ng parametro at address ng apektadong kontrata laban sa isang talaan ng mga huling araw o oras. Kung lumipas na ang huling araw o oras, babalik ang tawag.

Maaaring maantala ng Pamamahalang Panahon ng Kalamigan nang ilang beses kung may makikitang mga problema malapit sa petsa kung kailan dapat magsimulang i-lock ang

sarili nitong protokol. Halimbawa, ang Panahon ng Kalamigan ay maaari lamang maantala ng tatlong beses, bawat oras sa loob ng isang buwan, upang ang mga bagong ipinatupad na pag- aayos ng problema 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 panggarantiya**: Ang RAI ay susuportahan lamang ng ETH, ngunit ang iba pang mga indise ay susuportahan ng maraming uri ng panggarantiya at magagawa ng pamamahala upang pag-iba-ibahin ang panganib sa paglipas ng panahon

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

- **Pagsasaayos ng setter ng singil**: Magkakaroon ng mga parametro ang maagang monetary policy controllers na maaaring baguhin sa loob ng makatwirang mga hangganan (tulad ng inilalarawan ng Pamamahalang nakatali sa Aksyon at Oras)

- **Paglipat sa pagitan ng mga bersyon ng sistema**: sa ilang mga kaso, ang pamamahala ay maaaring mag patayo ng isang bagong sistema, bigyan ito ng pahintulot na mag-limbag ng mga token ng protokol at bawiin ang pahintulot na ito mula sa isang lumang sistema. Isinasagawa ang paglipat na ito sa tulong ng Modyul ng Pinaghihigpitang Migrasyon na nakabalangkas sa ibaba

Modyul ng Pinaghihigpitang Migrasyon

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

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

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

- Mayroong panahon ng cooldown sa pagitan ng pagmumungkahi ng isang bagong sistema at pag- withdraw 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-imprenta

Ang modyul ng migrasyon ay maaaring isama sa isang Panahon ng Kalamigan na awtomatikong nagbibigay ng pahintulot sa mga partikular na sistema na palaging makapag-imprenta ng mga token.

Awtomatikong Pagsasara ng Sistema

May mga kaso na maaaring awtomatikong makita ng sistema at bilang resulta ay nag-trigger ng pag-aayos nang mag-isa, nang hindi kinakailangang mag-sunog ng mga token ng protokol:

- **Matinding Pagkaantala sa Feed ng Presyo** : nakita ng sistema na ang isa o higit pa sa mga panggarantiya o feed ng presyo ng indise ay hindi na-update sa mahabang panahon

- **Migrasyon ng Sistema** : isa itong opsyonal na kontrata na maaaring mag-sara ng protokol pagkatapos lumipas ang panahon ng cooldown mula sa sandaling binawi ng pamamahala ang kakayahan ng mekanismo ng subasta ng utang na mag-imprenta ng mga token ng potokol (Modyul ng Pinaghihigpitang Migrasyon, Seksyon 5.4.1)

- **Naaalinsunod na Paglihis sa Presyo ng Merkado** : nakita ng sistema na ang presyo ng merkado ng indise ay naging *x%* katagal na lumihis kumpara sa presyo ng pagtubos

Magagawa ng Pamamahala na i-upgrade ang mga nagsasariling modyul ng pagsara na ito habang nililimitahan pa rin o hanggang sa magsimulang i-kandado ng Panahon ng Kalamigan ang ilang bahagi ng sistema.

Mga Orakulo

May tatlong pangunahing uri ng asset na kailangang basahin ng sistema ang mga feed ng presyo: ang indise, ang token ng protokol at ang bawat naka-whitelist na uri ng panggarantiya. Ang mga feed ng presyo ay maaaring ibigay ng mga orakulo na pinangungunahan ng pamamahala o ng mga naitatag nang network ng orakulo.

Mga Oracle na Pinangunahan ng Pamamahala

Ang mga may hawak ng token ng pamamahala o ang pangunahing grupo na naglunsad ng protokol ay maaaring makipagsosyo sa iba pang mga entidad na kumukuha ng maraming

mga feed ng presyo sa labas ng kadena 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 orakulo na imprastraktura kahit na ito ay dumating sa kapinsalaan ng kawalan ng tiwala.

