Augur: egy Decentralizált Jóslatpiac Platform

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander
Forecast Foundation
(Dated: 2018. április 13.)

Az Augur egy bizalom nélküli, decentralizált jóslatpiac platform. Az Augur jóslatpiac eredményeit azok az Augur hírnévtoken birtokosok választják ki, akik a tokenjeiket a ténylegesen látott kimenetelre helyezik, melyért cserébe elszámolási díjakat kapnak a piacoktól. Az Augur ösztönzőstruktúráját úgy tervezték, hogy biztosítsa, hogy mindig a becsületes és pontos eredményjelentés legyen a legprofitábilisabb lehetősége a hírnévtoken birtokosoknak. A tokenbirtokosok fokozatosan egyre nagyobb reputációs kötvényeket küldhetnek a vitatott piaci eredményekre. Ha ezeknek a kötvényeknek a mérete elér egy bizonyos határt, akkor a reputáció több verzióra oszlik, melyek mind egy lehetséges kimenetelt képviselnek a vitatott piacon. A tokentulajdonosoknak ekkor le kell váltaniuk a hírnévtokenjüket az egyik ilyen variációéra. Azok a hírnévtoken változatok, amelyek nem egyeznek meg a valós kimenettel értéktelenekké válnak, így senki sem fog részt venni a jóslatpiacon, csak ha biztos benne, hogy a piac megfelelően fog dönteni. Ezáltal a tokenbirtokosok a reputáció azon verzióját fogják választani, amelyről tudják, hogy továbbra is lesz értéke, azaz azt, amely megfelel a valóságnak.

Az Augur egy bizalom nélküli, decentralizált jóslatpiac platform. Egy jóslatpiacon az egyének spekulálni tudnak a jövőbeli események kimeneteléről. Azok, akik helyesen jósolják meg az eredményt, pénzt nyernek, míg azok, akik tévednek, pénzt veszítenek [1–3]. A jóslatpiac ára pontos és jól kalibrált mutató egy esemény bekövetkezésének valószínűségére [4–7].

Az Augur-t használva az emberek képesek lesznek a jóslatpiacon kereskedni nagyon alacsony költségek mellett. A résztvevőknek egyetlen jelentősebb kiadást kell fedezniük, ami a piac létrehozóinak járó kompenzációt és a piaci kimeneteleket megtörténésük után jelentő felhasználók fizetségét foglalja magába. Ennek eredménye egy olyan jóslatpiac, ahol a szükséges bizalom, a súrlódások és a díjjak olyan alacsonyak, amennyire a piaci verseny azt megengedi.

Történelmileg a predikciós piacok mindig is centralizáltak voltak. A legegyszerűbb módja annak hogy egy jóslatpiacon összegyűjsük a kereskedéseket, az az, hogy egy megbízható entitás fenn tart egy főkönyvet. Ehhez hasonlóan a legegyszerűbb módja annak, hogy meghatározzuk egy esemény kimenetelét és szétosszuk a kereskedők között a kifizetéseket, az az, ha egy pártatlan, megbízható bíró határozza meg a piacok kimeneteleit. A centralizált jóslatpiacok azonban számos korlátot és kockázatot tartalmaznak: nem teszik lehetővé a globális részvételt, korlátozzák, hogy milyen típusú piacokat lehet létrehozni, illetve megkövetelik a kereskedőktől, hogy bízzanak a piac üzemeltetőjében, hogy az nem lopja el a fogadásra feltett pénzeket és helyesen ítéli meg a piaci eredményeket.

Az Augur arra törekszik, hogy teljesen decentralizált piacokat hozzon létre. A decentralizált, bizalom nélküli hálózatok, mint a Bitcoin[8] és az Ethereum[9], kiküszöböli a kockázatot, hogy az önös érdekek korrupcióba vagy lopásba forduljanak. Az Augur fejlesztőinek csak annyi szerepük van, hogy okosszerződéseket készítsenek az Ethereum hálózaton. Az okosszerződések teljesen automatizáltak: a fejlesztőknek nincs meg a lehetőségük, hogy elköltsék a szerződésben letétként használt pénzeszközöket, nem kontrollálják a piaci eredményeket, nem fogadnak vagy utasítanak el kereskedéseket és egyéb tranzakciókat a hálózaton, nem tudnak meg nem történtté tenni kereskedéseket, illetve nem tudnak módosítani vagy törölni rendeléseket, stb. Az Augur *orákulum* lehetővé teszi, hogy az információ átkerüljön a való világból a blokkláncra, anélkül, hogy egy megbízott közvetítőre kellene támaszkodni. Az Augur lesz a világ első decentralizált jósa.

I. HOGYAN MŰKÖDIK AZ AUGUR

Az Augur piacok négy szakaszból állnak: *készítés*, *kereskedés*, *jelentés* és *egyezség*. Bárki létrehozhat egy piacot bármely valódi esemény alapján. A kereskedelem közvetlenül a piac létrehozása után kezdődik és minden felhasználó szabadon kereskedhet bármely piacon. A piac alapját képező esemény megtörténte után, annak kimenetelét az Augur orákulum határozza meg. Miután a kimenetelt meghatározták a kereskedők bezárhatják a pozíciójukat és összegyűjthetik a kifizetéseiket.

Az Augur natív tokenje a hírnévtoken (REP). REP szükséges a piacok készítői és jelentői számára, amikor jelentik az adott piac kimenetelét, mely az Augur platformon hoztak létre. A jelentők úgy közlik a piac eredményét, hogy a REP tokenjüket a piac egyik lehetséges kimenetelére *helyezik*. Ezzel a jelentők közlik, hogy a kimenetel, amelyre a tokenjüket helyezték megegyezik a piac alapjául szolgáló, való világban történt esemény kimenetelével. A piac jelentőinek konszenzusa „igaznak" tekintett, olyan célból, hogy meghatározza a piac kimenetelét. Ha egy riporter jelentése eltér a többi riporter jelentéséből összeállt konszenzus eredményétől, akkor az Augur a konszenzus eredményétől eltérő kimenetelt jelentő riporterek REP tokenjeit szétosztja azok között, akik a konszenzust létrehozták.

A REP token birtoklásával és a pontos eredmény jelen-

tésével a tokenbirtokosok jogosultak a platform díjainak egy részére. Minden egyes elhelyezett REP feljogosítja annak birtokosát a piac díjaiból való egyenlő arányú részesedésre. Minnél több REP tokent birtokol a jelentő - és helyesen jelent - annál több díjból fog részesülni, amiért biztonságossá teszi a platformot.

Habár a REP központi szerepet játszik az Augur működésében mégsem használható kereskedésre az Augur piacain. A kereskedőknek nincs szükségük a REP használatára, mivel nem kell, hogy részt vegyenek a jelentés folyamatában.

A. Piackészítés

Az Augur bárki számára lehetővé teszi, hogy létrehozzon egy piacot egy közelgő eseményhez. A *piac készítője* beállítja az *esemény végének idejét* és *kiválasztja a riportereket*, akik jelentik az esemény kimenetelét. A kijelölt riporterek nem tudnak önkényesen dönteni a kimenetelről, a közösségnek mindig van lehetősége vitatni és kijavítani a kijelölt riporterek jelentését.

Ezután a piac készítője kiválasztja a *forrást*, amelyet a jelentőknek használnia kellene, hogy meghatározzák a kimenetelt. A forrás lehet egyszerűen „általános ismeret" vagy egy konkrét dolog, mint például az „Egyesült Államok Energiaügyi Hivatala", a `bbc.com` vagy egy adott API végpont címe. [1] Ezen kívül be kell állítania a *készítői díjat*, amely az adott piacon kereskedők által fizetendő díj a piac létrehozójának (A díjak részletei az I D fejezetben találhatóak). Végül a piac létrehozója kétféle kötvényt ad ki: az *érvényességi kötvényt*, és a *kijelölt jelentést elmulasztó kötvényt* (röviden *jelentés elmulasztó kötvényt*).

Az érvényességi kötvényt ETH-ben kell kifizetni, mely visszakerül a piac készítőjéhez, ha a piac eredménye bármely más, mint *érvénytelen*.[2] Az érvényességi kötvény ösztönzi a piac készítőjét, hogy olyan piacokat hozzon létre, amelyek jól definiálható eseményeket, objektíven és megfelelő kimenetelekkel írnak le. Az érvényességi kötvény mérete dinamikusan állítódik a korábbi piacok érvénytelen kimeneteleinek függvényében.[3]

A jelentés elmulasztása kötvény két részből áll: a *jelentés elmulasztása gázkötvényből*, amelyet ETH-be fizetnek, és a *jelentés elmulasztása REP kötvényből*, amit REP-be fizetnek. Ezek a kötvények visszafizetésre kerülnek a piac készítőjének, ha a piac kijelölt riporterei bejelentik a kimenetelt a *piaci esemény végét* követő első három napban. Ha a kijelölt riporterek nem adják le a jelentésüket a megadott 3 napos időszakban, akkor a piac készítője elveszíti a jelentés elmulasztása kötvényt, mely átadásra kerül az *első nyilvános jelentőnek*, aki jelenti a kimenetelt (lásd ezt az I C 6 fejezetben). Ez ösztönzi a piac készítőjét, hogy megbízható riportereket jelöljön ki, mely segíti a piac gyors lezárását.

A jelentés elmulasztása gázkötvény az első nyilvános riporter gázköltségét hivatott fedezni. Ez megakadályozza azt, hogy az első nyilvános riporter gázköltsége túl magas legyen ahhoz, hogy a jelentése nyereséges legyen. A jelenés elmulasztása gázkötvény ára a korábbi díjablak idején fennálló átlagos gázköltség kétszeresére van állítva.

Ha a kijelölt riporter elmulasztja a jelentést, a jelentés elmulasztása REP kötvény az első nyilvános jelentőhöz kerül, ha az helyes kimenetelt ad meg. Az érvényesség kötvényhez hasonlóan, a jelentés elmulasztása REP kötvény dinamikusan beállított a korábbi díjablak idején a jelentést elmulasztó kijelölt riporterekkel egyenes arányban.[4]

A piac készítője elkészíti a piacot és elküldi a szükséges kötvényeket egy Ethereum tranzakcióval. Amint a tranzakció megerősítésre kerül, a piac él és megkezdődhet a kereskedés.

B. Kereskedés

A piaci résztvevők megjósolják az esemény kimenetelét úgy, hogy azon esemény kimeneteleinek *részvényeivel* kereskednek. A *teljes részvénykészlet* olyan részvények gyűjteménye, amelyek az esemény minden egyes lehetséges eredményének részvényeit tartalmazzák [10]. A teljes készlet az Augur szerződéspárosító motorjával készül, amire a kereskedések teljesítéséhez van szükség.

Például vegyünk fontolóra egy piacot, aminek két lehetséges kimenetele van `A` és `B`. Alice 0,7 ETH akar fizetni az `A` részvényért, míg Bob 0,3 ETH-t a `B` részvényért. [5] Elsőként az Augur párosítja ezeket a rendeléseket és összegyűjti az összesen 1 ETH-t Alice-től és Bob-tól.[6] Ezután az Augur elkészíti a teljes részvénycsomagot úgy, hogy Alice-nek adja az `A` részvényt és Bob-nak a `B`-t. Így kerülnek a kimenetelek részvényei a körforgásba. Miután

---

[1] Például ha a piac a „2018. április 10-i hőmérséklet csúcsról szól (Fahrenheitben) a San Francisco-i Nemzetközi Repülőtéren és a forrás a Weather Underground" `https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html`, akkor a riportereknek csak el kell menniük a megadott URL-re és az ott mutatott legmagasabb hőmérsékletet kell beleírniuk a jelentésükbe.

[2] Az *érvénytelen piac* a jelentők által válik érvénytelenné, amikor a megadott lehetséges kimenetelek közül egyik sem felel meg a valóságnak, vagy ha a piaci megfogalmazás homályos, illetve szubjektív. Ennek részleteit lásd a III F fejezetben.

[3] Részletekért lásd az E 1 függeléket.

[4] Lásd az E 2 függeléket a további részletekért.

[5] Kezdetben az Augur piacon való kereskedéshez az Ethereum natív érméjét, az ETH-t fogjuk használni. Az ezt követő kiadásokban az Augur támogatni fogja az Ethereum hálózaton kibocsátott önkényesen választott tokeneket, beleértve más piacok részvényeit és a dollárhoz rögzített, úgynevezett „stabilérméket" is, ha/amikor ezek elérhetővé válnak.

[6] Az 1 ETH-t csak a beszélgetés egyszerűsítése érdekében használjuk. A valódi költsége a teljes részvénycsomagnak sokkal kevesebb ennél, ennek valós mértékét a `docs.augur.net/#number-of-ticks` láthatod.

