# Augur: decentralizuota prognozavimo rinkų platforma

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander
*Forecast Foundation*
(Dated: 2018 m. gegužės 24 d.)

Augur yra patikimas, decentralizuotas orakulas ir prognozių rinkų platforma. Augur prognozavimo rinkų rezultatus pasirinko vartotojai, kurie turi Augur reputacijos žetonus ir juos naudoja sistemoje pateikdami faktinius spėjimų rezultatus ir už tai gauna atsiskaitymo mokesčius iš rinkų. Augur atlygio struktūra sukurta siekiant užtikrinti, kad sąžiningai ir tiksliai raportuojantys apie rezultatus reporteriai visada būtų gautų daugiausiai naudos. Žetonų savininkai gali skelbti palaipsniui didėjančias reputacijos obligacijas, kad ginčytų siūlomus rinkos rezultatus. Jei šių obligacijų dydis pasiekia tam tikrą ribą, reputacijos žetonai suskaidomi į keletą versijų, po vieną kiekvienam galimam ginčijamos rinkos rezultatui; žetonų turėtojai turi iškeisti savo turimus reputacijos žetonus į vieną iš šių versijų. Reputacijos versijos, kurios neatitinka tikroviško rezultato, taps nereikalingos, nes niekas nedalyvaus prognozavimo rinkose, nebent jie bus tikri, kad rinkos tinkamai išsispręs. Todėl žetono savininkai pasirinks vienintelę reputacijos versiją, kurią jie žino, ir kuri toliau bus vertinga, tikrovę atitinkanti versija.

Augur yra pasitikėjimo, decentralizuotų spėjimų ir prognozavimo rinkos platforma. Prognozuojant rinką, žmonės gali spekuliuoti ateities įvykių rezultatais; tie, kurie prognozuoja, kad rezultatai teisingai, laimi pinigus, ir tie, kurie prognozuoja neteisingai praranda pinigus [1–3]. Prognozuojamos rinkos kaina gali būti tikslus ir gerai kalibruotas rodiklis, kokio tikimasi įvykio [4–7].

Naudodamiesi Augur, žmonės turės galimybę prekiauti rinkose savo prognozėmis labai mažomis sąnaudomis. Vieninteliai reikšmingi dalyvių išlaidų skaičiai - tai kompensacija rinkos kūrėjams ir vartotojams, kurie praneša apie rinkų rezultatus, įvykus įvykiui. To pasekoje, Augur yra prognozių rinka, kurioje pasitikėjimo reikalavimai, trintis ir mokesčiai bus tokie žemi, kaip ir konkurentų.

Istoriškai prognozavimo rinkos buvo centralizuotos. Paprasčiausias būdas sudaryti sandorius prognozuojamoje rinkoje yra apskaitos žurnalą palaikymas; taip pat tai yra paprasčiausias būdas nustatyti įvykio rezultatą ir paskirstyti išmokas prekybininkams, kuris yra patikimas nešališkam, patikimam teisėjui, kuris nustato rinkų rezultatus. Tačiau centralizuotos prognozavimo rinkos turi daugybę pavojų ir apribojimų: nėra galimas visuotinis dalyvavimas, apribotos rinkų rūšys, ir reikalauja, kad dalyviaiai pasitikėtų rinkos operatoriumi, kad jie nepasisavintų lėšų ir tinkamai išspręstų spėjimų baigtis.

Augur siekia padaryti rinkas visiškai decentralizuotas. Decentralizuoti, patikimi tinklai, tokie kaip Bitcoin[8] ir Ethereum[9], pašalina riziką, kad savanaudiškumas kels korupciją ar vagystę. Vienintelis Augur kūrėjų vaidmuo yra paskelbti išmanias sutartis su Ethereum tinklu. Augur sutartys yra visiškai automatizuotos: kūrėjai neturi galimybės išleisti lėšų, kurios laikomos sąlyginio deponavimo sutartimi, nekontroliuoja, kaip rinkos išsisprendžia, nepatvirtina ar neatmeta sandorių, negali atšaukti sandorių ir t.t. Augur *orakulas* leidžia informaciją perkelti iš realaus pasaulio į blokų grandinę, nesinaudojant tarpininku. Augur bus pirmasis pasaulyje decentralizuotas orakulas.

## I. KAIP VEIKIA AUGUR

Augur rinkos vykdomos keturių pakopų progresija: *sukūrimas*, *investavimas*, *reportingas* ir *išsprendimas*. Kiekvienas gali sukurti rinką, pagrįstą bet kuriuo realiu įvykiu. Prekyba prasideda iškart po rinkos sukūrimo ir visi vartotojai gali laisvai prekiauti bet kurioje rinkoje. Pasibaigus įvykiui, kuria rinka grindžiama, įvykio baigtį lemia Augur orakulas. Paaiškėjus rezultatui, prekybininkai gali uždaryti savo pozicijas ir susirinkti išmokas.

Augur turi savo žetoną Reputation (REP). REP reikalingas rinkų kūrėjams ir reporteriams, kurie praneša apie Augur platformos sukurtų rinkų rezultatus. Reporteriai praneša apie rinkos baigtį, *statydami* savo REP už vieną iš rinkos galimų rezultatų. Tai darydamas, reporteris pareiškia, kad rezultatas, ant kurio buvo statyta, atitinka realaus pasaulio įvykio rezultatą. Rinkos reporterio reportas yra laikomas "tiesa", siekiant nustatyti rinkos rezultatus. Jei pranešėjo pranešimas apie rinkos rezultatus neatitinka kitų žurnalistų pasiekto sutarimo, Augur perskirsto REP, teisingai rezultatą pranešusiems reporteriams.

Turėdami REP ir tiksliai reportuodami, žetono turėtojai turi teisę į dalį platformos mokesčių. Kiekvienas registruotas REP žetonas suteikia jo turėtojui tokią pačią Augur rinkos kainą. Kuo daugiau REP reporteriui priklauso ir kuo daugiau jis teisingai praneša, tuo daugiau mokesčių jis uždirbs už savo darbą, užtikrinant platformos saugumą.

Nepaisant to, kad Augur operacijose REP atlieka pagrindinį vaidmenį, jis nėra naudojamas prekybai Augur rinkose. Prekybininkams nereikia REP, kadangi jiems nereikia dalyvauti reportavimo procese.

### A. Rinkos sukūrimas

Augur leidžia kiekvienam kurti rinką bet kokiam artėjančiam įvykiui. *Rinkos kūrėjas* nustato *vietą ir laiką* ir parenka *reporterį* pranešti apie įvykio rezultatus.


1 pav.. Supaprastinta rinkos schema.

Paskirtasis pranešėjas vienašališkai nenusprendžia rinkos rezultatų; bendruomenė visada turi galimybę ginčyti ir ištaisyti paskirtą pranešėjo pranešimą.

Be to, rinkos kūrėjas pasirenka *atsakymo šaltinį* kurį reporteriai naudos nustatytį įvykio baigtį. Sprendimo šaltinis gali būti "bendros žinios" arba jis gali būti konkretus šaltinis, pvz., "Jungtinių Amerikos Valstijų energetikos departamentas", bbc.com, arba tam tikro API adreso pabaiga.[1] Jie taip pat nustato *kūrėjo mokestį*, kuris yra rinkliavos, kurią prekybininkai sumoka rinkos sutartyje (žr. I D dėl mokesčių). Galiausiai, rinkos kūrėjas skelbia dvi obligacijas: *galiojimo obligacija* ir *nurodyto reporterio nepasirodymo obligacija* (taip pat žinoma kaip *nepasirodymo obligacija* trumpiau).

Galiojimo obligacija mokama ETH ir grąžinama rinkos kūrėjui, jei rinka išsprendžia bet kokį rezultatą, išskyrus *neteisingą*.[2] Galiojimo obligacija skatina rinkos kūrėjus kurti rinkas, pagrįstas gerai apibrėžtais įvykiais, su objektyviais ir nedviprasmiais rezultatais. Galiojimo obligacijos dydis nustatomas dinamiškai, atsižvelgiant į negaliojančių rezultatų santykį pastarosiose rinkose.[3]

Nepasirodymo obligacija susidaro iš dviejų dalių: *nepasirodymo mokesčio obligacija* (apmokama ETH) ir *nepasirodymo REP obligacija* (apmokama REP). Šios obligacijos grąžinamos rinkos kūrėjui, jei rinkos paskirtasis reporteris iš tikrųjų praneša per pirmąsias tris dienas po rinkos *įvykio pabaigos laiko*. Jei paskirtasis pranešėjas per ataskaitinį 3 dienų laikotarpį nepateikia savo ataskaitos, tada rinkos kūrėjas praranda nepasirodymo obligaciją ir nurodo *pirmą viešą reporterį* kuris praneša apie rinką (žr. I C 6). Tai skatina rinkos kūrėją pasirinkti patikimą paskirtą reporterį, kuris turėtų padėti rinkoms greitai išspręsti.

Neatskiriama gas jungtis skirta padengti pirmojo viešo reporterio gas išlaidas. Tai užkerta kelią scenarijui, kai pirmojo viešojo žurnalisto gas kainos yra pernelyg didelės, kad ataskaitų teikimas būtų pelningas. Nerodomo gas obligacija yra du kartus didesnė už vidutinę gas kainą už reportų teikimą per ankstesnį mokestinį langą.

Tuo atveju, jei paskirtasis reporteris nepateikia ataskaitos, nepasirodymo REP obligacija suteikiama pirmam viešajam pranešėjui už jų pateiktus rezultatus, todėl pirmasis viešas reporteris gautų nepasirodymo REP obligaciją tik jei praneša teisingai. Kaip ir su galiojimo obligacija, nepasirodymo REP obligacija koreguojama dinamiškai, atsižvelgiant į dalį paskirtų žurnalistų, kurie per ankstesnį mokestinį langą nepranešė apie baigtį laiku.[4]

Rinkos kūrėjas sukuria rinką ir pateikia visas reikalingas obligacijas per vieną Ethereum sandorį. Kai sandoris patvirtinamas, rinka yra aktyvi ir prasideda prekyba.

### B. Prekyba

Rinkos dalyviai prognozuoja įvykių rezultatus prekiaudami įvykio prognozėmis *akcijomis*. *Pilnas akcijų paketas* yra akcijų rinkinys, kurį sudaro viena dalis kiekvieno galimo galiojančio įvykio rezultato [10]. Pilni rinkiniai sukuriami Augur išmanijų sutarčių varikliuko, reikalingo norint užbaigti sandorius.

Pavyzdžiui, apsvarstykime rinką, turinčią du galimus rezultatus, A ir B. Alisa nori sumokėti 0,7 ETH už dalį A ir Bobas yra pasirengęs mokėti 0,3 ETH už dalįB.[5] Pirma, Augur priima šiuos užsakymus ir surenka viso 1 ETH iš Alice ir Bob.[6] Tuomet Augur sukuria visą akcijų rinkinį, suteikiant Alisai akcijas A ir Bobui akcijas B. Taip atsiranda įvykių baigčių akcijos. Sukūrus akcijas, jomis galima laisvai prekiauti.

Augur prekybos sutartyse yra užsakymų knyga kiekvienai platformos sukurtai rinkai. Bet kas gali sukurti naują užsakymą arba užpildyti esamą užsakymą bet kuriuo metu. Užsakymus užpildo automatinis atitikimo variklis, kuris yra Augur išmaniosiose sutartyse. Prašymai pirkti ar parduoti akcijas tuoj pat vykdomi, jei užsakymų knygelėje jau yra atitinkamas užsakymas. Tai gali būti padaryta perkant arba parduodant akcijas kitiems dalyviams, kurie gali būti susiję su naujų komplektų išleidimu arba galiojančių komplektų uždarymu. Augur sulyginimo varikliukas visada prideda minimalią akcijų

[1] Pvz., Jei "Oro temperatūros" ("Weather Underground") ataskaitoje "Aukšta temperatūra (laipsniais Fahrenheitu) 2018 m. Balandžio 10 d. San Francisko tarptautiniame oro uoste"`https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html`, reporteriai tiesiog naudosis šia nuoroda ir pateiks aukščiausią temperatūrą, pateiktą jų ataskaitoje.

[2] *neteisinga rinka* - tai rinka, kurią reporteriai laikė negaliojančia, nes nė vienas iš rinkos kūrėjo išvardytų rezultatų nėra teisingas arba dėl to, kad rinkos formuluotė yra dviprasmiška arba subjektyvi; žr. skirsnį III F diskusijai.

[3] Žr. E 1 detalesniam nagrinėjimui.

[4] Žr. E 2 detaliau.

[5] Iš pradžių prekybai Augur rinkose bus naudojama Ethereum valiuta, eteris (ETH). Vėlesnės Augur versijos palaikys rinkas, kitais žetonais, sukurtais Ethereum tinkle, įskaitant žetonus, susietus su fiat valiutomis ("stabilieji žetonai"), jei / kai jos taos prieinami.

