Augur: Oracolo e Piattaforma di Mercati di Previsione Decentralizzata

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams e Stephanie Alexander
Forecast Foundation
(Data: 3 febbraio, 2018)

Augur è un oracolo e piattaforma di mercati di previsione decentralizzata e affidabile. Gli esiti dei mercati di previsione di Augur vengono scelti dagli utenti che possiedono il REP token nativo di Augur e da chi scommette i propri token sull'effettivo risultato osservato e riceve in cambio delle commissioni di pagamento dai mercati. La struttura di incentivi di Augur è progettata per garantire che la presentazione onesta e accurata dei risultati sia sempre l'opzione più redditizia per i titolari del token REP. I possessori del token possono pubblicare obbligazioni in REP progressivamente crescenti per contestare gli esiti di mercato già proposti. Se la dimensione di queste obbligazioni raggiunge una certa soglia i REP vengono divisi in più versioni, una per ogni possibile risultato del mercato contestato; I titolari di token devono quindi scambiare i propri REP per una di queste versioni. Le versioni di REP che non corrispondono a risultati del mondo reale diverranno senza valore, poiché nessuno parteciperà ai mercati di previsione a meno che non vi sia la certezza che gli stessi si risolvano correttamente. Pertanto, i possessori del token selezioneranno l'unica versione di REP che sapranno continuerà ad avere valore: la versione che corrisponde alla realtà.

Augur è un oracolo e piattaforma di mercati di previsione affidabile e decentralizzata. In un mercato di previsioni, gli individui possono speculare sugli esiti di eventi futuri; Quelli che prevedono i risultati vincono del denaro mentre quelli che sbagliano la previsione perdono il denaro scommesso [1-3]. Il prezzo di un mercato di previsione può servire come indicatore, preciso e ben calibrato, della probabilità che un evento si verifichi [4-7]. Utilizzando Augur, le persone avranno la possibilità di fare trading nei mercati di previsione a un costo molto basso. Le uniche spese significative che i partecipanti dovranno sostenere sono i compensi verso i creatori del mercato e verso gli utenti che riportano gli esiti dei mercati una volta che l'evento si è realizzato. Il risultato sarà un mercato di previsione dove i requisiti di fiducia, l'attrito e le commissioni saranno tanto basse quanto le forze competitive di mercato possano guidarli. Storicamente, i mercati di previsione sono stati centralizzati. La maniera più semplice di aggregare le negoziazioni in un mercato di previsione è tramite un'entità affidabile che mantenga un registro; Similmente, il modo più facile di determinare l'esito di un evento e distribuire i pagamenti agli operatori è che un giudice imparziale e fidato determini i risultati dei mercati. Tuttavia, i mercati di predizione centralizzati hanno molti rischi e limitazioni: Non permettono una partecipazione globale, limitano i tipi di mercati che possono essere creati o scambiati e richiedono ai trader di fidarsi che operatore del mercato non ruberà i fondi e risolverà correttamente i mercati. Augur mira a risolvere questi mercati in maniera completamente decentralizzata. Reti decentralizzate e affidabili come Bitcoin [8] e Ethereum [9], eliminano il rischio che interessi personali si trasformino in corruzione o furti. L'unico ruolo degli sviluppatori di Augur è di pubblicare gli smart contract sulla rete Ethereum. I contratti di Augur sono totalmente automatizzati: Gli sviluppatori non hanno la possibilità di spendere i fondi trattenuti in garanzia sul contratto, non possono controllare come i mercati si risolvono, non possono approvare o rifiutare le transazioni o le negoziazioni sulla rete, non possono modificare o annullare gli ordini, ecc. L'oracolo di Augur consente di migrare le informazioni dal mondo reale a una blockchain senza fare affidamento su un intermediario di fiducia. Augur sarà il primo oracolo decentralizzato del mondo.

I. COME FUNZIONA AUGUR

I mercati di Augur seguono una progressione a quattro fasi: Creazione, negoziazione, reporting e risoluzione. Chiunque può creare un mercato basato su un evento del mondo reale. Il trading comincia immediatamente dopo la creazione del mercato e tutti gli utenti sono liberi di operare su qualsiasi mercato. Dopo che si è verificato l'evento sul quale si basa il mercato, l'esito dell'evento viene determinato dall'oracolo di Augur. Una volta determinato il risultato, i trader possono chiudere le loro posizioni e raccogliere i loro pagamenti.

Augur ha un token nativo, Reputation (REP). Il token REP è necessario ai creatori del mercato e ai reporter nel riferire sull'esito dei mercati creati sulla piattaforma di Augur. I reporter riferiscono su un mercato scommettendo i loro REP su uno dei possibili risultati. Facendo ciò, il reporter dichiara che l'esito sul quale è stata piazzata la scommessa corrisponde al risultato reale dell'evento sottostante del mercato. Il consenso dei reporter del mercato è considerato la "verità" al fine di determinare l'esito del mercato. Se il report di un reporter di un risultato del mercato non corrisponde al consenso raggiunto dagli altri reporter, Augur redistribuisce i REP scommessi sul risultato di non-consenso di questo reporter ai reporter che hanno riferito con il consenso.

Possedendo REP e partecipando accuratamente al reporting dei risultati degli eventi, i titolari del token hanno diritto a una porzione delle commissioni della piattaforma. Ogni token REP messo in gioco da diritto, al suo possessore, a una porzione uguale di commissioni di mercato di Augur. Più REP un reporter possiede e riporta correttamente, più commissioni guadagnerà per il lavoro di mantenimento in sicurezza della piattaforma

Sebbene REP svolga un ruolo contrale nelle operazioni di Augur, lo stesso non viene negoziato nei mercati di Augur. I trader non avranno mai bisogno di possedere o utilizzare REP, in quanto non sono necessari per partecipare al processo di reporting.

Figura 1. Schema semplificato della durata di un mercato di previsione.

A. Creazione del Mercato

Augur permette a chiunque di creare un mercato per qualsiasi evento imminente. Il creatore del mercato (*market creator*) imposta il momento di fine dell'evento (*event end time*) e sceglie un reporter designato (*deisgnated reporter*) che segnali il risultato dell'evento. Il reporter designato non decide unilateralmente l'esito del mercato; la community ha sempre l'opportunità di contestare e correggere quanto riportato dal reporter designato.

