Augur: Un oracol decentralizat si o platforma pentru piete de predictie

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander
Fundatia Forecast
(Dated: 21 aprilie 2018)

Augur este un oracol descentralizat,care nu necesita increderea intr-o persoana, si o platforma pentru pietele de predictie. Rezultatele pietelor de prognoza Augur sunt alese de utilizatorii care detin tokenul de reputatie nativa Augur, si care isi mizeaza propriile tokenuri cu privire la rezultatul observat efectiv si, in schimb, primesc comisioane din taxele de tranzactionare de pe piete. Structura stimulativa a platformei Augur este conceputa astfel incat sa asigure ca raportarea onesta si exacta a rezultatelor este intotdeauna cea mai profitabila optiune pentru titularii de tokenuri de reputatie. Proprietarii tokenurilor pot posta obligatiuni de reputatie progresiv mai mari pentru a contesta rezultatele de piata propuse. Daca marimea acestor obligatiuni atinge un anumit prag, reputatia se imparte in mai multe versiuni - una pentru fiecare rezultat posibil al pietei in litigiu. Astfel, titularii de tokenuri trebuie sa-si schimbe tokenul de reputatie pentru una dintre aceste versiuni. Versiunile de reputatie care nu corespund rezultatelor din lumea reala vor deveni lipsite de valoare, deoarece nimeni nu va participa la pietele de predictie daca nu sunt increzatori ca pietele se vor rezolva corect. Prin urmare, detinatorii de tokenuri vor selecta singura versiune a reputatiei despre care stiu ca va continua sa aiba valoare: versiunea care corespunde realitatii.

Augur este o platforma de piata care nu necesita increderea intr-o persoana, un oracol descentralizat si platforma pentru predictia pietelor. Intr-o piata de predictii, persoanele pot specula asupra rezultatelor evenimentelor viitoare; cei care prognozeaza rezultatul castiga in mod corect bani, iar cei care prognozeaza gresit, pierd bani [**? ? ?**]. Pretul unei piete de predictii poate servi drept indicator precis si bine calibrat al probabilitatii aparitiei unui eveniment [**? ? ? ?**].

Folosind Augur, oamenii vor avea abilitatea de a tranzactiona pe pietele de predictie la un cost foarte scazut. Singura cheltuiala semnificativa pe care o asuma participantii este recompensarea creatorilor de piata si a utilizatorilor care raporteaza cu privire la rezultatele pietelor odata ce evenimentul a avut loc. Rezultatul este o piata de previziuni in care cerintele de increder, frictiune si taxe vor fi atat de scazute cat fortele pietei concurentiale le pot conduce.

Din punct de vedere istoric, pietele de predictie au fost centralizate. Cea mai simpla modalitate de a agrega tranzactii pe o piata de predictie este ca o entitate de incredere sa mentina un registru; in mod similar, cea mai simpla modalitate de a determina rezultatul unui eveniment si de a distribui plati comerciantilor este ca un judecator impartial si de incredere sa determine rezultatele pietelor. Cu toate acestea, pietele centralizate de predictie au numeroase riscuri si limitari: nu permit participarea la nivel mondial, limiteaza tipurile de piete care pot fi create sau tranzactionate si cer comerciantilor sa aiba incredere in operatorul de piata pentru a nu fura fonduri si pentru a rezolva corect pietele.

Augur isi propune sa rezolve pietele intr-un mod complet decentralizat. Retelele descentralizate, care nu necesita increderea intr-o persoana, cum ar fi Bitcoin[**?**] si Ethereum[**?**], elimina riscul ca interesul propriu sa se transforme in coruptie sau furt. Singurul rol al programatorilor Augur este sa publice contracte inteligente catre reteaua Ethereum. Contractele Augur sunt complet automatizate: dezvoltatorii nu au capacitatea de a cheltui fonduri care sunt detinute in contul escrow pe baza de contract, nu controleaza modul in care pietele se rezolva, nu aproba sau resping niciun fel de tranzactii, nu pot anula tranzactii, nu pot modifica sau anula ordine etc. *Oracolul* Augur permite migrarea informatiilor din lumea reala intr-un blockchain fara a se baza pe un intermediar de incredere. Augur va fi primul oracol decentralizat din lume.

I. CUM FUNCTIONEAZA AUGUR

Pietele Augur urmaresc o evolutie in patru etape: *crearea*, *tranzactionare*, *raportarea*, and *decontarea*. Oricine poate crea o piata bazata pe orice eveniment din lumea reala. Tranzactionarea incepe imediat dupa crearea pietei, iar toti utilizatorii sunt liberi sa tranzactioneze pe orice piata. Dupa ce a avut loc evenimentul pe care se bazeaza piata, rezultatul evenimentului este determinat de oracolul Augur. Odata ce rezultatul este determinat, comerciantii isi pot inchide pozitiile si pot colecta platile.

Augur are un token nativ numit Reputation (REP). REP este necesar pentru creatorii de piata si pentru reporteri atunci cand acestia raporteaza rezultatul pietelor create pe platforma Augur. Reporterii raporteaza despre o piata *mizandu-si* propriile tokenuri REP pe unul din posibilele rezultate ale pietei. Realizand acest lucru, reporterul declara ca rezultatul pe care a fost plasat miza corespunde rezultatului din lumea reala a evenimentului de baza al pietei. Consensul reporterilor unei piete este considerat “adevarul” cu scopul de a determina rezultatul pietei. Daca raportul unor reporteri cu privire la rezultatul unei piete nu se potriveste cu consensul la care au ajuns ceilalti reporteri, Augur redistribuie tokenurile REP ale reporterilor care au mizat pe rezultatul opus consensului catre reporterii care au raportat cu consensul.

Prin detinerea de REP si participarea la raportarea exacta a rezultatelor evenimentelor, detinatorii tokenurilor au dreptul la o parte din taxele de pe platforma. Fiecare token REP da dreptul titularului sau la o parte egala din comisioanele de piata ale lui Augur. Cu cat mai multe tokenuri REP un reporter are, si rapoarteaza corect, cu atat va castiga mai multe pentru munca lui in mentinerea platformei in siguranta.

Desi tokenurile REP joaca un rol central in operatiunile lui Augur, acestea nu sunt folosite pentru tranzactionarea pe pietele Augur. Comerciantii nu vor avea niciodata nevoie sa detina sau sa utilizeze REP, deoarece nu sunt obligati sa participe la procesul de raportare.

A. Crearea pietei

Augur permite oricui sa creeze o piata despre orice eveniment viitor. *Creatorul pietei* stabileste *timpul de terminare al evenimentului* si alege un *reporter desemnat* pentru a raporta rezultatul evenimentului. Reporterul desemnat nu decide in mod unilateral rezultatul pietei; comunitatea are intotdeauna posibilitatea de a contesta si corecta raportul reporterului desemnat.

Apoi creatorul de piata alege o *sursa pentru rezolutie* pe care reporterii ar trebui sa o foloseasca pentru a determina rezultatul. Sursa de rezolutie poate fi pur si simplu "cunoastere comuna" sau poate fi o sursa specifica, cum ar fi "Departamentul de Energie al Statelor Unite", bbc.com sau adresa unui anumit punct final de API. [1] Ei seteaza de asemenea si *o taxa a creatorului de piata* care este taxa platita acestuia de catre comerciantii care tranzactioneaza cu contractul de piata (vezi sectiunea I D pentru detalii despre taxe). In cele din urma, creatorul de piata publica doua obligatiuni: *obligatiunea de validitate* si *raportul desemnat obligatiunea no-show* (denumit si "obligatiunea no-show" pentru eficienta).

Obligatiunea de valididate este platita in Ethereum (ETH) si este returnata creatorului de piata in cazul in care piata se rezuma la orice alt rezultat decat *invalid*.[2] Obligatiunea de valabilitate stimuleaza creatorii de piata sa creeze piete bazate pe evenimente bine definite, cu rezultate obiective si neechivoce. Dimensiunea obligatiunii de valabilitate este stabilita dinamic, in functie de proportia rezultatelor invalide pe pietele recente.[3]

Obligatiunea "no-show" este alcatuita din doua parti: *Obligatiunea no-show gas* (platita in ETH) si *Obligatiunea no-show REP* (platita in REP). Aceste obligatiuni sunt returnate creatorului de piata daca reporterul desemnat de piata raporteaza efectiv in primele trei zile dupa *inchereiea evenimentului*. In cazul in care reporterul desemnat nu isi prezinta raportul in timpul perioadei de 3 zile alocate, atunci creatorul pietei pierde obligatiunea no-show care este alocata catre *primul reporter public* care raporteaza pe piata (a se vedea sectiunea I C 6). Aceasta stimuleaza creatorul de piata sa aleaga un reporter desemnat de incredere, care ar trebui sa ajute la rezolvarea rapida a pietelor.

Obligatiunea "no-show gas" este destinata acoperirii costurilor de gas ale primului reporter public. Acest lucru impiedica scenariul in care costurile de gas ale primului reporter sunt prea mari pentru ca raportarea sa fie profitabila. Obligatiunea no-show gas este setata la dublul costului mediu al gas-ului pentru raportare in timpul ferestrei de taxe anterioare.

In cazul in care reporterul desemnat nu reuseste sa raporteze, obligatiunea no-show REP este data primului reporter public sub forma de miza asupra rezultatelor raportate, astfel incat primul reporter public primeste obligatiunea no-show REP daca si numai daca raporteaza corect. Ca si in cazul obligatiunilor de validitate, obligatiunea no-show REP este ajustata in mod dinamic, pe baza procentajului de reporteri desemnati care nu au raportat la timp pe durata ferestrei de taxe anterioare.[4]

Creatorul de piata infiinteaza piata si trimite toate obligatiunile necesare printr-o singura tranzactie Ethereum. Odata ce tranzactia este confirmata, piata este live si incepe tranzactionarea.

B. Tranzactionarea

Participantii pietei prognozeaza rezultatele evenimentelor prin tranzactionarea *paritlor* acestor rezultate de piata. Un *set complet de actiuni* este o colectie de actiuni care consta in o parte din fiecare posibil rezultat valabil al evenimentului [**?**]. Seturile complete sunt create de motorul de potrivire al contractelor incheiat Augur, dupa cum este necesar pentru a incheia tranzactiile.

De exemplu, sa luam in considerare o piata care are doua rezultate posibile, `A` si `B`. Alice este dispusa sa plateasca 0,7 ETH pentru o parte din A, iar Bob este dispus sa plateasca 0,3 ETH pentru o parte din B.[5] In primul rand, Augur potriveste aceste ordine si colecteaza un to-

---

[1] De exemplu, daca o piata pe "Temperatura inalta (in grade Fahrenheit) pe 10 aprilie 2018 la Aeroportul International San Francisco, raportata de Weather Underground" specifica o sursa de rezolutie a textului https://www .wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html, reporterii ar merge pur si simplu la acea adresa URL si ar introduce in raportul lor temperatura ridicata afisata acolo.

[2] O *piata invalida* este o piata determinata a fi nevalida de reporteri pentru ca niciuna din rezultatelor enumerate de creatorul de piata nu este corecta sau deoarece formularea pe piata este ambigua sau subiectiva; consultati sectiunea III F pentru discutie.

[3] Vezi Anexa E 1 pentru detalii.

[4] Vezi Anexa E 2 pentru detalii.

[5] Initial, tranzactiile pe pietele Augur vor folosi moneda nativa Ethereum, Ether (ETH). Eliberarile ulterioare ale Augur vor include suport pentru piete denominate in tokenuri arbitrare emise pe reteaua Ethereum, inclusiv actiuni ale altor piete, precum si tokenuri fixate pe monede fiat ("stablecoins"), daca si cand vor deveni disponibile.

Figura 1. Reprezentare simplificata a duratei de viata a pietei de predictie.

tal de 1 ETH de la Alice si Bob.[6] Apoi Augur creeaza un set complet de actiuni, oferind lui Alice cota de A si lui Bob cota de B. In acest fel apar parti ale rezultatelor. Odata ce actiunile sunt create, ele pot fi tranzactionate in mod liber.

Contractele de tranzactionare Augur mentin un registru de comenzi pentru fiecare piata creata pe platforma. Oricine poate crea o comanda noua sau poate completa o comanda existenta in orice moment. Comenzile sunt completate de un motor de potrivire automata care exista in contractele inteligente Augur. Solicitarile de a cumpara sau de a vinde actiuni sunt indeplinite imediat daca exista deja o comanda de potrivire in registrul de comenzi. O solicitare poate fi completata prin cumpararea de actiuni de la sau prin vanzarea de actiuni catre alti participanti, ceea ce poate implica emiterea de seturi complete noi sau inchiderea seturilor complete existente. Motorul de potrivire al lui Augur sechestreaza intotdeauna suma minima de actiuni si / sau numerarul necesar pentru acoperirea valorii la risc. Daca nu exista o comanda de potrivire sau cererea poate fi completata doar partial, restul solicitarii este plasat in registrul de comenzi ca o comanda noua.

