Augur: decentralizované orákulum a platforma pro predikční trhy

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams a Stephanie Alexander
Forecast Foundation
(Datum: 24. května 2018)

Augur je decentralizované orákulum a platforma pro predikční trhy bez nutnosti důvěry mezi účastníky. Výsledky predikčních trhů na Auguru určují uživatelé, kteří drží nativní reputační token Auguru (Reputation, REP), ty sázejí na skutečný pozorovaný výsledek a za to z těchto trhů obdrží poplatky za vypořádání. Struktura incentiv Auguru je navržena tak, aby pro držitele REP pravdivé a přesně hlášení výsledků bylo vždy nejvýnosnější volbou. Držitelé tokenů mohou tyto výsledky zpochybňovat, když vloží do zástavy určitou zvyšující se část svých tokenů. Pokud množství těchto tokenů dosáhne určité úrovně, REP se rozdělí na několik verzí, jednu pro každý možný výsledek sporného trhu. Držitelé tokenů poté musí vyměnit své REP za jednu z těchto verzi. Verze, které neodpovídají výsledkům z reálného světa, se stanou bezcennými, protože se nikdo nebude chtít účastnit predikčních trhů, pokud si nebude jistý, že budou vyhodnoceny správně. Proto si držitelé tokenů vyberou pouze verzi REP, o které vědí, že bude stále mít hodnotu, verzi, která odpovídá realitě.

Augur je decentralizované orákulum a platforma pro predikční trhy. Na predikčním trhu mohou jednotlivci spekulovat na výsledky budoucích událostí. Ti, co předpovědí tyto události správně, získají peníze, a ti, kteří je předpovědí nesprávně, peníze ztratí. [4, 10, 11]. Cena na predikčním trhu může sloužit jako přesný a dobře kalibrovaný indikátor toho, jak pravděpodobné je, že událost nastane [3, 5, 8, 12].

Pomocí Auguru budou mít lidé možnost obchodovat na predikčních trzích za velmi nízkou cenu. Jediné významné náklady, které budou účastníci mít, sestávají z kompenzace tvůrcům trhů a uživatelům, kteří oznamují výsledky trhů poté, co událost nastala. Výsledkem je predikční trh, kde jsou požadavky na důvěru mezi účastníky, rozdíl mezi poptávkou a nabídkou a poplatky tak nízké, jak je u kompetitivních tržních sil možné.

V minulosti byly predikční trhy centralizovány. Nejjednodušším způsobem, jak vypořádávat obchody na predikčním trhu, je spravovat záznam o nich důvěryhodnou osobou. Podobně nejjednodušším způsobem, jak určit výsledek události a vyplatit výhry obchodníkům, je určit výsledky trhů pomocí nestranného, důvěryhodného soudce. Avšak centralizované predikční trhy mají mnoho rizik a omezení: neumožňují globální účast, omezují typy trhů, které lze vytvořit a ve kterých lze obchodovat, a vyžadují, aby obchodníci věřili provozovateli trhu, že nezcizí prostředky a že správně vypořádá trhy.

Augur se snaží trhy vypořádávat plně decentralizovaným způsobem. Decentralizované sítě bez nutnosti důvěry, jako je Bitcoin[6] a Ethereum[1], eliminují riziko, že se vlastní zájem zvrhne v korupci nebo krádež. Role vývojářů platformy Augur spočívá v publikování chytrých kontraktů (smart contracts) na síti Ethereum. Kontrakty Auguru jsou plně automatizovány: vývojáři nemohou utrácet peníze, které jsou drženy v úschově kontraktů, nemají kontrolu nad vypořádáním trhů, nemohou odmítat nebo schvalovat obchody nebo ostatní transakce na síti, nemohou stornovat obchody, nemohou měnit nebo rušit nabídky, atd. *Orákulum* platformy Augur dovoluje, aby se informace dostaly z reálného světa do blockchainu bez toho, aby závisely na důvěryhodném prostředníkovi. Augur bude první decentralizované orákulum na světě.

I. JAK AUGUR FUNGUJE

Trhy v platformě Augur procházejí čtyřmi fázemi: *vytvoření*, *obchodování*, *reportování* a *vypořádání*. Kdokoliv může vytvořit trh pro jakoukoliv světovou událost. Obchodování začíná ihned po vytvoření trhu a všichni uživatelé mohou obchodovat na všech trzích. Poté, co událost, pro kterou je trh založen, nastane, je její výsledek určen orákulem platformy Augur. Po určení výsledku mohou obchodníci zavřít své pozice a vybrat své zisky.

Augur má vlastní token, Reputaci (REP). REP potřebují tvůrci trhu a reportéři, když oznamují výsledky trhů vytvořených na platformě Augur. Reportéři oznamují výsledky trhu tak, že *sázejí* své REP na jeden z možných výsledků trhu. Tím reportér deklaruje, že výsledek, na který vsadil, odpovídá výsledku příslušné události z reálného světa. Shoda reportérů trhu je považována za „pravdu“ pro účel určení výsledku trhu. Pokud se výsledek, který reportér oznámil, neshoduje s výsledky oznámenými ostatními reportéry, Augur vezme REP vsazené na výsledek, na kterém nebyla shoda, a rozdělí je mezi reportéry, kteří oznámili výsledek, na kterém shoda nastala.

Tím, že vlastní REP, a účastí na přesném oznamování výsledků událostí, mají držitelé tohoto tokenu nárok na část poplatků na této platformě. Každý vsazený REP přináší jeho majiteli nárok na poměrnou část poplatků z trhů na platformě Augur. Čím více REP reportér vlastní, tím více poplatků získá, pokud oznamuje výsledky správně, za svůj příspěvek k zabezpečení této platformy.

REP sice hraje hlavní roli v provozu platformy Augur, nepoužívá se však k obchodům na trzích na Auguru. Obchodníci nemusí vlastnit ani používat REP, účast v pro-

cesu oznamování výsledků se po nich nepožaduje.

A. Vytvoření trhu

Augur umožňuje komukoliv, aby vytvořil trh pro jakoukoliv nastávající událost. *Tvůrce trhu* nastavuje *koncový čas události* a vybírá *zadaného reportéra*, který bude oznamovat výsledek události. Zadaný reportér neurčuje definitivně výsledek události. Komunita má vždy možnost zpochybnit a opravit výsledek oznámený zadaným reportérem.

Posléze tvůrce trhu vybere *relevantní zdroj*, který by měli reportéři používat pro určení výsledku. Zdroj informací o výsledku může být jednoduše obecné povědomí, nebo to může být určený zdroj jako například „ministerstvo energetiky Spojených států“, `bbc.com` nebo adresa koncového bodu některého API.[1] Také nastavují *poplatek tvůrce trhu*, což je poplatek, který tvůrcům trhu platí obchodníci, kteří vypořádávají své obchody s chytrým kontraktem trhu (pro podrobnosti o poplatcích viz oddíl I D). Nakonec tvůrce trhu složí dvě jistiny: *jistinu validity* a *jistinu za přítomnost zadaného reportéra* (také pro zkrácení nazývanou *přítomnostní jistina*).

Jistina validity se platí v ETH a v případě, že bude konečný výsledek trhu jiný než *neplatný*, se vrací tvůrci trhu.[2] Jistina validity incentivizuje tvůrce trhu, aby vytvářeli trhy založené na dobře definovaných událostech s objektivními, jednoznačnými výsledky. Velikost jistiny validity se nastavuje dynamicky podle procenta neplatných výsledků v nedávných trzích.[3]

Přítomnostní jistina sestává ze dvou částí: *přítomnostní jistiny sítě* (placené v ETH) a *přítomnostní jistiny v REP* (placené v REP). Tyto jistiny se vracejí tvůrci trhu v případě, že zadaný reportér trhu oznámí výsledek trhu během prvních tří dnů po *koncovém času události*. Pokud zadaný reportér nepředloží svůj report během tohoto třídenního okna, tvůrce trhu ztrácí přítomnostní jistinu, která bude přidělena *prvnímu veřejnému reportérovi*, který o tomto trhu bude reportovat (Viz oddíl I C 6). To incentivizuje tvůrce trhu k tomu, aby vybral spolehlivého zadaného reportéra, který předloží report rychle.

Přítomnostní jistina sítě je zamýšlena pro pokrytí nákladů na transakci na síti Ethereum prvního veřejného reportéra. To zamezuje scénáři, kdy jsou náklady na transakci veřejného reportéra příliš vysoké, než aby se podání reportu vyplatilo. Tato část jistiny je nastavena na dvojnásobné průměrné náklady na transakci pro reportování během posledního časového okna pro reportování.

Pokud zadaný reportér nepředloží report, přítomnostní jistina v REP bude předána prvnímu veřejnému reportérovi ve formě sázky na jím reportovaný výsledek, takže první veřejný reportér dostane tuto část jistiny pouze a jen v případě, že reportuje správně. Stejně jako u jistiny validity je tato část jistiny upravována dynamicky podle procenta zadaných reportérů, kteří včas nepředložili report během posledního časového okna. [4]

Tvůrce trhu vytváří trh a posílá všechny požadované jistiny v rámci jedné transakce na síti Ethereum. Po potvrzení této transakce je trh veřejný a obchodování začíná.

B. Obchodování

Účastníci trhů předpovídají výsledky událostí tak, že obchodují s *podíly* na těchto výsledcích. *Úplná množina podílů* je množina podílů, která obsahuje jeden podíl na každém možném platném výsledku trhu [2]. Úplné množiny jsou vytvářeny platformou Augur při párování obchodů v rámci kontraktu tak, jak je potřeba pro provedení obchodu.

Například mějme trh se dvěma možnými výsledky, `A` a `B`. Alice je ochotná zaplatit 0,7 ETH za podíl na `A` a Bob je ochotný zaplatit 0,3 ETH za podíl na `B`.[5] Nejprve Augur páruje tyto dva obchody a vybere dohromady jeden ETH od Alice a Boba.[6] Poté Augur vytvoří úplnou množinu podílů a dá Alici podíl na `A` a Bobovi podíl na `B`. Tímto způsobem podíly na výsledku vznikají. Po vytvoření lze podíly volně obchodovat.

Obchodní kontrakty platformy Augur udržují účetní knihu pro každý trh vytvořený na této platformě. Kdokoliv může kdykoliv vytvořit nový pokyn nebo uspokojit existující pokyn. Ty se automaticky párují softwarem, který existuje v kontraktech platformy Augur. Požadavky na nákup nebo prodej podílů jsou splněny okamžitě, pokud v účetní knize již existuje odpovídající opačný pokyn. Mohou být splněny koupí nebo prodejem podílů od jiných účastníků, což může zahrnout vytvoření nové úplné množiny nebo doplnění existující úplné množiny. Software platformy Augur vždy zajistí minimální množství podílů nebo peněz, které je potřebné

---

[1] Například pro trh „Nejvyšší teplota na mezinárodním letišti v San Franciscu (ve stupních Fahrenheita) dne 10. dubna 2018 podle serveru Weather Underground“ je relevantním zdrojem `https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html`. Reportéři jednoduše přejdou na tuto adresu a zadají nejvyšší teplotu, která je zde uvedena.

[2] *Neplatný* trh je trh, o kterém reportéři rozhodli, že je neplatný, protože žádný z výsledků, které zadal tvůrce trhu, není správný, nebo protože je popis trhu nejednoznačný nebo subjektivní. Podrobnosti viz oddíl III F.

[3] Podrobnosti naleznete v příloze E 1.

[4] Pro podrobnosti viz přílohu E 2.

[5] Zpočátku budou obchody v Auguru používat vlastní měnu platformy Ethereum, Ether (ETH). Následná vydání Auguru budou podporovat trhy používající jakékoliv tokeny vydané na síti Ethereum, včetně podílů v jiných trzích a tokenů svázaných s fiat měnami („stablecoins“), pokud budou dostupné.

[6] Množství 1 ETH zde používáme kvůli jednodušší mu vysvětlení. Skutečná cena úplné množiny podílů je mnohem nižší, viz `docs.augur.net/#number-of-ticks` pro podrobnosti.