Pamamahalang Pinangunahan ng Orakulo

Ang Pamamahalang Pinangunahan ng Orakulo ay isang matalinong kontrata na nagbabasa ng mga presyo mula sa maraming pinagkukunan na hindi direktang kinokontrol ng pamamahala (hal. Uniswap V2 pool sa pagitan ng isang indiseng panggarantiyang uri at iba pang stablecoin) at pagkatapos ay ginagawang panggitnaan ang lahat ng resulta. Gumagana ang ONM tulad ng sumusunod:

- Sinusubaybayan ng aming kontrata ang mga naka-whitelist na network ng orakulo na maaari nitong tawagan upang humiling ng mga panggarantiya na presyo. Ang kontrata ay pinondohan ng bahagi ng labis na naipon ng sistema (gamit ang Labis na Pananalapi, Seksyon 11). Ang bawat network ng orakulo 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 sistema, ang lahat ng mga orakulo ay kailangang tawagan muna. Kapag tumatawag ng orakulo, pinapalitan muna ng kontrata ang ilang bayad sa katatagan sa isa sa mga tinatanggap na token ng oracle. Pagkatapos tumawag ng 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 "Bawiin" ay iba't ibang bagay depende sa bawat uri ng orakulo:

    - Para sa mga nakabatay sa pag-hila na orakulo, kung saan makakakuha

tayo kaagad ng resulta, kailangang magbayad ang ating kontrata ng bayad at direktang kunin ang presyo

- Para sa mga nakabatay sa pag-tulak na orakulo, binabayaran ng aming kontrata ang bayad, tumawag sa orakulo at kailangang maghintay ng isang 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 orakulo at kung ang array ay may sapat na wastong punto ng datos para makabuo ng mayorya (hal. ang kontrata ay nakatanggap ng wastong data mula sa 3/5 na orakulo), ang mga resulta ay pinagbubukod-bukod at pipiliin ng kontrata ang median

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

Backup sa Network ng Orakulo

Maaaring magdagdag ang pamamahala ng backup na opsyon sa orakulo na magsisimulang mag-tulak ng mga presyo sa sistema kung hindi mahanap ng tagapamagitan ang karamihan ng mga wastong network ng orakulo nang maraming beses nang magkakasunod.

Ang backup na opsyon ay dapat itakda kapag ang tagapamagitan 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 indise, sinuman ay maaaring magdeposito at gumamit ng kanilang panggarantiyang crypto sa loob ng Safes. Habang binuksan ang isang SAFE,

magpapatuloy ito sa pag-iipon ng utang ayon sa sinil ng paghiram ng nakadeposito na panggrantiya. Habang binabayaran ng gumawa ng SAFE ang kanilang utang, mas marami na silang ma-withdraw ng kanilang naka-kandadong panggarantiya.

Siklo ng Buhay ng SAFE

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

- Magdeposito ng panggarantiya sa SAFE

  Kailangan muna ng gumagamit na lumikha ng bagong SAFE at magdeposito ng panggarantiya dito.

- Bumuo ng mga indise na sinusuportahan ng panggarantiya ng SAFE

  Tinukoy ng user kung gaano karaming mga indise ang gusto nilang buuin. Lumilikha ang sistema ng pantay na halaga ng utang na magsisimulang maipon ayon sa singil ng paghiram ng panggarantiya.

- Bayaran ang SAFE na utang

  Kapag gustong bawiin ng SAFE creator ang kanilang garantiya, kailangan nilang bayaran ang kanilang paunang utang kasama ang naipon na interes.

- Mag-withdraw ng garantiya

Pagkatapos mabayaran ng gumagamit ang ilan o lahat ng kanilang utang, pinapayagan silang bawiin ang kanilang garantiya.