1. ábra. Egy jóslatpiac életútjának egyszerűsített vázlata.

a részvények elkészítésre kerültek, szabadon kereskedhetővé válnak.

Az Augur kereskedési-szerződések minden egyes a felületen készített piachoz fenntartanak egy megrendelői könyvet. Bárki, bármikor megadhat egy új rendelést vagy elfogadhat egy létezőt. A rendelések elfogadását egy az Augur okosszerződésekben elhelyezett összepárosító motor végzi automatikusan. A részvény vételi vagy eladási kérvény azonnal teljesítésre kerül, ha a megrendelői könyvben már találhatók összepárosítható rendelések. Rendelés betöltődhet részvény vásárlásával vagy annak eladásával egy másik résztvevő számára, ez maga után vonhatja új, teljes készletek kibocsátását, vagy a meglévő készletek zárását. Az Augur párosító-motorja mindig elkülöníti a minimális részvénymennyiséget és/-vagy készpénzmennyiséget, amely szükséges a kockáztatott érték fedezéséhez. Ha nincs összepárosítható rendelés, vagy a rendelés csak részben teljesíthető, akkor a maradék összeg a megrendelői könyvbe kerül egy új rendelés formájában.

Rendelések sohasem jöhetnek létre rosszabb áron, mint az a limit-ár amelyet a kereskedő beállított, azonban jobb áron végrehajtódhatnak. A nem betöltött, vagy részben betöltött rendelések bármikor törölhetők a megrendelői könyvből a rendelés készítője által. A díjakat a kereskedő csak akkor fizeti ki, amikor a teljes részvénykészlet eladásra került. Az elszámolási díjakról az I D fejezetben tájékozódhat részletesebben.

Míg a legtöbb részvénykereskedés várhatóan a piaci elszámolás előtt fog történni, a kereskedés a piac elkészültétől kezdve bármikor megkezdhető. Minden Augur eszköz, beleértve a piaci kimenetelek részvényei, a részvételi tokenek, a vitakötvények és még a piac birtoklása is folyamatosan átruházható.

C. Jelentés

Miután a piaci esemény bekövetkezik, a kimenetelt meg kell határozni, hogy a piac lezárása elkezdődhessen. A kimeneteleket az Augur jósa határozza meg, amely nyereségorientált riporterekből áll, akik jelentik a valós eredményt. Bárki részt vehet a jelentésben és az eredmények megvitatásában, aki birtokol REP tokent. Azok a riporterek, akiknek a jelentése egybehangzik a konszenzussal végül jutalomban részesülnek, míg azok akiknek a jelentése eltér attól büntetésben (lásd a I D 3) fejezetet).

1. Díjablakok

Az Augur jelentő rendszere egy egymást követő 7 napos *díjablakon* keresztül fut. Minden díj, amelyet az Augur az adott díjablakban összegyűjt hozzáadódik a *jelentési díjablak alapjához*. A díjablak végén a jelentési díjalapot azoknak a REP birtokosoknak fizetik ki, akik részt vettek a jelentési folyamatban. A riporterek a feltett REP mennyiségükkel arányosan kapják meg a jutalmukat. A részvétel magában foglalja a kezdeti jelentés során megtett tételeket, a kísérleti kimenetel megvitatását, illetve a *részvételi tokenek* vásárlását.

2. Részvételi tokenek

Az új díjablak alatt a REP birtokosok bármilyen mennyiségben vásárolhatnak részvételi tokeneket egészen egy attorep-ig [7]. A díjablak végén beszámíthatják a részvételi tokenjeiket minimálisan egy attorep összegéig a *jelentési díjalapból* való arányos részesedésért. Ha nem volt semmilyen művelet (*pl.*jelentés benyújtása vagy egy másik felhasználó által benyújtott jelentés vitatása), akkor a riporter vásárolhat részvételi tokeneket, hogy jelezze a megjelenésüket a díjablakban. Hasonlóan a REP tételekhez, a részvételi tokeneket a tulajdonosok beválthatják a *rájuk eső* díjablakban összegyült díjért.

Ahogy a II-es fejezetben is megbeszéltük, fontos, hogy a REP birtokosok készen álljanak részt venni a piac lezárásához szükséges esetleges osztódásban. A részvételi token ösztönzésként szolgál a REP birtokosoknak, hogy azok felkeressék az Augur-t legalább egyszer egy héten, és így készen álljanak a részvételre ha az szükséges. Még azok a REP birtokosok is, akik nem akarnak részt venni a jelentése folyamatában ösztönözve vannak, hogy ránézzenek az Augur-ra egy héten egyszer, hogy részvételi tokeneket vásároljanak és díjakat gyűjtsenek. Ez a rendszeres aktív bejelentkezés biztosítani fogja, hogy ismerjék az Augur használatát, tudatában legyenek az osztódásoknak és így felkészültek legyenek az esetleges osztódásokban való részvételre.

3. A piaci helyzet előrehaladása

Az Augur piacok 7 különböző állapotban lehetnek az elkészítésüket követően. A lehetséges állapotok vagy „fá-

[7] Egy *attorep* az 10^{-18} REP.

zisok" a következők:

- Előzetes jelentés
- Kijelölt jelentés
- Nyitott jelentés
- Várakozás a következő díjablak nyitására
- Vitakör
- Osztódás
- Véglegesítés

Ezen állapotok közötti kapcsolat látható a 2-es ábrán.

4. Előzetes jelentés

Az *előzetes jelentés* vagy *kereskedés* fázisa (1. ábra) az az időszak, amely a kereskedés megkezdése után következik, de még az esemény bekövetkezése előtt van. Általában ez a legaktívabb kereskedési időszak bármelyik Augur piac számára. Miután az esemény végének ideje bekövetkezett, a piac belép a *kijelölt jelentés* fázisába (2. ábra (a)).

5. Kijelölt jelentés

A piac készítője, amikor elkészíti a piacot szükséges, hogy válasszon kijelölt riportereket és kiadja a jelentés elmulasztása kötvényt. A kijelölt jelentés fázisában (2. ábra (a)) a piac kijelölt riportereinek 3 napjuk van jelenteni az esemény eredményét. Ha a kijelölt riporter az adott 3 napban nem jelent, a piac készítője elveszíti a jelentés elmulasztása kötvényt és a piac automatikusan belép a *nyitott jelentés* fázisába (2. ábra (b)).

Ha a kijelölt riporter leadja a jelentését időben, akkor a jelentés elmulasztása kötvény visszakerül a piac készítőjéhez. A kijelölt riporternek le kell tennie a kijelölt riporter letétet[8] a jelentett eredményre, amelyet elveszít, ha a piac az általa bejelentettől eltérő kimenetelt véglegesít.[9] Amint a kijelölt riporter leadja a jelentését a piac belép a *következő díjablak megnyitására várás* fázisába (2. ábra (c)) és a jelentett eredmény a piac kísérleti *eredményévé* válik.

6. Nyitott jelentés

Ha a kijelölt riporter nem jelent a megadott három napban, a piac készítője elveszíti a jelentés elmulasztása kötvényt és a piac azonnal belép a *nyitott jelentés* fázisába (2. ábra (b)). Ebben a fázisában bárki jelentheti a piac kimenetelét. Amikor a kijelölt riporter elmulasztja a jelentést, az első riportert, aki jelenti a végeredményt *első nyilvános riporternek* nevezik.

A piac első nyilvános riportere megkapja az elvesztett jelentés elmulasztása kötvényt, úgy, mint a választott döntésére helyezett letétet, tehát kérheti a jelentés elmulasztása REP kötvényt, ha a jelentett kimenetel megegyezik a piac véglegesített kimenetelével. Továbbá, megkapja a jelentés elmulasztása gázkötvényt is miután a piac véglegesítette az eredményt, de ezt is csak akkor ha az megegyezik a bejelentett eredménnyel.

Az első nyilvános riporternek *nincs* szüksége saját REP tokenre amikor jelenti a piac kimenetelét. Így bármelyik piac, amelynek a kijelölt riportere elmulasztja a jelentést rövid időn belül eredményt tud hirdetni, ha *valaki* jelenti az eredményt miután az belépett a nyitott jelentés fázisába.

Ha egy *előzetes jelentés* megérkezik egy előzetes jelentőtől (legyen az kijelölt riporter vagy első nyilvános jelentő), a bejelentett kimenetel a piac kísérleti eredményévé válik és a piac belép a következő díjablak megnyílására való várakozás fázisába (2. ábra (c)).

7. Várakozás a következő díjablak nyitására

Miután a piac megkapja az előzetes jelentést, belép a következő díjablak nyitására való várakozás fázisába (2. ábra (c)). Ebben a fázisban a piacra vonatkozó jelentések a jelenlegi díjablak lezárásáig tartanak. Amint a következő díjablak elkezdődik a piac belép a *vitakör* fázisába.

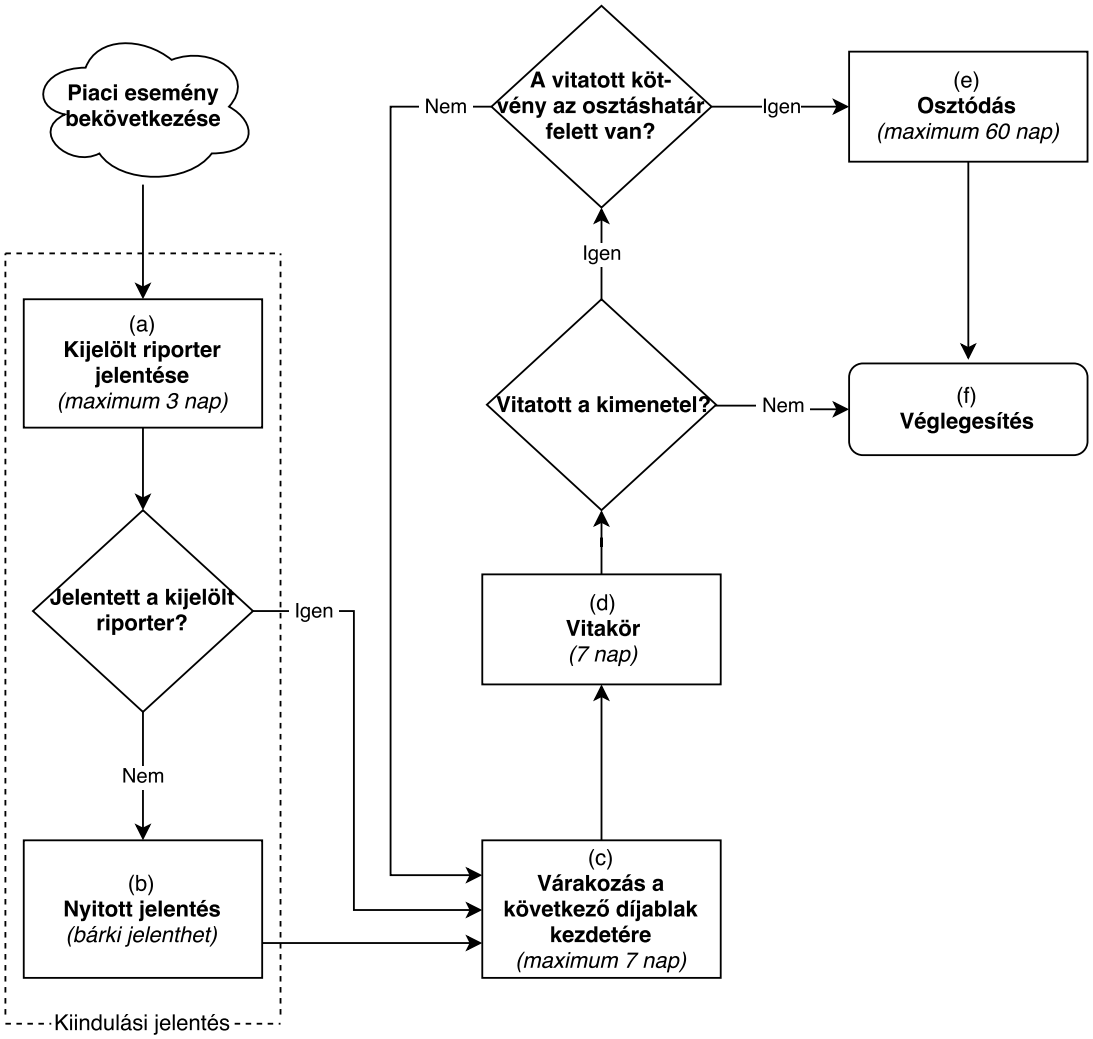
8. Vitakör

A vitakör (2. ábra (d)) egy 7 napos periódus, amely során bármely REP tulajdonosnak lehetősége van megvitatni a piac *kísérleti eredményét*.[10] (A vitakör elején a piac kísérleti eredménye az az eredmény, ami a piac végleges eredményévé válik, ha nem kerül sikeres megvitatásra a REP birtokosok között.) A vita tartalmazhat *letéti* REP-et (másnéven *vitaletétet*) a piac jelenlegi kísérleti eredményétől *eltérő* eredményen. A vita *sikeres*, ha a teljes vitaletét összeg valamelyik eredményen eléri a *vitakötvény méretét*, ami szükséges az adott körben. A vitakötvény méret számítása a következőképpen történik.