Obrázek 1. Zjednodušené znázornění životního cyklu predikčního trhu.

pro pokrytí požadované hodnoty. Pokud neexistuje odpovídající pokyn, nebo lze požadavek splnit jen částečně, je zbytek zaznamenán do účetní knihy jako nový pokyn.

Obchodní pokyny nejsou nikdy splněny za horší cenu, než je limitní cena zadaná obchodníkem, ale mohou být splněny za lepší cenu. Nenaplněné a částečně naplněné pokyny lze kdykoliv odstranit z účetní knihy zadavatelem pokynu. Obchodníci platí poplatky pouze když jsou prodány úplné množiny podílů. Poplatky za vypořádání jsou podrobněji popsány v oddílu I D.

Většina obchodování s podíly se sice očekává před vypořádáním trhu, avšak podíly lze obchodovat kdykoliv po vytvoření trhu. Vlastnictví všech aktiv v platformě Augur — včetně podílu na výsledcích trhu, účastnických tokenů, podílů v disputačních jistinách i vlastnictví trhů samotných — lze vždy měnit.

C. Reportování

Poté, co vlastní událost trhu nastane, musí být pro finalizování trhu a zahájení vypořádání určen výsledek. Výsledky určuje orákulum platformy Augur, které se skládá z reportérů motivovaných ziskem, kteří jednoduše oznamují skutečný výsledek události z reálného světa. Kdokoliv, kdo vlastní REP, se může účastnit reportování a zpochybňování výsledků. Reportéři, jejichž reporty jsou konzistentní s ostatními reportéry, jsou finančně odměňováni, zatímco ti, jejichž reporty nejsou konzistentní s ostatními, jsou finančně penalizováni (viz oddíl I D 3).

1. *Poplatková časová okna*

Reportování platformy Augur probíhá v cyklech po sobě jdoucích sedmidenních *poplatkových časových oken*. Všechny poplatky, které Augur vybere během jednoho poplatkového časového okna, jsou přidány do *souhrnných prostředků za reportování* pro toto poplatkové časové okno. Na konci tohoto časového okna budou tyto prostředky vyplaceny držitelům REP, kteří se účastnili reportování. Reportéři obdrží proporcionální část REP, které vsadili v tomto poplatkovém časovém okně. Účast zahrnuje: skládání jistin během počátečního reportování, disputace předběžného výsledku nebo zakoupení *účastnických tokenů*.

2. *Účastnické tokeny*

Během poplatkového časového okna mohou držitelé REP zakoupit jakékoliv množství účastnických tokenů, každý za jeden attorep[7]. Na konci poplatkového časového okna mohou za účastnické tokeny získat zpět své REP a navíc proporcionální podíl *souhrnných poplatků za reportování* tohoto poplatkového časového okna. Pokud nenastane žádná akce (*mj.* podání reportu nebo disputace reportu podaného jiným reportérem), která vyžaduje reportéra, reportéři mohou nakupovat účastnické tokeny, aby dali najevo, že jsou v tomto poplatkovém časovém okně přítomni. Stejně jako vsazené REP mohou být účastnické tokeny proměněny jejich majiteli za *pro rata* část poplatků v tomto časovém okně.

Jak je popsáno v oddílu II, je důležité, aby držitelé REP byli připraveni na vypořádání trhu v případě forku. Účastnický tokem vytváří incentivy pro držitele REP, aby monitorovali tuto platformu alespoň jednou za týden a tak byli připraveni k účasti, pokud to bude nutné. I držitelé REP, kteří se nechtějí účastnit procesu reportování, jsou incentivizováni ke kontrole platformy Augur jednou za sedm dní kvůli kupování účastnických tokenů a získávání poplatků. Tyto pravidelné a aktivní návštěvy zajišťují, že budou vědět, jak používat Augur, budou si vědomi forků, když nastanou, a měli by tedy být připraveni k účasti na forku, když nastane.

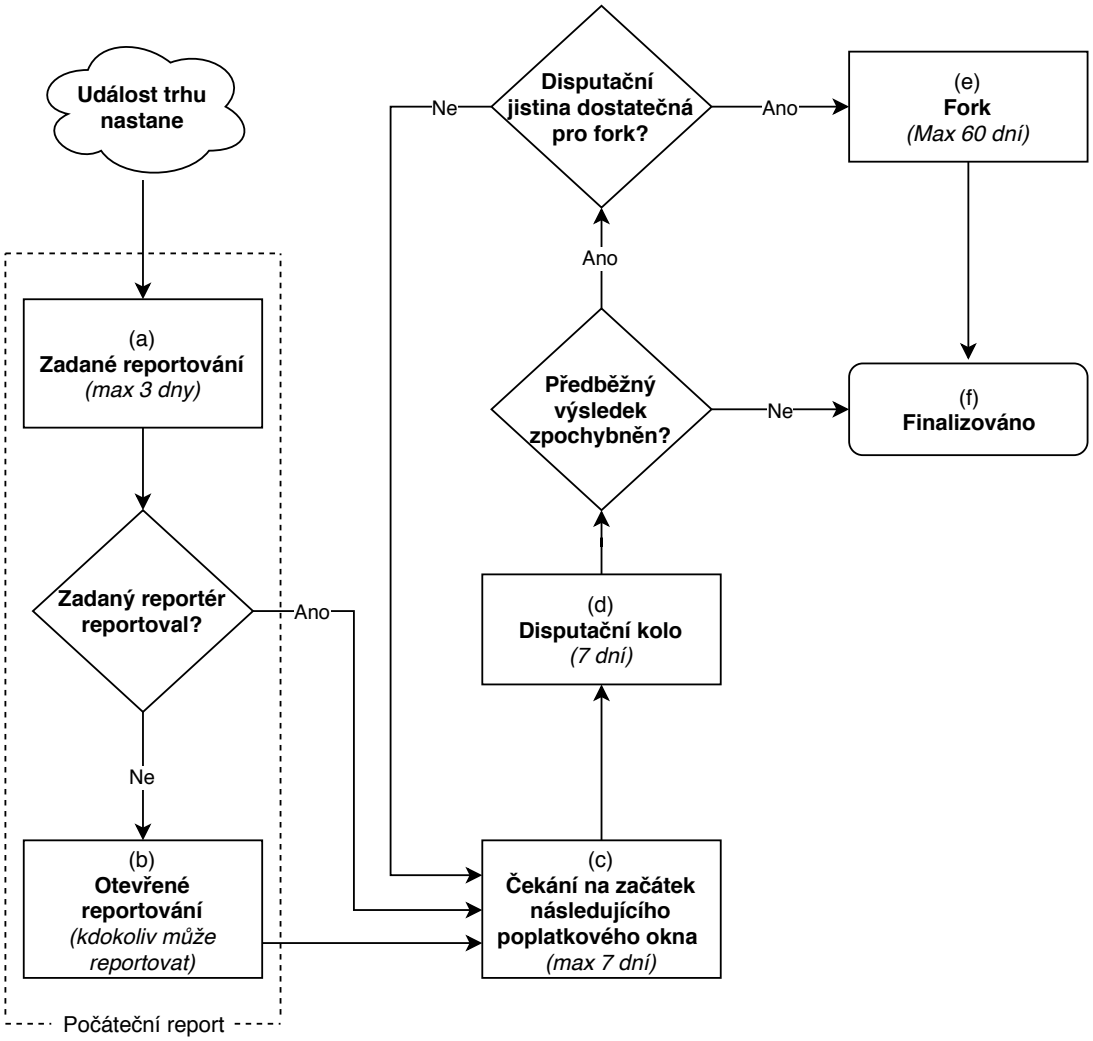
3. *Vývoj stavu trhu*

Trhy platformy Augur mohou být po vytvoření v sedmi různých stavech. Potenciální stavy neboli „fáze“ trhu na Auguru jsou následující:

- Předběžné reportování
- Zadané reportování
- Otevřené reportování
- Čekání na začátek následujícího poplatkového časového okna
- Disputační kolo
- Fork
- Finalizováno

Vztahy mezi těmito stavy lze vidět na obrázku 2.

[7] Jeden *attorep* je 10^{-18} REP.



Obrázek 2. Diagram reportování.

4. *Předběžné reportování*

Fáze *předběžného reportování* neboli *obchodování* (obr. 1) je časové období, které začíná poté, co se na trhu začalo obchodovat, ale předtím, než událost trhu nastala. Obecně je to na každém trhu systému Augur doba, kdy se nejvíce obchoduje. Poté, co nastal konec události, trh přechází do fáze *zadaného reportování* (obr. 2a).

5. *Zadané reportování*

Při vytváření trhu se po tvůrci trhu vyžaduje, aby vybral zadaného reportéra a složil za něj jistinu. Během fáze zadaného reportování (obr. 2a) má zadaný reportér trhu až tři dny na podání reportu o výsledku události trhu. Pokud zadaný reportér nepodá report během zadaných tří dnů, tvůrce trhu ztrácí přítomnostní jistinu a trh automaticky vstupuje do fáze *otevřeného reportování* (obr. 2b).

Pokud zadaný reportér předloží report včas, vrací se přítomnostní jistina tvůrci trhu. Po zadaném reportérovi se vyžaduje, aby na reportovaný výsledek vsadil sázku zadaného reportéra[8], kterou prohraje, pokud bude konečný výsledek trhu jiný než ten, který reportoval.[9] Poté, co zadaný reportér předloží svůj report, přejte trh do fáze *čekání na zahájení poplatkového časového okna* (obr. 2c) a reportovaný výsledek se stane *předběžným výsledkem trhu*.

[8] Viz přílohu E 3 pro podrobnosti o velikosti sázky zadaného reportéra.

[9] Prohraná sázka se přidá k poplatkům za reportování v poplatkovém časovém okně, které bylo trhu přiděleno, a používá se pro odměňování korektních reportérů a účastníků, kteří reporty zpochybňují. Podrobnosti naleznete v oddílu I D 3.

6. Otevřené reportování

Pokud zadaný reportér nepředloží report během přidělených tří dnů, tvůrce trhu ztrácí přítomnostní jistinu a trh okamžitě vstupuje do fáze *otevřeného reportování* (obr. 2b). Jakmile trh vstoupí do fáze otevřeného reportování, kdokoliv může oznámit výsledek trhu. Pokud zadaný reportér nepředloží report, první reportér, který předloží report o výsledku trhu, se nazývá *prvním veřejným reportérem*.

První veřejný reportér trhu dostane propadlou přítomnostní jistinu ve formě sázky na výsledek, který reportoval, takže ji získá pouze v případě, že jím reportovaný výsledek souhlasí s konečným výsledkem trhu. Také po finalizaci trhu získá přítomnostní jistinu sítě pouze v případě, že jím reportovaný výsledek souhlasí s konečným výsledkem trhu.

První veřejný reportér *nemusí* vsadit vlastní REP, když reportuje o výsledku trhu. Takto se očekává, že pro kterýkoliv trh, jehož zadaný reportér nepředložil report, *někdo* předloží report velmi brzy poté, co přejde do fáze otevřeného reportování.

Poté, co první reportér (ať již to byl zadaný reportér, nebo první veřejný reportér), odevzdá *počáteční report*, reportovaný výsledek se stane předběžným výsledkem trhu a trh přejde do fáze čekání na začátek následujícího poplatkového časového okna (obr. 2c).

7. Čekání na začátek následujícího poplatkového časového okna

Poté, co trh dostane počáteční report, přejde do fáze čekání na začátek následujícího poplatkového časového okna (obr. 2c). Během této fáze je reportování pro tento trh pozastaveno, dokud současné poplatkové časové okno neskončí. Poté, co nastane následující poplatkové časové okno, přejde trh do fáze *disputačního kola*.

8. Disputační kolo

Disputační kolo (obr. 2d) je 7denní interval, během něhož může kterýkoliv držitel REP zpochybnit (disputovat) *předběžný výsledek* trhu.[10] (Na začátku disputačního kola je předběžný výsledek trhu výsledkem, který se stane konečným výsledkem trhu, pokud jej úspěšně nezpochybní držitelé REP.) Disputace spočívá ve *vsazení* REP (označované v tomto kontextu jako *disputační sázka*) na výsledek, který je *odlišný* od současného předběžného výsledku trhu. Disputace je *úspěšná*, pokud celkové množství disputační sázky na některý výsledek dosahuje *velikosti disputační jistiny* vyžadované pro současné kolo. Velikost disputační jistiny se počítá následovně.