[6] Čia naudojamas 1 ETH skaičius, kad būtų lengviau diskutuoti. Faktinės viso akcijų paketo kainos yra daug mažesnės; žr. `docs.augur.net/#number-of-ticks` detalesniam nagrinėjimui.

ir (arba) pinigų sumą, reikalingą rizikai padengti. Jei nėra tinkamo užsakymo arba prašymas gali būti tik iš dalies užpildytas, likusioji dalis įtraukiama į užsakymų knygą kaip į naują užsakymą.

Užsakymai niekada neįvykdomi už blogesnę kainą nei prekiautojo nustatyta ribinė kaina, bet gali būti įvykdyta už geresnę kainą. Neužpildytus ir iš dalies užpildytus užsakymus bet kuriuo metu galite pašalinti iš užsakymų knygos užsakymo kūrime. Prekiautojai moka mokesčius tik tada, kai parduodami visi akcijų paketai; Atsiskaitymo mokesčiai išsamiau aptariami 4 skyriuje I D.

Nors dauguma prekybos akcijomis turėtų įvykti prieš atsiskaitymą rinkoje, akcijomi galima prekiauti bet kuriuo metu po rinkos sukūrimo. Visas Augur turtas, įskaitant rinkos rezultatų dalis, dalyvavimo žetonus, ginčų obligacijų dalis ir netgi nuosavybės teises į rinkas, visada gali būti perleidžiamas.

### C. Reportingas

Pasibaigus pagrindiniam rinkos įvykiui, turi būti nustatytas rezultatas, kad rinka galėtų būti užbaigiama ir prasidėtų išmokėjimai. Rezultatus nustato Augur orakulas, kurį sudaro pelno siekiantis reporteris, kuris tiesiog praneša apie faktinius realaus pasaulio įvykio rezultatus. Kiekvienas REP turėtojas, gali dalyvauti teikiant reportus ir ginčydamas rezultatus. Reporteriai, kurių ataskaitos atitinka konsensusą, yra finansiškai atlyginami, o tie, kurių ataskaitos neatitinka konsensuso, yra finansiškai nuostolingos (žr. Skyrių I D 3).

#### *1. Mokesčių langai*

Augur ataskaitų teikimo sistema veikia per septynių dienų trukmės ciklo *mokesčių langus*. Visi Augur renkami mokesčiai per mokestinį langą pridedami prie *reportingo mokesčio bazės*. Mokesčio lango pabaigoje ataskaitų teikimo mokestis išskirstomas REP turėtojams, dalyvavusiems ataskaitų teikimo procese. Reporteriai gauna premijas proporcingai REP sumai, kurią jie sumokėjo per šį mokesčio langą. Dalyvavimas apima: pradinės ataskaitos pateikimą, preliminaraus rezultato ginčijimą ar *dalyvio žetonų* pirkimą.

#### *2. Dalyvio žetonai*

Kiekvieno mokestinio lango metu REP turėtojai gali pirkti bet kokį dalyvavimo žetonų skaičių už vieną attorep'ą[7]. Pasibaigus mokesčio langui, jie gali išpirkti savo dalyvavimo žetonus už kiekvieną attorep'ą, be proporcingos mokesčio lango dalies *reportavimo bazėje*. Jei nebuvo veiksmų (*pvz.*, pranešimo pateikimo ar ginčijimo dėl kito naudotojo pateikto pranešimo), reporteris gali įsigyti dalyvavimo žetonus, norėdami įrodyti savo dalyvavimą. Kaip ir statomus REP, dalyvių žetonus gali išpirkti jų savininkai *proporcingai* daliai sumokėtų mokesčių per mokesčių langą.

Kaip aptarta skyriuje II, svarbu, kad REP turėtojai būtų pasirengę dalyvauti sprendžiant rinkos klausimus skilimo atveju. Dalyvavimo žetonas skatina REP turėtojus bent kartą per savaitę stebėti platformą ir, jei reikia, dalyvauti. Net REP turėtojai, kurie nenori dalyvauti ataskaitų teikimo procese, yra skatinami įsiregistruoti Augur vieną kartą per 7 dienų mokestį, kad galėtų nusipirkti dalyvavimo žetonus ir rinkti mokesčius. Toks aktyvus dalyvavimas užtikrina, kad jie yra susipažinę su Augur naudojimu, žinos apie skilimo atsiradimą, todėl jie turėtų būti labiau pasirengę dalyvauti skilimuose, kai tai įvyks.

#### *3. Rinkos būklės chronologija*

Augur rinkos gali būti septynių skirtingų būsenų po sukūrimo. Augur rinkos galimos būsenos ar "fazės" yra tokios:

- Prieš-reportingas
- Numatytas reportingas
- Laisvas reportingas
- Kito lango laukimas
- Ginčas
- Skilimas
- Uždarymas

Santykis tarp šių būsenų yra pavaizduotas pav 2.

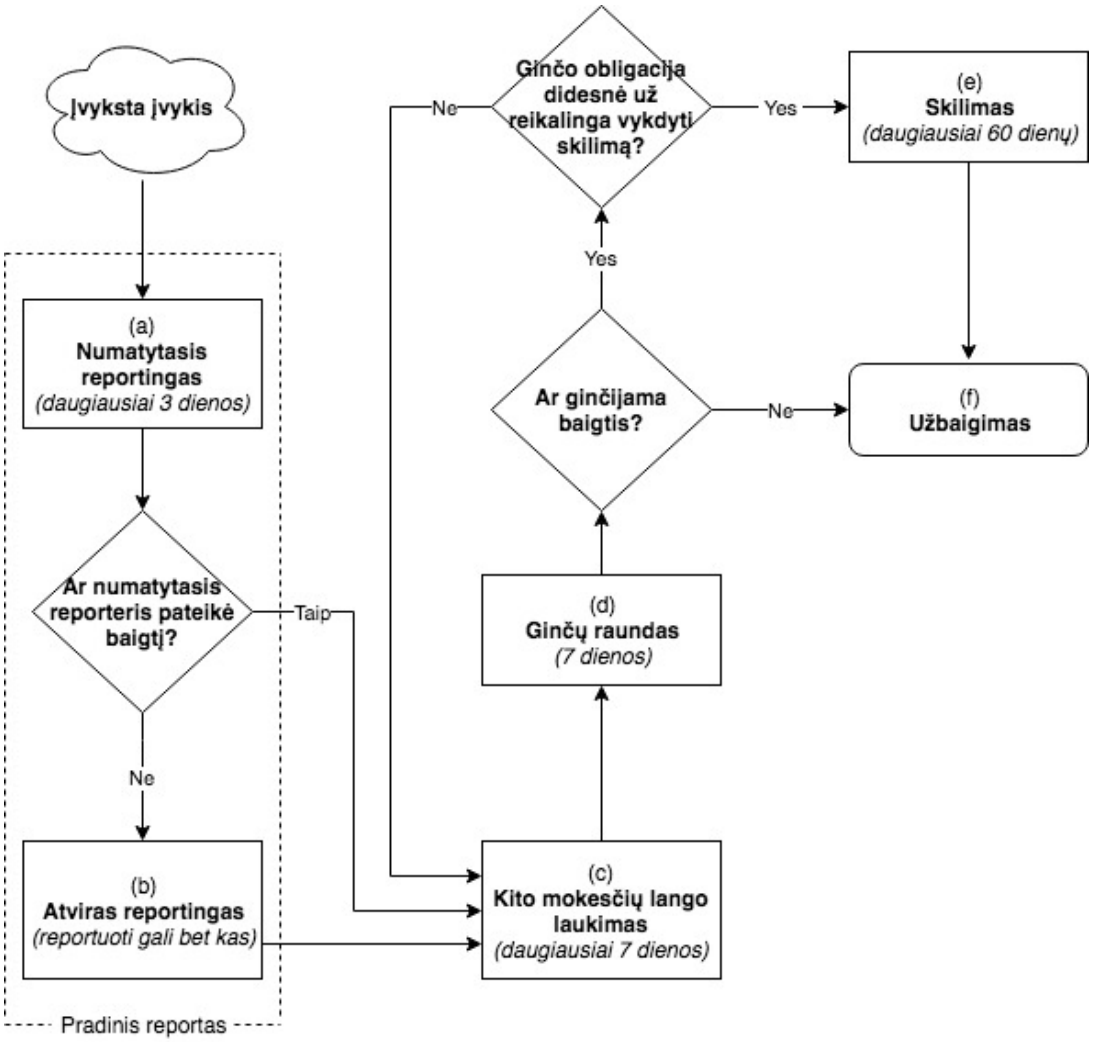
#### *4. Prieš-reportingas*

*Prieš-reportingo* arba *investavimo* fazė (Fig. 1) yra laikotarpis, kuris prasideda po to, kai pradedama prekyba rinkoje, tačiau ne vėliau, nei pasibaigia įvykis. Paprastai tai yra labiausiai aktyvus prekybos laikotarpis bet kuriai Augur rinkai. Pasibaigus įvykiui, rinka pereina į *numatyto reportingo* fazę (Fig. 2a).

#### *5. Numatytasis reportingas*

Kuriant rinką, rinkos kūrėjai privalo pasirinkti paskirtą reporterį ir paskelbti neribotą obligaciją. Per nustatytą ataskaitų pateikimo etapą (pav. 2a) rinkai paskirtas reporteris turi iki trijų dienų pranešti apie įvykio rezultatus. Jei paskirtasis pranešėjas per tris dienas nepateikia

[7] Vienas *attorep'as* yra $10^{-18}$ REP.




2 pav.. Reportingo diagrama.

ataskaitos, rinkos kūrėjas praranda nepasirodymo obligaciją ir rinka automatiškai patenka į *laisvo reportingo* fazę (Fig. 2b).

Jei paskirtasis reporteris pateikia ataskaitą laiku, tada nesirodymo obligacija grąžinama rinkos kūrėjui. Paskirtasis pranešėjas privalo paskelbti paskirtą reporterio akcijų paketą[8] apie pranešta rezultatą, kurio jis neteks, jei rinka pasibaigs bet kokiu kitu rezultatu nei tas, apie kurį pranešė.[9] Kai tik paskirtasis reporteris pateikia savo ataskaitą, rinka pereina į *kito lango laukimo* fazę (Pav. 2c), ir pranešti rezultatai tampa rinkos *baigtimi*.

[8] Žr. E 3 dėl išsamesnės informacijos apie paskirto pranešėjo akcijų dydį.

[9] Negrąžinami akcijų paketai pridedami prie atsiskaitymų rinkinio, skirto rinkos nustatyto mokesčio langui, ir naudojami atlyginti sąžiningiems reporteriams ir ginčų sprendimui; žr. skirsnį I D 3 detalesniam apibendrinimui.

### 6. *Laisvas Reportingas*

Jei paskirtasis pranešėjas per tris dienas nepateikia ataskaitos, rinkos kūrėjas praranda nepasirodymo obligaciją, o rinka nedelsdama pereina į *laisvo reportingo* fazę (Pav. 2b). Kai tik rinka patenka į laisvą ataskaitų teikimo etapą, kiekvienas gali pranešti apie rinkos rezultatus. Kai paskirtasis pranešėjas nepraneša, pirmasis pranešėjas, kuris praneša apie rinkos rezultatus, yra vadinamas rinkos *pirmu viešu reporteriu*.

Pirmasis rinkos viešas reporteris gauna prarastą obligacijų nebenaudojamą akcijų dalį pasirinkto rezultato forma, todėl jis gali reikalauti nedalyvaujančios REP obligacijos tik tuo atveju, jei jų pateikti rezultatai atitinka rinkos galutinį rezultatą. Jie taip pat gauna neribotą gas jungtį po to, kai rinka bus baigta, tik jei jų pateiktos išvados atitinka rinkos galutinį rezultatą.

Pirmasis viešas reporteris *nestato* savo REP reportuodamas įvykio baigtį. Tokiu būdu tikimasi, kad bet kuri rinka, kurios paskirtasis reporteris nepateiks ataskai-

tos, turės naują*reporterį*, kuris labai greitai, pradės atvirą ataskaitų teikimo etapą.

Kai *pradinė ataskaita* gaunama iš pradinio pranešėjo (ar jis buvo paskirtasis reporteris, ar pirmasis viešas žurnalistas), praneštas rezultatas tampa rinkos preliminariu rezultatu, o rinka prasideda laukiant kito mokesčio lango (pav. 2c).

### 7. *Kito lango laukimas*

Kai rinka gauna pradinę ataskaitą, ji pradeda laukti kito mokesčio lango (pav. 2c). Šiame etape ataskaitos apie rinką yra sulaikomos iki dabartinio mokesčio lango pabaigos. Kai tik prasideda kitas mokesčio langas, rinka pateks į textit (ginčo turas) etapą.

### 8. *Ginčas*

Ginčas (Fig. 2d) yra 7 dienų laikotarpis, per kurį bet kuris REP turėtojas turi galimybę ginčyti rinkos *baigtį*.[10] (Ginčų ciklo pradžioje rinkos preliminarus rezultatas yra rezultatas, kuris taps rinkos galutiniu rezultatu, jei REP turėtojas nepadengs jo ginčų.) Ginčas susideda iš REP *statymo* (žinomo kaip *ginčo statymo* šiame kontekste) ant baigties, *kitokios nei* dabartinė rinkos baigtis. Ginčas yra *sėkmingas*, jei bendra ginčo suma tam tikriems rezultatams atitinka *ginčo obligacijos dydį*, reikalingą dabartiniam ginčo raundui. Ginčo obligacijos skaičiavimo dydis nurodytas toliau.