Comenzile nu sunt executate niciodata la un pret mai scazut decat pretul limita stabilit de comerciant, dar pot fi executate la un pret mai bun. Comenzile necompletate si partial completate pot fi eliminate din registrul de ordine de catre creatorul comenzii in orice moment. Taxele sunt platite de comercianti numai atunci cand sunt vandute seturi complete de actiuni; taxele de tranzactionare sunt discutate mai detaliat in sectiunea I D.

In timp ce majoritatea tranzactiilor de actiuni se asteapta sa se intample inainte de tranzactionarea pe piata, acestea pot fi tranzactionate in orice moment dupa crearea pietei. Toate activele Augur - inclusiv actiunile rezultatelor de pe piata, tokenurile de participare, actiunile in obligatiunile de diferenta, si chiar proprietatea asupra pietelor insele - sunt transferabile in orice moment.

C. Raportarea

Odata ce se produce evenimentul de baza al unei piete, rezultatul trebuie determinat pentru ca piata sa se finalizeze si sa inceapa decontarea. Rezultatele sunt determinate de oracolul Augur, care consta in reporteri motivati de profit, care raporteaza pur si simplu rezultatul real al evenimentului. Oricine detine tokenuri REP poate participa la raportarea si contestarea rezultatelor. Reporterii ale caror rapoarte sunt conforme cu consensul sunt recompensate financiar, iar cele ale caror rapoarte nu sunt in concordanta cu consensul sunt penalizate din punct de vedere financiar (vezi sectiuneaI D 3).

1. *Ferestrele de taxe*

Sistemul de raportare Augur ruleaza pe un ciclu de ferestre consecutive de sapte zile *de ferestre de taxe*. Toate taxele colectate de catre Augur in timpul unei anumite ferestre de taxe se adauga la *taxa fondului* pentru acea fereastra de taxe. La sfarsitul ferestrei de taxare, fondurile de raportare sunt platite titularilor de REP care au participat la procesul de raportare. Reporterii primesc recompense proportional cu suma REP pe care au mizat-o in timpul acestei ferestre de taxe. Participarea include: mizarea in timpul unui raport initial, contestarea unui rezultat tentativ sau achizitionarea de *token-uri de participare*.

2. *Tokenuri de participare*

In timpul oricarei ferestre de taxe, detinatorii de REP pot achizitiona orice numar de tokenuri de participare pentru fiecare attorep [7] fiecare. La sfarsitul ferestrei de taxe, ei isi pot rascumpara tokenurile de participare pentru cate un attorep fiecare, in plus fata de o parte proportionala din fereastra de taxe *a fondului*. Daca nu au existat actiuni (de exemplu, trimiterea unui raport sau contestarea unui raport trimis de alt utilizator) necesare unui reporter, reporterul poate cumpara tokenuri de participare pentru a indica faptul ca au aparut pentru fereastra de taxe. La fel ca tokenurile REP mizate, tokenurile de participare pot fi rascumparate *pro rata* de catre proprietari pentru o parte din taxe in aceasta fereastra de taxe.

Asa cum s-a discutat in II, este important ca detinatorii de rapoarte sa fie pregatiti sa participe la solutionarea pietei in cazul unui fork. Tokenul de participare ofera stimulente pentru ca titularii de REP sa monitorizeze platforma cel putin o data pe saptamana si, prin urmare, sa

[6] 1 ETH este utilizata aici pentru a facilita discutia. Costul real al unui set de actiuni complet este mai mic decat atat; vezi docs.augur.net/#number-of-ticks pentru detalii.

[7] Un *attorep* este de 10^{-18} REP.

fie gata sa participe in cazul in care este nevoie. Chiar si detinatorii de REP care nu doresc sa participe la procesul de raportare sunt stimulati sa se inregistreze pe Augur o singura data pe fereastra de 7 zile pentru a cumpara tokenuri de participare si pentru a colecta taxe. Aceasta verificare regulata si activa va asigura ca ei sunt familiarizati cu modul de utilizare al platformei Augur, vor fi constienti de fork-uri atunci cand apar si astfel ar trebui sa fie mai pregatiti sa participe la acestea atunci cand se intampla.

3. Progresul statului de piata

Pietele Augur pot exista in sapte state diferite dupa creare. Starile potentiale sau "fazele" unei piete Augur sunt dupa cum urmeaza:

- Pre-raportarea
- Reportarea desemnata
- Reportarea deschisa
- Asteptarea ca o noua fereastra de taxe sa inceapa
- Runda de dispute
- Fork
- Finalizare

Relatia dintre aceste faze poate fi vazuta in Fig. 2.

4. Pre-raportarea

Faza *de pre-raportare* sau *de tranzactionare* (Fig. 1) este perioada de timp care incepe dupa debutul tranzactionarii pe piata, dar inainte ca evenimentul pietei sa se fi intamplat. In general, aceasta este perioada cea mai activa de tranzactionare pentru orice piata Augur. Odata ce data de incheiere a evenimentului a trecut, piata intra in faza de *raportare desemnata* (Fig. 2a).

5. Raportare desemnata

Atunci cand se creeaza o piata, creatorii de piata trebuie sa aleaga un reporter desemnat si sa introduca o obligatie no-show. In timpul fazei de raportare desemnate (Fig. 2a) reporterul desemnat al pietei are pana la trei zile pentru a raporta rezultatul evenimentului. In cazul in care reporterul desemnat nu reuseste sa raporteze in termen de trei zile alocate, creatorul pietei pierde obligatiunea no-show si piata intra automat in faza de *raportare deschisa* (Fig. 2b).

In cazul in care reporterul desemnat prezinta un raport la timp, atunci obligatiunea no-show este returnata creatorului pietei. Reporterul desemnat este obligat sa trimita miza reporterului desemnat[8] pe rezultatul raportat, pe care il va pierde daca piata finalizeaza orice alt rezultat decat cel pe care l-au raportat[9] De indata ce reporterul desemnat prezinta raportul, piata intra in faza de *asteptare pentru urmatoarea fereastra de taxe sa inceapa* (Fig. 2c), iar rezultatul raportat devine rezultatul *tentativ* al pietei.

6. Raportare deschisa

Daca reporterul desemnat nu reuseste sa raporteze in decursul celor trei zile alocate, creatorul pietei pierde obligatiunea no-show si piata intra imediat in faza de *raportare deschisa* (Fig. 2b). De indata ce piata intra in faza de raportare deschisa, oricine poate raporta rezultatul pietei. Atunci cand reporterul desemnat nu reuseste sa raporteze, primul reporter care raporteaza rezultatul unei piete se numeste "reporter public" al pietei.

Primul reporter public al pietei primeste obligatiunea no-show sub forma de miza pe rezultatul ales, astfel incat acesta sa poata revendica obligatiunile REP doar daca rezultatele raportate de el sunt in concordanta cu rezultatul final al pietei. El primeste, de asemenea, si obligatiunea no-show gas dupa ce piata a fost finalizata numai daca rezultatele raportate sunt in concordanta cu rezultatul final al pietei.

Primul reporter public *nu* are nevoie sa-si mizeze propriile tokenuri REP atunci cand raporteaza rezultatul pietei. In acest fel, in orice piata al carei reporter desemnat nu reuseste sa raporteze, este de asteptat ca rezultatul sa fie raportat de *altcineva* foarte curand dupa intrarea in faza de raportare deschisa.

Odata ce *raportul initial* a fost primit de catre reporterul initial (fie ca a fost reporterul desemnat, fie primul reporter public), rezultatul raportat devine rezultatul tentativ al pietei, iar piata intra in asteptarea urmatoarei ferestre de taxe pentru a incepe faza (Fig. 2c).

7. Asteptarea pentru deschiderea urmatoarei ferestre de taxe

Odata ce piata primeste raportul initial, intra in faza de asteptare pentru urmatoarea fereastra de taxe (Fig. 2c). In aceasta faza, raportarea pentru piata este blocata pana la sfarsitul ferestrei de taxa curenta. Odata ce urmatoarea fereastra de taxe incepe, piata intra in faza *rundei de dispute.*

---

[8] Vezi appendix E 3 entru detalii privind dimensiunea pachetului reporter desemnat

[9] Miza pierduta este adaugata la fondul de taxe de raportare a ferestrei de taxe alocate pietei si este folosit pentru a recompensa reporterii onorati si disputele. Pentru detalii, va rugam sa consultati Sectiunea I D 3.

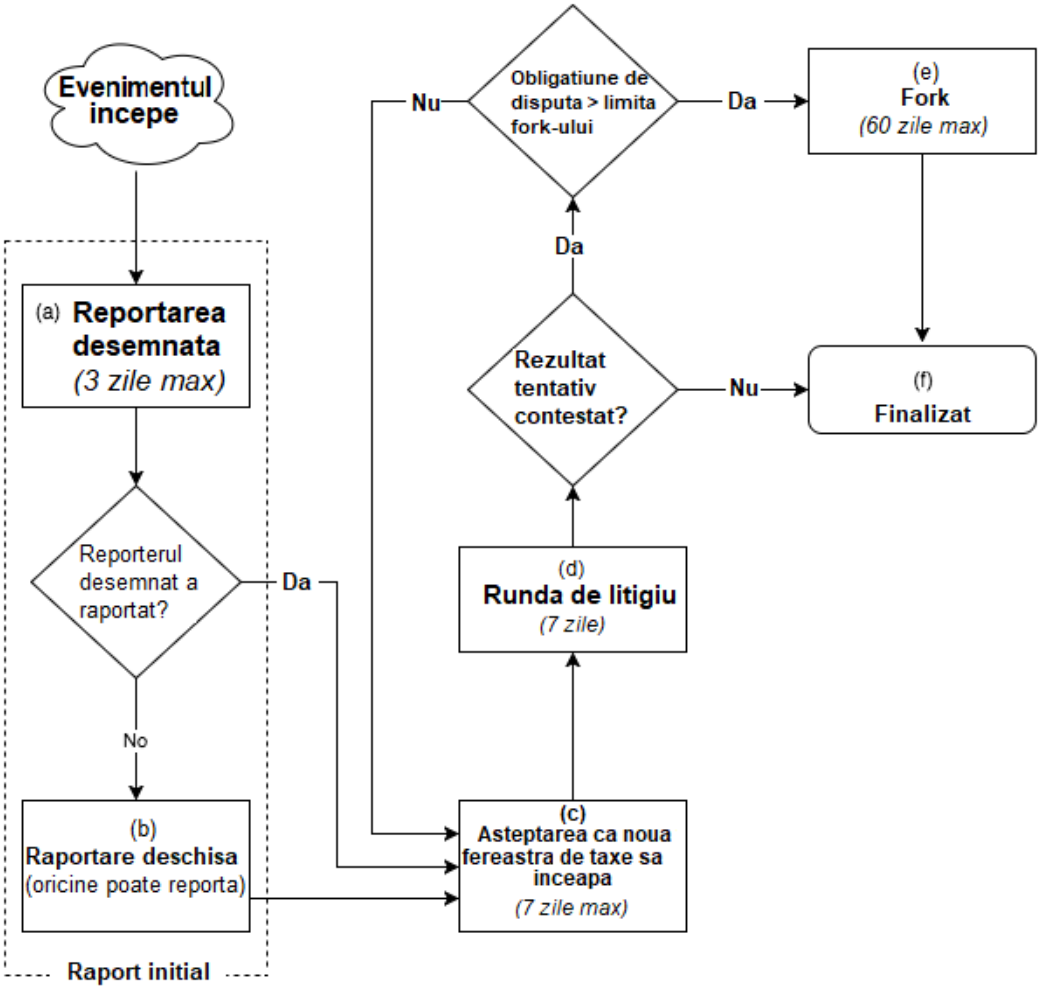

Figura 2. Diagrama de reportare.

8. *Runda de litigiu*

Runda de litigiu (Fig. 2d) este o perioada de 7 zile in care orice titular REP are posibilitatea de a contesta *rezultatul tentativ* al pietei.[10] (La inceputul unei runde de litigiu, rezultatul provizoriu al unei piete este rezultatul care va deveni rezultatul final al pietei daca nu este contestat cu succes de titularii REP.) Un litigiu consta in *mizarea* REP (denumit in continuare *miza de litigiu* pe un rezultat *altul decat* rezultatul actual tentativ al pietei. Un litigiu este *de succes* daca valoarea totala a mizei de contestatie cu privire la un anumit rezultat corespunde *dimensiunii obligatiunii de litigiu* necesara pentru runda actuala. Dimensiunea obligatiunilor de disputa se calculeaza dupa cum urmeaza.