Nechť A_n je celková sázka pro všechny výsledky trhů na začátku disputačního kola n. Nechť ω je výsledek trhu *odlišný* od předběžného výsledku trhu na začátku tohoto disputačního kola. Nechť $S(\omega, n)$ je celková velikost sázek na výsledek ω na začátku disputačního kola n. Potom velikost *disputační jistiny*, která je potřebná pro úspěšnou disputaci aktuálního předběžného výsledku a přijetí nového výsledku ω během kola n, kterou zapisujeme $B(\omega, n)$, se vypočítá jako:

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

Velikosti jistin jsou vybrány tímto způsobem, aby byla zajištěna pevná hodnota návratnosti vložených prostředků 50% pro reportéry, kteří úspěšně zpochybní nepravdivé výsledky (viz oddíl II D).

Disputační jistina nemusí být celá složena jedním uživatelem. Platforma Augur umožňuje uživatelům, aby se na disputační jistiny skládali. Uživatel, který vidí nesprávný předběžný výsledek, může tento výsledek zpochybnit tak, že vsadí REP na výsledek jiný, než je předběžný výsledek. Pokud nějaký výsledek (jiný než předběžný výsledek) shromáždí dostatečné množství sázek pro disputaci, aby se naplnila jeho disputační jistina, aktuální předběžný výsledek bude úspěšně zpochybněn.

V případě úspěšné disputace trh buď projde dalším disputačním kolem, nebo přejde do stavu *forku* (obr. 2e). Pokud je velikost složené disputační jistiny větší než 2,5% všech REP, přejde trh do stavu forku. Pokud je velikost složené disputační jistiny menší než 2,5% všech REP, stane se nově vybraný výsledek novým předběžným výsledkem trhu a trh vstoupí do dalšího disputačního kola.

Všechny disputační sázky jsou během disputačního kola drženy v úschově. Pokud není disputace úspěšná, vrací se disputační sázky jejich majitelům na konci disputačního kola. Pokud není úspěšná žádná disputace během sedmidenního disputačního kola, přechází trh do *finalizovaného* stavu (obr. 2f) a jeho předběžný výsledek je přijat jako jeho *konečný výsledek*. Konečný výsledek trhu je předběžný výsledek, který projde disputačním kolem bez toho, aby byl úspěšně zpochybněn, nebo je určen pomocí forku. Kontrakty platformy Augur přistupují ke konečným výsledkům jako k *pravdě* a příslušným způsobem rozdělují prostředky.

Všechny neúspěšné disputační sázky se na konci každého disputačního kola vracejí svým majitelům. Všechny úspěšné disputační sázky se použijí na výsledek, na který jsou vsazeny, a zůstávají na něm, dokud není trh finalizován (nebo dokud nenastane v některém jiném trhu platformy Augur fork). Všechny disputační sázky (ať již úspěšné, nebo neúspěšné) získají část *souhrnných*

[10] Fakt, že je délka disputačního kola stejná jako poplatková časová okna, je pouze užitečnou shodou okolností. V principu mohou být délky disputačních kol a poplatkových časových oken rozdílné.

poplatků za reportování[11] z aktuálního časového okna.

9. Fork

Stav fork (obr. 2e) je speciální stav, který trvá až 60 dnů. Fork je rozhodnutí o výsledku trhu poslední záchrany. Je to velmi rušivý proces a jeho výskyt by měl být vzácný. Fork nastává, když existuje trh s výsledkem, jenž je úspěšně zpochybněn a jenž má disputační jistinu ve velikosti alespoň 2,5% všech REP. Tento trh je označován jako *forkující trh.*

Po zahájení forku nastává 60denní[12] *interval forku.* Disputace všech nefinalizovaných trhů je odložena, než tento fork skončí. Interval forku je mnohem delší, než ostatní časová okna, protože držitelé REP a poskytovatelé služeb (jako jsou peněženky a směnárny) potřebují více času na přípravu. Konečný výsledek forku nelze zpochybnit.

Každý trh na Auguru a všechny tokeny REP existují v nějakém *univerzu.* Tokeny REP lze používat pro reportování výsledků (a tak získávat poplatky) *pouze* pro trhy, které existují ve stejném univerzu jako tyto tokeny REP. Když bude Augur poprvé spuštěn, všechny trhy a všechny tokeny REP budou existovat v *počátečním univerzu.*

Když se trh forkuje, jsou vytvořena nová univerza. Fork vytvoří nové *dceřiné univerzum* pro každý možný výsledek forkujícího trhu (včetně `neplatného`, jak je popsáno v oddílu I D 2). Například „binární“ trh má tři možné výsledky: `A`, `B` a `Neplatný`. Proto vytvoří binární forkující trh tři nová dceřiná univerza: univerzum `A`, univerzum `B` a univerzum `Neplatný`. Zpočátku jsou tato nově vytvořená univerza prázdná: neobsahují žádné trhy nebo tokeny REP.

Při zahájení forku zůstane *rodičovské univerzum* permanentně *zamčeno.* V zamčeném univerzu nelze vytvářet žádné nové trhy. Uživatelé mohou pokračovat v obchodech s podíly v trzích v zamčených univerzech a trhy v zamčených univerzech mohou stále získávat úvodní reporty. Avšak nevyplácí se zde žádné odměny za reportování a trhy v zamčených univerzech nelze finalizovat. Aby byly trhy nebo tokeny REP v zamčeném univerzu užitečné, je nutné je nejprve převést do dceřiného univerza.

Držitelé tokenů REP v rodičovském univerzu mohou převést své tokeny do dceřiného univerza, které si vyberou. Tento výběr by měl být proveden pozorně, protože tento převod je jednosměrný, nelze jej vzít zpět. Tokeny nelze poslat z jednoho dceřiného univerza do druhého. *Tato migrace je trvalým převodem tokenů REP na určitý výsledek trhu.* Tokeny REP, které byly převedeny do jiných dceřiných univerz, by měly být považovány za úplně odlišné tokeny a poskytovatelé služeb jako peněženky a směnárny by k nim tak měli přistupovat.

Při zahájení forku jsou všechny sázky REP, které byly vsazeny na všech neforkujících trzích, *zrušeny*, takže je lze během intervalu forku převádět do dceřiných univerz.[13]

Kterékoliv dceřiné univerzum získá na konci intervalu forku nejvíce převedených REP, se stává *vítězným univerzem* a jeho odpovídající výsledek se stává konečným výsledkem forkujícího trhu. Nefinalizované trhy z rodičovského univerza lze převést pouze do vítězného univerza a v případě, že mají počáteční report, jsou resetovány zpět do fáze čekání na začátek následujícího poplatkového časového okna.

Pro převádění tokenů z rodičovského univerza do dceřiných univerz není žádný časový limit. Tokeny lze převádět po ukončení intervalu forku, ale nebudou se počítat pro určení vítězného univerza. Kvůli zvýšení účasti během intervalu forku získají držitelé tokenů, kteří převedou své REP do 60 dnů od začátku forku, ve dceřiném univerzu, do kterého se rozhodli své tokeny převést, dodatečných 5% REP [14]. Tato odměna je získána vytvořením nových tokenů.[15]

Reportéři, kteří vsadili REP na jeden z výsledků forkujícího trhu, nemohou během intervalu forku změnit svou pozici. REP, který byl vsazen na výsledek v rodičovském univerzu, lze převést pouze do dceřiného univerza, které odpovídá tomuto výsledku. Například pokud reportér během nějakého disputačního kola pomohl složit disputatční jistinu k úspěšné disputaci ve prospěch výsledku `A`, pak REP, které vsadil na výsledek `A`, lze během forku převést pouze do univerza `A`.

Sourozenecká univerza jsou úplně oddělená. Tokeny REP, které existují v jednom univerzu, nelze použít k reportování o událostech nebo získávání odměn z trhů v jiném univerzu. Vzhledem k tomu, že uživatelé zřejmě nebudou chtít vytvářet nebo obchodovat na trzích v univerzu, jehož orákulum je nedůvěryhodné, REP, které existuje v univerzu, které neodpovídá objektivní realitě, nemá velkou šanci vydělat svému vlastníkovi nějaké poplatky, a proto by nemělo mít výraznou tržní hodnotu.

---

[11] Poplatky za vypořádání a jistiny validity shromážděné během poplatkového časového okna se přidají k souhrnným poplatkům za reportování tohoto poplatkového časového okna. Na konci tohoto poplatkového časového okna se tyto prostředky vyplatí uživatelům proporcionálně k množství REP, které vsadili během tohoto okna.

[12] Intervaly forků mohou mít méně než 60 dnů: interval forku končí buď po uplynutí 60 dnů, nebo poté, co je více než 50% všech počátečních REP přesunuto do některého z možných dceřiných univerz.

[13] Jedinou výjimkou jsou REP vsazené počátečním reportérem, když prováděl počáteční report. Tyto REP zůstávají vsazené na první reportovaný výsledek a jsou automaticky převedeny do dceřiného univerza, které vyhraje fork.

[14] To nastane, i když interval forku skončí dříve kvůli tomu, že bylo více než 50% REP převedeno do některého dceřiného univerza

[15] Tento efekt má malý vliv na celkovou zásobu REP. Například pokud je 20% existujících REP převedeno během intervalu forku, tento bonus vyústí v 1% zvýšení celkové zásoby REP. Kromě toho by měl fork být velice vzácnou událostí.

Proto by tokeny REP, které byly přesunuty do univerza, které neodpovídá objektivní realitě, neměly mít tržní hodnotu, bez ohledu na to, jestli se toto objektivně nepravdivé univerzum stane po forku vítězným univerzem, nebo ne. To má důležité bezpečnostní důsledky, o kterých se pojednává v oddílu II.

10. *Finalizováno*

Trh vstoupí do finalizovaného stavu (obr. 2f), pokud projde sedmidenním disputačním kolem bez toho, aby byl jeho předběžný výsledek úspěšně zpochybněn, nebo po skončení forku. Výsledek forku nelze po konci intervalu forku zpochybnit a je vždy brán jako konečný. Po finalizování trhu mohou obchodníci vypořádat své pozice přímo na trhu. Když trh vstoupí do finalizovaného stavu, nazýváme jeho vybraný výsledek *konečným výsledkem.*

D. Vypořádání trhu

Obchodník může zavřít svou pozici jedním ze dvou způsobů: prodejem podílů, které drží, jinému obchodníkovi výměnou za peníze, nebo vypořádáním svých podílů na trhu. Připomeňme, že každý podíl vzniká jako část úplné množiny, když je do platformy Augur vložen celkem 1 ETH.[6] Pro získání tohoto 1 ETH zpět ze zástavy musí obchodníci Auguru buď vrátit úplnou množinu, nebo, pokud byl trh finalizován, podíl na vítězném výsledku. Když tato výměna nastane, říkáme, že obchodníci provádějí *vypořádání s kontrakty trhu.*

Například mějme nefinalizovaný trh s možnými výsledky `A` a `B`. Předpokládejme, že Alice má podíl na výsledku `A`, který chce prodat za 0,7 ETH, a Bob má podíl na výsledku `B`, který chce prodat za 0,3 ETH. Nejprve Augur páruje tyto pokyny a získá od účastníků podíly na výsledcích `A` a `B`. Poté Augur dá 0,7 ETH (minus poplatky) Alici a 0,3 ETH (minus poplatky) Bobovi.

Jako druhý příklad mějme finalizovaný trh, jehož vítězný výsledek je `A`. Alice má podíl na `A` a chce vybrat své peníze. Pošle svůj podíl na `A` Auguru a nazpět získá 1 ETH (minus poplatky).