$A_n$ nurodo bendrą visų šių rinkos rezultatų dalį ginčų raundo pradžioje $n$. $\omega$ yra bet kuri įvykio baigtis, *išskyrus* dabartinio ginčo raundo metu esančią baigtį. $S(\omega, n)$ yra statymų suma $\omega$ pradžioje ginčų raundo $n$. *Ginčo obligacijos* dydis, reikalingas pakeisti dabartinę įvykio baigtį $\omega$ raundo $n$ metu yra $B(\omega, n)$ ir yra nustatomas, naudojantis formule:

$$B(\omega, n) = 2A_n - 3S(\omega, n) \quad (1)$$

Tokiu būdu pasirenkami obligacijų dydžiai, siekiant užtikrinti fiksuotą 50% investicijų grąžą reporteriams, kurie sėkmingai ginčija klaidingus rezultatus (žr II D).

Visų ginčų obligacijų nebūtina mokėti vienam vartotojas. Augur platforma suteikia dalyviams galimybę išspręsti ginčus. Bet kuris vartotojas, kuris mato neteisingą preliminarų rezultatą, gali ginčyti tokį rezultatą, statydamas REP dėl kito rezultato, nei preliminarus rezultatas. Jei bet koks rezultatas (išskyrus preliminarų rezultatą) sukaupia pakankamai ginčų, kad užpildytų ginčo obligaciją, preliminarūs rezultatai bus sėkmingai užginčyti.

Sėkmingo ginčo atveju, rinka pereis į kitą ginčų raundą, arba jis pateks į *skilimo* fazę (Pav. 2e). Jei ginčo obligacijos dydis yra didesnis nei 2,5% viso REP, tuomet rinka pereis į skilimo stadiją. Jei ginčo obligacijos dydis yra mažesnis nei 2,5% viso REP, tada naujai pasirinktas rezultatas tampa naujo rinkos preliminariu rezultatu, o rinka pereina dar vieną ginčo raundą.

Visi ginčo statymai yra laikomi atskirai ginčo raundo metu. Jei ginčas yra nesėkmingas, tuomet raundo pabaigoje ginčo obligacija grąžinama jo savininkams. Jei per 7 dienų ginčą nepavyksta pasiekti susitarimo, rinka įeina į *uždarymo* fazę (Pav. 2f), ir numatyta baigtis yra *galutinė*. Rinkos galutinis rezultatas - tai preliminarus rezultatas, kuris tęsiasi per ginčų nagrinėjimo raundą be sėkmingo ginčijimo arba nustatomas per skilimą. Augur sutartys traktuoja galutinius rezultatus *Tiesa* ir juos paskirsto proporcingai.

Visos nesėkmingų ginčų dalys grąžinamos jų savininkams kiekvieno ginčo turo pabaigoje. Visos sėkmingų ginčų dalys atitenka įvykio baigčiai, kuriuos jos gindavo, ir lieka ten, kol rinka bus baigta (arba kol atsiras kitas skilimas kitoje Augur rinkoje). Visas ginčo statymas (sėkmingas ar nesėkmingas) gaus dalį *reportingo mokesčių bazės*[11] Iš dabartinio mokesčio lango.

### 9. *Skilimas*

Skilimo fazė (Fig. 2e) yra ypatinga būsena, kuri trunka iki 60 dienų. Skilimas yra paskutinės išeities sprendimas dėl rinkos baigties nustatymo; tai yra labai skaldantis procesas ir yra retas atvejis. Skilimas vykdomas, kai yra rinka, kurios rezultatas yra sėkmingai užpildytas ginčų statymais bent 2.5% viso REP dydžio. Ši rinka vadinama *skilimo rinka*.

Kai skilimas pradedamas, 60-ties dienų[12] *skilimo laikotarpis* prasideda. Ginčai dėl visų kitų nebaigtų rinkų yra sustabdyti iki šio skilimo laikotarpio pabaigos. Skilimo laikotarpis yra daug ilgesnis už įprastą mokesčių langą, nes platformai turi būti suteikta pakankamai laiko REP turėtojams ir paslaugų teikėjams (pvz., piniginėms ir biržoms) pasirengti. Galutinio rezultato negalima ginčyti.

Visos Augur rinkos ir visi REP žetonai egzistuoja *bendroje žetonų visumoje*. REP žetonai gali būti naudojami pranešant apie rezultatus (ir taip uždirbti mokesčius). *tik* rinkoms, esančioms toje pačioje visatoje, kaip REP žetonai. Kai Augur pirmą kartą paleidžiamas, visos rinkos ir visas REP egzistuoja kartu *pirminėje visatoje*.

---

[10] Tas faktas, kad ginčų raundai sutampa su mokesčių lango trukme, yra tik patogumo klausimas; iš esmės ginčų ir mokestinių langų gali būti skirtinga.

[11] Visi mokesčių lange surinkti atsiskaitymo mokesčiai ir galiojimo obligacijos pridedami prie šio mokesčio lango ataskaitų mokesčio. Mokesčio lango pabaigoje naudotojų atsiskaitymo mokesčio sąskaita išmokama proporcingai REP sumai, kurią jie sumokėjo per šį mokesčio langą.

[12] skilimo laikotarpiai gali būti trumpesni nei 60 dienų: skilimo laikotarpis baigiasi praėjus 60 dienų arba kai daugiau nei 50% visų REP yra perkeltas į naują atskilusią visatą

Kai atskiriama rinka, yra sukuriama nauja žetonų visata. Atskyrimas sukuria *dukterinę visatą* kiekvienai galimai rinkos baigčiai (įskaitant neteisingą, kaip aptarta skyriuje I D 2). Pavyzdžiui, binarinė rinka turi 3 galimus rezultatus: A, B, ir negaliojantis. Taigi, dvejetainė atskylanti rinka sukurs tris naujas dukterines visatas: visata A, visata B, ir visata negaliojanti. Iš pradžių šios naujai sukurtos visatos yra tuščios: jose nėra rinkų ar REP žetonų.

Kai vyksta skilimas, *motininė visata* tampa *užrakinta* visam laikui. Užrakintoje visatoje naujos rinkos negali būti sukurtos. Vartotojai gali tęsti prekybą užblokuotų visatų rinkose, o užrakintos visatos rinkos vis tiek gali gauti pradines ataskaitas. Tačiau čia nėra mokamos jokios atskaitomybės premijos, o užblokuotų visatų rinkų negalima užbaigti. Siekiant, kad rinkos ar REP žetonai užrakintoje visatoje būtų naudingi, juos pirmiausia reikia perkelti į naują visatą.

Motininės visatos REP žetonų turėtojai gali perkelti savo žetonus į savo pasirinktą naują visatą. Šis pasirinkimas turėtų būti atidžiai apsvarstytas, nes migracija yra vienkartinė; pasirinkimo negalima pakeisti. Žetonai negali būti siunčiami iš vienos naujos visatos į kitą. *Migracija yra nuolatinis REP žetonų įsipareigojimas tam tikram rinkos rezultatui.* REP žetonai, kurie perkeliami į skirtingas naujas visatas, turėtų būti laikomi visiškai atskirais žetonais, o paslaugų teikėjai, pavyzdžiui, piniginės ir rinkos, turėtų jas įtraukti į siūlomą sąrašą.

Kai inicijuojamas skilimas, visas pastatytas REP ant neskylinčių rinkų yra laikomas *nepastatytu*, ir jį galima perkelti į naują visatą per skilimo periodą.[13]

Nauja visata, kuri į kurią perkeliama daugiausiai REP iki skilimo laikotarpio pabaigos, tampa *laimėjusia visata*, o jos atitinkamas rezultatas tampa galutiniu skilimo rinkos rezultatu. Tolesnės visuotinės nebaigtosios rinkos gali būti perkeltos tik į laimėjusią visatą, o jei jos gavo pradinę ataskaitą, jos grąžinamos laukiant kito mokesčio lango pradžios.

*Nėra laiko apribojimo perkelti žetonus iš motininės visatos į naują visatą.* Žetonai gali būti perkelti po skilimo laikotarpio, tačiau jie nebus įskaičiuojami į laimėjusiąją visatą. Siekiant paskatinti aktyvesnį dalyvavimą žaidimo metu, visi žetonų turėtojai, kurie perkelia savo REP per 60 dienų nuo skilimo pradžios, gaus 5% papildomą REP naujoje visatoje, į kurią jie perkelti[14]. Šis atlygis mokamas už naujus REP žetonus.[15]

*Reporteriai, kurie sukūrė REP vienoje iš skilimo rinkų, negali pakeisti savo pozicijos per skilimą.* REP, kuris buvo nustatytas motininės visatos rezultatuose, gali būti perkeltas tik į naują visatą, kuri atitinka tą rezultatą. Pvz., Jei reporteriai padėjo sėkmingai išspręsti ginčą dėl rezultato A ginčo metu, tuomet REP jie gali perkelti tik į A visatą.

*Naujos dukterinės visatos yra visiškai atskiros.* Vienoje visatoje egzistuojantys REP žetonai negali būti naudojami pranešant apie įvykius ar gauti pelną iš kitoje visatoje esančių rinkų. Kadangi vartotojai greičiausiai nenorės kurti ar prekiauti visatos, kurios orakulas yra nepatikimas, rinkose, visame pasaulyje egzistuojanti REP, neatitinkanti objektyvaus tikroviškumo, mažai tikėtina, kad jo savininkas gautų kokius nors mokesčius ir todėl neturėtų turėti reikšmingos rinkos vertę. Todėl REP žetonai migruoti į visatą, kuri neatitinka objektyvios tikrovės, neturėtų turėti rinkos vertės, neatsižvelgiant į tai, ar objektyviai klaidinga visata tampa laiminga visata po skilimo. Tai turi svarbių pasekmių saugumui, apie kuriuos aptariame skyriujeII.

#### *10. Uždarymas*

Rinka patenka į galutinę būseną (pav. 2f) jei ji praeina per 7 dienų ginčą, nesant sėkmingo ginčo arba užbaigus skilimą. Skilimo rezultatas negali būti ginčijamas ir laikomas galutiniu. Kai rinka bus užbaigta, prekybininkai gali tiesiogiai išspręsti savo pozicijas rinkoje. Kai rinka patenka į uždarymo būklę, mes pasirinktą rezultatą laukome *galutine baigtimi.*

### D. Atsiskaitymas

Prekybininkas gali uždaryti savo poziciją vienu iš dviejų būdų: parduodamas turimas akcijas kitam prekybininkui mainais už valiutą arba atsiskaitydamas savo akcijomis rinkoje. Prisiminkite, kad kiekviena akcija yra rinkinio dalis, 1 ETH dydžio Augur statymo pavyzdyje.[6] Norint gauti tą 1 ETH iš statymo, prekybininkai turi pateikti Augur arba visą rinkinį, arba, jei rinka yra baigta, laimėjusių rezultatų akcijas. Kai vyksta šie mainai, mes sakome, kad prekybininkams *yra atsiskaitoma.*

Pavyzdžiui, apsvarstykite nebaigtą rinką su galimais rezultatais A ir B. Tarkime, kad Alisa turi rezultatų dalį A kurią ji nori parduoti už 0,7 ETH, o Bobas - dalį B kurią jis nori parduoti už 0,3 ETH. Pirma, Augur priima šiuos užsakymus ir surenka A ir B akcijas iš dalyvių. Tada Augur suteikia 0,7 ETH (atėmus mokesčius) už Alice ir 0,3 ETH (atėmus mokesčius) Bobui.

Kaip antrą pavyzdį apsvarstykite galutinę rinką, kurios laimėtojai yra A. Alisa turi akcijų A ir nori jas išsigryninti. Ši siunčia akcijas A į Augur ir už tai gauna 1 ETH (atėmus mokesčius).

---

[13] Vienintelė išimtis yra REP, kurį pradinis reporteris pateikė po pradinės ataskaitos pateikimo. Šis REP lieka pastatytas ant pradinės rezultatų ataskaitos ir automatiškai perkeliamas į naują visatą, kuri laimi skilimą.

[14] Tai įvyksta net tada, kai atskilimo etapas pasibaigė anksčiau dėl daugiau nei 50 % viso REP numigravusio į naują visatą.

[15] Šis papildymas REP pinigų pasiūloje yra nedidelis. Pavyzdžiui, jei 20% visos esamos REP yra perkelta per atskilimo periodą, dėl šios priemokos 1% padidės REP cirkuliacija. Be to, manoma, kad atskyrimas vyks labai retai.

#### 1. Atsiskaitymo mokesčiai

Vienintelis Augur rinkliavos mokestis yra tada, kai rinkos dalyviai atsiskaito naudodami rinkos sutartį. Atsiskaitymo metu Augur apmokestina du mokesčius: kūrėjo mokestį ir ataskaitų mokestį. Abu šie mokesčiai yra proporcingi sumai, kuri yra mokama. Taigi, anksčiau pateiktame anksčiau pateiktame atsiskaitymo pavyzdyje, kur Alice gauna 0,7 ETH, o Bob gauna 0,3 ETH, Alice sumokėtų 70% mokesčių, o Bob moka 30%.