Likidasyon ng SAFE

Upang mapanatiling nakakatunaw ang sistema at masakop ang halaga ng buong natitirang utang, maaaring likidahin ang bawat SAFE kung sakaling ang panggarantiyng katumbas nito ay bumaba sa ilalim ng isang tiyak na kasukatan o threshold. Kahit sino ay maaaring mag-trigger ng likidasyon, kung saan kukumpiskahin ng sistema ang garantiya ng SAFE at ibebenta ito sa isang *subasta ng panggarantiya*.

Insurance sa Likidasyon

Sa isang bersyon ng sistema, maaaring magkaroon ng opsyon ang mga lumikha ng SAFE na pumili ng *trigger* para kapag nalikida ang kanilang mga SAFE. Ang mga trigger ay mga matalinong kontrata na awtomatikong nagdaragdag ng higit pang garantiya sa isang SAFE at potensyal na i-salba ito mula sa likidasyon. Ang mga halimbawa ng mga trigger ay mga kontrata na nagbebenta ng mga maiikling posisyon o kontrata na nakikipag-ugnayan sa mga protokol 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 panggarantiya: *ligtas* at *panganib*. *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-likida lang sila kapag ang panggarantiya ng SAFE ay mas mababa sa threshold ng panganib.

Subasta sa Panggarantiya

Para magsimula ng subasta sa panggarantiya, kailangang gumamit ang sistema ng variable na tinatawag *liquidationQuantity* upang matukoy ang halaga ng utang na sasakupin ng bawat subasta at ang katumbas na halaga ng garantiya na ibebenta. Ang *liquidation penalty* ay ilalapat sa bawat SAFE na naka subasta.

Mga Parametro ng Subasta sa Panggarantiya

Pangalan ng Parametro	Paglalarawan
minimumBid	Pinakamababang halaga ng mga barya na kailangan iaalok sa isang taya (bid)
discount	Diskwento ng ibinebentang panggarantiya

lowerCollateralMedianDeviation	Pinakamababang hangganan ng paglihis na maaaring magkaroon ng panggitnang panggarantiya kumpara sa ang presyo ng orakulo
upperCollateralMedianDeviation	Pinakataas na hangganan ng paglihis na maaaring magkaroon ng panggitnang panggarantiya kumpara sa ang presyo ng orakulo
lowerSystemCoinMedianDeviation	Pinakamababang hangganan ng paglihis na maaaring magkaroon ng barya ng sistema ng feed ng presyo ng orakulo kumpara sa barya ng sistema ng presyo ng orakulo
upperSystemCoinMedianDeviation	Pinakataas na hangganan ng paglihis na maaaring magkaroon ng panggitnang panggarantiya kumpara sa barya ng sistema ng presyo ng orakulo
minSystemCoinMedianDeviation	Pinakamababang paglihis para sa resulta ng panggitnang barya ng sistema kumpara sa presyo ng pagtubos upang kunin ang panggitna sa account

Mekanismo ng Subasta sa Panggarantiya

Ang nakapirming diskwento na subasta ay isang direktang paraan (kumpara sa subastang Ingles) para maglagay ng panggarantiya para sa pagbebenta kapalit ng mga barya ng sistema na ginamit upang bayaran ang masamang utang. Kinakailangan lamang ng mga tumataya (bidder) na payagan ang bahay ng subasta na ilipat ang kanilang safeEngine.coinBalance at pagkatapos ay maaaring tumawag sa buyCollateral upang mapalitan ang kanilang barya ng sistema para sa panggarantiya na ibinebenta nang may diskwento kumpara sa pinakahuling naitala nito presyo sa pamilihan.

Maaari ding suriin ng mga tumataya ang halaga ng panggarantiya na makukuha nila mula sa isang partikular na subasta sa pamamagitan ng pagtawag sa getCollateralBought o getApproximateCollateralBought. Tandaan na ang getCollateralBought ay hindi minarkahan bilang nakita dahil binabasa nito (at ina-update din) ang redemptionPrice mula sa relayer ng orakulo samantalang ang ApproximateCollateralBought ay gumagamit ng lastReadRedemptionPrice.

Subasta ng Utang

Sa senaryo kung saan hindi masakop ng subasta ng panggarantiya ang lahat ng masamang utang sa isang SAFE at kung ang sistema ay walang anumang labis na reserba, sinuman ay maaaring mag-trigger ng isang subasta ng utang.