1. *Poplatky za vypořádání*

Augur vybírá poplatky jen v jednom případě: když účastníci trhu vypořádávají své obchody s kontrakty trhu. Augur během vypořádávání vybírá dva druhy poplatků: poplatek tvůrci trhu a poplatek za reportování. Oba tyto poplatky jsou proporcionální k množství, které bude vyplaceno. Takže ve výše uvedeném příkladu vypořádání před finalizací, kde Alice dostane 0,7 ETH a Bob dostane 0,3 ETH, zaplatí Alice 70% poplatků a Bob zaplatí 30% poplatků.

Poplatek tvůrci trhu určuje tvůrce trhu během vytváření trhu a platí se tvůrci trhu při vypořádání. Poplatek za reportování se určuje dynamicky (viz oddíl II C) a platí se reportérům, kteří se účastní procesu reportování.

2. *Vypořádání neplatných trhů*

V případě, že je konečný výsledek trhu `neplatný`, dostanu obchodníci, kteří provedou vypořádání s kontrakty trhu, stejné množství ETH za podíly na každém výsledku. Pokud má trh N možných výsledků (nepočítáme-li výsledek `neplatný`), a cena úplné množiny podílů je C ETH, potom obchodníci dostanou C/N ETH za každý podíl vypořádaný s kontrakty trhu.[16]

3. *Redistribuce reputačních tokenů*

Pokud je trh finalizován bez forku, propadají všechny REP vsazené na výsledek jiný, než je konečný výsledek trhu, a jsou rozděleny uživatelům, kteří vsadili na správný konečný výsledek trhu, proporcionálně k množství REP, které vsadili. Velikosti disputačních jistin jsou vybrány tak, že kdokoliv, kdo úspěšně disputuje výsledek ve prospěch konečného výsledku trhu, je odměněn 50% návratností vložených prostředků na své sázce.[17] To je silnou pobídkou pro reportéry, aby disputovali nepravdivé předběžné výsledky.

II. INCENTIVY A ZABEZPEČENÍ

Mezi tržní kapitalizací REP a důvěryhodností forkujícího protokolu platformy Augur je silná závislost. Pokud je tržní kapitalizace REP dost vysoká[18] a útočníci jsou ekonomicky racionální, měl by výsledek, který převládne ve forku, odpovídat objektivní realitě. Ve skutečnosti by mělo být možné, aby Augur správně fungoval bez zadaných reportérů a disputačních kol. I *pouze* forky by zajistily, že bude orákulum reportovat správně.

Forky jsou však rušivé a časově náročné. Fork zabere až 60 dnů, než rozřeší jeden trh, a dokáže řešit pouze jeden trh v jeden okamžik. Během 60 dnů, během kterých je řešen forkující trh, jsou všechny ostatní nedokončené trhy odloženy.[19] Poskytovatelé služeb musí upravit své služby a držitelé REP musejí převést své REP do jednoho z nových dceřiných univerz. Proto by se forky měly

---

[16] Obchody nemohou být jednoduše zrušeny, když je konečný výsledek trhu `neplatný`, kvůli technickým omezením. Podíly na výsledcích jsou prostě jen tokeny, se kterými lze obchodovat přímo mezi uživateli. ETH a podíly tedy nejsou pod kontrolou platformy Augur a nelze je dát zpět původním vlastníkům, pokud je trh finalizován jako `neplatný`.

[17] Viz větu 3 v příloze A.

[18] Pro podrobnosti viz oddíl II A.

[19] Obchodníci mohou pokračovat v obchodování na těchto trzích, ale tyto trhy nelze finalizovat, dokud fork neskončí.

používat pouze v případě, kdy jsou naprosto nezbytné. Forkování je nejzazší možností.

Naštěstí poté, co jsme ukázali, že lze forku svěřit určení pravdy, lze pomocí incentiv vést účastníky k poctivému chování bez toho, že by se fork musel spouštět. *Mezi základní incentivy platformy Augur patří věrohodná hrozba forku a důvěra, že fork vyřeší situaci správně.*

Dále rozvádíme podmínky, za kterých lze forkovacímu systému věřit, že určí pravdu. Také probíráme systém incentiv a způsob, jakým podporuje rychlé a správné rozřešení trhu.

A. Integrita forkovacího protokolu

Zde probíráme spolehlivost forkovacího procesu a podmínky, za kterých mu lze věřit. Kvůli jednoduchosti budeme při probírání forku označovat dceřiné univerzum, které odpovídá objektivní realitě, jako `pravdivé` univerzum, a jakékoliv jiné dceřiné univerzum jako `nepravdivé` univerzum. Dceřiné univerzum, které získá během intervalu forku nejvíce převedených REP, budeme označovat jako vítězné univerzum a všechna ostatní dceřiná univerza jako prohrávající univerza.

Přirozeně vždy chceme, aby `pravdivé` univerzum bylo vítězným univerzem a aby `nepravdivá` univerza byla prohrávajícími univerzy. Řekneme, že na forkující protokol byl proveden úspěšný útok, když se `nepravdivé` univerzum stane vítězným univerzem forku – což způsobí, že bude forkující trh (a potenciálně všechny nedokončené trhy) vyplacen nesprávně.

Náš přístup k zabezpečení orákula spočívá v uspořádání věcí takovým způsobem, že maximální zisk úspěšného útočníka je menší než minimální náklady na provedení útoku. Toto je formálně zapsáno níže.

1. Maximální zisk účastníka

Útočník, který úspěšně zaútočí na orákulum, způsobí, že všechny nedokončené trhy na Auguru přejdou do `nepravdivého` univerza. Pokud útočník ovládá většinu REP v `nepravdivém` univerzu, může způsobit, že všechny nedokončené trhy budou finalizovány způsobem, jaký chce. V nejhorším případě také může získat všechny prostředky, které jsou drženy ve všech těchto trzích.[20]

Definice 1. Definujeme, a zapisujeme jako I_a, *vlastní souhrn vložených prostředků* Auguru jako hodnotu součtu všech prostředků uložených ve všech nedokončených trzích na Auguru.[21]

Definice 2. Definujeme *parazitický trh* jako trh, který Auguru neplatí poplatky za reportování, ale jehož konečný výsledek závisí na výsledku vlastního trhu platformy Augur.

Definice 3. Definujeme, a zapisujeme jako I_p, *parazitický souhrn vložených prostředků* jako hodnotu součtu všech prostředků uložených ve všech parazitických trzích, jejichž konečný výsledek závisí na nedokončených vlastních trzích platformy Augur.

V nejhorším případě může útočník také být schopen získat všechny prostředky ze všech parazitických trhů, jejichž výsledek závisí na nedokončených vlastních trzích platformy Augur.

Pozorování 1. Maximální (hrubý) zisk útočníka, který úspěšně zaútočí na orákulum, je $I_a + I_p$.

2. Velikost parazitického souhrnu vložených prostředků nelze určit

Augur může přesně a efektivně změřit I_a. Avšak I_p nelze obecně zjistit, protože může existovat libovolně mnoho offline parazitických trhů, každý s libovolným množstvím otevřených pozic. Jelikož maximální možný zisk útočníka zahrnuje nezjistitelnou hodnotu I_p, nemůže být nikdy úplně jisté, že je orákulum bezpečné před ekonomický racionálními útočníky.

Pokud však předpokládáme, že je I_p v praxi přiměřeným způsobem omezeno, můžeme definovat podmínky, za kterých můžeme zajistit, že je orákulum bezpečné.

3. Minimální náklady na úspěšný útok

Dále zvažme náklady na útok na orákulum. Nechť P je cena REP. Nechť ϵ označuje jeden attorep[22]. Nechť M označuje celkové existující množství REP („peněžní zásobu“ REP). Nechť S označuje poměr M, který bude přesunut do pravdivého univerza během intervalu forku.

Součin SM tak reprezentuje celkové množství REP přesunuté během intervalu forku do pravdivého univerza a součin PM je tržní kapitalizace REP.

Nechť P_f označuje cenu REP přesunutého do `nepravdivého` univerza vybraného útočníkem. Všimněme si, že kdyby $P \leq P_f$, nebylo by orákulum bezpečné před ekonomicky racionálními útočníky, protože by byl alespoň stejně výnosný převod REP do nepravdivého univerza jako vůbec REP nepřevádět.

[20] To by vyžadovalo, aby útočník získal *všechny* podíly na určitém výsledku a poté zařídil finalizaci trhu odpovídající tomuto výsledku.

[21] To zahrnuje externí trhy, které Auguru platí poplatky za reportování.

[22] Jeden *attorep* je 10^{-18} REP.

4. Integrita

Předpoklad 1. *Reportéři, kteří nejsou útočníky, nebudou během forku převádět REP do* nepravdivého *univerza.*[23]

Úspěšný útok na orákulum záměrně vyžaduje, aby bylo během intervalu forku přesunuto více REP do některého nepravdivého univerza než do pravdivého univerza. Předpoklad je, že do nepravdivého univerza přesune REP pouze útočník. Množství REP přesunutého během forku do pravdivého univerza se zapíše jako SM. Takto musí útočník pro zajištění úspěchu přesunut alespoň $SM + \epsilon$ REP. Pro jednoduchost budeme ignorovat zanedbatelné ϵ a řekneme, že úspěšný útok vyžaduje přesunutí alespoň SM REP, které mají před přesunutím hodnotu SMP, do nějakého nepravdivého univerza.

Pokud útočník během intervalu forku převede SM REP, získá SM REP v dceřiném univerzu, do kterého je převede.[24] Pokud útočník převede své prostředky do nepravdivého univerza, potom se hodnota těchto tokenů změní na SMP_f. Proto jsou minimální náklady útočníka $(P - P_f)SM$.

Pozorování 2. Minimální množství REP, které musí úspěšný útočník převést během intervalu forku do nepravdivého univerza, je SM, což stojí útočníka $(P - P_f)SM$.

Povšimněme si, že pokud $S > \frac{1}{2}$, je tento útok *nemožný*, protože neexistuje dostatečné množství REP vně pravdivého univerza na to, aby se nějaké nepravdivé univerzum stalo vítězným univerzem.

Ekonomicky racionálním útočníkům navzdory orákulum správně určí výsledek, který odpovídá objektivní realitě, pokud je maximální zisk útočníka menší než minimální náklady na útok. Z pozorování 1 a 2 vidíme, že toto nastane, kdykoliv $S > \frac{1}{2}$ nebo $I_a + I_p < (P - P_f)SM$. To nám dává formální definici integrity.

Definice 4. (Vlastnost integrity) Forkující protokol má *integritu*, kdykoliv $S > \frac{1}{2}$ nebo kdykoliv $I_a + I_p < (P - P_f)SM$.

Nerovnost výše lze vyřešit pro PM a tak ukázat vztah mezi integritou forkujícího protokolu a tržní kapitalizací REP.

Věta 1. *(Věta o bezpečné tržní kapitalizaci) Forkující protokol má integritu právě tehdy, když:*

1. $S > \frac{1}{2}$, *nebo*
2. $P_f < P$ *a tržní kapitalizace REP je větší než* $\frac{(I_a+I_p)P}{(P-P_f)S}$.

Důkaz. Předpokládejme, že forkující protokol má integritu. Potom z definice $S > \frac{1}{2}$ nebo $I_a + I_p < (P - P_f)SM$. Předpokládejme, že $I_a + I_p < (P - P_f)SM$. Vzhledem k tomu, že $I_a + I_p \geq 0$ a $SM > 0$, víme, že $P_f < P$. Potom, když vyřešíme $I_a + I_p < (P - P_f)SM$ pro PM, vidíme, že $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Takto je dokázán první směr.

Nyní předpokládejme, že $S > \frac{1}{2}$ nebo že $P_f < P$ a $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Pokud $S > \frac{1}{2}$, pak forkující protokol má z definice integritu. Pokud $P_f < P$ a $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$, pak řešení nerovností pro $I_a + I_p$ dává $I_a + I_p < (P - P_f)SM$ a forkující protokol má integritu. □

B. Naše předpoklady a jejich důsledky

Věříme, že by obchodníci nechtěli obchodovat na Auguru v univerzu, kde reportéři lhali. Také věříme, že tvůrci trhů nebudou platit za vytváření trhů v univerzu, kde nejsou žádní obchodníci. V univerzu bez trhů nebo obchodování REP neposkytuje svým držitelům žádné dividendy. Proto věříme, že REP poslaný do nepravdivého univerza nebude mít žádnou nezanedbatelnou tržní hodnotu a tuto skutečnost vyjadřujeme tak, že necháváme $P_f = 0$.