[10] Faptul ca rundele de litigiu coincid cu ferestrele de taxe este pur si simplu o chestiune de convenienta; in principiu, rundele de litigii si duratele de plata ale taxelor pot fi diferite.

Fie A_n miza totala asupra tuturor rezultatelor acestei piete la inceputul rundei de litigiului n. Fie ω orice rezultat de piata *altul decat* rezultatul tentativ de piata la inceputul rundei de litigiu. Fie $S(\omega, n)$ suma totala a mizei la rezultatul ω la inceputul rundei de litigiu n. Atunci marimea *obligatiunii de litigiu* necesara pentru a disputa cu succes rezultatul actual tenativ in favoarea noului rezultat ω pe durata rundei n este denotat $B(\omega, n)$ si este dat de:

$$B(\omega, n) = 2A_n - 3S(\omega, n) \tag{1}$$

Dimensiunile obligatiunilor sunt alese astfel pentru a asigura un ROI fix de 50% pentru reporterii care contesta cu succes rezultatele false (a se vedea SectiuneaII D).

Obligatiunile de litigiu nu trebuie sa fie platite in intregime de catre un singur utilizator. Platforma Augur permite participantilor sa imparta cu alti oameni obligatiunile de litigiu. Orice utilizator care vede un rezultat tentativ incorect, il poate contesta prin plasarea de REP pe un alt rezultat decat rezultatul tentativ. Daca vreun

rezultat (altul decat rezultatul provizoriu) acumuleaza suficienta miza de litigiu pentru a-si completa obligatiunea de litigiu, rezultatul curent tentativ va fi contestat cu succes.

In cazul unui litigiu de succes, piata va fi supusa unei alte runde de disputa sau va intra in starea de *fork* (Fig. 2e). Daca marimea obligatiunii de plata a contestatiilor este mai mare de 2,5% din toate REP, atunci piata va intra in starea de fork. In cazul in care dimensiunea obligatiunii de plata a litigiilor este mai mica de 2,5% din totalul rapoartelor repetate, rezultatul nou ales devine noul rezultat tentativ al pietei, iar piata este supusa unei alte runde de disputa.

Orice miza de contestatie este tinuta in escrow in timpul rundei de contestatie. Daca o obligatie de litigiu nu reuseste, atunci miza de disputa este returnata proprietarilor la sfarsitul rundei de disputa. Daca nicio disputa nu este reusita in timpul rundei de disputa de sapte zile, piata intra in starea de *finalizat* (Fig. 2f), si rezultatul tentativ este acceptat ca fiind *rezultatul final*. Rezultatul final al unei piete este rezultatul tentativ care trece printr-o runda de disputa fara a fi contestat cu succes sau este determinat printr-un fork. Contractele Augur trateaza rezultatele finale ca *adevarate* si platesc in consecinta.

Orice miza de contestatie nereusita este returnata initial proprietarilor la sfarsitul fiecarei runde de disputa. Toate mizele de succes ale litigiilor se aplica rezultatului pe care l-au sustinut si raman acolo pana cand piata este finalizata (sau pana cand un fork apare pe o alta piata Augur). Orice miza de contestatie (fie ea reusita sau nereusita) va primi o parte din *fondul de taxe de raportare*[11] din fereastra taxei curente.

9. Fork

Starea de fork (Fig. 2e) este o stare speciala care dureaza pana la 60 de zile. Forking este metoda de solutionare a pietei de ultima instanta; este un proces foarte perturbator si se intentioneaza a fi o situatie rara. Un fork este cauzat atunci cand exista o piata cu un rezultat cu o garantie de contestatie completa de succes de cel putin 2,5% din totalul de REP. Aceasta piata este denumita *piata de forking*.

Cand se initiaza un fork, o perioada de 60 de zile [12] *de forking* incepe. Contestarea pentru toate celelalte piete nefinalizate este pusa in asteptare pana la sfarsitul acestei perioade de forking. Perioada de forking este mult mai mare decat fereastra obisnuita a taxei, deoarece platforma trebuie sa ofere suficient timp pentru proprietarii de REP si furnizorii de servicii (cum ar fi portofelele si schimburile). Rezultatul final al forkului nu poate fi contestat.

Fiecare piata Augur si toate simbolurile REP exista in unele *universe*. Rapoartele REP pot fi folosite pentru a raporta rezultatele (si, astfel, a castiga taxe) *doar* pentru pietele care exista in acelasi univers ca si REP-urile. Atunci cand Augur se lanseaza prima data, toate pietele si toate REP vor exista impreuna in *universul de geneza*.

Cand o piata face fork, se creaza noi universuri. Forking-ul creeaza un nou *univers-copil* pentru fiecare rezultat posibil al pietei forking (inclusiv `Invalid`, asa cum s-a discutat in Sectiunea I D 2). De exemplu, o piata "binara" are 3 noi copii-univers: `A`, `B` si `Invalid A`. Initial, universul `B` si universul `Invalid`. Initial, aceste universuri nou create sunt goale: nu contin piete sau replici.

Cand se initiaza un fork, *universul parinte* devine permanent *blocat*. Intr-un univers blocat nu se pot crea noi piete. Utilizatorii pot continua sa tranzactioneze actiuni pe piete in universuri blocate, iar pietele dintr-un univers blocat pot primi in continuare rapoartele initiale. Cu toate acestea, nu se platesc recompense de raportare si pietele in universuri blocate nu pot fi finalizate. Pentru ca pietele sau tokenurile REP in universul incuiat sa fie utile, trebuie mai intai sa fie migrate spre un univers copil.

Titularii REP in universul parinte isi pot migra tokenurile catre un univers copil la alegerea lor. Aceasta alegere ar trebui examinata cu atentie, deoarece migratia nu poate fi inversata. Tokenurile nu pot fi trimise de la un univers la altul. *Migratia este un angajament permanent al tokenurilor REP la un anumit rezultat al pietei.* Tokenurile REP care migreaza catre universuri diferite de copii ar trebui considerate tokenuri separate, iar furnizorii de servicii precum portofelele si schimburile ar trebui sa le inscrie ca atare.

Cand un fork este initiat, toate tokenurile REP mizate pe toate pietele non-forking devin *nemizate* astfel incat sa poata fi migrate intr-un univers copil in timpul perioadei de forking. [13]

Oricare de univers-copil care primeste cel mai mult REP migrat pana la sfarsitul perioadei de forking devine universul *castigator*, iar rezultatul sau devine rezultatul final al pietei de forjare. Pietele nefinalizate din universul-parinte pot fi migrate numai catre universul castigator si, daca au primit un raport initial, sunt resetate inapoi la asteptarea pentru urmatoarea fereastra de taxa pentru a incepe faza.

---

[11] Toate comisioanele de tranzactionare si obligatiunile de valabilitate colectate in timpul unei ferestre de taxe se adauga la fondul de taxe de raportare al acestei taxe. La sfarsitul ferestrei de taxe, fondurile de raportare se platesc utilizatorilor proportional cu suma REP pe care au mizat-o in timpul acelei ferestre de taxe.

[12] Perioada de forking poate fi mai mica de 60 de zile: o aceasta se termina cand au trecut 60 de zile sau mai mult de 50% din toate REP de geneza sunt migrate catre un anumit univers-copil.

[13] Singura exceptie sunt tokenurile REP mizate de reporterul initial atunci cand au facut raportul initial. Reprezentantul respectiv ramane in continuare implicat in rezultatul raportat initial si se migreaza automat in universul copil care castiga forkul.

Nu exista limita de timp pentru a migra tokenurile din universul parinte intr-un univers copil. Tokenurile pot migra dupa perioada de forking, dar nu vor conta pentru determinarea universului castigator. Pentru a incuraja o participare mai mare in perioada de forking, toti posesorii de tokenuri care isi migreaza tokenurile REP intr-un interval de 60 de zile de la inceperea unui fork vor primi 5% tokenuri REP suplimentar in universul-copil la care au migrat[14]. Aceasta recompensa este platita prin redactarea unor simboluri REP noi.[15]

Reporterii care au mizat REP pe unul din rezultatele pietii de forking nu isi pot schimba pozitia in timpul unui fork. REP care a fost pus pe un rezultat in universul-parinte poate fi migrat numai la universul-copil care corespunde rezultatului. De exemplu, daca un reporter a reusit sa indeplineasca o obligatiune de litigiu dispusa in favoarea rezultatului `A` in timpul unei runde de disputa, atunci REP care a fost mizat pe rezultatul `A` poate fi migrat doar la universul `A` in timpul unui fork.

Universele inrudite sunt in intregime disjuncte. Tokenurile REP care exista intr-un singur univers nu pot fi folosite pentru a raporta evenimentele sau pentru a castiga recompense de pe pietele dintr-un alt univers. Intrucat utilizatorii nu vor dori sa creeze sau sa tranzactioneze pe pietele dintr-un univers al carui oracol nu este de incredere, REP care exista intr-un univers care nu corespunde realitatii obiective este putin probabil sa castige proprietarului vreun onorariu si, prin urmare, valoare. Prin urmare, tokenurile REP migrate intr-un univers care nu corespunde realitatii obiective nu trebuie sa detina nici o valoare de piata, indiferent daca universul obiectiv fals ajunge sa fie universul castigator dupa un fork. Acest lucru are consecinte importante de securitate, pe care le discutam in Sectiunea II.

10. Finalizat

O piata intra in starea finalizata (Fig. 2f) daca trece printr-o runda de disputa de sapte zile fara a-si contesta rezultatul tentativ sau dupa incheierea unui fork. Rezultatul unui fork nu poate fi contestat si este intotdeauna considerat definitiv la sfarsitul perioadei de forking. Odata ce o piata este finalizata, comerciantii isi pot stabili pozitiile direct pe piata. Cand o piata intra in starea finalizata, ne referim la rezultatul ales ca fiind *rezultatul final.*

[14] ceasta se intampla chiar si atunci cand perioada de forking s-a incheiat mai devreme din cauza faptului ca mai mult de 50% din toate REP sunt migrate la un anumit univers de copii

[15] Efectul acestei adaugiri la sursa de bani a REP este mic. De exemplu, daca 20% din toate REP-urile existente au migrat in timpul perioadei de forking, acest bonus ar duce la o crestere de 1% a ofertei de bani a REP. In plus, se asteapta ca forkurile sa fie evenimente extrem de rare.

D. Acord de tranzactionare

Un comerciant isi poate inchide pozitia in unul din urmatoarele doua moduri: vanzand actiunile pe care le detine unui alt comerciant in schimbul valutei sau prin decontarea actiunilor lor pe piata. Reamintim ca fiecare actiune apare ca parte a unui set complet atunci cand un Un c total de 1 ETH a fost escrowed cu Augur.[6] Pentru a obtine acel 1 ETH din escrow, comerciantii trebuie sa dea Augur fie un set complet, in cazul in care piata a finalizat, fie o parte din rezultatul castigator. Cand se intampla acest schimb, spunem ca comerciantii sunt *solutionati cu contractul de piata.*

De exemplu, luam in considerare o piata nefinalizata cu rezultate posibile `A` si `B`. Sa presupunem ca Alice are o parte din rezultatul `A` pe care vrea sa o vanda pentru 0.7 ETH si Bob are o parte din rezultatul `B` pe care vrea sa o vanda pentru 0.3 ETH. Mai intai, Augur potriveste aceste comenzi si colecteaza actiunile `A` si `B` de la participanti. Apoi Augur da 0,7 ETH (minus taxe) catre Alice si 0,3 ETH (minus comisioane) catre Bob.

Ca un al doilea exemplu, luam in considerare o piata finalizata al carei rezultat castigator este `A`. Alice are o parte din `A` si vrea sa fie platita. Ea trimite partea ei din `A` catre Augur si in schimb primeste 1 ETH (minus comisioane).

1. Taxele de decontare

Singura data in care Augur percepe taxe este atunci cand participantii de pe piata se stabilesc cu contractul de piata. Augur percepe doua taxe in timpul decontarii: taxa de creator si taxa de raportare. Ambele taxe sunt proportionale cu suma platita. Deci, in exemplul de decontare prefinalizat de mai sus, in cazul in care Alice primeste 0,7 ETH si Bob primeste 0,3 ETH, Alice ar plati 70% din comisioane in timp ce Bob ar plati 30%.

Taxa de creare este stabilita de creatorul pietei in timpul crearii pietei si este platita creatorului de piata dupa decontare. Taxa de raportare este stabilita dinamic (vezi Sectiunea II C) si este platita reporterilor care participa la procesul de raportare.