Ang mga subasta ng utang ay sinadya upang gumawa ng higit pang mga token ng protokol (Seksyon 10) at ibenta ang mga ito para sa mga indise na maaaring magpawalang-bisa sa natitirang masamang utang ng sistema.

Upang makapagsimula ng isang subasta ng utang, kailangang gumamit ang sistema ng dalawang parametro:

- `initialDebtAuctionAmount`: ang paunang halaga ng mga token ng protokol na gagawin pagkatapos ng subasta
- `debtAuctionBidSize`: ang paunang laki ng taya (kung gaano karaming mga indise ang dapat ialok kapalit para sa *initialDebtAuctionAmount na mga* token ng protokol)

Setting ng Parametro ng Nagkukusang Subasta ng Utang

Ang paunang halaga ng mga protokol na token na nagawa sa isang subasta ng utang ay maaaring itakda sa pamamagitan ng boto sa pamamahala o maaari itong awtomatikong iakma ng sistema. Ang isang awtomatikong bersyon ay kailangang isama sa mga orakulo (Seksyon 6) kung saan babasahin ng sistema ang token ng protokol at indiseng reflex na mga presyo sa merkado. Itatakda ng sistema ang paunang halaga ng mga token ng protokol (*initialDebtAuctionAmount*) na gagawin para sa debt*AuctionBidSize* na mga indise. Ang *initialDebtAuctionAmount* ay maaaring itakda sa isang diskwento kumpara sa aktwal na presyo ng merkado ng PROTOCOL/INDEX upang makapag-bigay insentibo ang pag-bid.

Mga Parametro ng Subasta ng Utang

Pangalan ng Parametro	Paglalarawan
amountSoldIncrease	Pagtaas sa dami ng token ng protokol na gagawa para sa parehong dami ng mga indise
bidDecrease	Ang susunod na minimum na pagbaba ng taya sa tinatanggap na halaga ng mga token ng protokol para sa parehong dami ng mga indise
bidDuration	Gaano katagal ang pag-taya pagkatapos ng bagong naisumiteng taya (naka segundo)
totalAuctionLength	Kabuuang haba ng subasta (naka segundo)
auctionsStarted	Ilang subasta ang nagsimula hanggang ngayon

Mekanismo ng Subasta ng Utang

Taliwas sa mga subastang panggarantiya, ang mga subasta ng utang ay mayroon lamang isang yugto:

`decreaseSoldAmount(uint id, uint amountToBuy, uint bid)`: Bawasan ang dami ng tinanggap ang mga protocol na token kapalit ng isang nakapirming halaga ng mga indise.

Ang subasta ay magsisimulang muli kung wala itong mga taya na inilagay. Sa tuwing magre-restart ito, mag-aalok ang sistema ng mas maraming token ng protokol para sa parehong dami ng mga indise. Ang bagong halaga ng token ng protokol ay kinakalkula bilang *lastTokenAmount* **amountSoldIncrease* / 100. Pagkatapos mag-ayos ang subasta, ang sistema ay gagawa ng mga token para sa pinakamataas na taya.

Mga Token ng Protocol

Gaya ng inilarawan sa mga naunang seksyon, ang bawat protokol ay kailangang protektahan ng isang token na nagawa sa pamamagitan ng mga subasta ng utang. Bukod sa proteksyon, ang token ay gagamitin para pamahalaan ang ilang bahagi ng sistema.

Gayundin, ang supply ng token ng protokol ay unti-unting mababawasan sa paggamit ng mga subasta ng kalabisan. Ang halaga ng kalabisan na kailangang maipon sa sistema bago i-subasta ang mga karagdagang pondo ay tinatawag na *surplusBuffer* at ito ay awtomatikong inaayos bilang isang porsyento ng kabuuang utang na ibinigay.

Pondo ng Insurance

Bukod sa token ng protokol, ang pamamahala ay maaaring lumikha ng isang pondo ng insurance na nagtataglay ng malawak na hanay ng mga hindi nauugnay na asset at maaaring magamit bilang tulong para sa mga subasta sa utang.