Kūrėjo rinkliavą nustato rinkos kūrėjas rinkos sukūrimo metu ir šis mokestis yra sumokamas rinkos kūrėjui atsiskaitymų metu. Pranešimo mokestis nustatomas dinamiškai (žr II C) ir mokamas reporteriams, kurie dalyvauja ataskaitų teikimo procese.

#### 2. Atsiskaitymas už negaliojančius įvykius

Kai rinkos baigtis negaliojantis, prekybininkai, kurie atsiskaito pagal rinkos sutartį, gauna tokį patį ETH už kiekvieno rezultato akcijas. Jei rinkoje buvo $N$ galimų rezultatų (neįskaitant negaliojančios baigties), o visos kainos už akcijas buvo $C$ ETH, tada prekybininkai gaus $C/N$ ETH už kiekvieną akciją, už kurią atsiskaityta pagal rinkos sutartį.[16]

#### 3. REP žetonų perskirstymas

Jei rinka baigs rengti be skilimo inicijavimo, visas pastatytas REP už bet kokį kitą rezultatą, išskyrus rinkos galutinį rezultatą, būtų atšauktas ir paskirstytas vartotojams, kurie pateko į rinkos galutinį rezultatą, proporcingai jų pakoreguotoms REP sumoms. Ginčų dydžių pasirinkimas yra toks, kad kiekvienas, kuris sėkmingai ginčija rezultatą dėl rinkos galutinio rezultato, yra apdovanotas 50% investicijų grąža nuo savo ginčų akcijų.[17] Tai yra didelė paskata reporteriams ginčyti klaidingus preliminarius rezultatus.

## II. PASKATINIMAI IR SAUGUMAS

Tarp REP rinkos dydžio ir Augur atskilimo protokolo patikimumo yra glaudus ryšys. Jei REP rinkos dydis yra pakankamai didelis[18], ir užpuolikai yra ekonomiškai racionalūs, tada laimėti turėtų rezultatai, atitinkantys realybę. Iš tiesų Augur galėtų tinkamai veikti be paskirtų reporterių ir ginčų. Naudojiant *tik* atskilimo procesą, baigtys būtų nurodomos tiksliai.

Tačiau skilimai yra pavojingi ir reikalauja daug laiko. Norint išspręsti rinką, skilimas trunka iki 60 dienų ir gali vienu metu išspręsti tik vieną rinką. Per 60 dienų, kai yra išspręsta skilimo rinka, visos kitos nebaigtosios rinkos yra užšaldytos. Footnote Prekybininkai gali tęsti prekybą šiose rinkose, tačiau šios rinkodaros negali būti užbaigtos iki pasibaigs tolesnis skilimo etapas. Paslaugų teikėjai turi atnaujinti informaciją, o REP turėtojai turi perkelti savo REP į vieną iš naujųjų visatų. Todėl, skilimai turi būti naudojami tik tada, kai jie yra absoliučiai būtinos. Skilimas yra branduolinė alternatyva.

Laimei, kai tik skilimo dėka gali būti nustatytas teisingas sprendimas, skilimas gali būti naudojamos paskatinti dalyvius sąžiningai elgtis bei iš tikrųjų inicijuoti skilimą. textit Patikima skilimo grėsmė ir tikėjimas, kad skilimas teisingai išspręs, yra pagrindiniai Augur skatinimo sistemos pagrindai.

Toliau aptariamos sąlygos, kuriomis galima pasikliauti skilimo sistema, kad būtų nustatyta tiesa. Toliau aptariame paskatų sistemą ir kaip ji skatina greitą ir teisingą visų rinkų sprendimą.

### A. Atskilimo protokolo vientisumas

Čia mes aptarinėjame tolesnio proceso patikimumą ir sąlygas, kurioms jis gali būti patikimas. Kad būtų lengviau diskutuoti, kalbant apie atskilimą, mes vadinsime dukterinę visatą, atitinkančią objektyvią realybę kaipTeisinga visata, ir kitą dukterinę visatą kaip Neteisinga visata. Mes kalbėsime apie naują visatą, į kurią perkeliama daugiausiai REP ginčo metu, kaip laiminčiąją visatą, o visos kitos dukterinės visatos bus nurodomos kaip pralaimėjusios visatos.

Žinoma, mes visada norime Teisinga visata būtų laiminti visata, ir Neteisinga visata būtų pralaiminti. Mes sakome, kad atskilimo protokolas buvo sėkmingai užpultas, kai Neteisinga visata pasidaro laiminčiaja - tokiu būdu rinka (ir, galbūt, visos nebaigtos rinkos) yra neteisingai išmokėtos.

Mūsų požiūris į orakulo apsaugą - parengti tokią sistemą, kad maksimali nauda sėkmingam užpuolikui būtų mažesnė nei minimali aukos vykdymo kaina. Mes formalizuosime žemiau.

#### 1. Maksimali nauda atakuojančiajam

Užpuolikas, kuris sėkmingai atakuoja orakulą, priverstų visas nebaigtas Augur rinkas migruoti į Neteisingą visatą. Jei užpuolikas kontroliuoja daugumą REP Neteisingoje visatoje, tuomet jis gali priversti visas nebaigtas rinkas išspręsti pagal savo norus. Labiausiai kraštutiniu atveju jis taip pat sugebėtų užfiksuoti visas lėšas, kurios

[16] Prekyba negali būti paprasčiausiai užbaigta, jei rinka nurodoma `negaliojančia` dėl techninių apribojimų. Rezultatų dalys yra tik žetonai, kuriais galima tiesiogiai prekiauti vartotojams; ETH ir akcijos nėra kontroliuojamos Augur ir negali būti grąžinamos pirmiausiam savininkui, jei rinka bus galutinai suformuota `negaliojančia`.

[17] Žr. Teoriją 3 priede A.

[18] Žr. II A detaliau

buvo iškraipytos visose šiose rinkose.[19]

**Apibrėžimas 1.** Mes apibrėžiame ir pažymime $I_a$, Augur'o *pradines atviras palūkanas* kaip visų lėšų, išskaitytų neužbaigtose Augur rinkose, sumos vertę.[20]

**Apibrėžimas 2.** Mes apibrėžiame *(*parazitinę rinką) kaip bet kurią rinką, kuri neprivalo sumokėti pranešimo mokesčių Augur, bet išsisprendžia pagal vietinę Augur rinką.

**Apibrėžimas 3.** Mes apibrėžiame ir pažymime $I_p$, *parazitines atviras palūkanas* kaip visų lėšų, išskaidytų visose parazitinėse rinkose, kurios išsprendžia pagal nebaigtas, vietines Augur rinkas, sumos vertę.

Labiausiai kraštutiniu atveju užpuolikas taip pat sugebės užfiksuoti visas lėšas visose parazitinėse rinkose, kurios išsprendžia pagal nebaigtas, vietines Augur rinkas.

**Pastebėjimas 1.** Maksimali (gryna) nauda užpuolikui, sėkmingai atakavusiam orakulą, yra $I_a + I_p$.

### *2. Parazitinės atviros palūkanos yra nežinomos*

Augur gali tiksliai ir efektyviai išmatuoti $I_a$. Tačiau, $I_p$ apskritai negalima žinoti, nes gali būti daug savavališkai neprisijungusių parazitinių rinkų, kurių kiekviena turi savavališkai didelį atvirą susidomėjimą. Kadangi maksimali galima nauda užpuolėjui apima nežinomą kiekį $I_p$, niekada negalima objektyviai įsitikinti, kad orakulas yra saugus nuo ekonomiškai racionalių užpuolikų.

Tačiau galime teigti, jog $I_p$ yra praktiškai pagrįstas, galime apibrėžti sąlygas, pagal kurias galime teigti, kad orakulas yra saugus.

### *3. Minimalios sėkmingos atakos išlaidos*

Toliau apsvarstykime atakų prieš orakulą kainą. $P$ nurodo REP kainą. $\epsilon$ nurodo vieno attorep[21]. $M$ nurodoma bendra REP suma (REP pinigų pasiūla). $S$ nurodo $M$ proporciją, kuri pereis į Teisingą visatą atskilimo metu.

Taigi, skaičius $SM$ rodo absoliučią migruojančio REP sumą į Teisingą visatą atskilimo metu, o $PM$ yra REP rinkos vertė.

$P_f$ nurodo REP kainą, kuri perėjo į Neteisingą visatą pagal atakuojančiojo pasirinkimą. Atkreipkite dėmesį, jog kai $P \leq P_f$ tada orakulas nebūtų apsaugotas nuo ekonomiškai racionalių užpuolikų, nes būtų bent jau taip pat naudinga perkelti REP į neteisingą visatą, kaip visiškai neperkelti REP.

[19]Tai reikalautų, kad užpuolikas užvaldytų *visas* norimų rezultatų akcijas ir priverstų rinką pasibaigti norima baigtimi.

[20]Tai apima ir išorines rinkas, kuriose Augur moka ataskaitų rinkimo mokesčius.

[21]1 *attorep* yra $10^{-18}$ REP.

### *4. Vientisumas*

**Prielaidos 1.** *Reporteriai, kurie nėra užpuolikai, niekada neperkelia REP į* `Neteisingą` *visatą atskilimo metu.*[22]

Pagal sumanymą, sėkmingai atakuoti orakulą reikia daugiau REP perkelti į Neteisingą visatą nei į Teisingą visatą atskilimo metu. Pagal prielaidą, tik užpuolikas perkelia REP į Neteisingą visatą. REP kiekis, perkeltas į Teisingą visatą yra nurodomas kaip $SM$. Taigi, užpuolikas norėdamas būti sėkmingas, turi perkelti ne mažiau kaip $SM + \epsilon$ REP. Paprastumo dėlei mes ignoruojame nereikšmingą $\epsilon$, ir sakome, kad sėkmingam išpuoliui reikia migruoti bent $SM$ REP, kuris turi $SMP$ vertę prieš judėjimą, į Neteisingą visatą.

Jei užpuolikas perkelia $SM$ REP per atskilimo laikotarpį, jie gaus $SM$ REP į naują visatą, į kurią juos perkelia.[23] Jei užpuolikas pereina į Neteisingą visatą tada šių žetonų vertė tampa $SMP_f$. Taigi minimali kaina puolančiajam yra $(P - P_f)SM$.

**Pastebėjimas 2.** Minimalus REP kiekis, kuris turi būti perkeltas į `Neteisingą` visatą atskilimo metu yra $SM$, kuris puolančiajam kainuoja $(P - P_f)SM$.

Atkreipkite dėmesį, jei $S > \frac{1}{2}$ tuomet ataka yra *neįmanoma* nes nėra pakankamai REP neskaitant Teisingos visatos bet kokiai Neteisingai visatai tapti laimėjusia visata.

Ekonomiškai racionaliems racionaliai mąstant užpuoliko maksimali nauda turi būti didesnė už minimalią atakų kainą. Atkreipkime dėmesį, kad 1 & 2 atsitinka tik tuomet, kai $S > \frac{1}{2}$ arba $I_a + I_p < (P - P_f)SM$. Tai suteikia mums savo oficialų vientisumo apibrėžimą.

**Apibrėžimas 4.** (Vientisumo nuosavybė) Atskeltas protokolas yra *vientisas* visada, kai $S > \frac{1}{2}$ arba kai $I_a + I_p < (P - P_f)SM$.

Aukščiau išdėstyta nelygybė gali būti išspręsta kaip $PM$, kad būtų galima sužinoti, koks yra santykis tarp protokolo vientisumo ir REP rinkos kapitalizacijos.

**Teorema 1.** *(Rinkos dydžio saugumo teorema) Vientisumo nuosavybė yra vientisa tik kai:*

1. $S > \frac{1}{2}$, *arba*
2. $P_f < P$ *ir REP rinkos dydis yra didesnis nei* $\frac{(I_a+I_p)P}{(P-P_f)S}$.

[22]Gali būti atvejų, kai kai kurie nekenksmingi reporteriai perkelia REP į `Neteisingą` visatą netyčia. Tačiau toks elgesys praktiškai nėra atskirtas nuo bendradarbiavimo su užpuoliku.

[23]Praktiškai užpuolikas gaus $1.05SM$ REP dukterinėje visatoje dėl 5% premijos už perkėlimą per 60 dienų nuo skilimo pradžios. Mes ignoruojame 5% kad būtų lengviau diskutuoti. Norėdami pamatyti diskusiją, kurioje yra 5% premiją, žr. priedą C.

*Proof.* Tarkime, kad atskilimo protokolas yra vientisas. Tada pagal apibrėžimą, $S > \frac{1}{2}$ arba $I_a + I_p < (P - P_f)SM$. Tarkime $I_a + I_p < (P - P_f)SM$. Tuomet $I_a + I_p \geq 0$ ir $SM > 0$, žinome $P_f < P$. Tuomet sprendžiant $I_a + I_p < (P - P_f)SM$ už $PM$, matome, kad $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Taigi pirmoji nelygybė yra įrodyta.