2. Solutionarea pietelor nevalide

In cazul in care o piata este rezolvata ca `invalida`, comerciantii care se stabilesc cu contractul de piata primesc o suma egala de ETH pentru actiunile fiecarui rezultat. Daca piata a avut rezultate N posibile (fara a include rezultatul `invalid`), iar costul unui set complet de actiuni a fost de C ETH, atunci comerciantii vor primi C/N ETH pentru fiecare actiune decontata cu contractul de piata.

[16]

3. Redistribuirea reputatiei

In cazul in care o piata finalizeaza fara a initia un In c fork, toate REP care se implica in orice alt rezultat decat rezultatul final al pietei sunt retinute si distribuite utilizatorilor care au mizat pe rezultatul final al pietei, proportional cu suma REP pe care au mizat-o. Marimea obligatiunilor de litigii este aleasa astfel incat orice persoana care contesta cu succes un rezultat in favoarea rezultatului final al pietei este recompensata cu 50% din rentabilitatea investitiei (ROI) pe miza lor de contestare.[17] Acesta este un stimulent puternic pentru reporteri pentru a contesta rezultatele tentative false.

II. STIMULENTE SI SECURITATE

Exista o relatie puternica intre plafonul de piata al REP si gradul de incredere al protocolului de fork Augur. In cazul in care plafonul de piata al REP este suficient de mare, [18], iar atacatorii sunt rationali din punct de vedere economic, atunci rezultatul care castiga forkul ar trebui sa corespunda realitatii obiective. De fapt, ar fi posibil ca Augur sa functioneze corect fara a folosi reporteri desemnati si runde de dispute. Folosind *doar* procesul de forking, oracolul ar raporta cu sinceritate.

Cu toate acestea, fork-urile sunt perturbatoare si consumatoare de timp. Un fork dureaza pana la 60 de zile pentru a rezolva o piata unica si poate rezolva o singura piata la un moment dat. In timpul celor 60 de zile in care piata de forking este rezolvata, toate celelalte piete nefinalizate sunt suspendate. [19] roviderii de servicii ar trebui sa updateze, iar titularii REP trebuie sa-si migreze REP la unul din noile universuri-copil. Prin urmare, fork-urile trebuie folosite doar atunci cand sunt absolut necesare. Forkingul este optiunea nucleara.

Din fericire, odata ce s-a stabilit ca forkurile pot fi de incredere in determinarea adevarului, stimulentele pot fi folosite pentru a incuraja participantii sa se comporte sincer fara a trebui sa initieze un fork. *Amenintarea credibila a unui fork si convingerea ca forkul se va rezolva corect sunt pietrele de temelie ale sistemului de stimulare al lui Augur.*

In continuare, discutam despre conditiile in care se poate avea incredere in sistemul de forking pentru a determina adevarul. Discutam apoi despre sistemul de stimulare si despre modul in care acesta incurajeaza solutionarea rapida si corecta a tuturor pietelor.

A. Integritatea protocolului de forking

Aici discutam despre fiabilitatea procesului de forking si despre conditiile in care se poate avea incredere. Pentru a facilita discutia, atunci cand ne referim la forkuri vom face referire la universul-copil care corespunde realitatii obiective ca universul `adevarat` si oricarui alt univers-copil ca un univers `fals`. Vom vorbi despre universul-copil care primeste cea mai mare parte a migratiei de REP in timpul perioadei de forking ca universul-castigator si despre toate celelalte universuri-copil ca universuri care pierd.

Fireste, intotdeauna am dori ca universul `adevarat` sa fie universul castigator, iar universurile `false` sa fie universurile care pierd. Spunem ca protocolul de forking a fost atacat cu succes ori de cate ori universul `fals` ajunge sa fie universul castigator al unui fork - ceea ce a dus la platirea incorecta a pietei (si, eventual, a tuturor pietelor nefinalizate) .

Abordarea noastra pentru securizarea oracolului este de a organiza lucrurile astfel incat beneficiul maxim pentru un atacator de succes sa fie mai mic decat costul minim al efectuarii atacului. Formalizam acest lucru mai jos.

1. Beneficii maxime pentru un atacator

Un atacator care ataca cu succes oracolul ar face ca toate pietele Augur nefinalizate sa migreze intr-un univers `fals`. Daca atacatorul controleaza majoritatea REP in universul `fals`, atacatorul poate forta toate pietele nefinalizate sa se rezolve precum doreste el. In cel mai extrem caz, el va putea, de asemenea, sa capteze toate fondurile escrowate pe toate pietele respective. [20]

Definitie 1. Definim si denumim cu I_a *interesul nativ deschis*) al Augur ca valoare a sumei tuturor fondurilor escrow in pietele Augur nefinalizate. [21]

Definitie 2. Definim o *piata parazita* ca orice piata care nu plateste catre Augur taxe de raportare, dar rezolva in conformitate cu rezolutia unei piete originale Augur.

Definitie 3. Definim si denotam cu I_p, *interes parazitar deschis* ca valoare a sumei tuturor fondurilor escrowate

[16] Tranzactiile nu pot fi desfiintate in cazul in care o piata se rezolva ca `invalida` din cauza limitarilor tehnice. Actiunile rezultatelor sunt doar simboluri, care pot fi tranzactionate direct intre utilizatori; astfel, ETH si actiunile nu sunt sub controlul Augur si nu pot fi restituite proprietarului initial in cazul in care piata se finalizeaza ca `invalida`.

[17] Vezi teorema 3 in Appendix A.

[18] Vezi Sectiunea II A pentru detalii.

[19] Comerciantii pot continua tranzactionarea pe aceste piete, insa acele piete nu pot fi finalizate decat dupa perioada de forking.

[20] Aceasta ar cere atacatorului sa captureze *toate* actiunile unui anumit rezultat si apoi sa forteze finalizarea pietei la acest rezultat.

[21] Aceasta include si pietele externe care platesc taxe de raportare catre Augur.

pe toate pietele parazitare care se rezolva in conformitate cu pietele originale Augur nefinalizate.

In cel mai extrem caz, un atacator ar putea, de asemenea, sa capteze toate fondurile de pe toate pietele parazitare, care se rezolva in conformitate cu pietele originale Augur nefinalizate.

Observatie 1. Beneficiul maxim (brut) pentru un atacator care ataca cu succes oracolul este $I_a + I_p$.

2. *Interesul parazitar deschis este necunoscut*

Augur poate masura cu acuratete si eficienta I_a. Cu toate acestea, I_p nu pot fi cunoscute in general, deoarece pot exista in mod arbitrar multe piete parazitare offline, fiecare avand un interes deschis in mod arbitrar. Din moment ce beneficiul maxim posibil pentru un atacator include cantitatea neconditionata I_p, nu putem fi niciodata siguri ca oracolului este securizat impotriva atacatorilor rationali economici.

Cu toate acestea, daca suntem dispusi sa afirmam ca I_p este limitat in mod rezonabil in practica, atunci putem defini conditiile sub care putem afirma ca oracolul este sigur.

3. *Costul minim al unui atac de succes*

Luam in considerare costul de a ataca oracolul. Fie ca P sa denumeasca pretul REP. Fie ϵ un attorep [22]. Fie M suma totala de REP existente (oferta REP). Fie S proportia M care va fi migrata in universul adevarat in timpul perioadei de forking al unui fork.

Astfel, produsul SM reprezinta suma absoluta a REP care a migrat la universul adevarat in timpul perioadei de forking a unui fork, iar produsul PM este plafonul de piata al REP.

Fie P_f pretul REP mutat intr-un univers `fals` la alegerea atacatorului. Notam ca daca $P \leq P_f$ atunci oracolul nu ar fi sigur impotriva atacatorilor rationali din punct de vedere economic, deoarece ar fi cel putin la fel de profitabil sa migram REP la universul fals, asa cum ar fi sa nu migram deloc.

4. *Integritate*

Presupunere 1. *Reporterii care nu sunt atacatori nu vor migra niciodata REP intr-un univers* `fals` *in timpul unui fork.*[23]

Prin proiectare, un atac de succes asupra oracolului necesita mai mult REP pentru a fi migrat intr-un univers `fals` decat in universul `adevarat` in timpul perioadei de forking. Presupunem ca doar atacatorul va migra REP intr-un univers `fals`. Cantitatea de REP care a migrat in universul `adevarat` in timpul perioadei de raportare este notata cu SM. Astfel, pentru ca un atacator sa aiba succes, trebuie sa migreze cel putin $SM + epsilon$ REP. Pentru simplificare, vom ignora neglijabilul *epsilon* si spunem ca un atac de succes necesita migrarea a cel putin SM REP, care are o valoare de SMP inainte de migrare, intr-un univers `fals`.

Daca un atacator migreaza SMREP in perioada de raportare al unui fork, acesta va primi SM REP pe universul-copil la care migreaza.[24] Daca atacatorul migreaza intr-un univers `fals`, valoarea acestor monede devine SMP_f. Astfel, costul minim pentru atacator este $(P - P_f)SM$.

Observatie 2. Suma minima de REP a unui atacator de succes care trebuie sa migreze intr-un univers `fals` in timpul unui fork este SM, care costa atacatorul $(P - P_f)SM$.

Retineti ca daca $S > \frac{1}{2}$ atunci un atac este *imposibil* deoarece nu exista suficient REP in afara universului `adevarat` pentru orice univers `fals` fiind universul castigator.

Pitted against economically rational attackers, the oracle will resolve to outcomes that correspond to objective reality if the maximum benefit to an attacker is less than the minimum cost of attack. By observations 1 & 2 we can see that this occurs whenever $S > \frac{1}{2}$ or $I_a + I_p < (P - P_f)SM$. This gives us our formal definition of integrity.

Fiind impotriva atacatorilor rationali economici, oracolul va rezolva rezultatele care corespund realitatii obiective daca beneficiul maxim pentru un atacator este mai mic decat costul minim al atacului. Prin observatiile 1 & 2 putem vedea ca acest lucru apare ori de cate ori $S > \frac{1}{2}$ sau $I_a + I_p < (P - P_f)SM$. Aceasta ne da definitia formala a integritatii.

Definitie 4. (Prioprietatea integritatii) Protocolul de forking are *integritate* ori de cate ori $S > \frac{1}{2}$ sau ori de cate ori $I_a + I_p < (P - P_f)SM$.

Inegalitatea de mai sus poate fi rezolvata pentru PM pentru a vedea relatia dintre integritatea protocoalelor de forking si plafonul de piata al REP.

Teorema 1. *(Teorema securitatii plafonului pietei) Protocolul de forking are integritate daca si numai daca:*

---

[22] Un *attorep* este egal cu 10^{-18} REP

[23] Exista cazuri in care unii reporteri bine intentionati migreaza accidental sau din neatentie REP intr-un univers `fals`. Cu toate acestea, un astfel de comportament nu este, in practica, distinctibil de colaborarea cu un atacator.

[24] In practica, atacatorul ar primi $1.05SM$ REP in universul copilului din cauza bonusului de 5% pentru migrarea in termen de 60 de zile de la inceperea unui fork. Noi ignoram bonusul de 5% aici pentru o discutie usoara. Pentru a vedea o discutie care include bonusul de 5%, vezi Anexa C.

1. $S > \frac{1}{2}$, *sau*

2. $P_f < P$ *iar plafonul de piata al REP este mai mare decat* $\frac{(I_a+I_p)P}{(P-P_f)S}$.

Demonstraţie. Sa presupunem ca protocolul de forking este integru. Apoi, prin definitie, $S > \frac{1}{2}$ sau $I_a + I_p < (P - P_f)SM$. Sa presupunem ca $I_a + I_p < (P - P_f)SM$. Deoarece $I_a + I_p \geq 0$ si $SM > 0$, stim ca $P_f < P$. Apoi, rezolvand $I_a + I_p < (P - P_f)SM$ pentru PM, vedem ca $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Astfel se dovedeste prima directie.

Acum, sa presupunem ca $S > \frac{1}{2}$, sau ca $P_f < P$ si $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Daca $S > \frac{1}{2}$, atunci protocolul de forking are integritate prin definitie. Daca $P_f < P$ si $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$, atunci rezolvand inegalitatea pentru $I_a + I_p$, vedem ca $I_a + I_p < (P - P_f)SM$, iar protocolul de forking are integritate. □

B. Ipotezele noastre si consecintele acestora

Credem ca comerciantii nu vor dori sa tranzactioneze intr-un univers in care reporterii au mintit. De asemenea, credem ca cei care creeaza piata nu vor plati pentru a crea piete Augur intr-un univers in care nu exista comercianti. Intr-un univers fara piete sau fara tranzactionare, REP nu ofera niciun dividend acelora care il detin. Prin urmare, consideram ca REP trimis intr-un univers `fals` nu va detine nicio valoare de piata ne-neglijabila si vom modela acest lucru permitand $P_f = 0$.