Myslíme, že lze rozumně očekávat, že alespoň 20% existujících REP bude během intervalu forku převedeno do pravdivého univerza, a tuto skutečnost vyjadřujeme tak, že necháváme $S \geq \frac{1}{5}$. Jsme také ochotni připustit parazitické otevřené pozice ve výši až 50% vlastních otevřených pozic, takže máme $I_a \geq 2I_p$.

Za těchto předpokladů nám věta 1 říká, že forkující protokol má integritu, kdykoliv má tržní kapitalizace REP hodnotu alespoň 7,5 krát větší než vlastní souhrn vložených prostředků.[25]

C. Hýbání s tržní kapitalizací

Augur získává informace o ceně REP stejným způsobem, jako získává jakékoliv jiné informace o reálném světě: prostřednictvím trhu platformy Augur. Tímto způsobem Augur může zjistit aktuální tržní kapitalizaci REP. Augur tak také může měřit aktuální vlastní souhrn vložených prostředků a může tak určovat, jaká by tržní kapitalizace měla být, aby byly splněny požadavky na jeho integritu.

---

[23] Mohou existovat případy, kdy poctiví reportéři převedou REP do nepravdivého univerza náhodou nebo z nepozornosti. Takové chování však v praxi nelze odlišit od spolupráce s útočníkem.

[24] V praxi útočník získá $1,05SM$ REP v dceřiném univerzu kvůli 5% bonusu za převedení před uplynutím 60 dnů intervalu forku. Tento 5% bonus zde pro jednoduchost nepočítáme. Diskuzi, která zahrnuje tento 5% bonus, naleznete v příloze C.

[25] Další alternativní předpoklady a jejich důsledky naleznete v příloze B.

Každé univerzum začíná s výchozím poplatkem za reportování ve výši 1%. Pokud je aktuální tržní kapitalizace níže než cílová, poplatky za reportování se automaticky zvýší (ale nikdy nebudou vyšší než 33,3%), což vyvine tlak na zvýšení ceny REP nebo tlak na snížení nového vlastního souhrnu vložených prostředků. Pokud je aktuální tržní kapitalizace výše než cílová, poplatky za reportování se automaticky sníží (ale nikdy nebudou nižší než 0,01%), takže obchodníci nebudou platit více, než je nutné, za zabezpečení platformy.

Poplatky za reportování se určují následovně. Nechť r je poplatek za reportování z předchozího časového okna, nechť t je cílová tržní kapitalizace a nechť c je aktuální tržní kapitalizace. Potom poplatek za reportování pro aktuální poplatkové časové okno se vypočítá jako $\max\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10{,}000}\right\}$.

D. Využití hrozby forku

Jak již bylo zmíněno výše, forky jsou rušivým a pomalým způsobem, jak finalizovat trhy. Augur nepoužívá forky k rozhodnutí všech trhů, ale využívá *hrozbu* forku k efektivnímu rozhodnutí o výsledku trhu.

Připomínáme, že jakákoliv sázka, která úspěšně zpochybní výsledek ve prospěch konečného výsledku trhu, má návratnost 50%.[26] V případě forku by měl veškerý REP vsazený na nepravdivé výsledky trhu ztratit veškerou ekonomickou hodnotu a REP vsazený na pravdivý výsledek trhu je odměněn 50% REP ve dceřiném univerzu, které odpovídá pravdivému výsledku trhu (bez ohledu na výsledek forku). Proto v případě vynucení forku držitelé REP, kteří zpochybní nepravdivé výsledky ve prospěch pravdivých výsledků, vždy dopadnou lépe, a REP vsazené na nepravdivé výsledky ztratí veškerou ekonomickou hodnotu.

Věříme, že tato situace je dostatečná pro zajištění, že všechny nepravdivé předběžné výsledky budou úspěšně zpochybněny.

III. POTENCIÁLNÍ PROBLÉMY A RIZIKA

A. Parazitické trhy

Připomeňme, že parazitický trh je trh, který neplatí poplatky za reportování Auguru, ale rozhoduje se na základě výsledku vlastního trhu platformy Augur. Protože parazitické trhy nemusí platit poplatky za reportování, mohou nabídnout stejné služby jako Augur s nižšími poplatky. To může mít vážné následky pro integritu forkujícího protokolu platformy Augur.

Zvláště pokud parazitické trhy přetahují obchodní pokyny od Auguru, reportéři Auguru dostanou méně na poplatcích za reportování. To může vyvinout tlak na snížení tržní kapitalizace REP. Pokud se tržní kapitalizace REP příliš sníží, integrita forkujícího protokolu je ohrožena (věta 1). Ve výsledku mohou parazitické trhy ohrožovat dlouhodobou životaschopnost platformy Augur a měly by být tvrdé potlačovány.

Naší nejlepší obranou před parazitickými trhy je zlevnit obchodování na Auguru tak, jak je to jen možné (a přitom stále udržovat integritu orákula), aby se minimalizoval zisk z provozování parazitických trhů.

B. Volatilita souhrnu vložených prostředků

Velké, náhlé a neočekávané změny ve velikosti souhrnu vložených prostředků – jako ty, které mohou nastat při populárních sportovních událostech – vyústí v rychlé zvýšení požadavku na tržní kapitalizaci kvůli integritě forkujícího protokolu (věta 1). Když požadavek na tržní kapitalizaci přesáhne vlastní tržní kapitalizaci, existuje riziko, že ekonomicky racionální útočníci vyvolají fork, který nebude správně vyřešen. Augur se sice během takových situací snaží posunout tržní kapitalizaci výše (viz oddíl II C), ale tyto posuny nejsou dostatečné a dají se provést pouze během 7denního poplatkového časového okna.

Stojí však za zmínku, že spekulanti, kteří vidí náhlý nárůst souhrnu vložených prostředků, mohou koupit REP v očekávání pohybu tržní kapitalizace a tak zvýšit tržní kapitalizaci, snad až do bodu, kde již integrita forkujícího protokolu není ohrožena. Takže doba, během níž je orákulum zranitelné, nemusí být dost dlouhá na to, aby útočník úspěšně tuto zranitelnost využil.

C. Nekonzistentní nebo podvodné zdroje pro reportování

Při vytváření trhu tvůrci trhu určují zdroj pro reportování, pomocí kterého by reportéři měli určit výsledek příslušné události. Pokud tvůrce trhu vybere nekonzistentní nebo podvodný zdroj pro reportování, poctiví reportéři mohou ztratit peníze.

Například řekněme, že příslušný trh má výsledky `A` a `B` a že tvůrce trhu Serena vybrala jako zdroj pro reportování vlastní webovou stránku, `attacker.com`. Po uplynutí koncového času události trhu Serena – která je pro tento trh také zadaným reportérem – reportuje výsledek `A` a aktualizuje `attacker.com`, takže bude sdělovat, že správný výsledek je `B`. Poctiví reportéři, kteří zkontrolují `attacker.com`, zjistí, že počáteční report je nesprávný, a během prvního disputačního kola by měli úspěšně zpochybnit předběžný výsledek ve prospěch výsledku `B`. Serena opět aktualizuje stránku `attacker.com`, která teď bude sdělovat, že správný výsledek je `A`, a trh vstoupí do druhého disputačního kola. Reportéři, kteří zkont-

[26] Měřeno v REP, který existuje v univerzu, které odpovídá konečnému výsledku trhu. Viz větu 3 v oddílu A.

rolují attacker.com, opět zjistí, že předběžný výsledek (výsledek B) je nesprávný, a mohou jej úspěšně zpochybnit. Serena může toto chování opakovat, dokud nebude trh dokončen. Bez ohledu na konečný výsledek trhu někteří poctiví reportéři ztratí peníze.

Existuje několik druhů tohoto útoku. Jednoduché ignorování trhu s pochybnými zdroji pro reportování není dostatečné, protože v případě, že takový trh způsobí fork, budou všichni držitelé REP muset vybrat dceřiné univerzum, do kterého přesunou své REP. Reportéři by měli zůstat obezřetní ohledně trhů s pochybnými zdroji pro reportování. Takové zdroje by měly být veřejně označeny, takže reportéři mohou spolupracovat a zajistit, že konečný výsledek takových trhů bude neplatný.

D. Dotazy orákula na sebe sama

Trhy, na kterých se obchoduje s informacemi o budoucím chování platformy Augur, mohou mít na chování orákula samotného nepříznivý vliv [7]. Například si představme trh, který obchoduje s otázkou „Vyskytne se před 31. prosincem 2018 zadaný reportér, který nepředloží report během třídenního reportovacího okna?“ Sázky umístěné na výsledek Ne mohou fungovat jako pobídka pro zadané reportéry, aby úmyslně nepředložili report. Pokud zadaný reportér dokáže koupit dostatek podílů Ano za dostatečně nízké ceny, aby se mu vykompenzovala ztráta za přítomnostní jistinu, může úmyslně nepředložit report.

Pokud je tržní kapitalizace REP dostatečně vysoká (věta 1), potom tyto dotazy orákula na sebe sama nebudou ohrožovat integritu forkujícího protokolu. Mohou však negativně ovlivnit efektivitu Auguru tím, že způsobí prodlevy ve finalizacích trhů. Trhy by se sice stále měly finalizovat správně, ale toto chování je rušivé a nechtěné.

E. Nejistá účast ve forku

Předem nelze zjistit, jaké množství REP bude během intervalu forku převedeno do pravdivého univerza, a proto nelze předem vědět, jestli je tržní kapitalizace dostatečně vysoká, aby orákulum mělo integritu (věta 1). Naše víra v integritu forkujícího protokolu nemůže být silnější než naše víra v naše předpoklady o dolní hranici poctivé účasti během intervalu forku. Předpokládáme, že alespoň 20% všech REP bude během intervalu forku převedeno do pravdivého dceřiného univerza, ale nemůžeme to garantovat.

Forky platformy Augur se liší od forků na blockchainu v jednom důležitém aspektu: po forku na blockchainu bude mít uživatel, který vlastnil token v rodičovském blockchainu, vlastnit tento token v obou dceřiných blockchainech. Pokud ignorujeme útoky přenesení transakcí (replay attacks), nejsou forky na blockchainu pro uživatele moc rizikové. Po forku na Auguru však uživatel, který vlastní REP v rodičovském univerzu, může tento token převést pouze do jednoho dceřiného univerza. Pokud uživatel převede svůj token do univerza, které není vítězným univerzem, jeho token může ztratit veškerou hodnotu. Proto je převedení REP během intervalu forku předtím, než je známo, které dceřiné univerzum získalo konsensus, pro uživatele rizikové. Toto riziko může uživatele odradit od účasti na řešení kontroverzních forků.

Ve snaze o kompenzaci tohoto rizika a podpoře účasti během intervalu forku dostanou všichni držitelé REP, kteří převedou své tokeny během šedesáti dnů od začátku forku, 5% dodatečných REP ve dceřiném univerzu, do kterého je převedli (viz oddíl I C 9). Nemůžeme však vědět předem, jestli tento 5% bonus bude dostatečný pro kompenzaci tohoto rizika a podporu účasti během intervalu forku.

F. Nejednoznačné nebo subjektivní trhy

Jako trhy na Auguru jsou vhodné pouze události s objektivně zjistitelnými výsledky. Pokud si reportéři myslí, že trh není vhodný pro určení výsledku pomocí této platformy – například pokud je nejednoznačný, subjektivní, nebo pokud výsledek není znám ihned po uplynutí události – měli by výsledek tohoto trhu reportovat jako neplatný. Pokud je konečný výsledek trhu neplatný, obchodníkům se vyplatí poměrné množství za všechny možné výsledky. Na skalárních trzích obchodníci dostanou střední hodnotu mezi minimální cenou na trhu a maximální cenou na trhu.