[8] Lásd az E 3 függeléket ennek mértékéről.

[9] Az elvesztett letét hozzáadódik a piac díjablakának jelentési alapjához és így a becsületes vitázókat és riportereket jutalmazza (lásd a I D 3 fejezetet további részletekért).

[10] Az a tény, hogy a vitakör egybeesik a díjablak idejével pusztán a kényelem műve, a gyakorlatban ez a kettő időtartam máskorra is eshet.



2. ábra. Jelentési folyamatábra.

Jelölje A_n a teljes letét összegét a piac összes kimenetelére az n. vitakör kezdetén. ω legyen bármely piaci kimenetel, amely *eltér* a kör eleji kísérleti kimeneteltől. $S(\omega, n)$ jelölje a teljes letéti összeget ω kimeneten az n. vitakör elején. A *vitakötvény* méretét egy sikeres vitához a jelenlegi kisérleti kimenetellel szemben ω javára az n körben jelölje $B(\omega, n)$, mely az alábbi módon számolandó:

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

A kötvény méretet úgy választottuk ki, hogy 50%-os ROI-t biztosítson a riportereknek, akik sikeresen vitatnak egy hamis kimenetelt (lásd a II D fejezetben).

A vitakötvényeket nem egyetlen felhasználónak kell teljes egészében kifizetni. Az Augur platform lehetővé teszi a résztvevők számára, hogy közösségi finanszírozzák a vitakötvényeket. Bármely felhasználó, aki helytelen kísérleti eredményt lát, vitathatja azt a kimenetelt, ha REP-et helyezz el egy ettől eltérő kimenetelen. Ha bármelyik kimenet (más mint a kísérleti kimenet) felhalmoz elegendő vitaletétet, hogy kitöltse a vitakötvényt, akkor a jelenlegi kísérleti eredmény sikeresen megvitatásra került.

Sikeres vita esetén a piac vagy belép egy másik vitakörbe vagy belép az *osztódás* állapotába (2. ábra (e)). Ha a betöltött vitakötvény mérete nagyobb, mint 2,5%-a az összes REP-nek, akkor a piac az osztódás állapotába lép. Ha ennél kevesebb, akkor az újonnan kiválasztott eredmény válik az új kísérleti kimenetellé, és a piac egy újabb vitakörbe kezd.

Minden vitaletétet a vitakör során elkülönítve kezelnek. Ha a vitakötvény sikertelen, akkor a vitaletét visszatérítésre kerül a birtokosának a vitakör végén. Ha nincs sikeres vita a 7 napos vitakör során, akkor a piac belép a *véglegesítés* állapotába (2. ábra (f)), és a kísérleti eredmény *végső eredménnyé* válik. A piac végső eredménye az a kísérleti eredmény, amelyik sikerrel végigmegy a vitakörökön anélkül, hogy leváltanák azt. Az Augur szerződések a végső eredményeket *igaz*-ként kezelik és ez alapján eszközlik a kifizetéseket.

Minden sikertelen vitaletét visszakerül a birtokosához

minden egyes vitakör végeztével. Minden sikeres vitaletét a végül helytálló eredményre kell, hogy elhelyezve legyen és ott maradjon az osztódás és a piac véglegesítéséig (vagy amíg az osztódás megtörténik valamelyik másik Augur piacon). Minden vitaletét (legyen az sikeres vagy sikertelen) részt kap a jelenlegi díjablak [11] *jelentési alapjából.*

9. Osztódás

Az osztódás állapot (2. ábra (e)) egy speciális állapot, amely eltarthat egészen 60 napig. Az osztódás a piac lezárásának végső megoldása, mely egy nagyon bomlasztó folyamat és szándékaink szerint csak ritkán fog bekövetkezni. Az osztódás akkor történik, amikor a piacon valamelyik kimenetel sikeresen összegyűjtötte a vitakötvény betöltéséhez szükséges legalább 2,5% REP-et. Ezt a piacot úgy is nevezzük hogy *osztódó piac.*

Amikor az osztódást elindítjuk egy 60 napos[12] *osztódási periódus* veszi kezdetét. Az összes többi, nem véglegesített piaccal szemben a vitát az osztódási időszak végéig tartjuk meg. Az osztódási időszak sokkal hosszabb, mint az általános díjablak hossza, mert a platformnak szüksége van, hogy elegendő időt biztosítson a REP birtokosoknak és a szolgáltatóknak (mint a pénztárcák és váltók), hogy felkészüljenek. Az osztódás végső eredménye nem vitatható.

Minden Augur piac és minden REP token valamely *univerzumban* létezik. A REP tokeneket használhatjuk kimenetelek bejelentésekor (hogy díjakban részesülhessünk) *de csak* olyan piacokon, amelyek egy azonos univerzumban léteznek. Amikor az Augur először el fog indulni, minden piac és minden REP egy *kiindulási univerzumban* fog együtt létezni.

Amikor a piac osztódik, akkor új univerzum keletkezik. Az osztódás új, *leszármazott univerzumot* készít minden lehetséges kimenetelnek (beleértve az `érvénytlent` is, amelyet I D 2 fejezetben beszéltünk meg). Például, egy „bináris" piacon három lehetséges kimenetel van: `A`, `B` és `érvénytelen`. Így egy bináris piac osztódása 3 új, leszármazott univerzumot hoz létre: univerzum `A`-t, univerzum `B`-t és az `érvénytelen` univerzumot. Kezdetben ezek az újonnan elkészített univerzumok üresek, azaz nem tartalmaznak majd piacokat vagy REP tokeneket.

Amikor az osztódás elkezdődik a *szülőuniverzum* véglegesen *zárolásra kerül.* Egy zárolt univerzumban nem lehet új piacokat létrehozni. A felhasználók továbbra is folytathatják a részvények kereskedését a piacon és egy zárolt piac is megkapja a kezdeti jelentést. Azonban a jelentési jutalom nem itt kerül kifizetésre és a zárolt univerzum piacai nem véglegesíthetők. Azért, hogy a zárolt univerzum piacai és REP tokenjei hasznosíthatók legyenek, át kell őket költöztetni a leszármaztatott gyerekuniverzumba.

A szülőuniverzum REP birtokosai átköltöztethetik a REP tokenjeiket a gyerekuniverzumba saját választásuk szerint. Ezt a döntést gondosan meg kell fontolni, mert a költöztetés egyirányú, azaz nem lehet visszacsinálni. Tokent nem lehet átküldeni az egyik testvéruniverzumból a másikba. *Az átköltöztetés egy végleges elköteleződése a REP tokeneknek az adott piaci kimenetelhez.* A REP tokeneket, amelyek különböző gyerekuniverzumokba költöztetésre kerültek, teljesen különálló tokenként kezelik a pénztárcák és a váltók is.

Amikor egy osztódás megkezdődik minden letétbe helyezett REP, amely nem az osztódó piacon van *felszabadul* és így szabadon átköltöztető a gyerekuniverzumba az osztódás ideje alatt.[13]

Amelyik gyerekuniverzum megkapja a legtöbb átköltöztetett REP-et az osztódás végén, az válik a *győztes univerzummá* és annak eredménye lesz a végső kimenetel. A szülőuniverzumban a nem véglegesített piacok a nyertes univerzumba vándorolhatnak és ha már kaptak egy kezdeti jelentést, akkor visszaállnak a következő díjablakra való várakozás fázisába.

Nincs időlimit, hogy átköltöztess REP tokeneket a szülőuniverzumból a gyerekuniverzumba. A tokenek átköltöztethetők az osztódás periódusa után is, de nem fognak beleszámolódni a győztes univerzum meghatározásába. Azért, hogy növeljük a részvételi arányt az osztódás periódusában, minden tokenbirtokos, aki átköltözteti a REP tokenjét 60 napon belül 5% további REP-et fog kapni abban a gyerekuniverzumban, amelybe költöztette azt [14]. Ezt a jutalmat új REP tokenek bányászásával fizetik ki. [15]

Azok a riporterek, akik a REP tokenjeiket elhelyezték valamely osztódó piac kimenetelén nem tudják módosítania pozíciójukat az osztódás ideje alatt. Az a REP, amely letétként lett elhelyezve a szülőuniverzum egy kimenetelén átköltöztethető a gyerekuniverzumba, de csak abba, amelyik kimenetele megegyezik a szülőuniverzuméval. Például, ha a riporter sikeresen segítette a vitakötvény betöltődését az `A` kimenetelre valamely vitakörben, akkor a REP, amelyet az adott kimenetelre helyezett

[11] Bármely elszámolási díj és érvényességi kötvény, amely az adott díjablak idején lett összegyűjtve, hozzáadódik a díjablak jelentési alapjához. A díjablak lezárulásakor a jelentési alap kifizetésre kerül a REP letétek mennyiségének függvényében.

[12] Egy osztódási periódus lehet kevesebb mint 60 nap: végződhet amikor elérjük a 60 napot vagy akkor, amikor több mint az 50%-a kezdeti REP mennyiségnek átkerült egy leszármaztatott gyerek univerzumban.

[13] Az egyetlen kivétel ezalól az a REP letét, amelyet a kezdeti riporter tett le a kezdeti jelentés elkészítésekor. Ez a REP letétként marad a kezdeti riporton és automatikusan átköltöztetése kerül abba a gyerekuniverzumba, amely megnyeri az osztódást.

[14] Ez akkor is érvényes, amikor az osztódási periódus korán végződik köszönhetően az 50%-os arány elérésének.

[15] A további tokenek piachoz történő hozzáadásának hatása elhanyagolható. Például, ha az összes létező REP 20%-a átköltöztetésre kerül az osztódás időszakában, akkor ez a bónusz egy 1%-os növekedést eredményez a token darabszámban. Ezen felül az osztódás várhatóan nagyon ritka esemény lesz.

csak abba az univerzumba költöztethető az osztódás ideje alatt, amelynek kimenetele szintén A.

A testvéruniverzumok teljesen különállóak. A REP token, amely létezik az egyik univerzumban nem használható esemény jelentésére vagy jutalom összegyűjtésére a másik univerzumban. A felhasználók feltehetően nem akarnak olyan univerzumban lévő piacot létrehozni vagy azon kereskedni, amelynek jósa megbízhatatlan. A REP token, amely ilyen univerzumban létezik a valósággal nem megegyező kimenetelt állít, ezért valószerűtlen, hogy tulajdonosának jutalmat hoz. Az ide átköltöztetett REP tokenek, amelyek nem fedik a valóságot értéktelenek, függetlenül attól, hogy az adott univerzum megnyeri-e az osztódást vagy sem. Ennek fontos biztonsági következményei vannak, amelyről bővebben a II fejezetben tájékozódhat.

10. Véglegesítés

A piac beléphet a véglegesítés állapotába (2. ábra (f)), ha áthalad a 7 napos vitakörön anélkül, hogy a kísérleti eredményt sikeresen leváltanák, illeve osztódással is. Az osztódás kimenetele nem vitatható és mindig végső eredménynek tekintendő. Miután a piac véglegesedett, a kereskedők elhelyezhetik pozícióikat közvetlenül a piacon. Amikor a piac belép a véglegesítés állapotába annak eredményét *végleges eredménynek* tekintjük.

D. Egyezség

A kereskedők az alábbi két módon zárhatják pozícióikat: eladhatják részvényeiket egy másik kereskedőnek pénzért vagy megegyezhetnek a piaccal. Emlékezzünk vissza, hogy minden egyes részvény egy teljes készlet részeként jön létre, így ekkor már letétbe helyeztünk összesen 1 ETH-t az Augur-nál. [6] Azért, hogy kereskedő visszakapja azt az 1 ETH-t a letétből vissza kell adnia egy teljes részvénykészletet, vagy ha a piac véglegesedett, akkor egy darabot a győztes kimenetel részvényeiből. Amikor ez a kereskedés megtörténik, azt úgy nevezzük, hogy a kereskedő *egyezséget kötött piaci szerződéssel.*

Vegyünk például figyelembe egy véglegesített piacot, amely lehetséges kimenetelei A és B. Feltételezzük, hogy Alice rendelkezik egy A kimenetel részvénnyel, amelyet el szeretne adni 0,7 ETH-ért, illetve Bob is rendelkezik egy B kimenetel részvénnyel, amit el szeretne adni 0,3 ETH-ért. Először az Augur motorja összepárosítja ezeket a rendeléseket és összegyűjti A és B részvényt a résztvevőktől. Ezután az Augur odaadja a 0,7 ETH-t (mínusz a díj) Alice-nek és a 0,3 ETH-t (mínusz a díj) Bob-nak.