In seguito, il creatore del mercato sceglie una *fonte di risoluzione* (*resolution source*) che i reporter dovrebbero utilizzare per determinare il risultato. La fonte di risoluzione potrebbe semplicemente essere una "conoscenza comune" o una risorsa specifica, come "Il Dipartimento dell'Energia degli Stati Uniti", la bbc.com o l'indirizzo di un particolare API endpoint[1]. Inoltre, è stabilita una commissione per il creatore, che rappresenta la commissione pagata nei confronti del creatore del mercato dai trader che interagiscono con il contratto di mercato (vedi la Sezione I D per i dettagli sulle commissioni). Infine, il creatore del mercato pubblica due obbligazioni (bond): il *bond di validità* e il *report no-show bond designato* (anche noto come *no-show bond* per brevità). L'ammontare del bond di validità viene pagato in ETH e viene restituito al creatore del mercato se il mercato si risolve in un risultato che sia diverso dal risultato *Invalido (invalid)*[2]. Il bond di validità incentiva i creatori del mercato a creare mercati basati su eventi ben definiti, con esiti oggettivi e non ambigui. La dimensione del bond di validità è definita dinamicamente in base alla proporzione di esiti invalidi dei mercati recenti[3]. Il no-show bond è composto da due parti: il *no-show gas bond* (pagato in ETH) e il *no-show REP bond* (pagato in REP). Questi bond vengo restituiti al creatore del mercato se il reporter designato per il mercato di riferimento entro i primi tre giorni dopo il *momento di fine dell'evento*. Se il reporter designano non presenta il suo report durante l'assegnata finestra temporale di 3 giorni, il creatore del mercato perde il no-show bond che viene altrimenti consegnato al *primo reporter pubblico* che riferisce sul mercato (vedi la Sezione I C 6). Ciò incentiva il creatore del mercato a scegliere un reporter designato affidabile che dovrebbe aiutare a risolvere il mercato rapidamente.

Il no-show gas bond è programmato per coprire i costi di gas del primo reporter designato. Ciò impedisce lo scenario in cui i costi di gas del primo reporter pubblico sono troppo alti da rendere non redditizio il reporting. Il no-show gas bond è fissato al doppio del costo medio del gas usato per il reporting durante il precedente intervallo di pagamento.

Nel caso in cui il reporter designato fallisca nel reporting, il no-show REP bond viene consegnato al primo reporter pubblico sotto forma di stake sul risultato segnalato, coì che il primo reporter pubblico riceve il no-show REP bond se e solo se riporta correttamente. Come per il bond di validità, il no-show REP bond è regolato dinamicamente in base alla proporzione di reporter designati che hanno fallito nel riportare in tempo durante il precedente intervallo di pagamento[4].

Il market creator crea il mercato e pubblica tutti i bond richiesti tramite una singola transazione Ethereum. Una volta che la transazione viene confermata, il mercato è vivo e il trading comincia.

B. Trading

I partecipanti al mercato prevedono gli esiti degli eventi negoziando le *azioni* di tali eventi sul mercato. Un set completo di azioni (*complete set of shares*) è una collezione di azioni che consiste in un'azione di ogni possibile risultato valido dell'evento [10]. I set completi sono creati dal motore di accoppiamento on-contract di Augur, necessario per completare gli scambi.

Ad esempio, si consideri un mercato che abbia due possibili risultati, A e B. Alice è disposta a pagare 0.7 ETH per un'azione di A e Bob è disposto a pagare 0.3 ETH per un'azione di B[5]. In primo luogo, Augur abbina questi ordini e riscuote 1 ETH in totale da Alice e Bob[6]. Successivamente, Augur crea un set completo di azioni, dando ad Alice l'azione A e a Bob l'azione B. è così che le azioni degli esiti vengono create. Una volta che le azioni vengono create, possono essere negoziate liberamente.

---

[1] Ad esempio, se un mercato sulla "Temperatura più alta (in gradi Fahrenheit) il 10 aprile, 2018 all'aeroporto internazionale di San Francisco, come riportato da Weather Undergrouund" specifica una fonte di risoluzione di https:// www.wunderground.com/history/airport/KSFO/2018/4/10/ DailyHistory.html, i reporter vanno semplicemente a quell'URL e inseriscono nel loro report la temperatura più alta mostrata dal link.

[2] Un mercato Invalido è un mercato determinato Invalido dai reporter perché nessuno dei risultati elencati dal creatore del mercato è corretto o perché la terminologia del mercato è ambigua o soggettiva; vedere la sezione III F per le discussioni.

[3] Vedere l'appendice E 1 per i dettagli.

[4] Vedere l'appendice E 2 per i dettagli.

5 Inizialmente, le negoziazioni nei mercati di Augur useranno la moneta nativa di Ethereum, Ether (ETH). Le versioni successive di Augur includeranno il supporto per i mercati denominati in token arbitrari emessi sulla rete Ethereum, incluse azioni di altri mercati così come token ancorati a una valuta fiat ("stablecoin"). Quando/se diventeranno disponibili.

6 1 ETH è usato come esempio per facilitare la discussione. Il costo effettivo di un insieme completo di azioni è molto più piccolo di questo; Vedere docs.augur.net/#number-of-ticks per i dettagli

I contratti di trading di Augur mantengono un order-book per ogni mercato creato sulla piattaforma. Chiunque può creare un nuovo ordine o eseguirne uno esistente in qualsiasi momento. Gli ordini vengono eseguiti automaticamente da un motore di accoppiamento che esiste all'interno degli smart contract di Augur. Le richieste di compravendita di azioni vengono eseguite immediatamente se esiste già un ordine abbinabile nell'order-book. Può essere eseguito acquistando azioni o vendendo azioni ad altri partecipanti, il che potrebbe comportare l'emissione di nuovi set completi o la chiusura di quelli già esistenti. Il motore di accoppiamento di Augur prende in garanzia sempre la quantità minima di azioni e/o denaro necessario per coprire il valore messo a rischio. Se non esistono ordini abbinabili o la richiesta può essere eseguita solo parzialmente, il resto viene inserito nell'order-book sotto forma di nuovo ordine. Gli ordini non vengono mai eseguiti a un prezzo inferiore del prezzo limite impostato dal trader, ma potrebbero essere eseguiti a un prezzo superiore. Gli ordini ineseguiti o parzialmente eseguiti possono essere rimossi dall'order-book dal creatore dell'ordine stesso in qualunque momento. Le commissioni sono pagate dai trader solo quando set completi di azioni sono venduti; le commissioni di pagamento trovano discussione in maggior dettaglio nella Sezione I D. Sebbene la maggior parte delle negoziazioni di azioni dovrebbe avvenire prima della risoluzione del mercato, le azioni possono essere negoziate in qualsiasi momento dopo la creazione del mercato. Tutti gli asset di Augur – incluse le azioni degli esiti del mercato, token di intervalli di pagamento, azioni in bond di disputa e persino la proprietà dei mercati stessi – sono sempre trasferibili.