Lze si představit trhy, u kterých jsou si někteří reportéři jistí, že výsledek je A, a ostatní jsou si jistí, že výsledek je B. Například v roce 2006 TradeSports umožnil svým uživatelům spekulovat o tom, jestli Severní Korea před koncem července 2006 vypustí balistickou střelu, která přistane vně jejího vzdušného prostoru. 5. července 2006 Severní Korea úspěšně vypustila balistickou střelu, která přistála vně jejího vzdušného prostoru, a o této události podala zprávu mnohá světová média a potvrdilo ji mnoho zdrojů z vlády Spojených států. Avšak ministerstvo obrany Spojených států tuto událost nepotvrdilo, což bylo příslušným kontraktem u TradeSports vyžadováno. TradeSports dospěli k závěru, že podmínky kontraktu nebyly naplněny, a odpovídajícím způsobem vyplatili peníze.[27]

Toto je příklad, kdy duch trhu – předpovězení vypálení rakety – byl zřetelně naplněn, ale formální náležitosti trhu – předpovězení, jestli ministerstvo obrany Spojených států toto vypálení potvrdí – nebyly. TradeSports, což byla centralizovaná webová stránka, byl schopen jednostranně určit výsledek trhu. Pokud taková událost nastane na trhu platformy Augur, držitelé REP mohou mít na výsledek trhu různé názory a odpovídajícím způsobem

[27] Pro podrobnosti viz https://en.wikipedia.org/wiki/Intrade#Disputes.

vsadit své REP. V nejhorším případě to může vyústit do forku, kde si REP ve více než jednom dceřiném univerzu bude udržovat nenulovou tržní hodnotu.

PODĚKOVÁNÍ

Děkujeme Abrahamovi Othmanovi, Alexovi Chapmanovi, Sereně Randolphové, Tomovi Haileovi, Georgovi Hotzovi, Scottovi Bigelowovi a Peronetovi Despeignesovi za jejich podnětnou zpětnou vazbu a návrhy.

[1] Buterin, V.: A next generation smart contract and decentralized application platform. *https://github.com/ethereum/wiki/wiki/White-Paper*, 2013.

[2] Clark, J.; Bonneau, J.; Felten, E.; aj.: On Decentralizing Prediction Markets and Order Books. In *WEIS '14: Proceedings of the 10th Workshop on the Economics of Information Security*, June 2014.

[3] Goel, S.; Reeves, D.; Watts, D.; aj.: Prediction Without Markets. In *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, ACM, 2010, ISBN 978-1-60558-822-3, s. 357–366, doi:10.1145/1807342.1807400.

[4] Hanson, R.; Oprea, R.; Porter, D.: Information aggregation and manipulation in an experimental market. *Journal of Economic Behavior & Organization*, ročník 60, č. 4, 2006: s. 449–459.

[5] Manski, C.: Interpreting the Predictions of Prediction Markets. *NBER Working Paper No. 10359*, 2004.

[6] Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*, 2008.

[7] Othman, A.; Sandholm, T.: Decision Rules and Decision Markets. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: Volume 1 - Volume 1*, AAMAS '10, International Foundation for Autonomous Agents and Multiagent Systems, 2010, ISBN 978-0-9826571-1-9, s. 625–632.

[8] Pennock, D.; Lawrence, S.; Giles, C.; aj.: The real power of artificial markets. *Science*, ročník 291, 2001: s. 987–988.

[9] Peterson, J.; Krug, J.: Augur: a Decentralized, Open-Source Platform for Prediction Markets. *arXiv:1501.01042v1 [cs.CR]*, 11 2014, 1501.01042v1.

[10] Surowiecki, J.: *The Wisdom of Crowds*. Anchor, 2005.

[11] Wolfers, J.; Zitzewitz, E.: Prediction Markets. *Journal of Economic Perspectives*, ročník 18, č. 2, 2004: s. 107–126.

[12] Wolfers, J.; Zitzewitz, E.: Interpreting Prediction Market Prices as Probabilities. *NBER Working Paper No. 10359*, 2005.

Příloha A: Délka finalizace a redistribuce

Začínáme s některými zápisy, definicemi a pozorováními.

Definice 5. Nechť pro daný trh M je Ω_M prostor výsledků (nebo množina výsledků) M.

Definice 6. Nechť pro $n \geq 1$ a $\omega \in \Omega_M$ označuje $S(\omega, n)$ celkovou velikost sázky na výsledek ω na začátku disputačního kola n. To zahrnuje všechny sázky ze všech úspěšných disputačních jistin ve prospěch ω ve všech předchozích disputačních kolech.

Definice 7. Nechť pro $n \geq 1$ a $\omega \in \Omega_M$ označuje $S(\overline{\omega}, n)$ velikost sázky na všechny výsledky v Ω_M *kromě* ω na začátku disputačního kola n:

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

Definice 8. Nechť pro $n \geq 1$ označuje A_n celkovou sázku přes všechny výsledky M na začátku disputačního kola n:

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

Pozorování 3. Potom vyplývá, že $A_n - S(\omega, n) = S(\overline{\omega}, n)$.

Definice 9. Nechť pro $n \geq 1$ označuje $\hat{\omega}_n$ předběžný výsledek na začátku disputačního kola n. Například $\hat{\omega}_1$ je výsledek reportovaný počátečním reportérem.

Definice 10. Nechť pro $n \geq 1$ a $\omega \neq \hat{\omega}_n$ označuje $B(\omega, n)$ velikost sázky potřebné pro úspěšné složení disputační jistiny ve prospěch výsledku ω během disputačního kola n.

Připomínáme, že velikost sázky vyžadované pro úspěšné naplnění disputační jistiny ve prospěch výsledku ω během disputačního kola n, kde $\omega \neq \hat{\omega}_n$, je podle rovnice 1 $B(\omega, n) = 2A_n - 3S(\omega, n)$.

Pozorování 4. Pokud je během disputačního kola n úspěšně složena disputační jistina ve prospěch výsledku ω, potom $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. To znamená, že tato úspěšná disputační sázka je jedinou novou sázkou, která se na konci disputačního kola n použije na výsledek ω.

Pozorování 5. Pro všechny $\omega \neq \hat{\omega}_n$ platí $S(\omega, n-1) = S(\omega, n)$. To jest pokud disputační jistina není celá složena ve prospěch výsledku ω, není na začátku následujícího disputačního kola přidána k výsledku ω žádná dodatečná sázka. To je způsobeno tím, že se všechny neúspěšné disputační sázky vracejí uživatelům na konci disputačního kola.

Pozorování 6. Pro všechna $n \geq 2$ platí $A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$. To znamená, že celková sázka přes všechny výsledky na začátku disputačního kola je jednoduše celková sázka ze začátku předchozího disputačního kola plus úspěšná disputační sázka z předchozího disputačního kola. Všechny ostatní sázky se na konci předchozího disputačního kola vracejí uživatelům.

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

Důkaz. Předpokládejme, že trh vstoupí do disputačního kola n, kde $n \geq 2$. Během disputačního kola $n-1$ musel být výsledek $\hat{\omega}_{n-1}$ úspěšně zpochybněn ve prospěch výsledku $\hat{\omega}_n$. Podle rovnice 1 je velikost této disputační jistiny $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Z pozorování 3 lze toto zapsat jako

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

Víme, že během kola $n-1$ byla úspěšně naplněna disputační jistina. S použitím pozorování 4 vidíme, že $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. Pozorování 5 nám říká, že celkové množství vsazené na $\overline{\hat{\omega}_n}$ se nemění mezi koly $n-1$ a n, $2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$. Takto se rovnice A1 zjednodušuje na $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$. □

Věta 3. *Držitelé REP, kteří úspěšně zpochybní výsledek ve prospěch konečného výsledku trhu, budou mít 50% návratnost vložených prostředků na své disputační sázce (měřeno v REP, které existuje v univerzu, které odpovídá konečnému výsledku trhu), pokud trh není přerušen forkem způsobeným některým jiným trhem.*

Důkaz. Během forku dostanou uživatelé, kteří úspěšně složili disputační jistinu ve prospěch konečného výsledku trhu, (pomocí tokenů vytvořených během forku) 50% návrat ze své disputační sázky, když převedou svou disputační sázku do odpovídajícího dceřiného univerza. Takto je v případě, kdy probíraný trh způsobil fork, věta okamžitě pravdivá.

Nyní mějme případ, kdy se probíraný trh dokončí bez způsobení forku a reportování není přerušeno forkem způsobeným nějakým jiným trhem.

Konečný výsledek označíme jako ω_{Final} a předpokládáme, že bude trh dokončen na konci disputačního kola n, kde $n \geq 2$. To znamená, že předběžný výsledek pro kolo n je ω_{Final} a že výsledek není úspěšně zpochybněn během kola n. Jinými slovy: $\hat{\omega}_n = \omega_{\text{Final}}$. Potom z lemmatu 2 víme, že $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$.

Vzhledem k tomu, že se trh dokončí na konci kola n a k výsledku se nepřidá žádná další sázka, ukazuje rovnice výše konečnou velikost sázky na konečný výsledek trhu, ω_{Final}, a součet všech sázek na všechny ostatní výsledky trhu, $\overline{\omega_{\text{Final}}}$. Povšimněme si, že na konečný výsledek trhu je dvojnásobně větší sázka, než na všechny ostatní výsledky dohromady.

Augur redistribuuje všechny sázky na všechny výsledky jiné než je konečný uživatelům, kteří vsadili

na ω_{Final}, proporcionálně k množství REP, které vsadili. Proto uživatelé, kteří úspěšně složili disputační jistinu ve prospěch ω_{Final}, získají 50% návratnost vložených prostředků na své vsazené REP. □

Dále zvažme maximální počet disputačních kol, který je potřebný pro určení konečného výsledku trhu. Výraz 1 je minimalizován, když je ω vybráno jako výsledek, který není předběžný a který začíná v disputačním kole s nejvyšší hodnotou sázky. Z lemmatu 2 plyne, že výsledek, který není předběžný a má nejvyšší hodnotu sázky, je předběžný výsledek v předchozím disputačním kole. Proto nejmenší možná disputační jistina, kterou lze úspěšně naplnit během disputačního kola n, kde $n \geq 2$, je $B(\hat{\omega}_{n-1}, n)$.

Jinými slovy disputační jistina roste *nejpomaleji*, když se při disputaci opakovaně rozhoduje mezi dvěma výsledky, ve prospěch jednoho a pak druhého. Z toho vyplývá, že počet disputačních kol potřebných pro to, aby trh zahájil fork, je *maximální*, když se při disputaci opakovaně rozhoduje mezi dvěma výsledky, ve prospěch jednoho a pak druhého. Proto můžeme určit maximální počet disputačních kol, kterými může kterýkoliv trh projít před zahájením forku tak, že najdeme maximální možný počet disputačních kol, která mohou nastat v tomto zvláštním případě, kde se rozhoduje mezi dvěma výsledky, ve prospěch jednoho a pak druhého. Probereme nyní tento případ.

Předpokládejme, že každá následující disputační jistina je naplněna ve prospěch předběžného výsledku předchozího disputačního kola. Potom tyto dva předběžné výsledky, mezi kterými se opakovaně rozhoduje, jsou $\hat{\omega}_1$ a $\hat{\omega}_2$.

Pozorování 7. V případě, že se opakovaně rozhoduje mezi dvěma stejnými předběžnými výsledky, ve prospěch jednoho a pak druhého, $\hat{\omega}_n = \hat{\omega}_{n-2}$ pro všechna $n \geq 3$.

Definice 11. Nechť d označuje velikost sázky umístěné během zahajovacího reportu na $\hat{\omega}_1$. Vzhledem k tomu, že je v této situaci znám předběžný výsledek pro každé kolo, můžeme zjednodušit náš zápis pro velikosti disputačních jistin. Definujeme B_n, což bude zkráceně označovat velikost disputační jistiny vyžadované pro kolo n, takže $B_1 = 2d$ a $B_n = B(\hat{\omega}_{n-1}, n)$ pro všechna $n \geq 2$. To zlepší čitelnost a srozumitelnost.