Második példaként vegyünk egy véglegesített piacot, aminek a győztes kimenetele A. Alice-nek van egy A részvénye és szeretné azt kifizettetni. Alice elküldi az A részvényét az Augur-nak és cserébe megkapja az 1 ETH-t (mínusz a díj).

1. Egyezségi díj

Az egyetlen alkalom, amikor az Augur díjakat vet ki az akkor van, amikor a piac résztvevői egyezséget kötnek piaci szerződéssel. Az Augur két díjat vet ki az egyezség során: a készítő díját és a jelentés díját. Mindkét díj arányos a kifizetendő összeggel. Tehát egy véglegesítés előtt álló egyezség során, ahol Alice 0,7 ETH-t szeretne, míg Bob 0,3 ETH-t szeretne Alice-nek kell megfizetnie a díj 70%-át, míj Bob-nak a maradék 30%-ot.

A készítői díjat a piac készítője szabja meg, amely egyezség esetén az ő számára fizetendő. A jelentési díj dinamikusan állítódik (lásd II C fejezetet) és ez azon riporterek számára fizetendő, akik részt vettek a jelentési folyamatban.

2. Egyezség érvénytelen piacok esetén

Érvénytelen piac esetén az a kereskedő, aki piaci szerződéssel állapodik meg egyenlő mennyiségű ETH-t kap minden részvényéért. Ha a piacnak van N lehetséges kimenetele (nem számítva az érvénytelen kimenetet) és a teljes részvénykészlet költsége C ETH volt, akkor a kereskedő visszakap C/N ETH-t minden egyes piaci szerződéses megegyezésével. [16]

3. Hírnév újraelosztás

Ha a piac osztódás kezdeményezésével fejeződik be, akkor minden REP letét, amely a végső kimeneteltől eltér elkobzásra és arányos szétosztásra kerül azok között a felhasználók között, akik a piac végső eredményét választották. A vitakötvény mérete úgy lett kiválasztva, hogy sikeres vita esetén 50%-os ROI-val díjazza a vita kezdeményezőjét. [17] Ez egy erős ösztönzőerő a riportereknek, hogy vitatni kezdjék a hamis kísérleti eredményeket.

II. ÖSZTÖNZÉS ÉS BIZTONSÁG

Erős kapcsolat áll fenn a REP piaci kapitalizációja és az Augur osztódási protokolljának megbízhatósága között. Ha a piaci kapitalizáció elég nagy[18] és a támadók gazdaságilag racionálisak, akkor a győztes osztódáskimenetel meg fog egyezni az objektív valósággal. Tény,

---

[16] Technikai limitációk miatt a kereskedést nem lehet egyszerűen abbahagyni, ha a piac érvénytelenné válik. A kimenetelek részvényei csak tokenek, amelyek közvetlenül kereskedhetők a felhasználók között. Az ETH és a részvények ezáltal nincsenek az Augur irányítása alatt, így nem lehet visszaadni őket az eredeti tulajdonosoknak, ha a piac érvénytelenként zár.

[17] Lásd a 3-as elméletet az A függelékben.

[18] Lásd a II A fejezetet a további részletekért.

hogy az Augur megfelelően működhetne a kijelölt riporterek és vitakörök nélkül is. *Csak* az osztódási folyamatot használva a jós igazságosan jelentene.

Azonban az osztódások bomlasztóak és időigényesek. Egy osztódás 60 napig is eltarthat, és egyszerre csak egy piacot tud megoldani. A 60 nap alatt, amíg az osztódó piac megoldásra kerül, minden egyéb nem véglegesített piac várakoztatásra kényszerül.[19] A szolgáltatóknak frissíteni, a REP tulajdonosoknak, pedig át kell költöztetni a REP tokenjeiket egy új gyerekuniverzumba. Ezért osztódást csak akkor szabad használni, amikor feltétlenül szükség van rá.

Szerencsére, ha megállapítást nyer, hogy az osztódások megbízhatóak az igazság megállapításában, az ösztönzésként szolgál a résztvevők számára, hogy őszintén viselkedjenek és ne kelljen osztódást kezdeményezni. *Az osztódás hiteles fenyegetése és a hit, hogy az osztódás megfelelően fog dönteni alkotják az Augur ösztönző rendszerének sarokköveit.*

A következőkben bemutatjuk azokat a feltételeket, amelyek mellett az osztódás rendszer megbízható az igazság meghatározásában. Ezután megbeszéljük az ösztönző rendszert, hogy miként ösztönzi a piacok gyors és helyes lezárását.

A. Az osztódási protokoll becsületessége

Itt megbeszéljük az osztódás megbízhatóságát és a körülményeket, amelyek között az megbízható. A megvitatás megkönnyítéséhez osztódáskor azt a gyerekuniverzumot fogjuk `igaznak` nevezni, amely megegyezik az objektív valósággal, az összes többit `hamisnak` fogjuk hívni. Azt a gyerekuniverzumot, amely a legtöbb REP tokent kapja az osztódás periódusa alatt győztes univerzumnak fogjuk hívni míg az összes többit vesztes univerzumoknak.

Természetesen mindig azt akarjuk hogy az `igaz` univerzum legyen a győztes univerzum és a `hamisak` veszítsenek. Azt mondjuk, hogy az osztódási protokoll sikeresen támadható, ha a `hamis` univerzum győztes univerzumként kerül ki az osztódásból, azaz így az osztódó piac (és esetleg minden még nem véglegesített piac) helytelenül kerül kifizetésre.

A megközelítésünk az orákulum biztonságához az, hogy a sikeres támadások maximális nyeresége kevesebb legyen mint a támadáshoz szükséges minimális költség. Ezt az alábbiakban formalizáljuk.

1. A támadó maximális nyeresége

A támadó, aki sikeresen megtámadja a jóst, a még nem véglegesített Augur piacokat át tudja költöztetni a `hamis` univerzumba. Ha a támadó birtokában van a REP-ek többségének a `hamis` univerzumban, akkor minden nem véglegesített piacot rá tud kényszeríteni, hogy úgy záródjon, ahogy ő akarja. Extrém esetekben a letétként elhelyezett összegeket is meg tudja szerezni ezeken a piacokon. [20]

1. Definíció. Definiáljuk és jelöljük I_a értékkel az Augur *natív, nyitott kamatait* mint az összes pénzösszeg együttesét, amelyet a nem véglegesített Augur piacokon letétbe helyeztek. [21]

2. Definíció. *Parazita piacnak* definiáluk bármely olyan piacot, amely nem fizet jelentési díjat az Augur-nak, de a natív Augur piaccal összhangban véglegesíti a piacát.

3. Definíció. Definiáljuk és jelöljük I_p értékel a *parazita nyitott kamatait* mint az összes pénzt, amelyet letétbe helyeztek a parazita piacon, ami összhangban van a nem véglegesített natív Augur piaccal.

A legszélsőségesebb esetekben a támadó képes lenne minden pénzforrást felvenni minden olyan parazita piacról, amely a nem véglegesített natív Augur piacokkal összhangban kerül véglegesítésre.

1. Észrevétel. A maximális (bruttó) nyeresége a támadónak, aki sikeresen megtámadja a jósdát $I_a + I_p$.

2. A parazita nyitott kamata nem tudható

Az Augur pontosan és hatékonyan tudja mérni I_a-t. Azonban általánosságban I_p-t nem tudja, mivel számos offline parazita piac létezhet önkényesen nagy nyitott kamattal. Mivel a támadó számára a lehető legnagyobb haszon tartalmazza az ismeretlen I_p mennyiséget, ezért sohasem lehetünk teljesen biztosak abban, hogy a jós biztonságos a gazdaságilag racionális támadókkal szemben.

Ha azonban hajlandóak vagyunk azt állítani, hogy I_p ésszerűen korlátozott a gyakorlatban, akkor definiálhatjuk azokat a feltételeket, amelyek alapján kijelenthetjük hogy a jós biztonságos.

3. A támadás minimális költsége

Ezután vegyük figyelembe a jós támadásának költségét. Legyen P a REP token ára. ϵ jelöljön egy attorepet[22]. M jelölje a létező összes REP token mennyiségét (a REP „összdarabszámát"). Jelölje S azt az arányt, amely

[19] A kereskedők továbbra is kereskedhetnek ezeken a piacokon, de ezek a piacok nem véglegesíthetők az osztódási időszak végéig.

[20] Ez azonban megköveteli a támadótól, hogy *minden* részvényt birtokoljon az adott kimenetelhez és ezután a piacot azon kimenetel javára döntse el.

[21] Ez magában foglalja a külső piacokat is, amelyek jelentési díjat fizetnek az Augur-nak.

[22] Egy *attorep* az 10^{-18} REP.

M-ből átköltöztetésre kerül az igaz univerzumba az osztódás ideje alatt.

Így az SM szorzat képviseli az abszolút REP mennyiséget, ami átköltöztetésre került az igaz univerzumba az osztódás ideje alatt. Ekkor a PM a teljes piaci kapitalizációja a REP-nek.

Jelölje a támadó által választott `hamis` univerzumba átköltöztetett REP tokenek árát P_f. Figyeljük meg, hogy ha $P \leq P_f$, akkor a jós nem biztonságos gazdaságilag racionális támadókkal szemben, mert legalább ugyanolyan profitábilis lesz átköltöztetni a REP tokeneket a hamis univerzumban, mintha nem is mozgatnánk őket.

4. Becsületesség

1. Feltételezés. *Azok a riporterek akik nem támadók, sohasem fognak REP tokent* `hamis` *univerzumban átköltöztetni osztódáskor.* [23]

A tervezés szerint egy sikeres támadás a jós ellen megköveteli, hogy több REP token költözzön át osztódáskor a `hamis` univerzumba, mint az `igazba`. Feltételezzük, hogy csak a támadó fog REP tokeneket a `hamis` univerzumba vinni. A REP mennyiség, amelyet átköltöztetnek az `igaz` univerzumba SM. Ezáltal ahhoz, hogy a támadó sikerrel járjon, át kell költöztetnie legalább $SM + \epsilon$ REP-et. Az egyszerűség kedvéért el fogjuk hanyagolni ϵ-t, és azt mondjuk, hogy a sikeres támadáshoz szükséges minimális REP mennyiség az SM, amely értéke a `hamis` univerzumba való átköltöztetés előtt SMP.

Ha a támadó átköltöztet SM REP-et a jelentési időszak alatt, akkor SM mennyiségű REP-et fog kapni a gyerekuniverzumban. [24] Ha a támadó átköltöztet a `hamis` univerzumba, akkor azoknak a érméknek az értéke SMP_f-vé válik. Ezáltal a minimális költsége a támadónak $(P - P_f)SM$.

2. Észrevétel. A minimális REP mennyiség, amelyet a támadónak sikeresen a `hamis` univerzumba kell mozgatnia az osztódás során SM, amely költsége $(P - P_f)SM$.

Ne felejtsük el hogyha $S > \frac{1}{2}$, akkor a támadás *lehetetlen*, mert nincs elegendő REP az `igaz` univerzumon kívül, hogy valamely `hamis` univerzum győzhessen.

A gazdaságilag racionális támadókkal szemben az orákulum az objektív valóságnak megfelelő eredményeket könyveli el a támadó számára, ha a maximális nyereség kevesebb mint a minimális támadási költség. Az 1-es és 2-es megfigyelés alapján láthatjuk, hogy ez akkor történik amikor $S > \frac{1}{2}$ vagy $I_a + I_p < (P - P_f)SM$. Ez megadja nekünk a korábbi becsületesség definícióját.

4. Definíció. (Becsületesség) Az osztódási protokoll akkor *becsületes*, amikor $S > \frac{1}{2}$ vagy amikor $I_a + I_p < (P - P_f)SM$.

A fenti egyenlőtlenség megoldható PM-re, hogy lássuk az osztódási protokoll becsületessége és a REP piaci kapitalizációja közti kapcsolatot.

1. Tétel. *(A piaci kapitlizáció biztonságának elmélete) Az osztódási protokoll becsületes akkor és csak akkor, ha:*

1. $S > \frac{1}{2}$ *vagy*
2. $P_f < P$ *és a REP piaci kapitalizációja nagyobb, mint* $\frac{(I_a+I_p)P}{(P-P_f)S}$.

Bizonyítás. Feltételezzük, hogy az osztódási protokoll becsületes. Ekkor definíció szerint $S > \frac{1}{2}$ vagy $I_a + I_p < (P - P_f)SM$. Feltételezve, hogy $I_a + I_p < (P - P_f)SM$. Hiszen $I_a + I_p \geq 0$ és $SM > 0$, tudjuk, hogy $P_f < P$. Ekkor, ha megoldjuk $I_a + I_p < (P - P_f)SM$ PM-re, akkor láthatjuk, hogy $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Így az első irány bizonyítást nyert.