Tad sakykime, kad $S > \frac{1}{2}$, arba $P_f < P$ ir $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Jei $S > \frac{1}{2}$, tada atskilimo protokolas yra vientisas pagal apibrėžimą. Jei $P_f < P$ ir $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$, tada, sprendžiant nelygybę $I_a + I_p$, matome, kad $I_a + I_p < (P - P_f)SM$, o atsikilimo protokolas yra vientisas. □

### B. Mūsų prielaidos ir jų pasėkmės

Manome, kad prekybininkai nenorės prekiauti Augur visatoje, kurioje reporteriai melavo. Mes taip pat tikime, kad rinkos kūrėjai nemokės kurti Augur rinkų visatoje, kurioje nėra prekybininkų. Visur be rinkų ar prekybos, REP nesuteikia naudos tiems, kurie jį valdo. Todėl mes tikime, kad REP, išsiųstas į Neteisingą visatą turės nereikšmingą rinkos vertę, ir mes ją modeliuodami, darome prielaidą, kad $P_f = 0$.

Manome, kad per ataskaitinį laikotarpį mažiausiai 20% esamų REP bus perkelti į teisingą rezultatą ir modeliuojame tai, nustatant, kad $S \geq \frac{1}{5}$. Mes modeliuojame, kad parazitinis susidomėjimas bus iki 50% atvirojo susidomėjimo, taigi $I_a \geq 2I_p$.

Pagal šias prielaidas, Teorema 1 sako, kad atskilimo protokolas yra vientisas, kai REP rinkos apribojimas yra bent 7,5 karto didesnis už vietinį atvirą susidomėjimą.[24]

### C. Rinkos kapitalizacijos sąveika

Augur gauna informaciją apie REP kainą taip pat, kaip gauna bet kokią kitą informaciją apie realų pasaulį: per Augur rinką. Tai suteikia Augur galimybę apskaičiuoti dabartinę REP rinkos kapitalizaciją. Augur taip pat gali išmatuoti dabartinį vietinį atvirą susidomėjimą ir taip gali nustatyti, kokia rinkos riba turėtų būti tikslinama, kad atitiktų Augur vientisumo reikalavimus.

Kiekviena visata prasideda nuo numatyto 1% pranešimo mokesčio. Jei dabartinė rinkos kapitalizacija yra mažesnė už tikslą, pranešimo mokesčiai automatiškai padidinami (bet niekada nebus didesni už 33.3%), pakelti spaudimą dėl REP kainos ir (arba) mažinti spaudimą naujiems vietiniams atviriems interesams. Jei dabartinė rinkos riba viršija tikslą, pranešimo mokesčiai automatiškai sumažėja (bet niekada nebus mažesni už 0.01%) kad prekybininkai nemokėtų daugiau nei reikia, kad sistema būtų saugi.

[24] Žr. Priede B alternatyviems skaičiavimams.

Ataskaitų mokesčiai yra nustatomi pagal šį pavyzdį: tegul $r$ - ataskaitos mokestis iš ankstesnio langa, tegul $t$ - tikslinės rinkos riba, o $c$ tegul būna dabartinė rinkos kapitalizacija. Tuomet ataskaitinio mokesčio už dabartinį mokestį langas suteikiamas $\max\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10{,}000}\right\}$.

### D. Atskilimo rizikos valdymas

Kaip jau minėta, atskilimas yra skaldantis ir lėtas būdas rinkoms pasiekti galutinį rezultatą. Nepriklausomai nuo to, koks yra kiekvienos rinkos sprendimas, "Augur" valdo atskilimo *riziką*, tam kad išspręstų galimus ginčus.

Prisiminkite, kad bet kuri akcija, sėkmingai ginčydama rezultatą dėl rinkos galutinio rezultato, gaus 50% investicijos grąžą nuo ginčo statymo.[25] Atskilimo atveju, bet kokia REP, kuri susiduria su bet kokiomis rinkos klaidingomis išvadomis, turėtų prarasti visą ekonominę vertę, o bet kuri REP - rinkos rezultatai yra atlyginami 50% daugiau REP naujoje visatoje, kuri atitinka rinkos tikrąjį rezultatą (nepriklausomai nuo skilimo rezultato). Todėl, jei vyksta skilimas, REP turėtojai, kurie ginčija klaidingus rezultatus realių rezultatų naudai, visada išeis į priekį, o REP turėtojai, kurie sukūrė klaidingus rezultatus, matys, kad jų REP praranda visą ekonominę vertę.

Manome, kad ši situacija yra pakankama, kad būtų užtikrinta, jog visi klaidingi preliminarūs rezultatai būtų sėkmingai užginčyti.

## III. GALIMOS PROBLEMOS IR RIZIKOS

### A. Parazitinės rizikos

Prisiminkite, kad parazitinė rinka yra bet kuri rinka, kuri nemoka Augur pranešimo mokesčių, bet yra išsprendžiama pagal pagrindinę Augur rinką. Kadangi parazitinėse rinkose nėra jokių pranešėjų, kuriems yra mokama, jie gali pasiūlyti tokią pačią paslaugą kaip ir Augur, turėdami mažesnius mokesčius. Tai gali turėti rimtų pasekmių "Augur" skilimo protokolo vientisumui.

Visų pirma, jei parazitinės rinkos pritraukia prekybos interesus nuo Augur'o, tada Augur reporteriams bus mažiau mokama už ataskaitų teikimą. Tai sumažintų REP rinkos kapitalizaciją. Jei REP rinkos viršutinė riba pernelyg maža, grėsmę keliančiam protokolo vientisumui kyla pavojus (Teorema 1). Dėl to parazitinės rinkos gali kelti grėsmę ilgalaikiam Augur gyvybingumui ir turėtų būti griežtai opoziciojonuojamos.

Mūsų geriausia apsauga nuo parazitinių rinkų yra siekis, kad prekyba Augur platformoje būtų kuo pigesnė (vis

[25] Matuojamas REP, kuris egzistuoja visatoje ir atitinka rinkos galutinį rezultatą; žr. teoremą 3 priede A.

tiek išlaikant orakulo vientisumą), siekiant sumažinti atlygį už parazitinės rinkos veikimą.

### B. Atviro susidomėjimo svyravimas

Didelis, staigus ir netikėtas padidėjęs atviras susidomėjimas - panašus į tuos, kurie gali būti pastebėti per populiarų sporto renginį - dėl to greitai padidėja rinkos kapitalizacijos reikalavimas, kad būtų užtikrintas protokolo vientisumas (teorema 1). Kai rinkos kapitalizacijos reikalavimas viršija rinkos viršutinę ribą, yra ekonomiškai racionalių užpuolikų rizika, dėl kurios skilimas gali neteisingai nurodyti baigtis. Nors Augur tokiomis situacijomis bando pakelti rinkos viršutinę ribą (žr. II C), šios sąveikos yra reakcingos ir yra koreguojamos tik vieną kartą per 7 dienų mokesčio langą.

Tačiau verta paminėti, kad spekuliantai, kurie atsiranda, kai staiga padidėja atviras susidomėjimas, gali nusipirkti REP, tikėdamiesi, kad reakcingos rinkos apimtys sumažės, tokiu būdu sukeliant REP rinkos kapitalizaciją, galbūt iki to momento, kai protokolo vientisumui nėra grėsmės. Taigi laiko periodas, per kurį orakulas yra pažeidžiamas, gali būti pakankamai ilgas, kad užpuolikas galėtų sėkmingai išnaudoti pažeidžiamumą.

### C. Neatitinkantys tiesos arba kenksmingi šaltiniai

Rinkos kūrimo metu rinkos kūrėjai pasirinko sprendimo šaltinį, kurį reporteriai turėtų naudoti aptariamo įvykio rezultatams nustatyti. Jei rinkos kūrėjas pasirenka nenuoseklų ar kenksmingą sprendimo šaltinį, sąžiningi reporteriai gali prarasti pinigus.

Pavyzdžiui, tarkime, kad nagrinėjama rinka turi rezultatus A ir B, ir rinkos kūrėja, Serena, pasirinko savo svetainę, attacker.com, kaip atsakymo šaltinį. Po rinkos įvykio pabaigos Serena, kuri taip pat yra paskirta rinkos reporterė, praneša apie rezultatus A, ir atnaujina attacker.com nurodydama, jog B yra teisinga baigtis. Reporteriai, tikrinantys rezultatus attacker.com pamatys, kad pradinė ataskaita yra neteisinga ir per pirmąjį ginčų raundą turėtų būti sėkmingai ginčijamas išankstinis rezultatas B. Serena atnaujins attacker.com, nurodydama, jog A yra teisingas rezultatas, o rinka tada patektų į antrą ginčą. Vėlgi, reporteriai, kurie patikrina attacker.com matys, kad preliminarus rezultatas (rezultatas B) kad jis neteisingas, ir gali sėkmingai jį užginčyti. Serena gali pakartoti tokį elgesį, iki rinka bus išspręsta. Nesvarbu, kaip rinka išspręs, kai kurie sąžiningi reporteriai praranda pinigus.

Yra keletas šio išpuolio variantų. Tiesiog ignoruoti rinkas su abejotinais sprendimų šaltiniais nepakanka, nes tuo atveju, jei tokia rinka sukelia skilimą, visi REP turėtojai turės pasirinkti naują visatą, į kurią galėtų persikelti savo REP. Reporteriai turėtų būti budrūs rinkose, kuriose yra abejotinų problemų sprendimo šaltinių. Tokios rinkos turėtų būti viešai identifikuotos, kad reporteriai galėtų koordinuoti, kad tokios rinkos būtų užbaigtos kaip negaliojančios.

### D. Savarankiškos Orakulo Užklausos

Rinkos, kurios prekiauja ateities Augur orakulo elgesiu, gali turėti nepageidaujamo poveikio pačiam orakulo elgesiui [11]. Pavyzdžiui, apsvarstykite rinką, kurioje prekiaujama klausimu: "Ar bet kuris paskirtasis reporteris per tris dienas iki 2018 m. Gruodžio 31 d. Nepateiks ataskaitos?" Neteisingas šios rinkos rezultatas gali paskatinti paskirtąjį reporterį sąmoningai nepranešti. Jei paskirtas reporteris gali nusipirkti pakankamai Teisingų akcijų pakankamai pigiai tam, kad kompensuotų nepasirodymo netektį, jie gali specialiai nepranešti įvykio baigties.

Jei REP rinkos dydis yra pakankamai didelis (Teorema 1) tada šie savarankiški orakulų užklausos nesukelia grėsmės protokolo sujungimui. Tačiau jie gali neigiamai paveikti Augur našumą, todėl vėluojama užbaigti rinką. Nors rinkos vis tiek būtų tinkamai reportuotos, tačiau toks elgesys yra netinkamas ir nepageidaujamas.

### E. Nežinomybė dėl dalyvavimo atskilime

Negalime iš anksto žinoti, kiek REP bus perkelta į Teisingą visatą atskilimo metu, todėl negalime iš anksto žinoti, ar rinkos kapitalizacija yra pakankamai didelė, kad orakulo protokolas galėtų būti vientisas (Teorema 1). Mūsų įsitikinimas, kad protokolas yra vientisas, gali būti ne stipresnis nei mūsų įsitikinimas mūsų prielaidos dėl apatinės ribos sąžiningam dalyvavimui atskilimo laikotarpio metu. Manome, kad bent 20% viso REP bus perkelta į Teisingą naują visatą atskilimo metu, tačiau mes to negalime garantuoti.

Augur atskyrimas skiriasi nuo įprastinių blokų atskyrimų: po atsiskyrimo, įprastai, vartotojas, kuris priklauso grandinei, turi abiejų šakų monetas. Todėl blokų atskyrimai kelia mažai rizikos vartotojams. Tačiau po Augur atskyrimo, vartotojas, kuris turi pagrindinės visatos REP žetoną, gali perkelti šią monetą tik į vieną iš naujų visatų. Jei vartotojas perkelia savo žetoną į bet kurią visatą, išskyrus konsensuso visatą, jų žetonas gali prarasti visą vertę. Taigi, migruojantis REP per atskyrimo periodą, turi būti įsitikinęs, kuri nauja visata pasiekė sutarimą ir tai kelia riziką vartotojui. Ši rizika gali trukdyti dalyvavimui ginčytinų atsiskyrimų laikotarpiu.

Siekdami kompensuoti šią riziką ir skatinti dalyvavimą skilimo laikotarpiu, visi žetonų turėtojai, perkeliantiys REP per 60 dienų nuo atsiskyrimo pradžios, gaus 5% REP premiją naujoje visatoje, į kurią jie perėjo. (žr I C 9). Visgi, mes negalime žinoti ar 5% premijos užteks, tam kad premija kompensuotų riziką ir paskatintų dalyvavimą per atsiskyrimo laikotarpį.