Pozorování 8. V případě, že se při disputaci opakovaně rozhoduje mezi dvěma výsledky, ve prospěch jednoho a pak druhého, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ pro $n \geq 3$. (To je, všechny ostatní úspěšné disputační jistiny jsou přidány ke stejnému výsledku.)

Lemma 4. *Pokud se při disputaci opakovaně rozhoduje mezi dvěma výsledky, ve prospěch jednoho a pak druhého, potom pro všechna n, kde $n \geq 3$:*

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

Důkaz. (Indukcí pro n)

Předpokládejme, že se při disputaci opakovaně rozhoduje mezi dvěma výsledky, ve prospěch jednoho a pak druhého.

(Počáteční případ) Z definice a výrazu 1 můžeme provést následující pozorování.

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

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, takže část 1 lemmatu platí pro $n = 3$.

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, takže část 2 lemmatu platí pro $n = 3$.

$B_3 = 6d = 3d2^{3-2}$, takže část 3 lemmatu platí pro $n = 3$.

Takže celé lemma platí pro počáteční případ $n = 3$.

(Indukce) Předpokládejme, že lemma platí pro n takové, že $3 \leq n \leq k$. Chceme ukázat že lemma platí pro $n = k + 1$. To znamená, že chceme ukázat, že:

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

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

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

Nejprve dokážeme část (a). Z pozorování 8:

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

Z pozorování 7 můžeme rovnici výše zapsat jako:

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

Podle indukčního kroku můžeme zapsat $S(\hat{\omega}_{k-2}, k-1)$ na pravé straně jako $\frac{2}{3}B_{k-2}$ a dostaneme:

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

Z indukčního kroku můžeme zapsat B_{k-2} jako $3d2^{k-4}$ a B_{k-1} jako $3d2^{k-3}$:

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

Použitím pozorování 7 na levou stranu dostaneme:

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

Nakonec si můžeme všimnout, že podle rovnice výše a indukční hypotézy $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. To dokazuje část (a).

Dále dokážeme část (b). Z pozorování 6:

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

Z indukčního kroku $A_k = 2B_{k-1}$:

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

Z indukčního kroku $B_{k-1} = 3d2^{k-3}$, takže pravou část lze zjednodušit na

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

Z indukčního kroku $B_k = 3d2^{k-2}$, takže pravou stranu lze zapsat jako

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

a část (b) je dokázána.

Nakonec dokážeme část (c). Z 1:

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

Z pozorování 8 můžeme napsat $S(\hat{\omega}_k, k+1)$ jako $S(\hat{\omega}_k, k-1) + B_{k-1}$:

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

Z pozorování 7 $\hat{\omega}_k = \hat{\omega}_{k-2}$:

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

Z pozorování 6 $A_{k+1} = A_k + B_k$:

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

Z indukčního kroku $A_k = 2B_{k-1}$ a $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$:

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

Z indukčního kroku $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ and $B_{k-2} = 3d2^{k-4}$. Provedení těchto nahrazení a zjednodušení nám dává:

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

To dokazuje část (c) a uzavírá důkaz lemmatu. □

Věta 5. *Pokud není trh přerušen forkem způsobeným jiným trhem, může každý trh bez finalizace nebo způsobení forku projít nejvýše 20 disputačními koly.*

Důkaz. Předpokládejme, že daný trh není přerušen forkem způsobeným některým jiným trhem. Potom, jak je ukázáno výše, víme, že počet disputačních kol vyžadovaných k tomu, aby trh zahájil fork, je maximální, když se opakovaně rozhoduje mezi dvěma výsledky, ve prospěch jednoho a pak druhého. Část 3 lemmatu 4 nám říká, že je v této situaci velikost disputační jistiny, která je potřebná pro úspěšné zpochybnění předběžného výsledku během kola n, dána jako $3d2^{n-2}$, kde d je velikost sázky umístěné během zahajovacího reportu.

Víme, že forky nastávají po úspěšném naplnění disputační jistiny ve výši alespoň 2,5% všech existujících REP a víme, že existuje 11 milionů REP. Proto fork nastává, když je složena disputační jistina ve výši 275 000 REP. Víme také, že $d \geq 0,35$ REP, protože minimální velikost sázky na zahajovací report je 0,35 REP[28].

Řešení $3(0,35)2^{n-2} > 275000$ pro $n \in \mathbb{Z}$ dává $n \geq 20$. Takto můžeme zaručit, že bude trh vyřešen, nebo způsobí fork po nejvýše 20 disputačních kolech. □

Příloha B: Alternativní předpoklady a důsledky

Připomínáme, že:

- S je část všech REP, která je během intervalu forku přesunuta do `pravdivého` univerza
- P je cena REP v `pravdivém` univerzu
- P_f je cena REP, který byl převeden do `nepravdivého` univerza vybraného útočníkem
- I_a je vlastní souhrn vložených prostředků platformy Augur
- I_p je parazitický souhrn vložených prostředků

Augur dělá pro určení cílové tržní kapitalizace určité předpoklady o S, P_f a I_p. Zejména Augur předpokládá, že alespoň 20% všech REP bude během intervalu forku převedeno do `pravdivého` univerza, REP převedené do `nepravdivého` univerza nebude mít nezanedbatelnou hodnotu a že parazitický souhrn vložených prostředků bude mít hodnotu nejvýše poloviny vlastního souhrnu vložených prostředků. Jinými slovy: $S \geq 0,2$, $P_f = 0$ a $I_a \geq 2I_p$. Za těchto předpokladů nám věta 1 říká, že forkovací protokol má integritu, kdykoliv je tržní kapitalizace REP větší než 7,5 krát vlastní souhrn vložených prostředků.

O S, P_f a I_p můžete vznést vlastní předpoklady a dospět k vlastním závěrům o tom, jak velká musí být tržní kapitalizace, aby mělo orákulum v praxi integritu. Zde pro vaše pohodlí předkládáme některé alternativní scénáře.

Scénář 1. Více než 50% existujících REP bude během intervalu forku převedeno do `pravdivého` univerza. V tomto případě vůbec nezáleží na P_f ani na I_p. Protože $S > \frac{1}{2}$, forkující protokol na má integritu bez ohledu na to, jaká je tržní kapitalizace. Neexistovalo by dostatečné množství zbývajících REP, aby mohl být útočník úspěšný.

Scénář 2. 48% existujících REP bude během intervalu forku převedeno do `pravdivého` univerza, neexistují parazitické trhy a REP převedený do `nepravdivého` univerza nemá žádnou hodnotu. V tomto případě $S = 0,48$, $I_p = 0$ a $P_f = 0$. Za těchto předpokladů musí být tržní kapitalizace REP přibližně dvakrát větší než vlastní souhrn vložených prostředků, aby měl forkující protokol integritu.

[28] viz přílohy E 2 a E 3

Scénář 3. 20% existujících REP bude během intervalu forku převedeno do pravdivého univerza, parazitický souhrn vložených prostředků je stejně velký jako vlastní souhrn vložených prostředků a REP převedené do nepravdivého univerza se obchoduje za 5% hodnoty REP převedeného do pravdivého univerza. V tomto případě $S = 0,2$, $I_p = I_a$ a $P_f = 0,05P$. Za těchto předpokladů musí být tržní kapitalizace REP větší než přibližně 10,5 krát vlastní souhrn vložených prostředků, aby měl forkující protokol integritu.

Scénář 4. Pouze 5% existujících REP bude během intervalu forku převedeno do pravdivého univerza, parazitický souhrn vložených prostředků je dvojnásobně větší než vlastní souhrn vložených prostředků a REP převedený do nepravdivého univerza se obchoduje za 5% hodnoty REP převedeného do pravdivého univerza. V tomto případě $S = 0,05$, $I_p = 2I_a$ a $P_f = 0,05P$. Za těchto předpokladů musí být tržní kapitalizace REP asi 63 krát větší než vlastní souhrn vložených prostředků, aby forkující protokol měl integritu.

Příloha C: Vliv bonusu za brzké převedení na integritu forkujícího protokolu

Pro jednoduchost jsme při diskusi o integritě forkujícího protokolu zanedbávali 5% bonus za brzké převedení a jeden malý člen. Zde opět odvodíme větu 1 s tím, že tyto dvě věci vezmeme do úvahy.

Jako předtím je množství REP převedené do pravdivého univerza během reportování zapsáno jako SM. Pro úspěšný útok musí tedy útočník převést alespoň $SM + \epsilon$ REP, jehož hodnota před převedením je $(SM + \epsilon)P$, do nějakého nepravdivého univerza.

Pokud útočník během intervalu forku převede $SM + \epsilon$ REP do nepravdivého univerza, získá $1,05(SM+\epsilon)$ REP v dceřiném univerzu, do kterého je převedl. Z definice P_f je hodnota těchto tokenů dána jako $1,05(SM + \epsilon)P_f$. Minimální náklady útočníka jsou tak $(SM + \epsilon)P - 1,05(SM + \epsilon)P_f$, což lze vyjádřit jako $(SM + \epsilon)(P - 1,05P_f)$.

Jako předtím je maximální (hrubý) zisk útočníka dán jako $I_a + I_p$. Proto můžeme říci, že forkující protokol má integritu, kdykoliv $S > \frac{1}{2}$ nebo:

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

Vyřešíme-li výše uvedenou nerovnost pro tržní kapitalizaci PM, vidíme, že forkující protokol má integritu právě tehdy, když:

1. $S > \frac{1}{2}$ nebo
2. $1,05P_f < P$ a tržní kapitalizace REP je větší než $\frac{P(I_a+I_p-\epsilon(P-1,05P_f))}{S(P-1,05P_f)}$

Jak vidíme, je vliv bonusu za brzký převod na tržní kapitalizaci velmi malý.

Příloha D: Vliv bonusu za brzký převod na minimální náklady na fork

Kvůli podpoře větší účasti během forku obdrží všichni držitelé tokenů, kteří převedou své REP během 60 dnů od začátku forku, 5% dodatečných REP v dceřiném univerzu, do kterého tyto tokeny převedli. Tato odměna je vytvořena pomocí inflace tokenu.

Tento bonus se může stát nechtěnou incentivou v případě, že jsou příliš nízké náklady na zahájení forku. Zvláště pokud útočník může získat více z tohoto bonusu 5% REP, než kolik ztratí zahájením forku, můžeme očekávat, že budou forky nastávat tak často, jak je to jen možné. Tento útok, který nazýváme *útok zneužití inflace*, by nevyústil v nesprávné reportování orákulem, ale vyústil by v častý výskyt rušivých forků.

Aby tomuto chování zamezil, potřebuje Augur zajistit, že náklady na zahájení forku jsou vyšší než maximální hodnota, kterou lze získat z 5% inflačního bonusu. Zde odvodíme dolní hranici nákladů na zahájení forku, aby se zamezilo této nechtěně incentivě.

Nechť P_0 označuje cenu REP před forkem a P_1 označuje cenu REP po forku. Nechť M_0 označuje peněžní zásobu před forkem a M_1 označuje peněžní zásobu po forku. Nechť S označuje procento M_0 převedené během intervalu forku do pravdivého univerza. Nechť b označuje množství REP, které musí být ekonomicky spáleno (to znamená vsazeno na nepravdivý výsledek) pro zahájení forku. Předpokládáme $b > 1$.

Pro účely tohoto oddílu přijímáme konzervativní předpoklad, že REP převáděný během intervalu forku ovládá útočník. Dále předpokládáme (protože to minimalizuje náklady tohoto útoku), že veškerý REP převáděný během intervalu forku je převáděn do pravdivého univerza.

V tomto zápise je SM_0 množství REP převedené během intervalu forku a $(1 - S)M_0$ je množství REP *nepřevedené* během intervalu forku.