C. Reporting

Una volta che si verifica l'evento sottostante del mercato, l'esito deve essere determinato al fine di finalizzare e liquidare il mercato. Gli esiti sono determinati dall'oracolo di Augur, che consiste in reporter motivati dal profitto, che semplicemente riportano l'esito reale e attuale dell'evento. Chiunque possieda REP può partecipare nel reporting e nella contestazione dei risultati. I reporter i cui report sono coerenti con il consenso generale vengono finanziariamente ricompensati, mentre quei report non coerenti con il consenso generale vengono finanziariamente penalizzati (vedere la Sezione I D 3).

1.Intervallo di pagamenti

Il sistema di reporting di Augur funziona su un ciclo consecutivo di intervalli di pagamenti lungo 7 giorni. Tutte le commissioni raccolte da Augur durante un intervallo di pagamenti vengono aggiunte al pool dei pagamenti di reporting (*reporting fee pool)* per questo intervallo. Al termine dell'intervallo di pagamenti, la pool delle commissioni reporting viene pagata ai possessori di REP che hanno partecipato nel processo di reporting. I reporter ricevono una ricompensa in proporzione alla quantità di REP che hanno messo in stake durante quell'intervallo di pagamenti. La partecipazione include: staking durante il rapporto iniziale, contestazione di un risultato provvisorio o l'acquisto di *Participation token.*

2. I Participation Token

Durante qualsiasi intervallo di pagamento, i possessori di REP potrebbero acquistare qualsiasi numero di Participation token per ogni attorep[7]. Alla fine dell'intervallo di pagamento, potrebbero riscattare i loro participation token per ogni attorep, in aggiunta a una quota proporzionale degli intervalli di pagamento del *pool di commissioni provenienti dal reporting*. Se non ci sono state azioni (es. invio di un report o la discussione di un report inviato da un altro utente) necessarie per un reporter, lo stesso reporter potrebbe acquistare i participation token per indicare che si sono presentati per l'intervallo di pagamento. Proprio come i REP messi in staking, i participation token potrebbero essere riscattati dai loro proprietari per una porzione *pro rata* di commissioni in questo intervallo di pagamento. Come già discusso nella Sezione II, è importante che i possessori di REP siano pronti a partecipare in una risoluzione di mercato in caso di fork. Il participation token fornisce l'incentivo, ai titolari di REP, di monitorare la piattaforma almeno una volta a settimana, e quindi a essere pronti a partecipare se ce n'è bisogno. Persino i possessori di REP che non vogliono partecipare al processo di reporting sono incentivati a controllare Augur una volta ogni 7 giorni di intervallo di pagamento al fine di acquistare i participation token e raccogliere le commissioni. Questo controllo regolare e attivo assicura che abbiamo familiarità nell'utilizzo di Augur e che vengano a conoscenza dei fork quando gli stessi accadono, pertanto dovrebbero essere maggiormente pronti a partecipare ai fork quando avvengono.

3. Progressione dello Stato del Mercato

I mercati di Augur possono essere in sette stati differenti dopo la loro creazione. Gli stati potenziali o "fasi" di un mercato di Augur sono i seguenti:

- Pre-reporting
- Reporting Designato
- Reporting Aperto
- Fase di Attesa dell'Inizio del successivo Intervallo di pagamento
- Round di disputa
- Fork
- Finalizzazione

La relazione intercorrente tra questi stati può essere vista in Fig. 2.

4. Pre-reporting

Il *pre-reporting* o *fase di trading* (Fig. 1) è il periodo di tempo che comincia dopo l'inizio delle negoziazioni del mercato, ma prima che l'evento del mercato si sia verificato. Generalmente, questo è il periodo di

[7] Un attorep è uguale a 10^{18} REP.