Most tegyük fel, hogy $S > \frac{1}{2}$ vagy, hogy $P_f < P$ és $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Ha $S > \frac{1}{2}$, akkor az osztódási protokoll definíció szerint becsületes. Ha $P_f < P$ és $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$, akkor megoldva az egyenlőtlenséget $I_a + I_p$-re, láthatjuk, hogy $I_a + I_p < (P - P_f)SM$, és az osztódási protokoll becsületes. □

B. A feltételezéseink és ezek következményei

Úgy hisszük, hogy a kereskedők nem fognak kereskedni olyan univerzumokban, ahol a riporterek hazudtak. Továbbá hisszük, hogy a piackészítők nem fognak fizetni azért, hogy készítsenek egy olyan Augur piacot, ahol nem történik kereskedés. Egy univerzumban, ahol nincsenek piacok vagy kereskedés, a REP nem biztosít semmilyen osztalékot a birtokosának. Ezért úgy hisszük, hogy a REP, amely `hamis` univerzumban van nem elhanyagolható piaci érték, és úgy modellezük, hogy $P_f = 0$ értéken hagyjuk.

Úgy véljük, hogy feltételezhetően legalább a meglévő REP 20%-a átköltöztetésre kerül az igaz kimenetelre a jelentési időszakban. Ezt így modellezzük: $S \geq \frac{1}{5}$. Hajlandóak vagyunk a parazita nyílt kamatozás akár 50%-át natív nyílt kamatozásként befogadni, ezért engedjük hogy $I_a \geq 2I_p$.

E feltételek szerint az 1-es elmélet azt mondja, hogy az osztódási protokoll akkor becsületes, amikor a REP piaci kapitalizációja legalább 7,5-szerese a natív kamatnak. [25]

---

[23] Előfordulhat néhány jóindulatú riporter, aki véletlenül vagy figyelmetlenségből a `hamis` univerzumba költözteti a REP tokenjét. Azonban ez a viselkedés a gyakorlatban megkülönböztethetetlen a támadóval való együttműködéstől.

[24] A gyakorlatban a támadó $1,05SM$ REP-et kap a gyerekuniverzumban az 5%-os bónusz miatt a 60 napos időszakon belül. Most elhanyagoljuk ezt 5%-os bónuszt az egyszerűség kedvéért. Egy az 5%-ot tartalmazó példát láthatsz a Cfüggelékben.

[25] További feltételezésekért és azok következményeiért lásd a B függeléket.

C. A piaci kapitalizáció lökete

Az Augur ugyanúgy kap információt a REP áráról, mint ahogy a valós világról, azaz az Augur piacon keresztül. Ez megadja a lehetőséget az Augur-nak, hogy kiszámítsa a jelenlegi piaci kapitalizációt. Az Augur emellett mérni tudja a natív nyitott kamatokat, és általa meg tudja határozni, hogy milyen piaci kapitalizációt kell megcéloznia, hogy megfeleljen az Augur becsületességi követelményeinek.

Az univerzum alapértelmezetten 1%-os jelentési díjjal indul. Ha a jelenlegi piaci kapitalizáció alacsonyabb a megcélzottnál, akkor a jelentési díj automatikusan növelésre kerül (de sosem lesz több mint 33,3%), így felfelé irányuló nyomást gyakorol a REP árára és/vagy lefelé irányuló nyomást gyakorol a natív nyitott kamatokra. Ha a jelenlegi piaci kapitalizáció a cél felett van, akkor a jelentési díj automatikusan csökkentésre kerül (de sosem lesz kevesebb mint 0,01%), így a kereskedők nem fizetnek többet, mint amennyi minimálisan szükséges ahhoz, hogy a rendszer biztonságos maradjon.

A jelentési díjak az alábbi módon kerülnek meghatározásra. Legyen r a jelentési díj a korábbi ablaktól számítva, legyen t a célzott piaci kapitalizáció, illetve c legyen a jelenlegi piaci kapitalizáció. Ekkor a jelentési díj a jelenlegi díjablakban a következőképpen alakul: $\max\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10{,}000}\right\}$.

D. Az osztódás fenyegetésének kihasználása

Ahogy azt fentebb említettük, az osztódás bomlasztó és lassú módja a piac véglegesítésének. Az osztódás használata helyett az Augur inkább az osztódás *fenyegetését* használja ki a piacok hatékony lezárására.

Emlékezzünk vissza arra, hogy minden olyan letét, amely sikeresen vitatja a kimenetelt a piac végső kimenetele felé 50%-os ROI-ban részesül. [26] Osztódás esetén bármely REP, amely a piac hamis kimeneteleire helyeztek, elveszti a gazdasági értékét, míg azok a REP tokenek, amelyek a piac igaz kimenetelére kerültek 50%-kal növekednek (függetlenül az osztódás kimenetelétől). Ezáltal, ha osztódásra kerül a sor, akkor a REP birtokosok, akik vitatják a hamis kimeneteleket az igazi kimenetelekkel szemben mindig jobban jönnek ki, mint azok a REP tulajdonosok, akik a hamis kimenetelre fogadtak, mivel ők el fogják veszíteni a REP tokenjük gazdasági értékét.

Úgy hisszük, hogy ez elegendő ahhoz, hogy garantáljuk, hogy minden hamis kísérleti eredmény sikeresen vitatásra kerüljön.

[26] A végleges piaci kimenettel azonos univerzumban létező REP-ben mérve. Lásd a 3-as szakaszt az A függelékben.

III. POTENCIÁLIS PROBLÉMÁK ÉS KOCKÁZATOK

A. Parazita piacok

Emlékeztetőül: a parazita piac olyan piac, amely nem fizet jelentési díjat az Augur-nak, de az Augur piaccal összhangban záródik le. Mivel a parazita piacoknak nincsenek fizetendő riporterei, ugyanazt a szolgáltatást tudják nyújtani az Augur piaci áraihoz képest alacsonyabban. Ennek komoly következményei lehetnek az Augur osztódási protokoll becsületességét illetően.

Különösen, ha a parazita piacok elvonzzák a kereskedési kamatokat az Augur-tól, mert ekkor az Augur riporterei kevesebb jelentési díjban részesülnek. Ez lefelé irányuló nyomást gyakorol a REP piaci kapitalizációjára. Ha a REP piaci kapitalizációja túl alacsony szintre süllyed, akkor az osztódási protokoll becsületessége veszélybe kerül (1-es elmélet). Ennek eredményeképpen a parazita piacoknak megvan a potenciális fenyegetése a hosszú távú Augur piac fenntartására, így ezek határozott ellenezése szükséges.

A legjobb védelmünk a parazita piacokkal szemben az az, hogy olyan olcsóvá tesszük a kereskedést az Augur platformon, amennyire csak lehetséges (fenntartva a jósda becsületességét), azért hogy csökkentsük a parazita piacok futtatásának nyereségességét.

B. A nyitott kamatok volatilitása

A nyitott kamatok nagy, hirtelen és váratlan növekedése (mint amelyeket láthatunk a népszerű sportesemények esetén is) a piaci kapitalizáció gyors növekedését eredményezi az Augur becsületességi osztódási protokollja számára (1-es elmélet). Amikor a piaci kapitalizáció követelménye meghaladja a pillanatnyi piaci kapitalizációt, akkor megvan a kockázata annak, hogy a gazdaságilag racionális támadók osztódást indítanak, hogy helytelen eredményt véglegesítsenek. Ilyenkor az Augur megpróbálja a piaci kapitalizációt felfelé mozgatni (lásd a II C fejezetet), azonban ezek a löketek reaktívak és csak egyszer állíthatók hetente a díjablak idején.

Érdemes megjegyezni, hogy habár a spekulánsok akik tanúi a nyitott kamatok hirtelen növekedésének talán elkezdenek REP-et vásárolni a reakciós piaci kapitalizáció löketre számítva, és így növelik a REP piaci kapitalizációját, feltehetően addig a pontig, ahol az osztódási protokoll becsületessége továbbá már nem fenyegetett. Így tehát, a jós fenyegetettségének ideje nem lesz elegendően hosszú a támadók számára, hogy sikeresen kihasználják a sebezhetőséget.

C. Inkonzisztens vagy rosszindulatú eredményforrások

A piac készítője annak elkészítése közben eredmény forrást kell hogy válasszon a riportereknek, akiknek ezt kell használniuk a kérdéses esemény kimenetelének jelentésére. Ha a piac készítője inkonzisztens vagy rosszindulatú eredményforrást választ, akkor a becsületes riporterek pénz veszíthetnek.

Tegyük fel például, hogy a szóbanforgó piacnak van `A` és `B` kimenetele és a piac készítője Serena kiválasztotta a saját weboldalát az `attacker.com`-ot, mint eredményforrást. Miután a piaci esemény befejeződik, Serena, aki egyben a piac kijelölt riportere is, jelenti `A` kimenetelt és frissíti az `attacker.com`-ot, hogy jelezze, hogy `B` kimenetel a valós eredmény. A becsületes riporterek, akik rámennek az `attacker.com`-ra látni fogják, hogy a kezdeti riport hibás és az első vitakör során sikeresen el kell hogy vessék a kísérleti eredményt a `B` kimenetel javára. Serena frissíti az `attacker.com`-ot, hogy jelezze, hogy az `A` kimenetel a korrekt eredmény, majd ezután a piac belép a második vitakörbe. A riporterek ekkor újra ellenőrzik az `attacker.com`-ot és látni fogják, hogy a kísérleti eredmény (vagyis `B` kimenetel) hibás, és sikeresen leváltják azt. Serena ezután újra és újra megismétli a korábbi cselekedeteit, míg a piac véglegesítődik. Nem számít, hogy a piac milyen eredményen végződik, néhány becsületes riporter el fogja veszíteni a pénzét.

Ennek a támadásnak számtalan variációja létezik. A a kétséges eredményforrásokkal rendelkező piacok elutasítása nem elegendő abban az esetben ha, egy ilyen piac osztódásba kezd, akkor az összes REP tulajdonosnak ki kell választania azt a gyerekuniverzumot, amelyekbe a REP-jét költözteti. A riportereknek ébernek kell lenniük a piacokon a kétséges eredményforrások miatt. Az ilyen piacokat nyilvánosan azonosítani kell, hogy a riporterek összehangolhassák cselekedeteiket, és így az ilyen piacok érvénytelenként végződjenek.

D. Önreferenciás orákulum lekérdezés

A piac, amely az Augur orákulum jövőbeli viselkedése alapján kereskedik nem kívánt eredményt gyakorolhat az orákulumra [11]. Például vegyünk fontolóra egy olyan piacot, ahol a következő kérdés alapján kereskednek: „Lesz olyan kijelölt riporter aki elmulasztja a riport leadását a háromnapos jelentési időszakban 2018. december 31. előtt?" A `nem` kimenetelre helyezett tétek egyfajta rossz ösztönzésként hatnak a kijelölt riporterekre, hogy szándékosan elmulasszák a jelentést. Ha egy kijelölt riporter fel tud vásárolni elegendő `igen` részvényt elég alacsony áron, hogy kompenzálja a veszteségét a jelentés elmulasztása kötvényből, akkor szándékosan elmulaszthatja a jelentést.

Ha a piaci kapitalizációja a REP-nek elegendően nagy (1-es elmélet), akkor ezek az önreferenciális orákulum lekérdezések nem fogják fenyegetni az osztódási protokoll becsületességét. Azonban esetlegesen negatívan fogják befolyásolni az Augur teljesítményét, úgy hogy a piac véglegesítését késleltetik. Habár a piacok megfelelően véglegesednek, ez a fajta viselkedés bomlasztó és nem kívánatos.

E. Bizonytalan osztódási részvétel

Nem tudhatjuk előre, hogy mennyi REP token kerül átköltöztetése az `igaz` univerzumba az osztódás ideje alatt, így azt sem tudhatjuk előre, hogy vajon a piaci kapitalizáció elegendően nagy lesz-e a jósnak, hogy becsületes maradjon (1-es elmélet). Úgy hisszük, hogy az osztódási protokoll becsületessége nem lehet erősebb, mint a hitünk a feltételezésünkben a becsületes részvétel alsó határáráról az osztódás ideje alatt. Feltételezzük, hogy legalább az összes REP 20%-a átkerül az `igaz` gyerekuniverzumba az osztódás alatt, de ezt nem tudjuk garantálni.