Mga Subasta ng Kalabisan

Ang mga surplus na auction ay nagbebenta ng mga bayad sa katatagan na naipon sa sistema para sa mga token ng protokol na sinusunog.

Mga Surplus na Parametro ng Auction

Pangalan ng Parametro	Paglalarawan
bidIncrease	Pinakamababang pagtaas sa susunod na taya
bidDuration	Gaano katagal ang subasta pagkatapos ng bagong naisumiteng taya (naka segundo)
totalAuctionLength	Kabuuang haba ng subasta (naka segundo)
auctionsStarted	Ilang subasta ang nagsimula hanggang ngayon

Mekanismo ng Subasta ng Kalabisan

Ang mga subasta ng kalabisan 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 protokol para sa parehong dami ng mga indise (sobra). Ang bawat bagong taya ay kailangang mas mataas sa o katumbas ng *lastBid* **bidIncrease* / 100. Ang subasta ay magtatapos paglipas ng *totalAuctionLength* na segundo o pagkatapos ng *bidDuration* na ilang segundo na ang lumipas mula noong pinakahuling taya at walang mga bagong tayang naisumite sa ngayon.

Magsisimula muli ang isang subasta kung wala itong mga taya. Sa kabilang banda, kung ang subasta ay may hindi bababa sa isang taya, i-aalok ng sistema ang sobra sa pinakamataas na tumaya at pagkatapos ay susunugin ang lahat ng nakalap na token ng protokol.

Pangangasiwa ng Indise ng Kalabisan

Sa bawat oras na bubuo ng mga indise ang isang gumagamit at tuwirang gumagawa ng utang, magsisimula ang sistema na maglapat ng singil ng paghiram sa gumagamit ng SAFE. Ang naipon na interes ay pinagsama-sama sa dalawang magkaibang matalinong kontrata:

- Ang *makina ng accounting* na ginamit upang magpalitaw ng utang (Seksyon 9.2) at labis (Seksyon 10.1) mga subasta
- 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 tesorerya ang namamahala sa pagpopondo ng tatlong pangunahing bahagi ng sistema:

- Modyul ng Orakulo (Seksyon 6). Depende sa kung paano nakaayos ang isang orakulo, ang tesorerya 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 orakulo. Ang tesorerya 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 malayang koponan na nagpapanatili ng sistema. Ang mga halimbawa ay ang mga grupo na nag-whitelist ng mga bagong uri ng panggarantiya o nagsasaayos ng setter ng singil ng sistema (Seksyon 4.2)

Maaaring i-set up ang tesorerya upang ang ilang mga sobra 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 subasta, pagpoproseso ng pandaigdigang pamayanan, paggawa ng merkado at pag-update ng mga feed ng presyo upang mapanatili ang kalusugan ng sistema.

Magbibigay kami ng mga paunang user interface at mga nagkukusang iskrip (automated script) para paganahin ang pinakamaraming tao hangga't maaari na panatilihing ligtas ang protokol.

Nababangit na Merkado

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

- **Sari-saring uri ng portfolio** : ginagamit ng mga namumuhunan ang RAI para magkaroon ng mababang pagkakalantad sa isang asset tulad ng ETH nang walang buong panganib na aktwal na humawak ng ether

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

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 pagpapa-liit ng pamamahala at mga mekanismo ng pagpuksa.

Gusto muna naming maglagay ng batayan para sa mga pamantayan sa hinaharap sa paligid ng mga protokol 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 garantiya at subasta sa utang.