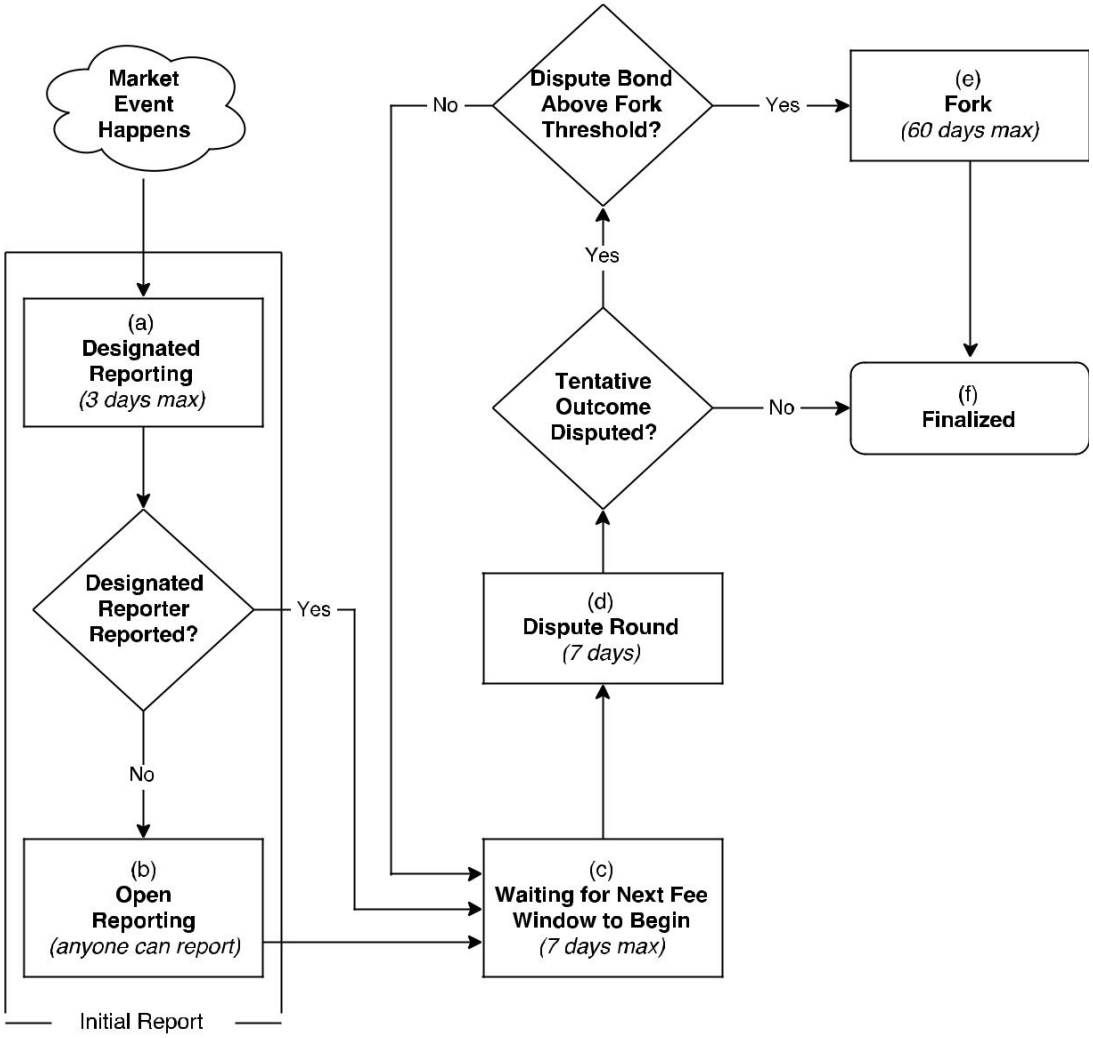

Figura 2. Reporting flowchart.

trading più attivo di qualsiasi dato mercato di Augur. Una volta superata la data finale dell'evento, il mercato entra nella fase di *reporting designato*(Fig.2).

5. *Reporting Designato*

Quando viene creato un mercato, viene richiesto ai creatori del mercato di scegliere un reporter designato e pubblicare un no-show bond. Durante la fase di reporting designato (fig. 2) il reporter designato del mercato ha fino a 3 giorni per riportare sull'esito dell'evento. Se il reporter designato fallisce nel riportare entro gli assegnati 3 giorni, il creatore del mercato perde il no-show bond e il mercato entra automaticamente nella fase di *reporting aperto* (Fig. 2b).

Se il reporter designato presenta il report in tempo, allora in no-show bond viene restituito al creatore del mercato. È richiesto al reporter designato di pubblicare il suo stake[8] sull'evento riportato, il quale perderà se il mercato finalizzerà in qualsiasi altro esito invece di quello sul quale ha riportato.[9] Non appena il reporter designato pubblica il suo report, il mercato entra nella fase di *attesa per l'inizio del prossimo intervallo di pagamento* (Fig. 2c) e l'esito riportato diviene il *risultato provvisorio* (*tentative outcome*) del mercato.

6. *Reporting Aperto*

il reporter designato dal mercato ha fino a 3 giorni per riportare sull'esito dell'evento. Se il reporter designato fallisce nel riportare entro gli assegnati 3 giorni, il creatore del mercato perde il no-show bond e il mercato entra automaticamente nella fase di reporting aperto (Fig. 2b).

---

[8] Vedi appendice E 3 per i dettagli sulla misura dello stake del reporter designato.

[9] Lo stake perso è aggiunto al pool delle commissioni di reporting dell'intervallo di reporting assegnato dal mercato, e viene usata per ricompensare i disputatori e i reporter onesti; vedere la sezione I D 3 per maggiori dettagli.

Non appena il mercato entra nella fase di reporting aperto, chiunque può riportare l'esito del mercato. Quando il reporter designato fallisce nel consegnare il report, il primo reporter che presenta un report sull'esito del mercato viene chiamato *primo reporter pubblico (first public reporter)* del mercato. Il primo reporter pubblico riceve il no-show bond precedentemente incamerato come forma di stake sul suo risultato prescelto, così potrà richiedere il no-show REP bond solo se il suo risultato riportato è coerente con l'esito finale del mercato. Riceverà anche il no-show gas bond dopo la finalizzazione del mercato solo se il suo risultato riportato è coerente con il risultato finale del mercato. Il primo reporter pubblico *non* necessita di mettere in stake alcuno dei suoi REP quando riporta l'evento del mercato. In questo modo, in qualsiasi mercato nel quale il reporter fallisce, dovrebbe esserci *qualcuno* che riporta l'esito molto presto dopo che il mercato è entrato nella fase di reporting aperto. Una volta che il *report iniziale* (*initial report*) è stato ricevuto dal primo reporter (sia se sia stato il reporter designato o il primo reporter pubblico), l'esito riportato diviene l'esito provvisorio del mercato, e lo stesso entra nella fase di attesta per l'inizio del prossimo intervallo di pagamento (Fig. 2c).

7. Attesta dell'Inizio del Successivo Intervallo di pagamento

Non appena il mercato riceve il suo report iniziale, entra nella fase di attesa dell'inizio del successivo intervallo di pagamento (Fig. 2c). Durante questa fase, il reporting del mercato è sospeso fino alla fine dell'attuale intervallo di pagamento. Una volta che il successivo intervallo di pagamento comincia, il mercato entra nella fase chiamata *round di disputa*.

8. Round di disputa

Il round di disputa (Fig. 2d) è un periodo di 7 giorni durante il quale ogni titolare di REP ha l'opportunità di contestare *l'esito provvisorio* del mercato[10]. (all'inizio di un round di disputa, un risultato provvisorio del mercato è il risultato che diventerà l'esito finale se non viene contestato con successo dai titolari di REP). Una controversia consiste nel mettere in staking i REP (in questo contesto indicato come *dispute stake*) su un esito diverso dall'attuale esito provvisorio del mercato.