Az Augur osztódása egy fontos tekintetben különbözik egy blokklánc szétágazásától. Egy blokklánc szétválása után a felhasználó, aki birtokolta az érmét a szülőláncon, az ezek után birtokolni fogja az érmét mindkettő láncon. A visszajátszás-támadásokat figyelmen kívül hagyva, a blokklánc elágazás alacsony kockázatot jelent a felhasználókra. Egy Augur osztódás után azonban a felhasználó, aki birtokolja a REP-et a szülőuniverzumban átköltözhetheti azt egy gyerekuniverzumba. Ha a felhasználó egy a győztestől eltérő univerzumba költözteti az érmét, akkor az elveszti értékét. Így az osztódás ideje alatt az átköltöztetés kockázatos a felhasználók számára, mely így megakadályozhatja a részvételt az osztódásban.

Ennek a kockázatnak a kompenzálása és az osztódási periódusokban való részvétel ösztönzésére minden olyan REP birtokos, aki átköltözteti a kijelölt 60 napos időszak alatt a tokenjeit 5%-os további REP-et fog kapni a gyerekuniverzumba, amelybe költöztette azt (lásd I C 9 fejezet). Azonban nem tudhatjuk előre, hogy vajon ez az 5%-os bónusz elegendő lesz-e arra, hogy kompenzálja a kockázatot és ösztönözze a részvételt az osztódásban.

F. Zavaros vagy szubjektív piacok

Csak olyan események megfelelőek az Augur piacok számára, amelyeknek objektíven tudható a kimenetele. Ha a riporterek úgy hiszik, hogy a piac nem megfelelő a platformhoz, például mert az zavaros, szubjektív vagy a kimenetel nem tudható az esemény végeztével, akkor jelenteniük kell a piacot, mint `érvénytelen` piac. Az `érvénytelenként` véglegesített piacon a kereskedők minden egyes kimenetelre azonos mértékben kerülnek kifizetésre, míg a skalárpiacokon a kereskedők a piaci minimum és maximum ár közötti értéken lesznek kifizetve.

Lehetséges elképzelni olyan piacot, ahol néhány riporter biztos benne hogy az `A` kimenetel, míg más riporterek

biztosak benne, hogy a B kimenetel a jó eredmény. Például 2016-ban a TradeSparts megengedte a felhasználóinak, hogy spekuláljanak, hogy vajon Észak Korea kilövi-e a ballisztikus rakétáit 2016. júliusa előtt úgy, hogy azok a légterükön kívül landolnak. 2016. július 5-én Észak Korea sikeresen kilőtte a ballisztikus rakétáit, melyek a saját légterükön kívül landoltak és ezt az eseményt széleskörben közvetítette a világsajtó és ezt számos amerikai kormányzati forrás megerősítette. Azonban az Amerikai Védelmiügyi Minisztérium nem erősítette meg az eseményt úgy, ahogy az szükséges lett volna a TradeSports szerződésében. A TradeSports úgy zárta az eseményt, hogy a szerződés feltételei nem találkoztak és ez alapján fizetett. [27]

Ez egy olyan eset, amikor a piac lelke, vagyis a rakéták kilövésének megjóslása tisztán teljesült, de a külső megerősítés, vagyis ebben az esetben az Amerikai Védelmi Minisztérium megerősítése nem. A TradeSports egy centralizált weboldal, amely egyoldalú döntést hozhatott a piac kimenetéről. Ha hasonló szituáció keletkezik egy Augur piacon, a REP birtokosoknak különböző véleménye lehet, hogy hogyan is záródjon a piac és ez alapján helyezhetik el a tokenjeiket. A legrosszabb esetben ez osztódással járhat, ahol a REP mennyiség nagyobb lehet, mint 0 több gyerekuniverzumban is.

KÖSZÖNETNYILVÁNÍTÁS

Köszönjük Abraham Othman, Alex Chapman, Serena Randolph, Tom Haile, George Hotz, Scott Bigelow és Peronet Despeignes hasznos visszajelzéseit és javaslatait.

[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.

[27] Lásd a https://en.wikipedia.org/wiki/Intrade#Disputes linket a további részletekért.

Függelék A: Véglegesítési idő és újraelosztás

Kezdjük néhény jelöléssel, definícióval és észrevétellel.

5. Definíció. Az adott M piacon legyen Ω_M az M piac kimenetel tere (vagy kimeneteinek együttese).

6. Definíció. Ha $n \geq 1$ és $\omega \in \Omega_M$, akkor jelölje $S(\omega, n)$ a teljes letét összegét az ω kimenetelen az n. vitakör elején. Ez tartalmazni fogja az összes letétet az összes sikeres vitakötvényből, amelyek ω-ra lettek elhelyezve.

7. Definíció. Ha $n \geq 1$ és $\omega \in \Omega_M$, akkor jelölje $S(\overline{\omega}, n)$ a teljes letéti összeget Ω_M-ben, *kivéve* az ω-ra elhelyezetteket az n. vitakör elején:

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

8. Definíció. Ha $n \geq 1$, akkor jelölje A_n az összes kimenetelre helyezett letéteket az M piacon az n. vitakör elején:

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

3. Észrevétel. Ez megfelel az $A_n - S(\omega, n) = S(\overline{\omega}, n)$ egyenletnek.

9. Definíció. Ha $n \geq 1$, akkor jelölje $\hat{\omega}_n$ a kísérleti kimenetelt az n. vitakör elején. Példaként $\hat{\omega}_1$ az a kimenetel, amelyet az első riporter jelentett.

10. Definíció. Ha $n \geq 1$ és $\omega \neq \hat{\omega}_n$, akkor jelölje $B(\omega, n)$ a szükséges letét mennyiségét, amely kitölti a vitakötvényt az ω kimenetelhez az n. vitakörben.

Emlékezzünk vissza, hogy a szükséges letét mennyisége, amely kitölti a vitakötvényt az ω kimenethez az n. vitakörben, ha $\omega \neq \hat{\omega}_n$ az 1-es egyenletből adódik ki: $B(\omega, n) = 2A_n - 3S(\omega, n)$.

4. Észrevétel. Ha a vitakötvény sikeresen kitöltésre került az ω kimenetelhez az n. vitakör során, akkor $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. Ez megadja az egyetlen sikeres vitaletétet, amely az új letét lehet az ω kimenetelen az n. vitakör végén.

5. Észrevétel. Minden $\omega \neq \hat{\omega}_n$ esetén $S(\omega, n-1) = S(\omega, n)$. Ez azt jelenti, hogy ha a vitakötvény nem teljesen került kitöltésre az ω kimenetellel, akkor nem adódik további letét az ω kimenetelhez a következő vitakör elején. Ez azért történik, mert a sikertelen vita esetén az összes elhelyezettt letét visszatérítésre kerül a felhasználóknak a vitakör végén.

6. Észrevétel. Minden $n \geq 2$ esetén $A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$. Ez azt jelenti, hogy a teljes letét összege az összes kimenetelen a vitakör elején egyszerűen az összes letét a korábbi vitakörből és a sikeres vitaletétek összege. Minden más letét visszakerül a felhasználókhoz a vitakör végén.

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

Bizonyítás. Tegyük fel, hogy a piac belép az n. vitakörbe, ahol $n \geq 2$. Az $n-1$. vitakör során az $\hat{\omega}_{n-1}$ kimenetel sikeresen vitatásra kellett, hogy kerüljön az $\hat{\omega}_n$ javára. Az 1-es egyenlet szerint, a vitakötvény mérete $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Használva a 3-as észrevételt, ezt írhatjuk az alábbi alakban is:

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

Tudjuk, hogy a vitakötvény sikeresen kitöltődött az $n-1$. vitakörben. Használva a 4-es észrevételt, láthatjuk, hogy $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. Az 5-ös észrevétel megadja, hogy a teljes letétmennyiség, amelyet elhelyeztek $\overline{\hat{\omega}_n}$ nem változott $n-1$ és n vitakör között, azaz $2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$. Így az A1 egyenlet $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$-re egyszerűsödik. □

3. Tétel. *Bármely REP birtokos, aki sikeresn vitatja a kimenetelt a végső kimenetel javára 50%-os ROI-ban részesül a letétje után (a piaci végeredménnyel megegyező univerzumban mért REP-ben), ha a piac nem kerül megzavarásra egy másik piac osztódása által.*

Bizonyítás. Azok a felhasználók, akik az osztódás ideje alatt sikeresen töltenek ki vitakötvényt a piac végső döntésével összhangban 50%-os jutalomban (az osztódás ideje alatt létrehozott) részesülnek a vitaletétük után a megfelelő gyerekuniverzumban. Így abban az esetben, amikor a piac osztódásra kényszerül, az elmélet azonnal igazzá válik.

Most képzeljünk el egy piacot, amely osztódás nélkül végződik és nem zavarja meg más piacok osztódása.

Jelöljük a piac végső döntését ω_{Final}-lel és feltételezzük, hogy a piac megoldódik az n. vitakör végén, úgy hogy $n \geq 2$. Ez azt jelenti, hogy a kísérleti kimenetel az n. körben ω_{Final}, és a kimenetelt nem vitatták sikeresen az n. vitakörben. Más szóval: $\hat{\omega}_n = \omega_{\text{Final}}$. Ekkor a 2-es lemma alapján tudjuk, hogy $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$.

Mivel a piac megoldódott az n. kör végén, ezért további letét nem adódik az eredményekhez. A fenti egyenlet megadja a végső letétek mennyiségét a piac végső kimenetelén, azaz ω_{Final}-n, és az összes többi piaci kimenetelen, azaz $\overline{\omega_{\text{Final}}}$-n. Jegyezzük meg, hogy pontosan kétszer annyi letét van a piac végső eredményén, mint az összes többin együttvéve.

Az Augur szétosztja az összes letétet, amely nem a piac végső eredményére lett helyezve azon felhasználók között, akik ω_{Final}-re fogadtak az elhelyezett REP mennyiséggükkel arányosan. Így a felhasználók, akik sikeresen betöltötték a vitakötvényt az ω_{Final} javára 50%-os ROI-ban részesülnek. □

Most vegyük fontolóra, hogy maximálisan hány vitakör szükséges egy piac lezárásához. Az 1-es egyenlet megoldása a lehető legkisebb, amikor ω nem a kísérleti kimenetel, amely elindítja a vitakört. A 2-es lemma maga után vonja, hogy az a nem kísérleti kimenetel, amely a legnagyobb letétet gyűjti az a korábbi vitakör kísérleti

eredménye. Ezáltal, a lehetséges legkisebb vitakötvény méret, amely sikeres lehet az n. vitakörben, úgy, hogy $n \geq 2$, az $B(\hat{\omega}_{n-1}, n)$.

Más szóval, a vitakötvény mérete a *leglassabban* növekszik, ha a két kimenetel felváltva győz a vitakörökben. Ez azt eredményezi, hogy az osztódáshoz szükséges vitakörök száma akkor *maximális*, ha a két eredmény felváltva győz a körökben. Így meg tudjuk határozni a maximális vitakörök számát az osztódásig. Most ezt az esetet vizsgáljuk meg.

Feltételezzük, hogy minden sikeres vitakötvény a korábbi vitakör kísérleti eredményére töltődött be. Ekkor a két kísérleti kimenetel, amelyek felváltva győztek $\hat{\omega}_1$ és $\hat{\omega}_2$.

7. Észrevétel. A két egymást folyamatosan legyőző kísérleti eredmény esetén $\hat{\omega}_n = \hat{\omega}_{n-2}$, minden $n \geq 3$ esetén.

11. Definíció. Jelöljük d-vel a letét mennyiségét, amelyet elhelyeztek $\hat{\omega}_1$-en a kezdeti jelentéskor. Mivel a kísérleti kimenetel minden egyes körben ismert, ezért egyszerűsíthetjük a vitakötvény méretére vonatkozó jelölést. Definiáljuk a B_n rövidítést, mely a szükséges kötvényméretet adja meg az n. vitakörben. Így $B_1 = 2d$ és $B_n = B(\hat{\omega}_{n-1}, n)$ minden $n \geq 2$ esetén. Ez egyszerűbb olvasatot és megértést fog lehetővé tenni.

8. Észrevétel. Amikor a két kísérleti kimenetel egymást váltogatva győz a vitakörökben $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ minden $n \geq 3$ esetén. (Ez azt jelenti, hogy minden sikeres vitakötvény hozzáadódik a megfelelő kimenethez.)

4. Lemma. *Ha a két kísérleti kimenetel felváltva vitatásra kerül, akkor minden n esetén, amikor* $n \geq 3$*:*

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

Bizonyítás. (n indukciójával)

Feltételezzük, hogy a két kisérleti kimenetel felváltva vitatott.

(Alapeset) Az 1-es egyenlet alapján a következő megfigyeléseket tehetjük:

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

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, tehát az első része a lemmának fennáll $n = 3$ esetén.

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, tehát a lemma második része is fennáll $n = 3$ esetén.

$B_3 = 6d = 3d2^{3-2}$, így a lemma harmadik része is fennáll $n = 3$ esetén.