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

Když je během intervalu forku převedeno celkem SM_0 REP, je celkem $0,05SM_0$ REP vytvořeno prostřednictvím inflace:

$$M_1 = 1,05SM_0 + (1 - S)M_0 \tag{D2}$$

Protože se zaměřujeme pouze na vliv inflace a kvůli jednoduchosti předpokládáme, že tržní kapitalizace po forku bude stejná, jako tržní kapitalizace před forkem[29]:

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

Vložení D1 a D2 do D3 a zjednodušení nám dává:

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

[29] Myslíme si, že toto je konzervativní předpoklad. V praxi očekáváme že se Tržní kapitalizace po forku sníží.

(Hrubý) zisk útočníka ze zahájení forku a získání bonusu za brzké převedení je hodnota jeho REP mínus hodnota jeho REP před převedením:

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

Vložením D4 do D5 dostaneme alternativní výraz pro (hrubý) zisk útočníka:

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

Připomínáme, že b je množství REP, které musí být ekonomicky spáleno pro zahájení forku. Náklady na zahájení forku jsou tak bP_0. Proto je zaplacení nákladů na fork za účelem získání bonusu za brzké převedení výhodné, kdykoliv je splněna následující nerovnost:

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

Pokud si všimneme, že $P_0 > 0$ a $S \neq -20$, vyřešíme pro b a vidíme, že útok je ziskový, pokud:

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

Kvůli zamezení této nechtěné incentivy musí Augur uspořádat záležitosti takovým způsobem, aby:

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

Všimneme-li si, že S je omezeno na interval $[0,1]$, vidíme, že hodnota na pravé straně nerovnosti D9 je maximální, když $S = 2\sqrt{105} - 20 \approx 0,4939$. To znamená, že tento útok je pro útočníka nejziskovější, když je během intervalu forku převedeno přibližně 49,39% všech existujících REP. Jako konzervativní odhad používáme pro S tuto hodnotu.[30]

Substitucí $S = 0,4939$ do D9 dostaneme $b \geq 0,012197M_0$. Proto pokud jsou náklady na zahájení forku alespoň 1,2197% existujících REP, není útok zneužití inflace ziskový.

Připomínáme, že fork je zahájen až poté, co je složena úspěšná disputační jistina ve výši alespoň 2,5% existujících REP. Předpokládejme, že taková disputační jistina byla složena ve prospěch výsledku ω a fork byl zahájen. Výsledek ω je buď pravdivý, nebo nepravdivý.

Pokud je výsledek ω nepravdivý, potom alespoň 2,5% existujících REP bylo vsazeno na nepravdivý výsledek a tedy ekonomicky spáleno. Takže zneužití inflace není ziskové, když je ω nepravdivý.

Pokud je ω pravdivý, potom lemma 2 říká, že alespoň 1,25% existujících REP (celkem) je vsazeno na nepravdivé výsledky a tedy ekonomicky spáleno. Takže zneužití inflace není ziskové ani v případě, že je ω pravdivý.

Právě z tohoto důvodu vyžaduje zahájení forku úspěšné naplnění disputační jistiny ve výši alespoň 2,5% existujících REP.

Příloha E: Úpravy velikostí jistin

Jistina validity, přítomnostní jistina v REP a sázka zadaného reportéra se dynamicky upravují podle chování účastníků během předchozího poplatkového časového okna. Zde popisujeme způsob, jakým tyto hodnoty upravujeme.

Definujeme funkci $f : [0,1] \to [\frac{1}{2}, 2]$ jako:[31]

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

Funkce f se používá pro určení násobku používaného v těchto úpravách, jak je popsáno v následujících oddílech. Ve stručnosti pokud nechtěné chování nastalo přesně v 1% případů během předchozího poplatkového časového okna, zůstává velikost jistiny nezměněna. Pokud bylo méně časté, bude velikost jistiny snížena až o polovinu. Pokud bylo častější, bude velikost jistiny zvýšena až na dvojnásobek.

1. Jistina validity

Během prvního poplatkového časového okna po spuštění bude jistina validity nastavena na 0,01 ETH. Poté bude zvýšena v případě, že více než 1% finalizovaných trhů v předchozím poplatkovém časovém okně bylo neplatných. Pokud bylo v předchozím poplatkovém časovém okně neplatných méně než 1% finalizovaných trhů, bude jistina validity snížena (ale nikdy nebude nižší než 0,01 ETH).

Pokud ν je procento trhů v předchozím poplatkovém časovém okně, které byly finalizovány jako neplatné a b_v je hodnota jistiny validity z předchozího poplatkového časového okna, potom jistina validity pro aktuální časové okno se vypočítá jako $\max\left\{\frac{1}{100}, b_v f(\nu)\right\}$.

2. Přítomnostní jistina v REP

V prvním poplatkovém časovém okně po spuštění bude přítomnostní jistina v REP nastavena na 0,35 REP. Stejně jako u jistiny validity bude přítomnostní jistina

[30] V praxi nemůže útočník zabránit ostatním účastníkům, aby během intervalu forku převáděli vlastní REP, a nemůže tedy zajistit, že S nepřesáhne přibližnou ideální hodnotu 0,4939. Protože se však snažíme zabránit nejhoršímu možnému scénáři, používáme $S = 0,4939$.

[31] Tento vzorec se může změnit poté, co získáme empirická data z reálných trhů.

v REP upravována směrem nahoru nebo dolů s cílovou hodnotou 1% trhů, u kterých se neobjeví zadaný reportér, a s minimem 0,35 REP.

Podrobně nechť ρ je procento trhů v předchozím poplatkovém časovém okně, jejichž zadaní reportéři včas nereportovali, a nechť b_r je velikost přítomnostní jistiny v REP z předchozího poplatkového časového okna. Velikost přítomnostní jistiny v REP pro aktuální poplatkové časové okno je $\max\{0, 35, b_r f(\rho)\}$.

3. Sázka zadaného reportéra

v prvním poplatkovém časovém okně po spuštění bude sázka zadaného reportéra v REP nastavena na 0,35 REP. Velikost sázky zadaného reportéra se dynamicky upravuje podle toho, kolik zadaných reportérů během předchozího poplatkového časového okna reportovalo chybně (lišilo se od konečného výsledku trhu).

Podrobně nechť δ je procento zadaných reportérů, kteří během předchozího poplatkového časového okna reportovali chybně, a nechť b_d je velikost sázky zadaného reportéra během předchozího poplatkového časového okna. Potom velikost sázky zadaného reportéra pro aktuální časové okno je $\max\{0, 35, b_d f(\delta)\}$.

Příloha F: Změny v návrhu

K současnému návrhu platformy Augur jsme dospěli po třech letech výzkumu a postupného vývoje. Návrh, který vyvstal z tohoto procesu, se podstatně liší od vize předestřené v naší staré bílé knize [9]. Zde probíráme tři podstatné změny a myšlenky, které vedly k těmto změnám.

1. Poplatky za reportování

Ve starém návrhu tvůrce trhu zadával poplatek za obchodování, který si rozděloval v poměru 50/50 s reportéry. V současném návrhu jsou poplatky pro tvůrce trhu a reportéry nezávislé a poplatky za reportování Augur mění dynamicky kvůli bezpečnosti platformy.

Poplatky placené reportérům ovlivňují cenu REP, což má přímý vliv na bezpečnost forkujícího protokolu (věta 1). Pokud jsou poplatky placené reportérům příliš nízké, je integrita orákula ohrožena. Pokud jsou poplatky placené reportérům příliš vysoké, zvyšuje se hrozba parazitických trhů. Proto je pro bezpečnost platformy Augur důležité, aby poplatky placené reportérům byly upravovány dynamicky a ne libovolně tvůrci trhů.

Oddělení poplatků pro reportéry od rozhodnutí tvůrců trhů také zajišťuje, že reportéři (a proto i integrita forkujícího protokolu) nejsou poškozování soutěží mezi tvůrci trhů o trhy s co nejnižšími poplatky. Kvalitní trhy a kvalitní reportování by měly být posuzovány a odměňovány odděleně. Měla by být možná soutěž, která táhne poplatky tvůrců trhu směrem k nule bez toho, aby se příslušně snižovaly i poplatky placené reportérům.

2. Poplatky za obchodování

Ve starém návrhu se od obchodníků vybíral poplatek za každý obchod. V novém návrhu se od obchodníků vybírá poplatek pouze při vypořádání s kontrakty trhu. Tato změna byla udělána částečně proto, že Augur nemá pod kontrolou obchodování offline. Podíly na výsledcích trhu jsou jednoduše tokeny, se kterými lze mezi uživateli svobodně obchodovat. Protože vybírání poplatků za každý obchod není proveditelné, Augur místo toho vybírá poplatky pouze při přímém vypořádání mezi obchodníky a kontrakty trhů. Přidanou hodnotou tohoto přístupu je, že snižuje průměrné poplatky placené obchodníky, což by mělo zlepšit konkurenceschopnost Auguru.

3. Univerza

Ve starém návrhu byla pouze jedna „verze“ REP a její celkové množství bylo pevně dané. V současném návrhu se může REP forkovat (rozvětvit) do mnoha různých verzí (univerz), každá s více nebo méně celkových REP, než bylo v původní verzi. Pokud je fork sporný, zásoba REP v každém dceřiném univerzu může být pouze zlomkem celkové zásoby v rodičovském univerzu. Pokud není fork sporný, bonus za brzké převedení pro účastníky forku může vyústit v dceřiné univerzum, které má více REP, než jeho rodičovské univerzum.

Všechny nové verze REP vytvořené forkem jsou odlišnými tokeny, každý s vlastní cenou a celkovou zásobou, a poskytovatelé služeb by k nim tak měli přistupovat. Když bude Augur poprvé spuštěn, bude existovat jediné univerzum (zahajovací univerzum) a jediná verze REP, tak jako existuje nyní. Avšak jakmile nastane fork, tato jediná verze REP se rozdělí do mnoha verzí: například forkující trh s výsledky `A` a `B` by vytvořil nové tokeny REP-`A`, REP-`B` a REP-`neplatný`. Peněženky a směnárny, které podporují REP, by nyní měly čtyři různé verze REP, které by (teoreticky) mohly podporovat – REP-`zahajovací` (původní verze REP, která by nyní byla zamčena), REP-`A`, REP-`B` a REP-`Neplatný`.[32]

Celková zásoba REP v každém dceřiném univerzu závisí na tom, kolik REP do něj bylo převedeno a kdy tento přesun nastal. Převedení REP během forku předtím, než je jasné, které dceřiné univerzum je vítězné, vystavuje uživatele malému (ale nenulovému) riziku (viz oddíl III E), které může odrazovat uživatele od účasti na sporném forku během intervalu forku. Kvůli podpoře

[32] V praxi může být pro poskytovatele služeb nejjednodušší (a nejméně problematické pro jejich uživatele) podporovat uživatele v účasti na forku a poté po vyřešení forku jednoduše podporovat vítězné univerzum.

účasti během forku musí být uživatelům toto riziko vynahrazeno.

Uživatelé, kteří se neúčastní během intervalu forku, mohou být penalizováni tak, že ztratí část svých REP. Ve skutečnosti měl starý návrh mechanismus „použít nebo ztratit“, který penalizoval ty, kteří se neúčastní, stejně jako reportéry, kteří reportovali nesprávně. Penalizace uživatelů, kteří se neúčastní, však vytváří vážné provozní problémy. Taková penalizace je problematická pro peněženky a směnárny, které spravují REP svých uživatelů. Pokud by nastal fork, směnárny by musely během intervalu forku převést REP svých uživatelů do některého dceřiného univerza nebo ztratit určitou část jejich REP.[33]

Místo penalizování neúčasti dostanou účastníci forku za převod během intervalu forku 5% bonus v univerzu, do kterého převádějí své REP. Pokud je 4,762% REP (nebo více) převedeno do prohrávajícího univerza – z čehož 1,25% až 2,5% již bylo umístěno jako disputační sázka – budou všechna univerza mít menší celkovou zásobu REP, než rodičovské univerzum.

[33] Také jsme přišli na tu praktickou překážku, že kód chytrého kontraktu, který by byl zapotřebí pro implementování odměn při forku pouze pomocí redistribuce, by byl příliš složitý. Složitost kódu kontraktu je sama o sobě bezpečnostním rizikem, takže jsme se snažili o zjednodušení implementace, kdekoliv je to možné.