Consideram ca este rezonabil sa ne asteptam ca cel putin 20% din REP sa fie migrate la rezultatul adevarat in timpul perioadei de raportare al unui fork si modelam acest lucru lasand $S \geq \frac{1}{5}$. Suntem, de asemenea, dispusi sa acomodam interesul deschis parazitar pana la 50% din interesul nativ deschis, si astfel lasam $I_a \geq 2I_p$.

In aceste ipoteze, teorema 1 ne spune ca protocolul de forking are integritate ori de cate ori plafonul de piata al REP este de cel putin 7,5 ori mai mare decat interesul nativ deschis. [25]

C. Ghionturi ale plafonului pietei

Augur primeste informatii despre pretul REP in acelasi mod in care primeste alte informatii despre lumea reala: printr-o piata Augur. Aceasta ofera Augur capacitatea de a calcula limita actuala de piata a REP. Augur poate masura, de asemenea, interesul actual nativ deschis si poate determina astfel ce limita de piata ar trebui directionata pentru a indeplini cerintele de integritate ale lui Augur.

Fiecare univers incepe cu o taxa de raportare implicita de 1%. In cazul in care plafonul actual al pietei este mai mic decat obiectivul, atunci ratele de raportare sunt majorate automat (dar niciodata nu vor fi mai mari de 33,3%), exercitand presiuni asupra pretului REP si / sau presiunii scazute asupra noului interes national. Daca plafonul de piata curent este mai mare decat obiectivul, atunci taxele de raportare sunt scazute automat (dar niciodata nu vor fi mai mici de 0,01%), astfel incat comerciantii sa nu plateasca mai mult decat este necesar pentru a mentine sistemul sigur.

Taxele de raportare sunt determinate dupa cum urmeaza. Fie r taxa de raportare din fereastra precedenta, fie t sa fie limita de piata tinta, si fie c plafonul actual al pietei. Apoi, taxa de raportare pentru fereastra curenta a taxei este data de $\max\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10{,}000}\right\}$.

D. Folosirea amenintarii cu fork-ul

Dupa cum s-a mentionat mai sus, fork-urile sunt un mod distructiv si lent pentru ca pietele sa ajunga la finalizare. In loc sa foloseasca procesul de forking pentru a rezolva fiecare piata, Augur foloseste *amenintarea* unui fork pentru a rezolva eficient pietele.

Amintiti-va ca orice miza care contesta cu succes un rezultat in favoarea rezultatului final al pietei va primi un 50% din ROI pentru miza lor de contestare. [26] In cazul unui fork, orice REP implicat pe oricare dintre rezultatele false ale pietei ar pierde toata valoarea economica. Rezultatul real este recompensat cu 50% mai mult REP in universul-copil care corespunde rezultatului real al pietei (indiferent de rezultatul forkului). Prin urmare, daca sunt impinsi intr-un fork, detinatorii REP care contesta rezultate false in favoarea rezultatelor adevarate vor iesi mereu in fata, in timp ce reprezentantii REP care au mizat pe rezultate false vor vedea ca REP isi pierd toata valoarea economica.

Consideram ca aceasta situatie este suficienta pentru a garanta faptul ca toate rezultatele falsificate vor fi contestate cu succes.

III. PROBLEME POTENTIALE & RISCURI

A. Piete parazitare

Amintiti-va ca o piata parazita este orice piata care nu plateste taxe de raportare catre Augur, dar se rezolva in conformitate cu rezolutia unei piete originale Augur. Deoarece pietele parazitare nu au reporteri sa plateasca, acestia pot oferi acelasi serviciu ca si Augur, cu taxe mai

[25] Vezi Appendix B pentru presupuneri alternative si consecintele lor.

[26] Masurat in REP care exista intr-un univers care corespunde rezultatului final al pietei; consultati teorema 3 in Appendix A.

mici. Acest lucru poate avea consecinte grave pentru integritatea protocolului lui Augur de forking.

In special daca pietele parazitare atrag interesul de tranzactionare de la Augur, atunci reporterii Augur vor primi mai putine taxe de raportare. Acest lucru ar pune presiune in jos asupra limitei de piata a REP. In cazul in care plafonul de piata al REP este prea scazut, integritatea protocolului de forking este pusa in pericol (Teorema **??**). Ca urmare, pietele parazitare au potentialul de a ameninta viabilitatea pe termen lung a Augur si ar trebui sa se opuna vehement.

Cea mai buna aparare impotriva pietelor parazitare este aceea de a face tranzactionarea pe platforma Augur cat mai ieftina posibil (mentinand in acelasi timp integritatea oracolului), pentru a minimiza recompensa pentru functionarea unei piete parazitare.

B. Volatilitatea interesului deschis

Cresterea mare, brusca si neasteptata a interesului deschis – cum ar fi cele observate in timpul unui eveniment sportiv popular – conduce la o crestere rapida a cerintei privind capacitatea de piata pentru integritatea protocoalelor de forking (Teorema: 1). Atunci cand cerinta privind capacitatea de piata depaseste plafonul de piata, exista riscul ca atacatorii rationali din punct de vedere economic sa determine un fork sa rezolve incorect. In timp ce Augur incearca sa omoare plafonul pietei in sus in astfel de situatii (vezi sectiunea **??**), aceste tentative sunt reactionare si sunt ajustate o singura data pe fereastra de 7 zile.

Este de remarcat, totusi, ca speculatorii care asista la o crestere brusca a interesului deschis pot cumpara REP in anticiparea reactiei de pe piata, reducand astfel plafonul de piata al REP, probabil intr-un punct in care integritatea protocolului de forking nu mai este amenintata. Deci, durata de timp in care oracolul este vulnerabil poate sa nu fie suficient de lunga pentru ca un atacator sa exploateze cu succes vulnerabilitatea.

C. Surse de rezolutie inconsistente sau rauvoitoare

In timpul crearii pietei, creatorii de piata au ales o sursa de rezolutie pe care reporterii ar trebui sa o utilizeze pentru a determina rezultatul evenimentului in cauza. Daca creatorul pietei alege o sursa de rezolutie inconsistenta sau rau intentionata, reporterii cinstiti pot pierde bani.

De exemplu, sa presupunem ca piata in cauza are rezultate `A` si `B`, iar creatorul de piata, Serena, si-a ales propriul site web, `atacatorul.com`. Dupa sfarsitul evenimentului de pe piata, Serena - care este, de asemenea, reporterul desemnat pentru piata - raporteaza rezultatul `A` si actualizeaza atacatorul.com pentru a indica ca rezultatul `B` rezultat. Reporterii cinstiti care verifica `atacatorul.com` vor vedea ca raportul initial este incorect si, in timpul primei runde de disputa, ar trebui sa conteste cu succes rezultatul tentativ in favoarea rezultatului `B`. Serena ar actualiza `atacatorul.com` pentru a indica ca rezultatul `A` este rezultatul corect, iar piata va intra apoi in cea de-a doua runda de disputa. Din nou, reporterii care verifica `atacatorul.com` vor vedea ca rezultatul temporar (rezultatul `B`) este incorect si pot contesta cu succes acest lucru. Serena poate repeta acest comportament pana cand piata va rezolva. Indiferent de modul in care piata rezolva, unii reporteri cinstiti vor pierde bani.

Exista mai multe variante ale acestui atac. Pur si simplu ignorarea pietelor cu surse dubioase de rezolutie nu este suficienta, pentru ca in cazul in care o astfel de piata cauzeaza un fork, toti titularii de REP vor trebui sa aleaga un univers-copil pentru a-si migra REP. Reporterii ar trebui sa ramana vigilenti impotriva pietelor cu surse dubioase de rezolutie. Astfel de piete ar trebui sa fie identificate in mod public, astfel incat reporterii sa poata coordona pentru a se asigura ca aceste piete se finalizeaza ca nevalabile.

D. Interogari ale oracolului de auto-referinta

Pietele care se ocupa de comportamentul viitor al oracolului lui Augur pot avea efecte nedorite asupra comportamentului oracolului in sine [**?**]. De exemplu, luam in considerare o piata care se ocupa de aceasta intrebare: “Va esua unul din reporterii desemnati sa prezente un raport in timpul perioadei de raportare de trei zile inainte de 31 decembrie 2018?” Pariurile plasate pe rezultatul `nu` pot actiona ca un stimulent viclean pentru reporterii desemnati sa nu raporteze in mod intentionat daca un reporter desemnat poate cumpara suficiente actiuni `da` la un pret suficient de mic pentru a compensa pierderea obligatiunii no-show.

In cazul in care plafonul de piata al REP este suficient de mare (Teorema **??**), atunci aceste interogari de auto-referinta ale oracolului nu vor ameninta integritatea protocolului de forking. Cu toate acestea, ele pot afecta negativ performanta lui Augur, cauzand intarzieri in finalizarile pietei. In timp ce pietele ar fi inca finalizate corect, acest tip de comportament este perturbator si nedorit.

E. Participarea nesigura la un fork

Nu putem sti in avans cat REP va fi migrat in universul `adevarat` in timpul perioadei de forking al unui fork, astfel incat nu putem sti in avans daca limita de piata este suficient de mare pentru ca oracolul sa aiba integritate (Teorema **??**). Credinta noastra in integritatea protocolului de forking nu poate fi mai puternica decat credinta noastra in ipotezele noastre despre limita inferioara a participarii cinstite in timpul perioadei de forking. Presupunem ca cel putin 20% din toate REP vor migra in

universul-copil `adevarat` in timpul perioadei de forking, dar nu putem garanta acest lucru.

Fork-urile Augur difera de fork-urile blockchainului intr-un aspect important: dupa un fork al blockchainului, un utilizator care detinea o moneda pe lantul-parinte va detine acum o moneda pe ambele lanturi. Ignorand atacurile de tip replay, fork-urile de blockchain prezinta un risc redus pentru utilizatori. Dupa un fork Augur, cu toate acestea, un utilizator care detine un token REP in universul-parinte poate migra aceasta moneda la doar unul din universurile copilului. Daca utilizatorul migreaza tokenul lor in orice alt univers decat universul consens, tokenul lor poate pierde toata valoarea. Astfel, REP care migreaza in timpul perioadei de forking, inainte de a fi clar ce univers-copil a obtinut un consens, expune utilizatorul la risc. Acest risc poate descuraja participarea in timpul perioadei de forking a fork-urilor de contencios.

In efortul de a compensa acest risc si de a incuraja participarea pe parcursul perioadelor de forking, toti detinatorii de tokenuri care isi migreaza REP intr-un interval de 60 de zile de la inceperea unui fork vor primi 5% REP suplimentar in universul-copil la care au migrat (vezi Sectiunea I C 9) Cu toate acestea, nu putem sti in avans daca acest bonus de 5% va fi suficient pentru a compensa riscul si pentru a stimula participarea pe parcursul unei perioade de furt.

F. Piete ambigue sau subiective

Doar evenimentele care au rezultate cunoscute in mod obiectiv sunt potrivite pentru utilizarea pe pietele Augur. Daca reporterii considera ca o piata nu este potrivita pentru rezolutie de catre platforma – de exemplu, deoarece este ambigua, subiectiva sau rezultatul nu este cunoscut pana la data de incheiere a evenimentului – acestia ar trebui sa raporteze piata ca fiind `invalida`. Daca o piata se rezolva ca `invalida`, comerciantii sunt platiti la valori egale pentru toate rezultatele posibile; pentru pietele scalare, comerciantii sunt platiti la jumatatea distantei dintre pretul minim al pietei si pretul maxim.

Este posibil sa ne imaginam piete in care unii reporteri sunt siguri ca rezultatul este `A` si altii sunt siguri ca rezultatul este `B`. De exemplu, in 2006, TradeSports a permis utilizatorilor sa speculeze daca Coreea de Nord ar lansa o racheta balistica care ar ateriza in afara spatiului sau aerian inainte de sfarsitul lui iulie 2006. Pe 5 iulie 2006, Coreea de Nord a lansat cu succes o racheta balistica care a aterizat in afara spatiului sau aerian, iar evenimentul a fost raportat pe larg de mass-media mondiala si confirmat de multe surse guvernamentale din SUA. Cu toate acestea, Departamentul de Aparare S.U.A. nu a confirmat evenimentul, asa cum a fost cerut de contractul TradeSports. TradeSports a concluzionat ca conditiile contractului nu au fost indeplinite si platit in mod corespunzator. [27]

Acesta este un caz in care spiritul pietei – pentru a anticipa lansarea rachetelor – a fost in mod clar satisfacut, dar scrisoarea pietei – de a anticipa daca Departamentul Apararii al S.U.A. ar confirma lansarea - nu a fost. TradeSports, fiind un site web centralizat, a fost capabil sa declare in mod unilateral rezultatul pietei. Daca o astfel de situatie apare pe o piata Augur, detinatorii de rapoarte pot avea opinii diferite cu privire la modul in care ar trebui sa rezolve piata si vor miza REP in mod corespunzator. In cel mai rau caz, aceasta ar putea duce la un fork in care REP in mai multe universuri-copil mentine o valoare de piata diferita de zero.