Így a lemma teljesen igaz $n = 3$ alapeset esetén.

(Indukció) Tegyük fel, hogy a lemma igaz minden n-re, ami $3 \leq n \leq k$ van. Be akarjuk bizonyítani, hogy a lemma igaz marad $n = k + 1$ esetén is. Ez azt jelenti, hogy:

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

(b) $A_{k+1} = 2B_k$ és

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

Először bizonyítsuk be az (a) részt. A 8-as megfigyelés alapján:

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

A 7-es megfigyelés alapján a fenti egyenletet írhatjuk a következőképpen:

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

Az indukciós hipotézis szerint átírhatjuk a jobb oldali $S(\hat{\omega}_{k-2}, k-1)$-t $\frac{2}{3}B_{k-2}$ alakra, amivel az alábbi alakot kapjuk:

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

Az indukciós hipotézis alapján átírhatjuk a B_{k-2}-t mint $3d2^{k-4}$ és B_{k-1} as $3d2^{k-3}$:

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

Alkalmazva a 7-es észrevételt a bal oldalra, a következőt kapjuk:

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

Végül, vegyük észre, hogy a fenti egyenlet és az indukciós hipotézis $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. Ez bebizonyítja az (a) részt.

Ezután bizonyítsuk be a (b) részt. A 6-os észrevétel szerint:

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

Az indukciós hipotézis alapján $A_k = 2B_{k-1}$, így a fenti egyenlet átírható az alábbi alakba:

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

Szintén az indukciós hipotézis alapján $B_{k-1} = 3d2^{k-3}$, így a jobb oldal egyszerűsíthető az alábbi formába:

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

Az indukciós hipotézis alapján $B_k = 3d2^{k-2}$, tehát a jobb oldal átírható az alábbi formába

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

és így a (b) rész bebizonyításra került.

Végül bizonyítsuk be a (c) részt is. Az 1-es egyenlet szerint:

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

A 8-as észrevétel alapján írhatjuk $S(\hat{\omega}_k, k+1)$-t a következő formában $S(\hat{\omega}_k, k-1) + B_{k-1}$, amivel az alábbi egyenletet kapjuk:

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

A 7-es megfigyelés szerint $\hat{\omega}_k = \hat{\omega}_{k-2}$:

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

A 6-os észrevételt alkalmazva $A_{k+1} = A_k + B_k$ és így:

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

Az indukciós hipotézis szerint $A_k = 2B_{k-1}$ és $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$:

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

Szintén az indukciós hipotézis szerint $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ és $B_{k-2} = 3d2^{k-4}$. Elvégezve a behelyettesítést és az egyszerűsítést:

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

Ez bizonyítja a (c) részt, és így a lemmát is. □

5. Tétel. *Ha nem zavarja meg a piacot más piacok osztódása, akkor az maximum 20 vitakörön eshet át a véglegesítés vagy az osztódás előtt.*

Bizonyítás. Feltételezzük, hogy a piacot nem zavarja meg más piac osztódása. Ekkor, ahogy az fent is látható, tudjuk, hogy a piac osztódásához szükséges vitakörök száma maximalizált, amikor a két kimenetel felváltva győz. A 4-es lemma 3. része alapján ebben az esetben a vitakötvény szükséges mérete a sikeres kisérleti kimenetel vitatásához az $n.$ körben az alábbi módon számítható: $3d2^{n-2}$, ahol d a kezdeti riporthoz letétbe helyezett összeg.

Tudjuk, hogy az osztódás akkor veszi kezdetét, amikor a vitakötvény mérete elérte az öszes REP legalább 2,5%-át. Továbbá, azt is tudjuk, hogy 11 millió REP token létezik. Így az osztódás akkor veszi kezdetét, ha a vitakötvény mérete 275.000 REP lesz. Szintén tudjuk, hogy $d \geq 0,35$ REP, mert a kezdeti riporton elhelyezett minimális letét az $0,35$ REP[28].

Megoldva a $3(0,35)2^{n-2} > 275.000$, úgy hogy $n \in \mathbb{Z}$ $n \geq 20$ kapunk. Így tehát garantálhatjuk, hogy a piac lezáródik vagy osztódásba kezd legfeljebb 20 vitakör után. □

[28]Lásd az E 2 és az E 3 függeléket

Függelék B: Alternatív feltételezések és azok következményei

Emlékezzünk, hogy:

- S az összes REP aránya, amely az `igaz` univerzumba lett átköltöztetve az osztódás alatt,
- P a REP ára az `igaz` univerzumban,
- P_f annak a REP-nek az ára, amely a támadó által választott `hamis` univerzumba lett költöztetve
- I_a az Augur natív nyitott kamata
- I_p a parazita nyitott kamat

Az Augur bizonyos feltételezésekkel él az S, P_f és I_p-vel kapcsolatban, hogy elérje a megcélzott piaci kapitalizációt. Az Augur feltételezi, hogy legalább az összes REP 20%-a át lesz költöztetve az `igaz` univerzumba az osztódás alatt. A REP-nek, amely a `hamis` univerzumba került átköltöztetésre nincs elhanyagolható értéke, illetve a parazita nyitott kamatok is ki fogják tenni legalább a felét a natív nyitott kamatnak. Más szavakkal: $S \geq 0,2$, $P_f = 0$ és $I_a \geq 2I_p$. Ezeket feltételezve az 1-es elmélet megadja számunkra, hogy az osztódási protokoll becsületes, amikor a REP piaci kapitalizációja több, mint 7,5-szerese a natív nyitott kamatnak.

Meghatározhatod a saját feltételezésedet S, P_f és I_p-ről, hogy megtudd mekkora piaci kapitalizáció szükséges ahhoz, hogy a jós becsületes legyen a gyakorlatban. A kényelem kedvéért megadunk néhány alternatív forgatókönyvet.

1. Forgatókönyv. A létező REP több, mint 50%-a átköltöztetésre kerül az `igaz` univerzumba az osztódás ideje alatt. Ebben az esetben P_f és I_p nem számít. Mivel $S > \frac{1}{2}$, az osztódási protokoll becsületes, nem számít mekkora a piaci kapitalizáció. Nem marad elegendő REP a piacon ahhoz, hogy a támadó sikerrel járjon.

2. Forgatókönyv. A létező REP 48%-a átköltöztetésre kerül az `igaz` univerzumba az osztódás ideje alatt és nincs parazita piac, illetve azoknak a REP tokeneknek, amik a `hamis` univerzumba lettek költöztetve nincs értékük. Ebben az esetben $S = 0,48$, $I_p = 0$ és $P_f = 0$. Ezekkel a feltételezésekkel a REP piaci kapitalizációja több, mint kétszer nagyobb kell hogy legyen, mint a natív nyitott kamat ahhoz, hogy az osztódási protokoll becsületes legyen.

3. Forgatókönyv. A létező REP 20%-a átköltöztetésre kerül az `igaz` univerzumba az osztódás ideje alatt, a parazita nyitott kamat megegyezik a natív nyitott kamattal, illetve a REP tokenek, amik a `hamis` univerzumba lettek költöztetve az `igaz` univerzum árához képest 5%-os árfolyamon kereskedhetők. Ezesetben $S = 0,2$, $I_p = I_a$ és $P_f = 0,05P$. A fenti feltételezésekkel a REP piaci kapitalizációjának 10,5-szer nagyobbnak kell lennie, mint a natív nyitott kamat ahhoz, hogy az osztódási protokoll becsületes legyen.

4. Forgatókönyv. A létező REP csak 5%-a kerül átköltöztetésre az `igaz` univerzumba az osztódás ideje alatt, a parazita nyitott kamat kétszerese a natív nyitott kamatnak, illetve a REP tokenek, amik a `hamis` univerzumba lettek költöztetve az `igaz` univerzum árához képest 5%-os árfolyamon kereskedhetők. Ekkor $S = 0,05$, $I_p = 2I_a$ és $P_f = 0,05P$. A fenti feltételezésekkel a REP piaci kapitalizációjának 63-szor nagyobbnak kell lennie, mint a natív nyitott kamat ahhoz, hogy az osztódási protokoll becsületes legyen.

Függelék C: A korai átköltöztetési bónusz hatása az osztódási protokoll becsületességére

Az egyszerűség kedvéért elhanyagoljuk az 5%-os korai átköltöztetési bónuszt, amikor az osztódási protokoll becsületességét tárgyaljuk meg. Itt idézzük fel az 1-es elméletet.

Mint korábban is, az `igaz` univerzumba költöztetett REP mennyiséget a jelentési időszakban SM-mel jelöljük. Így, hogy a támadó sikerrel járjon, szüksége van legalább $SM + \epsilon$ REP átköltöztetésére a `hamis` univerzumba, amely értéke a költöztetés előtt $(SM + \epsilon)P$.

Ha a támadó sikeresen átköltöztet $SM + \epsilon$ REP-et a `hamis` univerzumba a jelentési időszakban, akkor $1,05(SM + \epsilon)$ REP-et fog kapni az adott gyerekuniverzumban. A P_f definiciója szerint ezen érmék értéke az $1,05(SM + \epsilon)P_f$ egyenlet alapján számítható. Így a támadó minimális költsége $(SM + \epsilon)P - 1,05(SM + \epsilon)P_f$ lesz, amely kifejezhető, mint $(SM + \epsilon)(P - 1,05P_f)$.

Ahogy azt korábban is jelöltük, a maximális (bruttó) haszna a támadónak $I_a + I_p$. Ezért azt mondhatjuk, hogy az osztódási protokoll becsületes, ha $S > \frac{1}{2}$ vagy:

$$I_a + I_p < (SM + \epsilon)(P - 1,05P_f) \tag{C1}$$

A fenti egyenlőtlenséget megoldva a piaci kapitalizációra, azaz PM-re, láthatjuk, hogy az osztódási protokoll akkor és csak akkor becsületes, ha:

1. $S > \frac{1}{2}$ vagy
2. $1,05P_f < P$ és a REP piaci kapitalizációja nagyobb, mint a $\frac{P(I_a+I_p-\epsilon(P-1,05P_f))}{S(P-1,05P_f)}$

Ahogy láthatjuk, a korai átköltöztetési bónusz hatása a piaci kapitalizáció követelményeire nagyon alacsony.

Függelék D: A korai átköltöztetési bónusz hatása az osztódás minimális költségére

Hogy ösztönözzük a nagyobb részvételt az osztódásban minden token birtokos, aki átköltözteti a REP-jét 60 napon belül, 5%-os REP bónuszban részesül a gyerekuniverzumban, ahova azt költöztette. Ezt a jutalmat valutainflációval fizetjük.

Ez a bónusz egy rossz ösztönzéssé válhat, ha az osztódás kezdeményezési költsége túlságosan alacsony. Különösképpen, ha a támadó több előnyt szerez az 5%-os bónuszból, mint amennyit veszthet az osztódás kezdeményezésével. Ezt a támadást *inflációs fejési támadásnak* nevezzük. Ez nem okozza a jós helytelen döntését, de bomlasztó osztódásokhoz vezet.

Hogy megakadályozzuk ezt a viselkedést, az Augur-nak biztosnak kell lenni abban, hogy az osztódás kezdeményezési költsége nagyobb, mint az 5%-os inflációs bónuszból nyerhető maximális érték. A továbbiakban levezetjük az osztódás elindításának az alsó határköltségét, annak érdekében, hogy megakadályozzuk ezt a támadásformát.

Jelöljük P_0-al az osztódás előtti REP token árat, illetve P_1-el az osztódás utáni árat. Legyen M_0 a pénztartalék az osztódás előtt és M_1 azután. Jelöljük S-el az M_0 azon részét, amely az `igaz` univerzumba került átköltöztetésre az osztódás ideje alatt. b jelölje azt a REP mennyiséget, ami gazdaságilag elégetésre kerül (azt amit a `hamis` kimenetelre tettek) az osztódás megkezdésekor. Feltételezzük, hogy $b > 1$.

Ennek a szakasznak a céljaként azt a konzervatív felvetést állítjuk, hogy minden REP-et, amelyet átköltöztetnek az osztódás ideje alatt, a támadó kontrollál. Továbbá feltételezzük (mert ez csökkenti a támadó támadási költségét), hogy minden REP az `igaz` univerumba kerül átköltöztetésre.

Ezzel a jelöléssel SM_0 az a REP mennyiség, ami mozgatásra került az osztódás alatt, míg $(1 - S)M_0$ az a mennyiség, amely *nem*.