Una controversia ha esito positivo se l'ammontare totale della quota messa in staking su un determinato outcome soddisfa la dimensione del bond di disputa (*dispute bond size*) richiesta per il round corrente. La dimensione del bond di disputa viene calcolata nel seguente modo. Sia A_n la partecipazione totale di tutti gli esiti di questo mercato all'inizio del round di disputa n. Sia ω un qualsiasi esito del mercato diverso dal risultato provvisorio all'inizio di questo round di disputa. Sia S (ω, n) l'ammontare totale di stake sull'outcome ω all'inizio della fase di disputa n.

Allora la dimensione del bond di disputa necessaria per contestare con successo l'attuale esito provvisorio in favore del nuovo esito ω durante il round n è denotata da *B* (ω, n), e data da:

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

Le dimensioni del bond vengono scelte in questo modo per assicurare un ROI fisso del 50% per i reporter che hanno contestato con successo falsi risultati (vedi Sezione II D). I bond di disputa non devono necessariamente essere pagati interamente da un singolo utente. La piattaforma di Augur permette ai partecipanti di crowdsourcing i bond di disputa. Ogni utente che vede un esito provvisorio incorretto può contestare detto esito mettendo in staking i REP su un esito diverso da quello provvisorio. Se ogni risultato (oltre al risultato provvisorio) accumula una quota di contestazioni sufficiente da eseguire il suo bond di disputa, l'attuale esito provvisorio sarà contestato con successo.

Nel caso di una contestazione avvenuta con successo, il mercato sarà sottoposto a un altro round di disputa o entrerà in uno stato di *fork* (Fig. 2e). Se la dimensione del bond di disputa è maggiore del 2.5% di tutti i REP, allora il mercato entrerà nello stato di fork. Se la dimensione del bond di disputa è inferiore del 2.5% di tutti i REP, allora il nuovo esito scelto diventa il nuovo esito provvisorio del mercato e il mercato subisce un altro round di disputa.

Tutto lo stake della disputa viene trattenuto in escrow durante il round di disputa. Se un bond di disputa non ha successo, allora i fondi della disputa vengono restituiti ai rispettivi proprietari alla fine del round. Se nessuna disputa ha successo durante i 7 giorni di disputa, il mercato entra nello stato di finalizzazione (Fig. 2f) e il suo esito provvisorio viene accettato come *risultato finale* (*final outcome*). Il risultato finale di un mercato è il risultato provvisorio che passa attraverso un round di disputa senza essere contestato con successo o è determinato da un fork. I contratti di Augur trattano i risultati finali come veri ed emettono i pagamenti di conseguenza.

Tutte gli stake delle dispute che non hanno riscontrato successo vengono restituiti ai proprietari originali alla fine di ogni round. Tutti gli stake delle dispute realizzatesi con successo vengono applicati al risultato vincente e rimangono li fino alla finalizzazione del mercato (oppure fino a quando non avviene un fork in qualche altro mercato di Augur). Tutti gli stake delle dispute (sia con successo che non) riceveranno una porzione della pool delle commissioni di reporting[11] dall'intervallo di pagamento corrente.

9. Fork

Lo stato di fork (fig. 2e) è uno stato speciale che può durare fino a 60 giorni. Il fork è il metodo di risoluzione del mercato in ultima istanza;

---

10. Il fatto che i round di disputa coincidano con l'intervallo di pagamento è puramente una questione di convenienza; In principio, la durata del round di disputa e dell'intervallo di pagamento potrebbe essere differente.

[11] Eventuali commissioni di pagamento e bond di validità raccolti durante un intervallo di pagamento vengono aggiunte a questo intervallo di pagamento della pool delle commissioni di reporting. Alla fine dell'intervallo di pagamento, la pool delle commissioni di reporting viene distribuita agli utenti in proporzione all'ammontare di REP messi in gioco durante questo intervallo di pagamento.

È un Vero e processo dirompente, destinato ad essere un evento raro. Un fork è causato quando c'è un mercato con un risultato con un bond di disputa, eseguito con successo, grande quanto almeno il 2,5% di tutti i REP. Questo mercato viene identificato come *mercato in forking* (*forking market)*.

Quando viene avviato un fork, comincia il *periodo di forking* (*forking period*) di 60 giorni[12]. Le dispute di tutti gli altri mercati non finalizzati vengono messe in attesa fino alla fine del periodo di forking. Il periodo di forking è molto più lungo del solito intervallo di pagamento perché la piattaforma deve fornire abbastanza tempo ai possessori di REP e fornitori di servizi (come wallet ed exchange) per prepararsi. L'esito finale del fork non può essere contestato.

Ogni mercato di Augur e tutti i token REP esistono in un qualche *universo* (*universe*). I token REP possono essere usati per riportare sui risultati (e pertanto guadagnare commissioni) *solo* per i mercati che esistono nello stesso universo dei token REP. Quando Augur è lanciato per la prima volta, tutti i mercati e tutti i REP coesisteranno nell'*universo genesi* (*genesis universe*).

Quando avviene un fork su un mercato, vengono creati nuovi universi. Il forking crea un *universo figlio* (*child universe*) per ogni possibile risultato del mercato in forking (inclusi quelli invalidi, come discusso nella Sezione I D 2). Per esempio, un mercato "binario" ha 3 possibili risultati: A, B e Invalido. Pertanto, un mercato binario in forking creerà tre nuovi universi figlio: universo A, universo B e universo Invalido. Inizialmente, questi nuovi universi creati sono vuoti: non contengono né mercati né token REP. Quando accade un fork, l'*universo genitore* (*parent universe*) diviene permanentemente *bloccato (locked)*. In un universo bloccato non vi è la possibilità di creare nuovi mercati. Gli utenti possono continuare a scambiare le azioni in dei mercati in universi bloccati, e i mercati in un universo bloccato potrebbe ancora ricevere il suo report iniziale. Tuttavia, non vengono pagate ricompense di reporting, e i mercati presenti in universi bloccati non possono essere finalizzati. Al fine di poter essere utilizzati, i mercati o i token REP nell'universo bloccato devono essere migrati verso un universo figlio. I titolari dei token REP nell'universo genitore possono migrare i loro token verso un universo figlio di loro scelta. Questa scelta va considerata attentamente perché la migrazione non è reversibile. I token non possono essere inviati da un universo fratello a un altro. *La migrazione risulta in un impegno permanente dei token* REP *verso un particolare esito di mercato*. I token REP migrati verso un universo figlio differente dovrebbero essere considerati token completamente separati e i fornitori di servizi, come wallet ed exchange, dovrebbero listarli come tali.