ACKNOWLEDGMENTS

Ii multumim lui Abraham Othman, lui Alex Chapman, Serene Randolph, Tom Haile, George Hotz, Scott Bigelow si Peronet Despeignes pentru feedbackul si sugestiile lor utile.

[27] Vezi `https://en.wikipedia.org/wiki/Intrade#Disputes` pentru detalii.

Anexa A: Timp de finalizare & Redistribuire

Incepem cu niste notatii, definitii si observatii.

Definitie 5. Pentru o anumita piata M, fie Ω_M spatiul de rezultate (sau setul de rezultate) al M.

Definitie 6. Pentru $n \geq 1$ si $\omega \in \Omega_M$, fie $S(\omega, n)$ reprezinta miza totala a la rezultatul ω la inceputul rundei de disputa n. Aceasta include toate mizele de la toate obligatiunile de succes in litigiu in favoarea ω in toate rundele de contestatii anterioare.

Definitie 7. Pentru $n \geq 1$ si $\omega \in \Omega_M$, fie $S(\overline{\omega}, n)$ sa denotam valoarea mizei pentru toate rezultatele din Ω_M *cu exceptia* ω la inceputul rundei de disputa n:

$$S(\overline{\omega}, n) = \sum_{\substack{\gamma \in \Omega_M \\ \gamma \neq \omega}} S(\gamma, n)$$

Definitie 8. Pentru $n \geq 1$, fie A_n sa denote miza totala peste toate rezultatele M la inceputul rundei de disputa n:

$$A_n = \sum_{\omega \in \Omega_M} S(\omega, n)$$

Observatie 3. Rezulta $A_n - S(\omega, n) = S(\overline{\omega}, n)$.

Definitie 9. Pentru $n \geq 1$, fie $\hat{\omega}_n$ sa denumeasca rezultatul tentativ la inceputul litigiului din runda n. De exemplu, $\hat{\omega}_1$ este rezultatul raportat de reporterul initial.

Definitie 10. Pentru $n \geq 1$ si $\omega \neq \hat{\omega}_n$, fie $B(\omega, n)$ sa denumeasca suma de miza necesara pentru a completa cu succes o litigiu rezultat ω in timpul disputei n.

Amintim ca suma de miza necesara pentru a completa cu succes o obligatie de disputa in favoarea rezultatului ω in timpul disputei n, unde $\omega \neq \hat{\omega}_n$ este data de ecuatia . 1, $B(\omega, n) = 2A_n - 3S(\omega, n)$.

Observatie 4. Daca o obligatie de disputa este completata cu succes in favoarea rezultatului ω in timpul disputei n, atunci $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. Adica miza de succes a contestatiei este singura miza noua aplicata rezultatului ωla sfarsitul rundei de dispute n.

Observatie 5. Pentru toate $\omega \neq \hat{\omega}_n, S(\omega, n-1) = S(\omega, n)$. Adica, daca o obligatiune de disputa nu este completa in intregime in favoarea rezultatului ω, atunci nu se adauga o miza suplimentara la rezultatul ω la inceputul urmatoarei runde de disputa. Acest lucru se datoreaza faptului ca toate mizele de contestatie nereusite sunt returnate utilizatorilor la sfarsitul rundei de contestatie.

Observatie 6. Pentru toate $n \geq 2, A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$. Aceasta inseamna ca miza totala a tuturor rezultatelor la inceputul unei runde de disputa este pur si simplu miza totala de la inceputul rundei de disputa precedenta, plus miza de succes a diferendului din runda de contestatie anterioara. Toate celelalte mize sunt returnate utilizatorilor la sfarsitul rundei de contestatie anterioare.

Lema 2. *$S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$, for $n \geq 2$.*

Demonstraţie. Sa presupunem ca o piata intra in disputa in runda n, unde $n \geq 2$. In timpul rundei $n-1$, rezultatul $\hat{\omega}_{n-1}$ trebuie sa fi fost contestat cu succes in favoarea rezultatului $\hat{\omega}_n$. Potrivit ecuatiei 1, marimea acelei obligatiuni de disputa este $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Folosind observatia 3, aceasta poate fi rescrisa ca

$$B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = 2S(\overline{\hat{\omega}_n}, n-1) \qquad \text{(A1)}$$

Stim ca obligatiunea de disputa a fost completata cu succes in timpul rundei $n-1$. Utilizand observatia 4, vedem ca $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. Observatia 5 ne indica faptul ca suma totala pariata pe $\overline{\hat{\omega}_n}$ e neschimbata din runda $n-1$ to n, $2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$. Astfel, Eq. A1 se reduce la $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$. □

Teorema 3. *Orice detinatori de REP care contesta cu succes un rezultat in favoarea rezultatului final al unei piete vor primi o ROI de 50% pentru miza lor de disputa (masurata in REP care exista intr-un univers care corespunde rezultatului final al pietei), cu exceptia cazului in care piata este intrerupta de alte piete care provoaca un fork.*

Demonstraţie. In timpul unui fork, toti utilizatorii care au completat cu succes obligatiunile de contestare in favoarea rezultatelor finale ale pietei de forking sunt date (prin intermediul monedelor minate in timpul forkului) o rata de retinere de 50% a mizei lor de disputa atunci cand migreaza miza contestatiei catre universul-copil corespunzator. Astfel, in cazul in care piata in cauza a cauzat un fork, teorema este imediat adevarata.

Acum luam in considerare cazul in care piata in cauza se rezolva fara a provoca un fork, iar raportarea nu este intrerupta de o alta piata care provoaca un fork.

Notam rezultatul final al pietei cu ω_{Final} si presupunem ca piata se rezolva la sfarsitul rundei de litigiului n, unde $n \geq 2$.Aceasta inseamna ca rezultatul tentativ pentru runda n este ω_{Final}, iar rezultatul nu este contestat cu succes in timpul rundei n. Cu alte cuvinte: $\hat{\omega}_n = \omega_{\text{Final}}$. Apoi, considerand lema 2 stim ca $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$.

Deoarece piata se rezolva la sfarsitul rundei n, fara a mai fi adaugata nici o miza la niciun rezultat, ecuatia de mai sus arata suma finala a mizei pe rezultatul final al pietei, ω_{Final} si suma tuturor mizei pe toate celelalte rezultate ale pietei, $\overline{\omega_{\text{Final}}}$. Retinem ca exista exact o dubla participare la rezultatul final al pietei, deoarece exista o combinatie intre toate celelalte rezultate.

Augur redistribuie toate mizele pe rezultatele nefinalizate catre utilizatorii care au pariat pe ω_{Final}, in functie de suma de REP pe care au efectuat-o. Prin urmare,

utilizatorii care au completat cu succes o obligatiune de litigiu in favoarea ω_{Final} obtin o rentabilitate de 50% pe REP. □

Apoi luam in considerare numarul maxim de runde de contestatie necesare pentru a rezolva o piata. Ecuatia **??** este minimizata cand ω este ales ca fiind rezultatul tentativ care incepe runda de disputa cu cel mai mare numar de miza. lema **??** implica faptul ca rezultatul non-tentativ cu cea mai mare parte a mizei este rezultatul tentativ al rundei precedente. Prin urmare, cea mai mica dimensiune posibila a legaturii de disputa care poate fi completa cu succes in timpul disputarii in jurul valorii de n, unde $n \geq 2$, este $B(\hat{\omega}_{n-1}, n)$.

Cu alte cuvinte, marimea obligatiunii de disputa creste *cel mai lent* atunci cand aceleasi doua rezultate sunt contestate in mod repetat in favoarea celuilalt. Rezulta ca numarul de runde de disputa necesare pentru ca o piata sa initieze un fork este *maximizat* atunci cand cele doua rezultate sunt contestate in mod repetat in favoarea celuilalt. Prin urmare, putem determina numarul maxim de runde de contestatie la care orice piata poate fi supusa inainte de a initia un fork prin gasirea numarului maxim de runde de disputa care pot aparea in cazul particular in care aceleasi doua rezultate ale pietei sunt contestate in mod repetat in favoarea alteia. Acum examinam acest caz.

Sa presupunem ca fiecare legatura de succes a litigiului este indeplinita in favoarea rezultatului provizoriu al runda litigiilor anterioare. Apoi, cele doua rezultate tentative, care sunt contestate in mod iterativ in favoarea celuilalt, sunt $\hat{\omega}_1$ si $\hat{\omega}_2$.

Observatie 7. In cazul in care aceleasi doua rezultate tentative sunt contestate in mod repetat in favoarea unuia pentru altul, $\hat{\omega}_n = \hat{\omega}_{n-2}$ pentru toate $n \geq 3$.

Definitie 11. Fie d sa denote suma de miza plasata pe $\hat{\omega}_1$ in timpul raportului initial. Deoarece rezultatul tentativ pentru fiecare runda este cunoscut in aceasta situatie, putem simplifica notatia noastra pentru dimensiunile de obligatiuni ale litigiilor. Definim o stenografie B_n pentru a indica dimensiunea obligatiilor necesare pentru n runde, astfel ca $B_1 = 2d$ si $B_n = B(\hat{\omega}_{n-1}, n)$ pentru toate $n \geq 2$. Acest lucru va facilita citirea si intelegerea mai usoara.

Observatie 8. In cazul in care aceleasi doua rezultate tentative sunt contestate in mod repetat in favoarea celuilalt, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ pentru $n \geq 3$. (Adica, fiecare runda litigiu de succes este adaugata la acelasi rezultat.)

Lema 4. *Daca aceleasi doua rezultate tentative sunt contestate in mod repetat in favoarea celuilalt, atunci pentru toate n unde $n \geq 3$:*

1. $S(\hat{\omega}_{n-1}, n) = \frac{2}{3} B_{n-1}$
2. $A_n = 2B_{n-1}$ *and*
3. $B_n = 3d2^{n-2}$

Demonstraţie. (Prin inductie pe n)

Sa presupunem ca aceleasi doua rezultate tentative sunt in mod repetat contestate in favoarea celuilalt.

(Caz de baza) Prin definitie si folosind ecuatia 1 facem urmatoarele observatii.

- $S(\hat{\omega}_1, 1) = d$, $S(\hat{\omega}_2, 1) = 0$, $A_1 = d$, and $B_1 = 2d$
- $S(\hat{\omega}_1, 2) = d$, $S(\hat{\omega}_2, 2) = 2d$, $A_2 = 3d$, and $B_2 = 3d$
- $S(\hat{\omega}_1, 3) = 4d$, $S(\hat{\omega}_2, 3) = 2d$, $A_3 = 6d$, and $B_3 = 6d$

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, deci partea 1 a lemei este valabila pentru $n = 3$.

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, deci partea a doua a lemmei este valabila pentru $n = 3$.

$B_3 = 6d = 3d2^{3-2}$, deci partea a treia a lemmei este valabila pentru $n = 3$.

Prin urmare, lema, in intregime, este valabila pentru cazul de baza de $n = 3$.

(Inductie) Sa presupunem ca lema este adevarata pentru toate n astfel incat $3 \leq n \leq k$. Vrem sa aratam ca lema este valabila pentru $n = k + 1$. Adica, vrem sa aratam ca:

(a) $S(\hat{\omega}_k, k+1) = \frac{2}{3} B_k$

(b) $A_{k+1} = 2B_k$ si

(c) $B_{k+1} = 3d2^{k-1}$

In primul rand, demonstram partea (a). Prin observatia 8:

$$S(\hat{\omega}_k, k+1) = S(\hat{\omega}_k, k-1) + B_{k-1}$$

Folosind observatia 7 putem rescrie cele de mai sus ca:

$$S(\hat{\omega}_{k-2}, k+1) = S(\hat{\omega}_{k-2}, k-1) + B_{k-1}$$

Prin ipoteza de inductie, putem rescrie $S(\hat{\omega}_{k-2}, k-1)$ ca $\frac{2}{3}B_{k-2}$ pe partea din dreapta ca sa obtinem:

$$S(\hat{\omega}_{k-2}, k+1) = \tfrac{2}{3}B_{k-2} + B_{k-1}$$

Prin ipoteza de inductie, putem scrie B_{k-2} ca $3d2^{k-4}$ and B_{k-1} ca $3d2^{k-3}$:

$$S(\hat{\omega}_{k-2}, k+1) = d2^{k-1}$$

Aplicand observatia 7 la partea stanga obtinem:

$$S(\hat{\omega}_k, k+1) = d2^{k-1}$$

In cele din urma, retinem ca prin ecuatia de mai sus si ipoteza de inductie, $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. Aceasta dovedeste partea (a).