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

Amikor SM_0 REP kerül átköltöztetésre, akkor összesen $0,05SM_0$ REP kerül készítésre az inflációval:

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

Az infláció hatására fókuszálva, illetve az egyszerűség kedvéért feltételezzük, hogy a piaci kaptalizáció megegyezik az osztódás előtt és után [29]:

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

D1-et és D2-t behelyettesítve D3-ba, majd ezt egyszerűsítve kapjuk:

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

A támadó (bruttó) nyeresége az osztódás kezdeményezéséből és a korai átköltöztetési bónuszból az átköltöztetés utáni REP értéke minusz az átköltöztetés előtti értéke:

$$1,05SM_0P_1 - SM_0P_0 \tag{D5}$$

[29] Úgy gondoljuk, hogy ez konzervatív megközelítés. A gyakorlatban a piaci kapitalizáció várhatóan csökkeni fog.

D4-et behelyettesítve a D5-be egy alternatív kifejezést kapunk a támadó (bruttó) nyereségére:

$$1,05SM_0\frac{20P_0}{20+S} - SM_0P_0 \tag{D6}$$

Emlékezzünk vissza, hogy b az a REP mennyiség, amit gazdaságilag el kell égetni az osztódás megkezdéséhez. Így az osztódás kezdeményezési költsége bP_0. Ekkor az osztódás indításáért fizetett költség azért, hogy megszerezzük a korai átköltöztetési bónuszt akkor éri meg, amikor a következő egyenlőtlenség kielégíthető:

$$0 < 1,05SM_0\frac{20P_0}{20+S} - SM_0P_0 - bP_0 \tag{D7}$$

Észlelve, hogy $P_0 > 0$ és $S \neq -20$, ezt meg tudjuk oldani b-re és így láthatjuk, hogy a támadás akkor profitábilis, ha:

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

Ahhoz, hogy az Augur megakadályozza a rossz ösztönzést, az alábbi egyenlőtlenséget kell kialakítania:

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

Észrevéve, hogy S a $[0,1]$ intervallum között van limitálva, láthatjuk, hogy a D9-es egyenlőtlenség jobb oldala akkor maximális, ha $S = 2\sqrt{105} - 20 \approx 0,4939$. Ez azt jelenti, hogy a támadás akkor a legprofitábilisabb, amikor kb. a létező összes REP 49,39%-a átköltöztetésre kerül az osztódás alatt. Ezt a konzervatív értéket fogjuk használni S-re.[30]

Behelyettesítve az $S = 0,4939$-et a D9-be azt kapjuk, hogy $b \geq 0,012197M_0$. Így ha az osztódás kezdeményezési költsége legalább 1,2197%-a az összes REP-nek, akkor az inflációs fejési támadás nem profitábilis.

Emlékezzünk vissza, hogy az osztódás csak a vitakötvény legalább 2,5%-os kitöltése után kezdeményezhető. Feltételezzük, hogy egy ilyen vitakötvény kitöltésre került az ω kimenetelre és az osztódás megkezdődik. Az ω kimenetel vagy igaz, vagy nem.

Ha az ω kimenetel hamis, akkor a létező REP mennyiség legalább 2,5% hamis kimenetelen lett elhelyezve és elégetésre kerül. Így az inflációs fejés nem profitábilis, ha ω hamis.

Ha ω igaz, akkor a 2-es lemma alapján az összes REP legalább 1,25%-a lett elhelyezve a hamis kimenetelen, ami így elégetésre kerül. Így az inflációs fejés nem profitábilis, ha ω igaz.

Ez az oka annak, hogy a vitakötvénynek legalább az összes REP 2,5%-ával kell betöltődni a sikeres osztódáshoz.

[30] A gyakorlatban a támadó nem tudja megakadályozni, hogy más résztvevők is átköltöztessék a REP tokenjeiket az osztódás alatt, így azt sem tudja garantálni, hogy az S nem fogja átlépni az ideális 0,4939-es értéket. Azonban, mivel a legrosszabb helyzetet feltételezzük az $S = 0,4939$-et fogjuk használni.

Függelék E: Kötvényméret állítások

Az érvényességi kötvény, a jelentés elmulasztása REP kötvény és a kijelölt riporterek letétje dinamikusan állítódik a korábbi díjablak résztvevőinek viselkedése alapján. Most bemutatjuk, hogy hogyan állítjuk ezeket az értékeket.

Definiáljuk az f függvényt az alábbi szakaszon $f : [0,1] \to [\frac{1}{2}, 2]$ by:[31]

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

Az f függvény az állításban használt szorzó meghatározására szolgál, ahogy azt alább kifejtjük. Tömören: ha a kéretlen viselkedés az esetek pontosan 1%-ában történt a korábbi díjablak idején, akkor a kötvényméret változatlan marad. Ha ritkábban történt, akkor a kötvényméret a felével csökken. Ha gyakoribb volt, akkor 2-es szorzóval növekszik.

1. Érvényességi kötvény

Az első díjablak idején az érvényességi kötvény értéke 0,01 ETH-re lesz állítva. Ekkor, ha a véglegesített piacok több, mint 1%-a érvénytelen lett a díjablak idején, akkor az érvényességi kötvény növelésre kerül. Ha kevesebb, mint 1% lett érvénytelen, akkor csökkentésre kerül (azonban sosem lesz alacsonyabb, mint 0,01 ETH).

ν legyen a korábbi díjablak idején érvénytelenként lezárt piacok aránya és b_v legyen az érvényességi kötvények mennyisége a korábbi díjablakban. Ekkor az érvényességi kötvény ára a jelenlegi díjablakban $\max\left\{\frac{1}{100}, b_v f(\nu)\right\}$.

2. Jelentés elmulasztása REP kötvény

Az első díjablak idején a jelentés elmulasztása kötvény értéke 0,35 REP-re lesz állítva. Hasonlóan az érvényességi kötvényhez, ennek az értéke is fel-le lesz állítva az 1%-os arányt megcélozva 0,35 REP minimális értékkel.

Legyen ρ a korábbi díjablak idején kijelölt riporterek aránya, akik elmulasztották a jelentést és legyen b_r a jelentés elmulasztása REP kötvények száma a korábbi díjablakban. A jelentés elmulasztása kötvény értéke ekkor a jelenlegi díjablakban a következő: $\max\{0,35, b_r f(\rho)\}$.

3. A kijelölt riporterek letétje

Az első díjablak idején a kijelölt riporterek letétjének összege 0,35 REP lesz. Ez dinamikusan fog állítódni an-

[31] Ez a formula változhat, amikor kísérleti adatokat kapunk az élő piacokról.

nak függvényében, hogy hány riporter jelentett helytelenül (nem megegyezően a piac végső kimenetelével) a korábbi díjablakban.

Legyen δ a helytelenül jelentő riporterek aránya a korábbi díjablakban és legyen b_d a kijelölt riporterek letétjének nagysága a korábbi díjablakban. Ekkor a kijelölt riporterek letétjének értéke a jelenlegi díjablakban: $\max\{0, 35, b_d f(\delta)\}$.

Függelék F: Tervezési változtatások

3 év kutatás és iteráció után jutottunk el az Augur jelenlegi kialakításához. A folyamatból kiemelkedett szerkezet lényegesen eltér a korábbi dokumentációnkban [12] leírt látomásunktól. A következőkben részletezünk három jelentős változtatást és ezek okait.

1. Jelentési díjak

A korábbi szerkezetben a piac készítője állított volna be egy kereskedési díjat, amely 50/50-be lett volna elfelezve a riporterekkel. A jelenlegi rendszerben a piac készítőjének és a riportereknek a díja független egymástól és a riporterek díja dinamikusan állítódik az Augur által, hogy biztonságosan tartsa a rendszert.

A riportereknek fizetett díj hatással van a REP árára, ami hatással van az osztódási protokoll biztonságára (1-es elmélet). Ha a riportereknek fizetett díj túl alacsony, akkor a jós becsületessége veszélyben van. Ha a díj túl magas, akkor a parazita piacok növekedése indul meg. Ezen okokból fontos, hogy a riportereknek fizetett díj dinamikusan szabályozva legyen az Augur által és ne a piac készítői adják meg önkényesen.

A riporterek díjainak leválasztása a piac készítőjének lehetőségeiből biztosítja azt is, hogy a riporterek (és így az osztódási protokoll becsületessége) nem lesznek kitéve a piackészítők között folyó alacsonyabb díjjakért való versengésnek. A minőségi piacokat és a minőségi jelentéseket külön kellene mérni és jutalmazni. A piackészítők közötti verseny megengedett kellene, hogy legyen azért, hogy a díjak 0 felé konvergáljanak anélkül, hogy a riporterek díja is csökkene ezzel együtt.

2. Kereskedési díjak

A régi rendszerben a kereskedőktől a díjak kereskedésenként lettek volna begyűjtve. Az új rendszerben a díjakat akkor szedjük be, amikor a kereskedők megegyeznek piaci szerződésekkel. Ez a változtatás részben azért történt, mert az Augur nem tud felügyelni offline kereskedést. A piac kimeneteleinek részvényei egyszerűen tokenek, amelyek szabadon kereskedhetők. Mivel a díjak beszedése kereskedésenként megvalósíthatatlan, az Augur ehelyett csak akkor gyűjti azokat be, amikor a piaci szerződéssel törénik a megegyezés. Ennek egy további előnye, hogy így csökken az átlagos kereskedési díj, ami még versenyképesebbé teszi az Augur-t.

3. Univerzumok

A régi szerkezetben csak egy REP „verzió" létezett és az is limitált mennyiségben. Az új rendszerben a REP több különböző változatra (univerzumba) osztódhat, olyanokra amelyek végződhetnek úgy, hogy több vagy kevesebb REP lesz bennük, mint eredetileg. Ha az osztódás vitatott, akkor a REP mennyiség a gyerekuniverzumokban lehet, hogy csak a töredéke lesz a szűlőuniverzumokban lévőnek. A nem vitatott osztódások esetén a korai költöztetési bónusz miatt a gyerekuniverzumokban lehetséges, hogy több REP token lesz, mint a szülőkben.

Az osztódás miatt létrejött REP változatok különbözők, mindnek megvan a saját ára és mennyisége, ezért a szolgáltatóknak is eképpen kell kezelniük őket. Amikor az Augur először elindul csak egy univerzum lesz (az eredet univerzum) és csak egy REP verzió, mint ahogy most is. Azonban, amint egy osztódás megtörténik ez az egy verzió több alakra módosul: például egy osztódó piac `A` és `B` kimenetellel létre fog hozni új REP-`A`, REP-`B` és REP-`érvénytelen` tokeneket. A pénztárcák és váltók, akik támogatják a REP-et ekkor négy különböző verziót kellene hogy támogassanak (elméletileg) – REP-`eredetet` (az eredeti REP verziót, ami ekkor zárolva kellene, hogy legyen), REP-`A`-t, REP-`B`-t és REP-`érvénytelen`-t.[32]

A REP összdarabszáma a gyerekuniverzumokba attól függ, hogy mennyi REP került oda átköltöztetésre és az mikor történt. A REP átköltöztetése az osztódás alatt, mielőtt még nem egyértelmű, hogy melyik gyerekuniverzum lesz a győztes egy kis (de nem nulla) kockázatnak teszi ki a felhasználókat (lásd a III E fejezetet), amely így elbátortalaníthatja a résztvevőket az osztódásban való részvételtől. A felhasználókat kompenzálni kell a kockázatért, azért hogy növeljük a részvételt.

A felhasználók, akik nem vesznek részt az osztódásban bűntetésből elveszthetnék a birtokolt REP-jük egy részét. A korábbi rendszerben a „használd vagy elveszted" mechanizmust használtuk volna, hogy bűntessük a távolmaradókat, mintha riporterek lennének, akik hibásan jelentenek. Azonban ez a megoldás jelentős használhatósági problémákat eredményez a pénztárcák és a váltók számára. Az osztódás alatt a váltóknak egy bizonyos gyerekuniverzumba kellene vinniük a felhasználók REP-jét vagy annak egy részét. [33]

---

[32] A gyakorlatban a szolgáltatók számára a legegyszerűbb módja (és a legkevésbé bomlasztó a felhasználók számára) ennek, ha bátorítanák a felhasználókat az osztódásban való részvételre és egyszerűen csak a győztes univerzumot támogatnák az osztódás után.

[33] Gyakorlati szempontból azt találtuk, hogy az okosszerződésbe kellene implementálni az osztódási jutalom szétosztását, azonban ez túlságosan komplex lenne. A szerződés kódjának bonyolúltsága már önmagában biztonsági kockázat, ezért megpróbáltuk egyszerűsíteni a kivitelezést ahol csak lehetett.

A távolmaradók bűntetése helyett a résztvevők jutalmazása mellett döntöttünk, akik így 5%-os bónuszban részesülnek majd a gyerekuniverzumban, ahova költöztetik a REP-jüket. Ha az összes REP 4,762%-a (vagy még több) a vesztes univerzumba kerül – melyből 1,25% és 2,5% között valamennyi már vitaletétként elkötelezett – akkor minden univerzumban kevesebb lesz a teljes REP mennyiség, mint a szülőuniverumban.