### F. Negrynosios arba subjektyvios rinkos

Tik įvykiai, turintys objektyviai žinomų rezultatų, yra tinkami naudoti Augur rinkose. Jei reporteriai tiki, kad platforma nėra tinkama sprendimui spręsti, pavyzdžiui, nes ji yra dviprasmiška, subjektyvi, arba rezultatas nėra žinomas iki įvykio pabaigos datos, jie turėtų reportuoti rinką kaip Negaliojančią. Jei rinka nurodoma kaip Negaliojanti, prekybininkams mokamos vienodos sumos už visus galimus rezultatus; skalės rinkose prekybininkams yra mokama pagal rinkos minimalios ir didžiausios kainos vidurkį.

Galima įsivaizduoti rinkas, kuriose kai kurie reporteriai yra tikri, kad rezultatas yra A, o kiti yra įsitikinę, jog rezultatas yra B. Pavyzdžiui, 2006 m. "TradeSports" leido savo vartotojams spėlioti, ar Šiaurės Korėja prieš 2006 m. Liepos mėn. pabaigą užplauks balistinę raketą, kuri žemę patektų už jos oro erdvės ribų. 2006 m. Liepos 5 d. Šiaurės Korėja sėkmingai išleido balistinę raketą už jos oro erdvės ribų, o šį įvykį plačiai pranešė pasaulio žiniasklaida ir patvirtino daugelis JAV vyriausybės šaltinių. Tačiau JAV gynybos departamentas JAV nepatvirtino šio įvykio, kaip reikalavo "TradeSports" sutartis. "TradeSports" padarė išvadą, kad sutarties sąlygos nebuvo įvykdytos ir atitinkamai įvykdė mokėjimus.[26]

Tai yra atvejis, kai rinkos esmė - numatyti raketų paleidimą - buvo aiškiai patenkinta, tačiau rinkos sprendimas būdas - nuspėti, ar JAV gynybos departamentas tai patvirtins - nebuvo patenkintas. "TradeSports", kuri yra centralizuota svetainė, galėjo vienašališkai paskelbti rinkos rezultatus. Jei tokia situacija kyla Augur rinkoje, REP turėtojai gali turėti skirtingą nuomonę apie tai, kaip turėtų išspręsti rinka, ir atitinkamai atsižvelgti į jų REP. Blogiausiu atveju tai gali sukelti skilimą, kai REP daugiau nei vienoje naujoje visatoje turi ne nulinę rinkos vertę.

## PADĖKOS

Dėkojame Abraham Othman, Alex Chapman, Serena Randolph, Tom Haile, George Hotz, Scott Bigelow, ir Peronet Despeignes už pagalbą vystant projektą.

[1] J. Wolfers and E. Zitzewitz. Prediction markets. *Journal of Economic Perspectives*, 18(2):107–126, 2004.
[2] James Surowiecki. *The Wisdom of Crowds*. Anchor, 2005.
[3] R. Hanson, R. Oprea, and D. Porter. Information aggregation and manipulation in an experimental market. *Journal of Economic Behavior & Organization*, 60(4):449–459, 2006.
[4] D.M. Pennock, S. Lawrence, C.L. Giles, and F.A. Nielsen. The real power of artificial markets. *Science*, 291:987–988, 2001.
[5] C. Manski. Interpreting the predictions of prediction markets. *NBER Working Paper No. 10359*, 2004.
[6] J. Wolfers and E. Zitzewitz. Interpreting prediction market prices as probabilities. *NBER Working Paper No. 10359*, 2005.
[7] S. Goel, D.M. Reeves, D.J. Watts, and D.M. Pennock. Prediction without markets. In *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, pages 357–366. ACM, 2010.
[8] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*, 2008.
[9] V. Buterin. A next generation smart contract and decentralized application platform. *https://github.com/ethereum/wiki/wiki/White-Paper*, 2013.
[10] J. Clark, J. Bonneau, E.W. Felten, J.A. Kroll, A. Miller, and A. Narayanan. On decentralizing prediction markets and order books. In *WEIS '14: Proceedings of the 10th Workshop on the Economics of Information Security*, June 2014.
[11] A. Othman and T. Sandholm. Decision rules and decision markets. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: Volume 1 - Volume 1*, AAMAS '10, pages 625–632. International Foundation for Autonomous Agents and Multiagent Systems, 2010.
[12] J. Peterson and J. Krug. Augur: a decentralized, open-source platform for prediction markets. *arXiv:1501.01042v1 [cs.CR]*, 11 2014.

[26] Žr. `https://en.wikipedia.org/wiki/Intrade#Disputes` detaliau.

### Priedas A: Užbaigimo laikas ir perskirstymas

Pradedame nuo kai kurių užrašų, apibrėžimų ir pastebėjimų.

**Apibrėžimas 5.** Rinkoje $M$, tegul $\Omega_M$ yra rezultatų erdvė (ar rezultatų rinkinys) $M$.

**Apibrėžimas 6.** Kai $n \geq 1$ ir $\omega \in \Omega_M$, tegul $S(\omega, n)$ nurodo bendrą sumą, skirtą rezultatams $\omega$ pradžioje ginčų raundo $n$. Tai apima visų visų sėkmingų ginčų obligacijų palūkanas $\omega$ per visus prieš tai vykusius ginčų raundus.

**Apibrėžimas 7.** Kai $n \geq 1$ ir $\omega \in \Omega_M$, tegul $S(\overline{\omega}, n)$ nurodo bendrą sumą, skirtą rezultatams $\Omega_M$ *išskyrus* $\omega$ ginčų raundo pradžioje $n$:

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

**Apibrėžimas 8.** Kai $n \geq 1$, tegul $A_n$ nurodo bendrą sumą, skirtą rezultatams $M$ pradžioje ginčų raundo $n$:

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

**Pastebėjimas 3.** Tai rodo, jog $A_n - S(\omega, n) = S(\overline{\omega}, n)$.

**Apibrėžimas 9.** Kai $n \geq 1$, tegul $\hat{\omega}_n$ nurodo preliminarų rezultatą ginčo pradžioje $n$. Pavyzdžiui, $\hat{\omega}_1$ yra rezultatas, apie kurį pranešė pradinis pranešėjas.

**Apibrėžimas 10.** Jei $n \geq 1$ ir $\omega \neq \hat{\omega}_n$, tegul $B(\omega, n)$ nurodo, kokia suma reikalinga norint sėkmingai užpildyti ginčo sąsają naudai rezultatui $\omega$ ginčų raunde $n$.

Prisiminkite, kad akcijų suma, reikalinga norint sėkmingai užpildyti ginčą, yra naudinga rezultatams $\omega$ ginčų raunde $n$, kai $\omega \neq \hat{\omega}_n$ yra duota Eq. 1, $B(\omega, n) = 2A_n - 3S(\omega, n)$.

**Pastebėjimas 4.** Jei ginčo sprendimas sėkmingai pasiekiamas rezultatų naudai $\omega$ per ginčų raundą $n$, tuomet $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. Tai reiškia, kad sėkminga ginčų dalis yra vienintelis naujas rezultatas $\omega$ pabaigoje ginčų raundo $n$.

**Pastebėjimas 5.** Visada, kai $\omega \neq \hat{\omega}_n, S(\omega, n-1) = S(\omega, n)$. Tai reiškia, kad ginčo ryšys nėra visiškai naudingas rezultatams $\omega$, tada jokių papildomų akcijų nepridedama $\omega$ kito ginčų raundo pradžioje. Taip yra dėl to, kad ginčo aplinkybių pabaigoje vartotojams grąžinama visa nesėkminga ginčo dalis.

**Pastebėjimas 6.** Visada, kai $n \geq 2, A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$. Tai reiškia, kad bendras visų ginčo nagrinėjimo pradžioje pasiektų rezultatų lygis yra tik bendras ankstesnio ginčo nagrinėjimo etapo pradžios etapas ir sėkmingas ginčų, susijusių su ankstesniu ginčų nagrinėjimu, dalis. Visos kitos akcijos grąžinamos naudotojams ankstesnio ginčo ture.

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

*Proof.* Sakykime, kad ginčas prasideda raunde $n$, kai $n \geq 2$. Ginčo metu $n-1$, kai baigtis yra $\hat{\omega}_{n-1}$ turi būti sėkmingai ginčijamas dėl rezultato $\hat{\omega}_n$. Pagal sk. 1, ginčo obligacijos dydis yra $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Atsižvelgiant į tai, 3, tai gali būti perrašyta kaip

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

Mes žinome, kad ginčo sąsaja buvo sėkmingai užpildyta per $n-1$ apytikriai. Atsižvelgiant į tai, 4, matome, kad $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. Tai rodo, kad 5 visas statytas kiekis ant $\overline{\hat{\omega}_n}$ nepasikeitė nuo raundo $n-1$ iki $n$, $2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$. Todėl skaičiavimas A1 sumažinamas iki $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$. □

**Teorema 3.** *Visi REP turėtojai, sėkmingai ginčydami rezultatą dėl rinkos galutinio rezultato, gaus 50% investicijos gražą už jų ginčų pasiskirstymą (išmatuotas REP, kuris egzistuoja visatoje, kuris atitinka rinkos galutinį rezultatą), išskyrus atvejus, kai rinka kitoje rinkoje yra nutraukta ir sukelia šaką.*

*Proof.* Atskilimo metu, pateikti visi vartotojai, kurie sėkmingai užpildė ginčo obligacijas, siekdami galutinio rezultato atskirtoje rinkoje (atskilimo metu sukurtas monetas) 50% grąžinti savo ginčą, kai jie persikelia savo ginčą į atitinkamą vaiko visatą. Taigi tuo atveju, kai nagrinėjama rinka sukėlė šaką, teorema iš karto yra tiesa.

Dabar apsvarstykite atvejį, kai aptariama rinka išsprendžiama, nesukeliant atskilimo, o kai kuri kita rinka, dėl kurios atsiranda atskilimas, neatsako.

Apibūdinant rinkos galutinį rezultatą $\omega_{\text{Final}}$ ir tarkime, kad rinka išsprendžia ginčo pabaigą $n$, kai $n \geq 2$. Tai reiškia preliminarų raundo rezultatas $n$ yra $\omega_{\text{Final}}$, ir šis rezultatas nėra sėkmingai ginčijamas per raundą $n$. Kitaip tariant: $\hat{\omega}_n = \omega_{\text{Final}}$. Tada pagal Lemma 2 žinome, kad $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$.

Kadangi rinka išsprendžia apačioje esantį $n$ skaičių be jokių papildomų palūkanų, tai reiškia, kad galutinė rezultato dalis yra galutinė rezultatų dalis, $\omega_{\text{Final}}$, ir visų akcijų paketo dalis visiems kitiems rinkos rezultatams, $\overline{\omega_{\text{Final}}}$. Atkreipkite dėmesį, kad rinkos galutiniam rezultatui būdinga tikra dvigubai didesnė akcijų dalis, nes kartu yra ir kitų rezultatų.

"Augur" perskirsto visą nebaigtų rezultatų dalį naudotojams, kurie užsidėjo $\omega_{\text{Final}}$, proporcingai REP sumai, kurią jie sumokėjo. Todėl naudotojai, kurie sėkmingai užpildė ginčą, $\omega_{\text{Final}}$ naudai gauna 50% investicijos grąžą nuo užstatyto REP. □

Toliau, pagalvokite, koks yra didžiausias įmanomas ginčų raundų skaičius. Skaičius 1 yra minimalus, kai $\omega$ yra pasirenkamas kaip neprognozuojamas rezultatas, kuris prasideda ginčo aplinkoje su didžiausiu statymų skaičiumi. Lemma 2 reiškia, kad neprognozuojamas rezultatas su didžiausiu akcijų skaičiumi yra ankstesnis ginčo turo rezultatas. Todėl mažiausiai įmanomas ginčų dydis,

kuris gali būti sėkmingai užpildytas per ginčą apeinant $n$, kur $n \geq 2$, yra $B(\hat{\omega}_{n-1}, n)$.

Kitais žodžiais, ginčų akcija brangsta *lėčiausiai*, kai tie patys du rezultatai dar kartą ginčijami vienas kitam. Iš to išplaukia, kad ginčų raundų kiekis, reikalingas rinkai inicijuoti atskilimą, trunka *ilgiausiai*, kai tie patys du rezultatai dar kartą ginčijami vienas kitam. Todėl galime nustatyti maksimalų ginčų skaičių, kurį bet kuri rinka gali atlikti prieš pradedant šaką, rastant maksimalų ginčų etapų skaičių, kuris gali atsirasti konkrečiu atveju, kai tas pačias dvi rinkos pasekmes pakartotinai ginčijamas kitoje. Dabar mes nagrinėjame šį atvejį.

Tarkime, kad kiekviena sėkminga ginčo nuoroda užpildoma ankstesnio ginčo raundo preliminaraus rezultato naudai. Tada du preliminarūs rezultatai, kurie yra kartojasi vienas kitam, yra $\hat{\omega}_1$ ir $\hat{\omega}_2$.

**Pastebėjimas 7.** Tuo atveju, kai tie patys du preliminarūs rezultatai yra pakartotinai ginčijami vienas kitam, $\hat{\omega}_n = \hat{\omega}_{n-2}$ visada, kai $n \geq 3$.