In continuare, ne dovedim partea (b). Prin observatia 6:

$$A_{k+1} = A_k + B_k$$

Prin inductie, $A_k = 2B_{k-1}$:

$$A_{k+1} = 2B_{k-1} + B_k$$

Prin inductie, $B_{k-1} = 3d2^{k-3}$, sastfel incat partea dreapta poate fi simplificata la

$$A_{k+1} = 3d2^{k-2} + B_k$$

Prin inductie, $B_{k-1} = 3d2^{k-3}$, astfel incat partea dreapta poate fi simplificata la $B_k = 3d2^{k-2}$ pentru a rescrie partea dreapta ca

$$A_{k+1} = 2B_k,$$

si partea (b) este dovedita.

In cele din urma, dovedim partea (c). Prin ecuatia 1:

$$B_{k+1} = 2A_{k+1} - 3S(\hat{\omega}_k, k+1)$$

Prin observatia 8, putem scrie $S(\hat{\omega}_k, k+1)$ ca $S(\hat{\omega}_k, k-1) + B_{k-1}$:

$$B_{k+1} = 2A_{k+1} - 3\left(S(\hat{\omega}_k, k-1) + B_{k-1}\right)$$

Prin observatia 7, $\hat{\omega}_k = \hat{\omega}_{k-2}$:

$$B_{k+1} = 2A_{k+1} - 3\left(S(\hat{\omega}_{k-2}, k-1) + B_{k-1}\right)$$

Prin observatia 6, $A_{k+1} = A_k + B_k$:

$$B_{k+1} = 2\left(A_k + B_k\right) - 3\left(S(\hat{\omega}_{k-2}, k-1) + B_{k-1}\right)$$

Prin inductie, $A_k = 2B_{k-1}$ and $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$:

$$B_{k+1} = 2\left(2B_{k-1} + B_k\right) - 3\left(\tfrac{2}{3}B_{k-2} + B_{k-1}\right)$$

Prin inductie, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ si $B_{k-2} = 3d2^{k-4}$. Efectuand aceste substitutii si simplificand exponentii:

$$B_{k+1} = 3d2^{k-1}$$

Aceasta dovedeste partea (c) si incheie dovada lemmei. □

Teorema 5. *Daca nu este intrerupta de o alta piata care provoaca un fork, o anumita piata poate suferi cel mult 20 de runde de disputa inainte de a finaliza sau a provoca un fork.*

Demonstraţie. Sa presupunem ca o anumita piata nu este intrerupta de o alta piata care provoaca un fork. Apoi, dupa cum am aratat mai sus, stim ca numarul de runde de contestatie necesare pentru ca o piata sa initieze un fork este maximizat atunci cand aceleasi doua rezultate sunt in mod repetat contestate in favoarea celuilalt. Partea 3 din lema 4 ne spune ca, in aceasta situatie, marimea obligatiunii de disputa necesara pentru contestarea cu succes a rezultatului tentativ in timpul rundei n este data de $3d2^{n-2}$, unde d este suma mizei plasate in timpul raportului initial.

Stim ca fork-urile sunt initiate dupa indeplinirea cu succes a unei obligatiuni de diferend cu o dimensiune de cel putin 2,5% din toate REP-urile existente si stim ca exista 11 milioane REP in total. Astfel, un fork este initiat atunci cand se completeaza o obligatiune de disputa cu dimensiunea 275,000 REP. De asemenea, stim ca $d \geq 0.35$ REP, deoarece suma minima a mizelor din raportul initial este 0.35 REP[28].

Rezolvand $3(0.35)2^{n-2} > 275,000$ pentru $n \in \mathbb{Z}$ rezulta $n \geq 20$. Astfel, putem garanta ca o piata va rezolva sau va provoca un fork dupa cel mult 20 de runde de disputa. □

Anexa B: Ipoteze alternative & consecinte

Reamintim ca:

- S este proportia totala a REP care este migrata in universul `adevarat` in timpul perioadei de forking
- P este pretul REP in universul `adevarat`
- P_f este pretul REP care a fost migrat intr-un univers `fals` la alegerea atacatorului
- I_a este interesul deschis al lui Augur
- I_p este interesul parazitar deschis

Augur face anumite ipoteze despre S, P_f, and I_p pentru a ajunge la o limita tinta de piata. In special Augur presupune ca cel putin 20% din toate REP vor fi migrate in universul `adevarat` in timpul perioadei de forking al unui fork, REP migrata intr-un univers `fals` nu va avea nicio valoare ne-neglijabila, iar interesul parazitar deschis va fi cel mult jumatate din interesul nativ deschis. Cu alte cuvinte: $S \geq 0.2$, $P_f = 0$, si $I_a \geq 2I_p$. In aceste ipoteze, teorema 1 ne spune ca protocolul de forking are integritate ori de cate ori limita de piata a REP este mai mare de 7.5 ori mai mare decat interesul nativ deschis.

Puteti face propriile dvs. presupuneri despre S, P_f, si I_p pentru a ajunge la propriile concluzii despre cat de mare trebuie sa fie capacitatea de piata pentru ca oracolul sa aiba integritate in practica. Vom lista cateva scenarii alternative pentru confortul dvs.

Scenariu 1. Mai mult de 50% din REP existente migreaza catre universul `adevarat` in timpul perioadei de

[28] Vezi appendix E 2 si E 3

forking. In acest caz, P_f and I_p nu conteaza deloc. Deoarece $S > \frac{1}{2}$, protocolul de forking are integritate indiferent de care se intampla sa fie plafonul de piata. Nu ar exista destule REP pe piata pentru ca un atacator sa aiba succes.

Scenariu 2. 48% din REP-urile existente migreaza catre universul `adevarat` in timpul perioadei de forking, nu exista piete parazitare si REP trimis unui univers `fals` nu are nicio valoare. In acest caz $S = 0.48$, $I_p = 0$, si $P_f = 0$. In aceste ipoteze, limita de piata a REP trebuie sa fie mai mare decat aproximativ dublul interesului nativ deschis pentru ca protocolul de forking sa aiba integritate.

Scenariu 3. 20% din REP existente migreaza catre universul `adevarat` in timpul perioadei de forking, interesul parazitar deschis este egal cu interesul nativ deschis si REP migreaza intr-un univers `fals` tranzactioneaza la 5% din valoarea REP a migrat la universul `adevarat`. In acest caz $S = 0.2$, $I_p = I_a$, si $P_f = 0.05P$. In conformitate cu aceste ipoteze, plafonul de piata al REP trebuie sa fie mai mare decat aproximativ 10.5 ori mai mare decat interesul nativ deschis pentru ca protocolul forking sa aiba integritate.

Scenariu 4. Doar 5% din REP existente migreaza catre universul `adevarat` in timpul perioadei de forking, interesul parazitar este de doua ori mai mare decat interesul nativ deschis, iar REP trimis intr-un univers `fals` tranzactioneaza la 5% valoarea REP trimisa in universul `adevarat`. In acest caz $S = 0.05$, $I_p = 2I_a$, si $P_f = 0.05P$. In aceste ipoteze, plafonul de piata al REP trebuie sa fie mai mare de 63 ori decat interesul nativ deschis pentru ca protocolul de forking sa aiba integritate.

Anexa C: Efectul bonusului de migrare timpurie asupra integritatii protocolului de forking

Pentru usurarea discutiilor, am ignorat bonusul de migrare timpurie de 5% si un termen mic cand discutam despre integritatea protocolului forking. Aici vom revizui teorema 1 luand in considerare aceste doua lucruri.

Ca si inainte, suma de REP trimisa universului `adevarat` in timpul perioadei de raportare este notata cu SM. Astfel, pentru ca un atacator sa aiba succes, trebuie sa migreze cel putin $SM + \epsilon$ REP, care are o valoare de $(SM + \epsilon)P$ inainte de migrare, intr-un univers `fals`.

Daca un atacator migreaza $SM+\epsilon$ REP intr-un univers `fals` in timpul perioadei de raportare a unui fork, va primi $1.05(SM + \epsilon)$ REP in universul-copil la care au migrat. Prin definitia lui P_f, valoarea acestor monede este data de $1.05(SM+\epsilon)P_f$. Astfel, costul minim pentru atacator este $(SM + \epsilon)P - 1.05(SM + \epsilon)P_f$, care poate fi exprimat ca $(SM + \epsilon)(P - 1.05P_f)$.

Ca si inainte, profitul maxim (brut) pentru un atacator este dat de $I_a + I_p$. Asadar, se spune ca protocolul de forking are integritate ori de cate ori $S > \frac{1}{2}$ sau:

$$I_a + I_p < (SM + \epsilon)(P - 1.05P_f) \tag{C1}$$

Rezolvand inegalitatea de mai sus pentru plafonul de piata, PM, putem vedea ca protocolul de forking are integritate daca si numai daca:

1. $S > \frac{1}{2}$ sau
2. $1.05P_f < P$ si capitalul de piata al REP este mai mare decat $\frac{P(I_a+I_p-\epsilon(P-1.05P_f))}{S(P-1.05P_f)}$

Dupa cum se poate observa, efectul bonusului migratiei timpurii asupra cerintei privind capacitatea de piata este foarte mic.

Anexa D: Efectul bonusului migratiei timpurii asupra costului minim al unui fork

Pentru a incuraja o participare mai mare in timpul unui fork, toti posesorii de tokenuri care isi migreaza REP intr-un interval de 60 de zile de la inceperea unui fork vor primi 5% REP suplimentar in universul-copil la care au migrat. Aceasta recompensa este platita prin inflatia monetara.

Acest bonus poate deveni un stimulent pervers daca costul initierii unui fork este prea mic. In special daca un atacator poate castiga mai multa valoare din bonusul de 5% REP decat ar pierde prin initierea unui fork, atunci ne asteptam ca fork-urile sa se intample cat mai des posibil. Acest atac, la care ne referim ca fiind un *atac de muls inflatia*, nu ar duce la raportarea incorecta a oracolului, dar ar duce deseori la disfunctionalitatea fork-urilor.

Pentru a preveni acest comportament, Augur trebuie sa se asigure ca costul initierii unui fork este mai mare decat valoarea maxima care poate fi obtinuta din bonusul de inflatie de 5%. Aici derivam o limita inferioara pentru costul initierii unui fork, pentru a preveni acest stimulent pervers.

Fie P_0 sa exprime pretul REP inainte de fork si P_1 sa exprime pretul REP dupa fork. Fie M_0 rezerva de bani inainte de fork iar M_1 rezerva de bani dupa fork. Fie S proportia de M_0 migrand in universul `adevarat` in timpul perioadei de forking. Fie b cantitatea de REP care trebuie sa fie distrusa din punct de vedere economic adica mizata pe un rezultat `fals` pentru a initia un fork. Presupunem ca $b > 1$.

In scopul acestei sectiuni, facem presupunerea conservatoare ca toate REP care migreaza in timpul perioadei de forking sunt controlate de atacator. Mai presupunem (deoarece minimizeaza costul acestui atac) ca toate REP care migreaza in timpul perioadei de forking sunt migrate in universul `adevarat`.