Quando avviene un fork, tutti i REP messi in stake in mercati non in forking sono *rimossi dallo staking* (*unstaked*) in modo che possano essere migrati verso un universo figlio durante il periodo di forking[13].

Qualsiasi universo figlio che riceve la maggiore quantità di REP migrati alla fine del periodo di forking diventa l'universo vincitore (*winning universe*) e il suo esito corrispondente diviene l'esito naturale del mercato in forking. I mercati non finalizzati nell'universo genitore possono essere migrati solo verso l'universo vincitore e, se hanno ricevuto un report iniziale, vengono resettati alla fase di attesta dell'inizio del successivo intervallo di pagamento.

Non vi è alcun limite di tempo per migrare i token dall'universo genitore verso un universo figlio. I token possono essere migrati dopo il periodo di forking ma non avranno peso nella determinazione dell'universo vincitore. Per incoraggiare una maggiore partecipazione durante il periodo di forking, tutti i possessori di token che migrano i propri REP entro 60 giorni dall'inizio del fork riceveranno il 5% in più di REP nell'universo figlio verso il quale hanno migrato[14]. Questa ricompensa viene pagata coniando nuovi token REP[15].

I reporter che hanno messo in staking i REP *su uno degli esiti dei mercati in forking non possono cambiare la loro posizione durante il fork.* I REP messi in stake su un risultato nell'universo genitore possono essere migrati solo verso l'universo figlio che corrisponde a quel risultato. Ad esempio, se un reporter ha aiutato ad eseguire un bond di disputa in favore dell'esito A durante qualche bond di disputa, allora i REP messi in stake sull'esito A possono essere migrati solo verso l'universo A durante il fork.

Gli universi fratelli sono completamente disgiunti. I token REP che esistono in un universo non possono essere usati per riportare su degli eventi o guadagnare ricompense da mercati in un altro universo. Dato che presumibilmente gli utenti non vorranno creare o negoziare su mercati in un universo in cui l'oracolo è inaffidabile, i REP esistenti in un universo che non corrisponde alla realtà oggettiva è improbabile che facciano guadagnare ai loro proprietari delle commissioni, e pertanto lo stesso non dovrebbe avere alcun valore di mercato significativo. Pertanto, i token REP migrati verso un universo che non corrisponde ad una realtà oggettiva non dovrebbero detenere alcun valore di mercato, a prescindere se l'universo oggettivamente Falso finisce per essere l'universo vincitore dopo un fork. Ciò ha delle conseguenze di sicurezza importanti, che discuteremo nella Sezione II.

10. Finalizzazione

Un mercato entra nello stato di finalizzazione (Fig. 2f) se passa attraverso un round di disputa lungo 7 giorni senza subire una contestazione vincente del suo esito provvisorio o dopo il completamento di un fork. L'esito di un fork non può essere contestato ed è sempre considerato definitivo alla fine del periodo di forking. Una volta che un mercato e finalizzato, i trader possono liquidare le loro posizioni direttamente nel mercato. Quando un mercato entra nello stato finalizzato, denotiamo al suo esito come *esito finale* (*final outcome*).

12. I periodi di forking possono essere inferiori a 60 giorni: un periodo di forking termina quando sono trascorsi 60 giorni o più del 50% di tutti i REP genesi viene migrato in un universo figlio.

13. L'unica eccezione sono i REP messi in staking dal reporter iniziale quando è stato fatto il primo report. Quei REP rimangono in staking sull'esito inizialmente riportato e vengono automaticamente migrati verso l'universo figlio vincitore.

14. Ciò si verifica anche quando il periodo di forking è terminato in anticipo a causa della migrazione di oltre il 50% dei REP migrati verso un universo figlio.

15. L'effetto di questa aggiunta nell'offerta di moneta di REP è limitata. Ad esempio, se il 20% di tutti i REP esistenti viene migrato durante il periodo di forking, questo bonus comporterebbe un aumento dell'1% dell'offerta di REP. Inoltre, è previsto che i fork siano eventi estremamente rari.

D. Risoluzione del Mercato

Un trader può chiudere la sua posizione in uno o due modi: vendendo le azioni che possiede ad un altro trader in cambio di valuta, o liquidare le azioni nel mercato. Ricorda che ogni azione viene ad esistenza come parte di un set completo quando il totale di 1 ETH è stato messo in escrow con Augur[6]. Per togliere fuori 1 EHT dall'escrow, i trader devono dare ad Augur un set completo o, se il mercato è finalizzato, un'azione dell'esito vincente. Quando avviene questo scambio diciamo che i trader stanno *risolvendo il contratto del mercato*.

Ad esempio, consideriamo un mercato non finalizzato con i possibili esiti A e B. Supponiamo che Alice abbia un'azione del possibile esito A che vuole vendere a 0.7 ETH e Bob ha un'azione del possibile esito B che vuole vendere per 0.3 ETH. In primo luogo, Augur abbina questi ordini e raccoglie le azioni A e B dai partecipanti. In seguito, invia 0.7 ETH (al netto delle commissioni) ad Alice e 0.3 ETH (al netto delle commissioni) a Bob.

Come secondo esempio, consideriamo un mercato finalizzato nel quale l'esito vincente sia A. Alice possiede un'azione di A e vuole incassarla. Lei invia la sua corrispondente azione di A nei confronti di Augur e in cambio riceve 1 ETH (al netto delle commissioni).

1. Commissioni di Pagamento

L'unico momento in cui Augur riscuote delle commissioni è quando i partecipanti del mercato stanno risolvendo il contratto del mercato. Augur riscuote due commissioni durante il pagamento: la commissione del creatore e la commissione di reporting. Entrambe queste commissioni sono proporzionali alla quantità pagata. Quindi, nell'esempio di risoluzione precedentemente analizzato, dove Alice riceve 0.7 ETH e Bob riceve 0.3 ETH, Alice dovrebbe pagare il 70% delle commissioni mentre Bob dovrebbe pagarne il 30%.

La commissione del creatore viene stabilita dal mercato durante la creazione del mercato stesso ed è pagata al creatore del mercato alla risoluzione. La commissione di reporting viene stabilita dinamicamente (vedi la Sezione II C) ed è pagata ai reporter che partecipano al processo di reporting.