**Apibrėžimas 11.** Tegul $d$ nurodo statymo dydį ant $\hat{\omega}_1$ per pradinį reportingą. Kadangi šioje situacijoje yra žinomi kiekvieno etapo preliminarūs rezultatai, galime supaprastinti mūsų uždraustų ginčų dydžių žymėjimą. Apibrėžkime stenografiją $B_n$ apibūdinti akcijų dydį, reikalingą raunde $n$, tam kad $B_1 = 2d$ ir $B_n = B(\hat{\omega}_{n-1}, n)$ visada, kai $n \geq 2$. Tai padės lengviau skaityti ir suvokti.

**Pastebėjimas 8.** Tais atvejais, kai tie patys du preliminarūs rezultatai yra nuolat ginčijami vienas kitam, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ kai $n \geq 3$. (Tai reiškia, kad kiekviena kita sėkminga ginčo nuoroda pridedama prie to paties rezultato.)

**Teorema 4.** *Jei tie patys du preliminarūs rezultatai yra pakartotinai ginčijami vienas kitam, tuomet tai galiojam kiekvienam $n$ kai $n \geq 3$:*

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

*Proof.* (Instrukcija apie $n$)

Tarkime, kad tie patys du preliminarūs rezultatai yra nuolat ginčijami vienas kitam.

(Bazinis pavyzdys) Pagal aprašymą ir skaičiavimą. 1, mes darome šiuos skaičiavimus:

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

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, tad pirmoji teoremos dalis teisinga, kai $n = 3$.

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, tad antroji teoremos dalis teisinga, kai $n = 3$.

$B_3 = 6d = 3d2^{3-2}$, tad trečioji teoremos dalis teisinga, kai $n = 3$.

Tai įrodo, jog teorima yra visiškai teisinga baziniame pavyzdyje, kai $n = 3$.

(Indukcija) Sakykime, kad teorema teisinga visiems $n$, pavyzdžiui, $3 \leq n \leq k$. Norime įrodyti, jog teorema yra teisinga, kai $n = k + 1$. Tai įrodome taip:

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

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

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

Pirma, įrodinėjame dalį (a). Pagal pastebėjimą 8:

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

Pagal pastebėjimą 7, galime tai perrašyti į:

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

Pagal indukcijos hipotezę galime tai perrašyti į $S(\hat{\omega}_{k-2}, k-1)$, kai $\frac{2}{3}B_{k-2}$ dešinėje pusėje, tam kad gautume:

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

Pagal indukcijos hipotezę, galime teigti, jog $B_{k-2}$, kai $3d2^{k-4}$ ir $B_{k-1}$ as $3d2^{k-3}$:

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

Naudodami pastebėjimą 7 kairėje skaičiavimo pusėję, gauname:

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

Galiausiai, matome, kad pagal aukščiau pateiktą lygtį ir indukcijos hipotezę, $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. Tai įrodo dalį (a).

Toliau, įrodinėjame dalį (b). Paga; pastebėjimą 6:

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

Pagal indukcijos hipotezę, $A_k = 2B_{k-1}$:

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

Pagal indukcijos hipotezę, $B_{k-1} = 3d2^{k-3}$, tad dešinė skaičiavimo pusė gali būti supaprastinta į:

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

Pagal indukcijos hipotezę, $B_k = 3d2^{k-2}$ naudojame dešinės skaičiavimo pusės perrašymui:

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

ir dalis (b) yra įrodyta.

Galiausiai, įrodinėjame dalį (c). Pagal skaičiavimą, 1:

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

Pagal pastebėjimą 8, galime rašyti, jog $S(\hat{\omega}_k, k+1)$, kai $S(\hat{\omega}_k, k-1) + B_{k-1}$:

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

Pagal pastebėjimą 7, $\hat{\omega}_k = \hat{\omega}_{k-2}$:

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

Pagal pastebėjimą 6, $A_{k+1} = A_k + B_k$:

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

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

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

Pagal indukcijos hipotezę, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ ir $B_{k-2} = 3d2^{k-4}$. Darant šiuos pakeitimus ir suprastinus skaičiavimą:

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

Tai įrodo dalį (c) ir įrodo teoremą. □

**Teorema 5.** *Rinka gali pereiti ne daugiau 20 ginčų raundų iki pasiekiant sprendimą arba iki įvykstant skilimui.*

*Proof.* Tarkime, jog rinka nėra įtakojama kitos rinkos skilimo. Tuomet, kaip rašoma viršuje, žinome, jog ginčo baigtis ilgiausiai sprendžiama, kai paeiliui einantys ginčų raundai turi skirtingas baigtis. Trečioji Lemma dalis 4 nurodo, jog tokioje situacijoje ginčo obligacijos dydis, reikalingas sėkmingai išspręsti ginčą per raundą $n$ yra $3d2^{n-2}$, kai $d$ yra pradinio reporto statymo kiekis.

Žinome, jog skilimai yra incijuojami, kuomet surinktų ginčo obligacijų dydis viršija 2,5% viso egzistuojan2io REP ir žinome tai, kad iš viso yra 11 milijonų REP. To pasekoje, skilimas inicijuojamas surinkus 275 000 REP ginčo obligacijoje. Taip pat žinome, jog $d \geq 0.35$ REP, nes minimalus pradinio reporto dydis yra 0.35 REP[27].

Sprendžiant $3(0.35)2^{n-2} > 275,000$ kai $n \in \mathbb{Z}$ gaunam $n \geq 20$. To pasekoje, galime garantuoti, jog rinka bus išspręsta arba įvyks skilimas po daugiausiai 20 ginčų raundų. □

[27] Žr. priedus E 2 ir E 3

**Priedas B: Alteratyvios prielaidos ir jų pasėkmės**

Prisiminkime, kad:

- $S$ yra viso REP proporcija, perkeltų į Teisingą visatą skilimo metu
- $P$ yra REP kaina Teisingoje visatoje
- $P_f$ yra REP kaina žetonų, kurie perkelti į Klaidingą užpuolikų visatą
- $I_a$ yra Augur'o atvirų pozicijų suma
- $I_p$ yra parazituojančių pozicijų suma

Augur atlieka tam tikras prielaidas apie $S$, $P_f$, ir $I_p$ tam, kad pasiektų siekiama kapitalizacijos lygį. Tiksliau sakant, Augur atlieka prielaidą, jog bent 20% visų REP bus perkelti į Teisingą visatą atskilimo metu, REP perkeltas į Klaidingą visatą bus bevertis ir parazituojančių pozicijų suma bus ne daugiau nei pusė atviros pozicijos sumos. Kitaip tariant: $S \geq 0.2$, $P_f = 0$, ir $I_a \geq 2I_p$. Pagal šias prielaidas, Teorema 1 mums rodo, jog skilimo protokolas yra vientisas visada, kai REP kapitalizacija yra 7,5 karto didesnė nei atvirų pozicijų suma.

Galite turėti savo prielaidas apie $S$, $P_f$, ir $I_p$ apie reikiamą kapitalizacijos dydį tam , kad orakulas praktiškai būtų vientisas. Jūsų patogumui pateikiame kelis alternatyvius scenarijus.

**Pavyzdys 1.** Daugiau nei 50% visų egzistuojančių REP perkeliami į `Teisingą` visatą skilimo metu. Šiuo atveju $P_f$ ir $I_p$ nėra svarbūs. Kadangi $S > \frac{1}{2}$, skilimo protokolas yra vientisas nesvarbu, kokia yra rinkos kapitalizacija. Nebūtų pakankamai REP sėkmingai įvykdyti ataką.

**Pavyzdys 2.** 48% visų egzistuojančių REP perkeliami į `Teisingą` visatą skilimo metu, jokių parazituojančių rinkų nėra ir į `Klaidingą` visatą nusiųstas REP yra bevertis. Šiuo atveju $S = 0.48$, $I_p = 0$, ir $P_f = 0$. Pagal šias prielaidas, REP rinkos kapitalizacija privalo būti maždaug dvigubai didesnė nei atvirų pozicijų suma tam, kad skilimo protokolas būtų vientisas.

**Pavyzdys 3.** 20% visų egzistuojančių REP perkeliami į `Teisingą` visatą skilimo metu, parazitinių pozicijų suma yra lygi atvirų pozicijų sumai ir REP, perkeltas į `Klaidingą` visatą turi 5% REP vertės, perkeltos į `Teisingą` visatą. Šiuo atveju $S = 0.2$, $I_p = I_a$ , ir $P_f = 0.05P$. Pagal tai, REP rinkos kapitalizacija turi būti 10,5 karto didesnė, nei atvirų pozicijų suma, tam kad skilimo protokolas būtų vientisas.

**Pavyzdys 4.** Tik 5% visų egzistuojančių REP perkeliami į `Teisingą` visatą skilimo metu, parazitinių pozicijų suma yra dvigubai didesnė už atvirų pozicijų sumą ir REP, išsiųstas į `Neteisingą` visatą turi 5% REP, perkelto į `Teisingą` visatą vertės. Šiuo atveju, $S = 0.05$, $I_p = 2I_a$, ir $P_f = 0.05P$. Pagal tai, rinkos kapitalizacija turi būti maždaug 63 kartus didesnė, nei atvirų pozicijų suma tam, kad skilimo protokolas būtų vientisas.

### Priedas C: Ankstyvo perkėlimo premijos įtaka skilimo protokolo vientisumui

Vardan lengvesnio diskutavimo, ignoravome 5% ankstyvo perkėlimo premiją, diskutuojant apie skilimo protokolo vientisumą. Dabar apžvelgsime Teoremą 1 įskaičiuodami šį faktorių.

Kaip ir prieš tai,REP perkelta į Teisingą visatą reportavimo metu yra nurodomas kaip $SM$. Todėl atakuotojas, norėdamas sėkmingai atlikti savo veiksmus, privalo perkelti bent $SM + \epsilon$ REP, kurių vertė yra $(SM + \epsilon)P$ iki perkėlimo į Klaidingą visatą.

Jeigu atakuotojas perkelia $SM + \epsilon$ REP į Klaidingą visatą skilimo metu, tuomet jis gaus $1.05(SM + \epsilon)$ REP naujoje visatoje, į kurią žetonai buvo perkelti. Pagal $P_f$ apibrėžimą, šių žetonų vertė yra nustatoma pagal formulę $1.05(SM + \epsilon)P_f$. Todėl minimali atakuojančiojo kaina gali būti nustatoma pagal formulę $(SM + \epsilon)P - 1.05(SM + \epsilon)P_f$, arba $(SM + \epsilon)(P - 1.05P_f)$.

Kaip ir anksčiau, maksimali atakuojančiojo nauda yra $I_a + I_p$. Todėl sakome, jog skilimo protokolas yra vientisas, kai $S > \frac{1}{2}$ arba:

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

Sprendžiant viršuje pateiktą nelygybę rinkos kapitalizacijai, $PM$, matome, jog skilimo protokolas yra vientisas tik jei:

1. $S > \frac{1}{2}$ arba
2. $1.05P_f < P$ ir REP rinkos kapitalizacija yra $\frac{P(I_a+I_p-\epsilon(P-1.05P_f))}{S(P-1.05P_f)}$

Kaip matome, ankstyvo perkėlimo premijos efektas yra labai mažas.

### Priedas D: Ankstyvo perkėlimo premijos įtaka minimaliai atskilimo kainai

Tam, kas paskantitume didesnį aktyvumą skilimo metu, visi žetonų turėtojai, perkeliantys savo REP per 60 dienų nuo skilimo pradžios gaus papildomus 5% REP naujoje visatoje, į kurią jie perkelti. Ši premija mokama infliacijos principu.

Ši premija yra per maža vien tam, kad būtų pradėtas skilimas. Jeigu atakuojantysis gauna daugiau nei 5% REP vertės, inicijuojant skilimą, tokiu atveju mes spėtume, jog skilimai būtų vykdomi labai dažnai. Ši ataka, kurią mes vadiname *infliacijos išgręžimo ataka*, nesibaigtų klaidingu orakulo reportu, tačiau pasireikštų nuolat pasikartojančiais skilimais.

Tam, kad to būtų išvengta, Augur turi pasirūpinti, jog skilimo inicijavimo kaina viršytų 5% infliacijos premijos. Žemiau apskaičiuojame žemiausią įmanomą skilimo kainą, norėdami išvengti tokių atakų.

Tegul $P_0$ nurodo REP kainą iki skilimo ir $P_1$ nurodo REP kainą po skilimo. Tegul $M_0$ nurodo pinigų kiekį, reikalingą pradėti skilimą ir $M_1$ nurodo pinigų kiekį reikalingą po skilimo. Tegul $S$ nurodo $M_0$ proporciją, perkeliamą į Teisingą visatą skilimo metu. Tegul $b$ nurodo REP kiekį, kuris privalo būti ekonomiškai panaikintas (t.y. pastatys ant Neteisingos baigties) tam, kad būtų pradėtas skilimas. Darome prielaida, jog $b > 1$.

Darome konservatyvią prielaidą, jog visas REP, perkeltas skilimo metu yra kontroliuojamas atakuojančiojo asmens. Taip pat darome prielaidą (kadangi tai sumažina atakos kainą), kad visas perkaltas REP yra perkeltas į Teisingą visatą.

Pagal tai, $SM_0$ yra skilimo metu perkeltas REP, o $(1 - S)M_0$ yra REP kiekis *neperkeltas* skilimo metu.