Cu aceasta notatie, SM_0 este cantitatea de REP migrata in timpul perioadei de forking, in timp ce $(1-S)M_0$ este suma de REP ce *nu a fost* migrata in timpul perioadei de forking.

$$M_0 = SM_0 + (1 - S)M_0 \tag{D1}$$

Atunci cand un total de SM_0 REP este migrat in timpul perioadei de forking, un total de $0.05SM_0$ REP este creat prin inflatie:

$$M_1 = 1.05SM_0 + (1 - S)M_0 \tag{D2}$$

Concentrandu-se doar pe efectele inflatiei si, din motive de simplitate, presupunem ca limita de piata dupa fork va fi aceeasi cu cea a pietei inainte de fork [29]:

$$P_0M_0 = P_1M_1 \tag{D3}$$

Inlocuind D1 si D2 cu D3 si simplificand, rezulta:

$$P_1 = \frac{20P_0}{20 + S} \tag{D4}$$

Beneficiul (brut) al atacatorului pentru initierea unui fork si profitarea de bonusul de migratie timpurie este valoarea lui REP migrat dupa migrare, minus valoarea lui REP migrat inainte de migrare:

$$1.05SM_0P_1 - SM_0P_0 \tag{D5}$$

Inlocuind D4 in D5 obtinem o expresie alternativa pentru beneficiul (brut) pentru atacator:

$$1.05SM_0\frac{20P_0}{20 + S} - SM_0P_0 \tag{D6}$$

Reamintim ca b este cantitatea de REP care trebuie sa fie distrusa economic pentru a initia un fork. Astfel, costul initierii unui fork este bP_0. Prin urmare, plata costului de initiere a unui fork pentru a beneficia de bonusul de migratie timpurie este utila ori de cate ori este indeplinita urmatoarea inegalitate:

$$0 < 1.05SM_0\frac{20P_0}{20 + S} - SM_0P_0 - bP_0 \tag{D7}$$

Observand ca $P_0 > 0$, si $S \neq -20$, rezolvam pentru b si vedem ca atacul este profitabil atunci cand:

$$b < \frac{21M_0S}{S + 20} - M_0S \tag{D8}$$

Pentru a impiedica stimularea perversa, Augur trebuie sa aranjeze astfel incat:

$$b \geq \frac{21M_0S}{S + 20} - M_0S \tag{D9}$$

Observand ca S este limitat la intervalul $[0, 1]$, vedem ca valoarea partii drepte a inegalitatii D9 este maximizata atunci cand $S = 2\sqrt{105} - 20 \approx 0.4939$. Asta este, acest atac este cel mai profitabil pentru atacator atunci cand aproximativ 49.39% din toate REP-urile existente sunt migrate in timpul perioadei de forjare. Fiind conservatoari, folosim aceasta valoare pentru S.[30]

Inlocuind $S = 0.4939$ in D9 obtinem $b \geq 0.012197M_0$. Prin urmare, daca costul de a initia un fork este de cel putin 1,2197% din REP existenti, atunci atacul cu mulgere de inflatie nu este profitabil.

Amintim ca un fork este initiat numai dupa incheierea unei dispute de succes care este mai mare de 2,5 % din REP existente. Sa presupunem ca o astfel de obligatie de disputa a fost completata in favoarea rezultatelor ω si a unei fork au fost initiate. Rezultatul ω este fie adevarat, fie fals.

Daca rezultatul ω este fals, atunci cel putin 2,5% din REP existente au fost mizati pe un rezultat fals si, prin urmare, au ars economic. De aceea, mulsul de inflatie nu este profitabil cand ω este fals.

In cazul in care rezultatul ω este adevarat, atunci lema **??** ne spune ca cel putin 1,25 % din REP (total) este mizat pe rezultate false si, prin urmare, ars economic. De aceea, mulsul de inflatie nu este profitabil nici atunci cand ω este adevarat.

Din acest motiv, initierea forkului necesita completarea cu succes a unei obligatiuni de contestatie care este de cel putin 2,5% din numarul REP actual.

Anexa E: Ajustari de dimensiune a obligatiunilor

Legatura de valabilitate, obligatiunea REP fara retinere si miza reporterului desemnat sunt ajustate dinamic pe baza comportamentului participantilor in timpul ferestrei de taxare anterioare. Aici descriem modul in care ajustam aceste valori.

Definim functia $f : [0, 1] \to [\frac{1}{2}, 2]$ prin:[31]

$$f(x) = \begin{cases} \frac{100}{99}x + \frac{98}{99} & \text{pentru} \quad x > \frac{1}{100} \\ 50x + \frac{1}{2} & \text{pentru} \quad x \leq \frac{1}{100} \end{cases} \tag{E1}$$

Functia f este utilizata pentru a determina multipliul utilizat in aceste ajustari, asa cum este descris in subsectiunile de mai jos. Pe scurt, daca comportamentul nedorit a avut loc exact in 1% din timpul ferestrei de taxare anterioare, atunci dimensiunea obligatiunilor ramane aceeasi. Daca ar fi mai putin frecventa, dimensiunea obligatiunilor va fi redusa cu jumatate. Daca ar fi mai frecventa, atunci marimea obligatiunii va fi marita cu un factor de 2.

---

[29] Credem ca este conservator. In practica, ne asteptam ca dimensiunile pietei sa scada dupa un fork.

[30] In practica, atacatorul nu poate impiedica alti participanti sa migreze propriul REP in timpul perioadei de forking si astfel nu poate garanta ca S nu ar depasi valoarea ei ideala de aproximativ 0.4939. Cu toate acestea, deoarece aparam impotriva celui mai grav scenariu, folosim $S = 0.4939$.

[31] Aceasta formula se poate schimba dupa obtinerea datelor empirice din pietele live.

1. Validarea Obligatiunii

In prima fereastra de taxa dupa lansare, legatura de valabilitate va fi setata la 0,01 ETH. Apoi, daca mai mult de 1% din pietele finalizate din fereastra de taxare anterioara au fost nevalide, legatura de valabilitate va fi marita. In cazul in care mai putin de 1% din pietele finalizate din fereastra taxei anterioare au fost nevalide, atunci obligatiunile de valabilitate vor fi reduse (dar niciodata nu vor fi mai mici de 0,01 ETH).

In special, definim ν proportia pietelor finalizate din fereastra de taxare anterioara care este nevalida, iar b_v sa fie valoarea garantiei valabilitatii din fereastra de taxa anterioara. Atunci legatura valabilitatii pentru fereastra curenta este $\max\left\{\frac{1}{100}, b_v f(\nu)\right\}$.

2. Obligatiunea No-Show REP

In prima fereastra de taxare dupa lansare, obligatia REP no-show va fi setata la 0.35 REP. Ca si in cazul obligatiunilor de valabilitate, obligatiunea REP nu este reglata in sus sau in jos, directionand o rata de 1% fara afisare cu o limita inferioara de 0.35 REP.

Mai specific, definim ρ sa fie proportia pietelor din fereastra de taxare anterioara a carei reporteri desemnati nu au reusit sa raporteze la timp si definim b_r suma rambursarii REP de la fereastra de taxare anterioara. Suma obligatiunii REP fara taxa pentru fereastra curenta de taxe este $\max\{0.35, b_r f(\rho)\}$.

3. Miza pentru reporter recomandata

In prima fereastra de taxa dupa lansare, suma pachetului de reporter desemnata va fi stabilita la 0.35 REP. Valoarea mizei de reporter desemnate este ajustata dinamic in functie de numarul de rapoarte desemnate incorecte (nu a reusit sa concureze cu rezultatul final al pietei) in timpul ferestrei de taxare anterioare.

In particular, definim δ proportia rapoartelor desemnate care au fost incorecte in timpul ferestrei de taxare anterioare si definim b_d suma mizei reporter desemnate in timpul ferestrei taxelor anterioare, apoi valoarea mizei reporterului pentru fereastra curenta este $\max\{0.35, b_d f(\delta)\}$.

Anexa F: Modificari arhitecturale

Am ajuns la designul actual al lui Augur dupa trei ani de cercetare si iteratie. Designul care a iesit din acest proces difera substantial de viziunea prezentata in vechea noastra versiune de whitepaper [**?**]. Aici discutam trei schimbari semnificative, precum si rationamentul schimbarilor.

1. Taxele de raportare

In vechiul design, creatorul de piata ar stabili o taxa de tranzactionare care ar fi impartita 50/50 cu reporterii. In designul actual, taxele pentru creatorul de piata si reporterii sunt independente, iar taxele reporterilor sunt reglate dinamic de catre Augur pentru a mentine sistemul in siguranta.

Taxele platite reporterilor influenteaza pretul REP, care are un efect direct asupra securitatii protocolului de forking (Theorem 1). Daca taxele platite reporterilor sunt prea mici, atunci integritatea oracolului este in pericol. Daca taxele platite reporterilor sunt prea mari, atunci amenintarea pietelor parazitare creste. Astfel, este important ca taxele platite reporterilor sa fie ajustate dinamic pentru a pastra securitatea lui Augur, in loc sa fie luate in mod arbitrar de catre creatorii de piata.

Decuplarea comisioanelor de reporteri de la alegerile creatorilor de piata asigura, de asemenea, ca reporterii (si, prin urmare, integritatea protocoalelor) nu sunt afectati de concurenta dintre creatorii de piata pentru a crea piete cu cele mai mici taxe. Pietele de calitate si raportarea calitatii ar trebui masurate si recompensate separat. Concurenta ar trebui sa permita reducerea taxelor de creare a pietei la zero, fara a reduce si taxele platite reporterilor.

2. Taxele de tranzactionare

In vechiul design, taxele au fost colectate de la comercianti pentru fiecare comert. In noul design, taxele sunt colectate de la comercianti numai atunci cand se solutioneaza direct cu contracte de piata. Aceasta schimbare a fost facuta, partial, deoarece Augur nu poate face tranzactii offline. Cotele de rezultate ale pietei sunt simple simboluri, care pot fi tranzactionate in mod liber intre utilizatori. Deoarece colectarea taxelor pentru fiecare comert este imposibila, Augur colecteaza taxele numai atunci cand comerciantii se stabilesc direct cu contractele de piata Augur. Un avantaj suplimentar al acestei abordari il reprezinta reducerea comisioanelor medii platite de catre comercianti, ceea ce ar trebui sa faca pe Augur mai competitiva.

3. Universuri

In proiectul vechi, exista o singura "versiune" a lui REP, iar productia sa totala a fost fixata. In prezent, REP poate fi fork-uita in multe versiuni diferite (universuri), fiecare dintre acestea putand ajunge cu mai mult sau mai putin total REP in comparatie cu versiunea originala. Daca un fork este controversat, aprovizionarea REP in fiecare univers-copil ar putea fi doar o fractiune din totalul ofertei din universul-parinte. Intr-un fork fara contencios, bonusul de migrare timpurie catre participan-

tii la fork ar putea avea ca rezultat un univers-copil care are un numar mai mare de REP decat universul-parinte.

Noile versiuni ale REP sunt create de un fork, fiecare avand propriile preturi si cantitatea totala, iar furnizorii de servicii ar trebui sa le trateze ca atare. Cand Augur se va lansa prima data, va exista un singur univers (universul genezei) si o singura versiune a REP, la fel cum exista acum. Totusi, de indata ce se produce un fork, singura versiune a REP se va imparti in mai multe variante: de exemplu, o piata de forking cu rezultate `A` si `B`

ar creea token-urile noi REP-`A`, REP-`B`, si REP-`invalid`. Portofelele si schimburile care suporta REP vor avea acum patru versiuni diferite ale REP pe care ar putea sa le suporte (teoretic) – REP-`geneza` (versiunea originala a REP, care acum ar fi blocata), REP-`A`, REP-`B`, and REP-`invalid`.[32]

Rezerva totala de REP fiecare univers-copil depinde de cat de mult REP a migrat la ea si cand a avut loc aceasta migrare. Migrarea REP in timpul unui fork, inainte de a se clarifica ce univers-copil a obtinut un consens, expune utilizatorul la o cantitate mica de risc (dar nu zero) (vezi sectiunea III E), ce poate descuraja participarea in timpul perioada de forking a fork-urilor de contencios. Pentru a incuraja participarea in timpul unui fork, utilizatorii trebuie compensati pentru risc.

Utilizatorii care nu participa in timpul perioadei de forking al unui fork ar putea fi penalizati pierzand o parte din proprietatea lor de REP. De fapt, modelul vechi a avut un mecanism “utilizati-l sau pierdeti-l”, care penaliza ne-participantii ca si cum ar fi fost reporteri care au raportat incorect. Cu toate acestea, pedepsirea utilizatorilor care nu participa creeaza probleme semnificative de utilizare. Pedepsirea utilizatorilor care nu participa este problematica pentru portofelele si schimburile care sunt custodii REP. In cazul unui fork, schimburile ar trebui sa migreze REP-ul clientului lor la un anumit univers-copil in timpul perioadei de forking sau sa piarda o parte din proprietatilor lor de REP. [33]

In loc de a penaliza persoanele care nu participa, participantii la fork care migreaza in timpul perioadei de forking sunt recompensati prin crearea unui bonus de 5% in universul-copil la care acestia migreaza. In cazul in care 4.762% din REP (sau mai mult) migreaza intr-un univers pierzator – din care 1,25% pana la 2,5% au fost deja angajati ca miza de disputa – atunci toate universurile vor avea o cantitate totala redusa de REP fata de universul-parinte .

[32] Ca o problema practica, furnizorii de servicii pot considera ca este mai usor(si cel mai putin perturbator pentru utilizatorii lor) sa incurajeze utilizatorii lor sa participe in fork, iar apoi pur si simplu sa sustina universul castigator odata ce fork-ul s-a rezolvat.

[33] De asemenea, am constatat, ca o problema practica, ca contractul inteligent necesar pentru punerea in aplicare a recompenselor de forfecare numai prin utilizarea redistribuirii a fost extrem de complex. Complexitatea codului de contract este ea insasi un risc de securitate, asa ca am incercat sa simplificam punerea in aplicare ori de cate ori este posibil.