Mga Panganib at Pagbabawas

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

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

- **Kabiguan ng Orakulo**: magsasama-sama kami ng mga feed mula sa maraming network ng orakulo 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 makapagpakilala ng mga maling presyo

- **Panggarantiyang itim na sisne na mga kaganapan**: may panganib na magkaroon ng kaganapan sa itim na sisne sa pinagbabatayan na garantiya na maaaring magresulta sa mataas na halaga ng mga na-likidado na SAFE. Maaaring hindi masakop ng mga likidasyon ang buong hindi pa nababayarang masamang utang at sa gayon ay patuloy na babaguhin ng sistema ang buffer ng kalabisan nito upang masakop ang isang disenteng halaga ng inilabas na utang at makatiis ng mga *shocks* sa merkado

- **Mga hindi wastong parametro ng setter ng singil**: ang mga mekanismo ng nagkukusang tugon ay lubos na pang-eksperimento at maaaring hindi kumilos nang eksakto tulad ng inaasahan 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 na merkado**: ang mga liquidator ay mahahalagang aktor na tinitiyak na ang lahat ng inilabas na utang ay sakop ng panggarantiya. Plano naming lumikha ng mga interface at mga nagkukusang iskrip upang maraming tao hangga't maaari ay maaaring lumahok sa pagpapanatiling secure ng sistema.

Buod

Nagmungkahi kami ng protokol na unti-unting nagka-kandado sa sarili mula sa kontrol ng tao at naglalabas ng mababang pagkasumpungin, panggarantiyang asset na tinatawag na indiseng reflex. Una naming ipinakita ang nagkukusang mekanismo na nilalayong maimpluwensyahan ang presyo ng merkado ng indise at pagkatapos ay inilarawan kung paano maaaring limitahan ng ilang matalinong kontrata ang kapangyarihan na mayroon ang mga may hawak ng token sa sistema. Nag-balangkas kami ng pamamaraan ng pagpapatibay sa sarili para sa panggitnang feed ng presyo mula sa maraming malayang network ng orakulo at pagkatapos ay ilalahad ng pangkalahatang mekanismo para sa pag-gawa ng mga indise at pag-likidado 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”, anghttps://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

Indiseng Reflex : isang panggarantiyang asset na nagpapahina sa pagkasumpungin ng pinagbabatayan nito

RAI: ang aming unang indiseng reflex

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

Singil ng Pahiram: taunang singil ng interes na inilalapat sa lahat ng SAFE na may natitirang utang

Mekanismo ng Katugunan sa Singil ng Pagtubos (RRFM) : isang nagkukusang mekanismo na nagkukumpara sa merkado at mga presyo ng pagtubos ng isang indiseng reflex at pagkatapos ay nagka-kalkula ng singil ng pagtubos na dahan-dahang nakakaimpluwensya sa mga lumilikha ng SAFE na makabuo ng mas marami o mas kaunting utang (at tuwirang sinusubukang bawasan ang paglihis ng presyo sa merkado/pagtubos)

Setter ng Pamilihan ng Pera (MMS) : isang mekanismong katulad ng RRFM na kumukuha ng maraming levers ng salapi nang sabay-sabay. Sa kaso ng mga indiseng reflex, binabago nito ang parehong singil ng paghiram at ang presyo ng pagtubos

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

Modyul ng Pinaghihigpitang Pamamahala (RGM): isang hanay ng mga matalinong kontrata na nagbubuklod sa kapangyarihang taglay ng mga may hawak ng mga token ng pamamahala sa sistema. Ito ay maaaring magpatupad ng mga pagkaantala sa oras o nililimitahan ang mga posibilidad na ang pamamahala ay kailangang magtakda ng ilang partikular na parametro

Pamamahalang Kapanahunan ng Kalamigan: hindi nababagong kontrata na nagka-kandado sa karamihan ng mga bahagi ng isang protokol mula sa interbensyon sa labas pagkatapos lumipas ang isang tiyak na huling araw o oras

Makina ng Accounting : bahagi ng sistema na nag-trigger ng utang at mga subasta ng kalabisan. Sinusubaybayan din nito ang halaga ng kasalukuyang subasta ng utang, hindi naaaksyunan na masamang utang at ang labis na buffer

Labis na Buffer: halaga ng interes na maiipon at itago sa sistema. Anumang interes na naipon sa itaas ng hangganan o *threshold* na ito ay ibebenta sa mga subasta ng kalabisan na nagsusunog ng mga token ng protokol

Labis na Tesorerya: kontrata na nagbibigay ng pahintulot sa iba't ibang modyul ng sistema na bawiin ang naipon na interes (hal. ONM para sa mga tawag sa orakulo)