2. Risoluzione dei Mercati Invalidi

Nel caso in cui un mercato si risolva come Invalido, i trader che risolvono con il contratto del mercato ricevono una quantità uguale di ETH per le azioni di ogni esito. Se il mercato ha avuto N possibili esiti (non includendo l'esito Invalido) e il costo di un set completo di azioni è stato di C ETH, allora i trader riceveranno *C/N* ETH per ogni azione del contratto di mercato risolta[16].

3. Redistribuzione di Reputation

Se il mercato finalizza senza cominciare un fork tutti i REP messi in staking su ogni risultato diverso dal risultato naturale del mercato vengono incamerati e ridistribuiti agli utenti che hanno scommesso sul risultato naturale del mercato, in proporzione alla quantità di REP scommessa. Le dimensioni del bond di disputa sono scelte in modo tale che chiunque contesti con successo un risultato, in favore del risultato finale del mercato è ricompensato con il 50% di ROI sulla quantità messa in contestazione[17]. Questo rappresenta un forte incentivo per i reporter nel contestare falsi risultati provvisori.

II. INCENTIVI E SICUREZZA

C'è una forte relazione tra la capitalizzazione di mercato di REP e l'attendibilità del protocollo di forking di Augur. Se la capitalizzazione di REP è grande abbastanza[18] e gli attaccanti sono economicamente razionali, allora l'esito che vince il fork dovrebbe corrispondere all'oggettiva realtà. Infatti, sarebbe possibile per Augur funzionare correttamente senza l'utilizzo di reporter designati e round di disputa. Usando soltanto il processo di forking, l'oracolo riporterebbe onestamente.

Tuttavia, i fork sono dirompenti e richiedono del tempo. Un fork richiede fino a 60 giorni per risolvere un singolo mercato e può risolvere solo un mercato alla volta. Durante i 60 giorni nei quali il mercato questione di fork viene risolto, tutti gli altri mercati non finalizzati vengono messi in attesa[19]. I fornitori di servizi devono aggiornarsi e i possessori di REP devono migrare i loro token verso uno dei nuovi universi figlio. Di conseguenza, i fork dovrebbero essere usati solo in casi di assoluta necessità. Il forking è un'opzione nucleare. Fortunatamente, una volta stabilito che ci si può fidare dei fork per determinare la verità, gli incentivi possono essere utilizzati per incoraggiare i partecipanti a comportarsi onestamente senza dover iniziare un fork.

Sono la minaccia credibile di un fork e la credenza che il fork si risolverà correttamente i fondamenti del sistema di incentivi di Augur.

Successivamente, discuteremo delle condizioni sotto le quali il sistema di forking può essere affidabile nel determinare la verità. Discuteremo in seguito degli incentivi del sistema e di come incoraggiano e correggono la risoluzione di tutti i mercati.

---

16 le negoziazioni non possono semplicemente essere svolte se un mercato si risolve come Invalido a causa di limitazione tecniche. Le azioni dei risultati sono solo token, che possono essere scambiati direttamente tra utenti; ETH e le azioni sono quindi fuori dal controllo di Augur e non possono essere restituire al proprietario originale se il mercato si finalizza come Invalido.

17 Vedi teorema 3 nell'appendice A

18 Vedi Sezione II A per dettagli

19 I trader possono continuare a negoziare su quei mercati, ma quei mercati non possono essere finalizzati fino a dopo il periodo di forking.

A. Integrità del Protocollo di Forking

Qui discutiamo dell'affidabilità del processo di forking e delle condizioni sotto le quali ci si può fidare di questo processo. Per la facilità di discussione, quando ci riferiremo ai fork, faremo riferimento all'universo figlio che corrisponde alla realtà oggettiva come il Vero universo, e ad ogni altro universo figlio come il Falso universo. Faremo riferimento all'universo figlio che riceve la maggiore migrazione di REP durante il periodo di forking come l'universo vincitore, mentre a tutti gli altri universi come universi perdenti.

Naturalmente, vogliamo sempre che il Vero universo sia l'universo vincitore e che i Falsi universi siano gli universi perdenti. Diciamo che il protocollo di forking è stato attaccato con successo ogniqualvolta un Falso universo finisce per essere l'universo vincitore di un fork – pertanto risultando in un mercato in forking (e, potenzialmente, tutti i mercati non finalizzati) risolto incorrettamente.

Il nostro approccio per rendere sicuro l'oracolo è di mettere d'accordo i partecipanti al mercato che il massimo beneficio ottenibile da un'attaccante è inferiore del costo minimo di esecuzione di un attacco. A seguire la formalizzazione.

1. Massimo Beneficio per un Attaccante

Un attaccante che attacca con successo l'oracolo causerebbe la migrazione di tutti i mercati non finalizzati di Augur verso un Falso universo. Se l'attaccante controlla la maggioranza dei REP nel Falso universo può forzare tutti i mercati non finalizzati a risolversi quando vuole. Nel caso più estremo, sarebbe anche in grado di catturare tutti i fondi in escrow di questi mercati[20].

Definizione 1. Definiamo e denotiamo con I_a, *l'open interest nativo (native open interest)* di Augur come il valore della somma di tutti i fondi in escrow in tutti i mercati non finalizzati di Augur[21].

Definizione 2. Definiamo come *mercato parassita* (*parasitic market*) ogni mercato che non paga le commissioni di reporting ad Augur, ma si risolve in conformità alla risoluzione di un mercato nativo di Augur.

Definizione 3. Definiamo e denotiamo con I_p l'*open interest parassita* (*parasitic open interest*) come il valore della somma di tutti i fondi in escrow in ogni mercato parassita che si risolve in conformità ai mercati nativi non finalizzati di Augur.

Nel caso più estremo, un attaccante dovrebbe anche essere in grado di catturare tutti i fondi in tutti i mercati parassita che si risolvono in conformità ai mercati nativi non finalizzati di Augur.

Osservazione 1. Il beneficio massimo (lordo) per un attaccante che attacca con successo l'oracolo è $I_a + I_p$.

20. Ciò richiederebbe all'attaccante di catturare tutte le azioni di un determinato risultato e poi forzare il mercato a finalizzare verso tale risultato.
21. Ciò include i mercati esterni che pagano le commissioni di reporting ad Augur.