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

Kai visas $SM_0$ REP kiekis yra perkeltas atskilimo metu, tuomet $0.05SM_0$ REP yra sukurta infliacijos:

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

Susitelkiant tik į infliacijos efektą ir paprastumo vardan, mes darome prielaidą, kad rinkos kapitalizacija po skilimo bus tokia pat kaip ir prieš skilimą[28]:

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

Keičiame D1 ir D2 į D3 ir paprastumo dėlei mums duoda:

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

Grynas atakuotojo pelnas, inicijuojant ataką ir siekiant pasinaudoti ankstyvo perkėlimo premija žetonams, kurie buvo perkelti atėmus žetonų vertę iki perkeliant:

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

Keičiame D4 į D5 gauname alternatyvią atakuotojo pelno išraišką:

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

Atminkite, kad b yra REP kiekis, kuris turi būti ekonomiškai panaikintas tam, kad būtų inicijuojamas skilimas. Pagal tai, skilimo inicijamo kaina yra $bP_0$. Pagal tai, skilimą inicijuoti apsimoka tik tada, kai ši nelygybė yra teisinga:

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

Jei $P_0 > 0$, ir $S \neq -20$, sprendžiame, kad, sėkmingos atakos įvykdymui, $b$ reikšmė turi būti:

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

---

[28] Manome, jog tai yra konservatyvus sprendimas. Praktiškai, mes manome, jog rinkos kapitalizacija po skilimo sumažėtų.

Augur, norėdamas išvengti atakos turi pasirūpinti, kad:

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

Atsižvelgiant, kad $S$ yra intervale $[0,1]$, matome, kad dešinioje nelygybės pusė D9 yra didžiausia, kai $S = 2\sqrt{105} - 20 \approx 0.4939$. Tai yra, ataka yra labiausiai apsimokanti, kai skilimo metu atakuojančiojo naudai perkeliami maždaug 49.39% visų REP žetonų. Žvelgiant konservatyviai, naudojame $S$ vertę.[29]

Keičiame $S = 0.4939$ į D9 ir gauname, kad $b \geq 0.012197M_0$. Tad skilimo inicijamui reikia bent 1.2197% viso egzistuojančio REP tam, kad infliacijos nugręžimo ataka nebūtų pelninga.

Atminkite tai, kad skilimas yra pradedamas tik po sėkimingo ginčų raundo, kai ginčo obligacijos dydis yra daugiau nei 2.5% viso egzistuojančio REP. Atlikime prielaidą, kad tokia ginčo obligacija buvo užpildyta įvykio baigties $\omega$ naudai ir skilimas buvo pradėtas. Baigtis $\omega$ yra arba teisinga arba neteisinga.

Jei baigtis $\omega$ yra neteisinga, tuomet bent 2.5% viso egzistuojančio REP buvo pastatyta ant neteisingos baigties ir yra ekonomiškai panaikinami. To pasekoje infliacijos nugręžimas nėra pelningas, kai $\omega$ yra neteisinga baigtis.

Jei $\omega$ is teisinga baigtis, tuomet Teorema 2 mums sako, kad bent 1.25% viso egzistuojančio REP yra statomas ant neteisingos baigties ir yra ekonomiškai panaikinamas. Tad infliacijos nugręžimas nėra pelningas, kai $\omega$ yra teisinga baigtis.

Taip yra todėl, kad skilimo pradėjimas reikalauja ginčo obligacijos dydžio, prilygstančio bent 2.5% viso egzistuojančio REP.

## Priedas E: Obligacijų dydžio keitimas

Galiojimo obligacija, nepasinaudojimo REP obligacija, ir parinkto reporterio užmokestis yra dinamiškai keičiami pagal dalyvių elgesį per prieš tai buvusį užmokesčio langą. Žemiau pateikiame kaip mes keičiame minėtas vertes.

Nurodome, jog funkcija $f : [0,1] \to [\frac{1}{2}, 2]$ pagal:[30]

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

Funkcija $f$ naudojama nustatyti daugiklį šiuose pakeitimuose, kaip nurodyta aukščiau. Trumpai tariant, jei nepageidautinas elgesys vyko 1% praėjusio lango laiko, tuomet obligacijos dydis išlieka toks pats. Jeigu jis buvo dažnesnis, tuomet obligacijos dydis bus sumažintas perpus. Jeigu buvo dažnesnis, tuomet obligacijos dydis bus padvigubintas.

### 1. Galiojimo obligacija

Per patį pirmą mokesčių langą po paleidimo, galiojimo obligacija bus nustatyta 0.01 ETH vertės. Tuomet, jei daugiau nei 1% visų pasibaigusių rinkų buvo negaliojančios, tuomet galiojimos obligacijos dydis bus padidintas. Jei mažiau nei 1% visų pasibaigusių rinkų praėjusiame lange buvo negaliojančios, tuomet galiojimo obligacija bus sumažinta (bet niekada nebus mažesnė nei 0.01 ETH).

Nustatome, kad $\nu$ yra užbaigtų rinkų proporcija praėjusiame mokesčių lange, kurie buvo negaliojantys ir $b_v$ yra galiojimo obligacijų kiekis praėjusiame mokesčių lange. Tuomet galiojimo obligacija dabartiniame lange yra $\max\left\{\frac{1}{100}, b_v f(\nu)\right\}$.

### 2. Nepasirodymo REP obligacija

Per patį pirmą mokesčių langą po paleidimo, nepasirodymo REP obligacija bus 0.35 REP dydžio. Kaip ir galiojimo obligacija, nepasirodymo REP obligacija yra didinama arba mažinama pagal 1% nepasirodymo lygį, tačiau nemažiau nei 0.35 REP.

Tiksliau, tegul $\rho$ yra rinkų proporcija praėjusiame mokesčių lange, kurio nurodytieji reporteriai nepranešė įvykio baigties laiku, ir tegul $b_r$ yra nepasirodymo REP obligacijos dydis praėjusiame mokesčių lange. Nepasirodymo REP obligacijos dydis šiame mokesčių lange yra $\max\{0.35, b_r f(\rho)\}$.

### 3. Nustatytas reporterio užmokestis

Per patį pirmą mokesčių langą po paleidimo, reporterio mokestis bus nustatytas ties 0.35 REP. Šis kiekis yra dinamiškai keičiamas pagal tai nepateiktų baigčių kiekį buvusiame mokesčių lange.

Tegul $\delta$ yra neteisingų reportų proporcija praėjusiame mokesčių lange, tegul $b_d$ yra nustatytas reporterio užmokestis praėjusiame mokesčių lange, tuomet dabartinio lango užmokestis yra $\max\{0.35, b_d f(\delta)\}$.

## Priedas F: Veikimo principų keitimas

Dabartiniai veikimo principai buvo nustatyti po trijų metų tyrimų ir bandymų. Dabartinis principas stipriai skiriasi nuo prieš tai pateiktųjų [12]. Toliau aptarsime tris pagrindinius skirtumus, lyginant su senąja versija.

[29] Praktikoje, atakuojantysis negali išvengti kitų dalyvių REP perkėlimo skilimo metu ir negali garantuoti, kad $S$ neviršytų idealios maždaug 0.4939 reikšmės. Kita vertus, kadangi skaičiuojame blogiausią įmanomą scenarijų, laikysime, kad $S = 0.4939$.

[30] Ši formulė gali keistis, kai gaunama empirinė informacija iš tuo metu veikiančių rinkų.

### 1. Reportavimo mokesčiai

Pagal senuosius principus, rinkos kūrėjas nustato kūrėjo mokestį, kuris dalinmas pusiau su reporteriais. Dabartinėje versijoje kūrėjo ir reporterių mokesčiai yra nepriklausomi nuo vienas kito ir reporterio mokesčiai yra dinamiškai nustatomi Augur, norint išlaikyti sistemą saugesnę.

Reporteriams mokami mokesčiai veikie REP kainą, kuri turi tiesioginį poveikį skilimo protokolo saugumui (Teorema 1). Jeigu reporteriams mokami per maži mokesčiai, tuomet orakulo saugumui kyla rizika. Jeigu reporteriams mokami per aukšti mokesčiai, tuomet didėja parazitinių rinkų rizika. Todėl yra svarbu dinamiškai keisti reporterių mokesčius, siekiant išlaikyti Augur'o saugumą, neatiduodant to į rinkų kūrėjų rankas.

Reporterių ir rinkų kūrėjų mokesčių atskyrimas taip pat saugo reporterių (ir tuo pačiu skilimo protokolo vientisumo) interesus, neleidžiant rinkų kūrėjams konkuruoti žemiausiais mokesčiais. Kokybiškos rinkos ir kokybiškas reportavimas turėtų būti vertinami atskirai. Konkurencija turėtų būti skatinama rinkų kūrėjų mokesčiams artėjant link nulio, nemažint reporterių mokesčio.

### 2. Dalyvio mokesčiai

Senojoje versijoje mokesčiai iš dalyvių buvo surenkami už kiekvieną atliekamą statymą. Atnaujintoje versijoje, mokesčiai yra surenkami tik tuomet, kai yra išsprendžiama rinkos baigtis. Šis pokytis buvo įvykdytas, iš dalies, nes Augur negali prižiūrėti veiksmų, vykstančių neprisijungus. Rinkos akcijos yra žetonai, kurie gali būti perkami ir parduodami tarp vartotojų. Kadangi mokesčių rinkamas kiekvieno statymo metu nėra priimtinas, Augur surenka mokesčius tik tuomet, kai paaiškėja įvykio baigtis. Tai taip pat sumažina dalyvių mokesčius, kas daro Augur labiau konkurencingą.

### 3. Visatos

Senojoje versijoje, buvo tik viena REP "versija" ir visas REP kiekis buvo fiksuotas. Dabartinėje versijoje, REP gali būti išskaidytas į daug skirtingų versijų (visatų), kurių kiekviena gali turėti daugiau arba mažiau REP, nei pradinė versija. Jei skilimas yra ginčytinas, tuomet REP kiekis kiekvienoje naujoje visatoje gali būti tik maža dalis motininės visatos. Jeigu skilimas nėra ginčytinas, tuomet ankstyvo perėjimo premija, skirta dalyviams, gali nulemti, jog naujoje visatoje yra daugiau REP, nei motininėje.

Naujos atskirtos REP versijos yra skirtingi žetonai, kiekvienas su skirtinga kaina ir kiekiu. Kai Augus bus paleistas, bus viena visata (pradinė visata) ir viena REP versija, kuri egzistuoja šiuo metu. Kitavertus, kai tik įvyks skilimas, viena REP versija skils į daugybę versijų: pavyzdžiui, skylanti rinka su A ir B baigtimis skiltų į naujus žetunus REP-A, REP-B, ir REP-Negaliojantis. Piniginės ir biržos, palaikančios REP turėtų keturias skirtas REP versijas, kurios (teoriškai) galėtų būti palaikomos – REP-pradinis (originali REP versija, kuri šiuo metu būtų užšaldyta), REP-A, REP-B ir REP-Negaliojantis.[31]

Visas REP kiekis naujoje visatoje priklauso nuo to, kiek REP buvo perkelta ir kada vyko perkėlimas. REP perkėlimas skilimo metu prieš tai, kuri visata pasiekė susitarimą, sukelia mažą (bet ne nulinę) riziką (Žr. III E), kuri gali atbaidyti nuo dalyvavimo skilime. Siekiant paskatinti dalyvavimą skilime vartotojų dalyvavimas privalo būti kompensuojamas.

Vartotojai, kurie nedalyvauja skilime, galėtų būti nubausti dalies REP praradimu. Senojoje versijoje buvo "naudok arba netek" mechanizmas, kuris bausdavo nedalyvaujančiuosius taip pat, kaip reporterius, teikiančius baigtį klaidingai. Kitavertus, vartotojų baudimas sukuria rimtas naudojimosi spragas. Nedalyvaujančiųjų baudimas būtų problematiškas piniginėms ir biržoms, kuriose vartotojai laiko savo REP. Skilimo atveju, biržos turėtų perkelti savo klientų REP į naują visatą skilimo metu arba prarasti dalį savo REP.[32]

Vietoj bausmių, vartotojai bus premijuojami 5% naujoje visatoje nuo viso perkelto žetonų kiekio. Jei 4.762% visų REP žėtonų yra perkeliami į pralaiminčiąją visatą, iš kurių tarp 1.25% iki 2.5% yra jau sumokėti ginčo mokesčiui, tuomet visos visatos turės mažesnį žetonų kiekį, nei motininė visata.

---

[31] Praktiškumo vardan, paslaugų tiekėjams turbūt būtų paprasčiaus (ir mažiausiai žalinga vartotojams) paskatinti vartotojus dalyvauti skilime ir pasirinkti laimančiąją visatą, kai skilimas būna išspręstas.

[32] Taip pat išsiaiškinome, jog išmaniosios sutarties kodas galėjo išduoti skilimo premijas tik naudodamas labai sudėtingą paskirstymo metodą. Sutarties kodo sudėtingumas yra savaime didelė rizika, tad jį supaprastinome, kur įmanoma.