2. L'Open Interest Parassita è Inconoscibile

Augur può accuratamente ed efficientemente misurare I_a. Tuttavia, I_p non può essere conosciuto in generale, siccome potrebbero esistere molti marcati parassita offline, ognuno dei quali con un open interest arbitrariamente grande. Siccome il beneficio massimo possibile ottenibile da un attaccante include la quantità sconosciuta I_p, non è possibile essere oggettivamente certi che l'oracolo sia al sicuro contro attacchi economicamente razionali.

Tuttavia, se siamo disposti ad asserire che I_p è ragionevolmente limitato nella pratica, allora possiamo definire le condizioni sotto le quali potremmo dire che l'oracolo è al sicuro.

3. Costo Minimo di un Attacco Riuscito

Successivamente, consideriamo il costo di un attacco all'oracolo. P denota il prezzo di REP. ε denota un attorep[22]. M denota l'ammontare totale di REP in esistenza ("l'offerta di moneta" di REP). S denota la proporzione di M che verrà migrata verso il Vero universo durante il periodo di forking di un fork.

Pertanto il prodotto SM rappresenta l'ammontare assoluto di REP migrati verso il Vero universo durante il periodo di forking di un fork, e il prodotto PM è la capitalizzazione di mercato di REP.

Sia P_f il prezzo dei REP migrati verso un Falso universo scelto dell'attaccante. Nota che se $P \leq P_f$ allora l'oracolo non sarebbe sicuro contro attacchi economicamente razionali dell'attaccante, perché sarebbe almeno altrettanto proficuo migrare i REP verso il Falso universo rispetto a quanto lo sarebbe non facendoli migrare affatto.

4. Integrità

Assunzione 1. *I reporter che non sono attaccanti non migrerebbero mai i* REP *verso un* Falso *universo durante un fork*[23].

Di design, Un attacco riuscito contro l'oracolo richiede la migrazione di più REP verso un Falso universo che verso un Vero universo durante il periodo di forking di un fork. Per assunzione, solo l'attaccante migrerebbe i REP verso un Falso universo. La quantità di REP migrati verso il Vero universo durante il periodo di reporting è denotata da SM. Pertanto, un attaccante per avere successo deve far migrare almeno SM + ε REP. Per semplicità, ignoriamo il trascurabile e diciamo che un attacco di successo richiede la migrazione di almeno SM REP, che ha un valore di SMP prima della migrazione verso un Falso universo.

22 Un attorep equivale a 10^{18} REP.
23. Potrebbero esserci casi in cui qualche reporter non malevolo migra accidentalmente o incautamente i propri REP verso un Falso universo. Tuttavia, tale comportamento è, in pratica, indistinguibile dalla collaborazione con un attaccante malevolo.

Se un attaccante migra SM REP durante il periodo di reporting di un fork, riceverà SM REP sull'universo figlio verso il quale ha effettuato la migrazione[24]. Se l'attaccante effettua una migrazione verso un Falso universo allora il valore di quelle monete diventa S M P_f. Pertanto il costo minimo per l'attaccante è (P - P_f) SM.

Osservazione 2. La quantità minima di REP che un attaccante dovrebbe migrare con successo verso un Falso universo durante un fork è SM, che costa all'attaccante (P - P_f) SM.

Nota che se S > ½ allora un attacco risulta *impossibile* perché non esistono abbastanza REP al di fuori del Vero universo per un qualsiasi Falso universo affinché diventi l'universo vincitore.

In competizione con l'attaccante economicamente razionale, l'oracolo risolverà gli esiti che corrispondono a una realtà oggettiva se il massimo beneficio ottenibile da un'attaccante è inferiore al costo minimo dell'attacco. Dall'osservazione 1 e 2 possiamo vedere che ciò accade ogniqualvolta S > ½ o $I_a + I_p$ < (P - P_f) SM. Ciò fornisce la definizione formale di integrità.

Definizione 4. (Proprietà di Integrità) Il protocollo di forking è *integro* ogniqualvolta S > ½ oppure quando $I_a + I_p$ < (P - P_f) SM.

La disequazione precedente può essere risolta per PM per vedere la relazione tra l'integrità del protocollo di forking e la capitalizzazione di mercato di REP.

Teorema1. (*Teorema di Sicurezza della Capitalizzazione di Mercato*) *Il protocollo di forking è integro se e solo se:*

1. S > 1/2, *oppure*
2. P_f < P *e la capitalizzazione di mercato di REP è maggiore di* $\frac{(I_a+I_p)P}{(P-P_f)S}$.

Dimostrazione. Si supponga che il protocollo di forking è integro. Allora, secondo la nozione S > ½ o $I_a + I_p$ < (P – P_f) SM. Si supponga che $I_a + I_p$ < (P – P_f) SM. Siccome $I_a + I_p \geq 0$ e SM > 0, sappiamo che P_f < P. Allora risolvendo Ia +Ip < (P – P_f) SM per PM, vediamo che $\frac{(I_a+I_p)P}{(P-P_f)S}$. Quindi la prima direzione è dimostrata. Adesso si supponga che S > ½, o che P_f < P e $\frac{(I_a+I_p)P}{(P-P_f)S}$. Se S > ½, allora il protocollo di forking è integro per definizione. Se P_f < P e $\frac{(I_a+I_p)P}{(P-P_f)S}$ < PM, allora, risolvendo la disuguaglianza per $I_a + I_p$, vediamo che $I_a + I_p$ < (P - P_f) SM, e il protocollo di forking è integro.

24. In pratica, l'utente malintenzionato riceverà 1.05 SM REP nell'universo figlio a causa del bonus del 5% per la migrazione entro 60 giorni dall'inizio del fork. Qui ignoriamo il bonus del 5% per rendere la comprensione più facile. Per una trattazione che include il 5% di bonus vedere l'appendice C.

B. Le Nostre Ipotesi e le Loro Conseguenze

Crediamo che i trader non vogliano fare trading su Augur in un universo dove i reporter hanno mentito. Crediamo anche che i creatori di mercati non pagherebbero per creare dei mercati su Augur in un universo dove non ci sono trader. In un universo sprovvisto di mercati o di trading, I REP non pagano alcun dividendo a chi li possiede. Di conseguenza, crediamo che i REP inviati ad un Falso universo non abbiano alcun valore di mercato trascurabile e lo rappresentiamo lasciando $P_j = 0$.

Crediamo che sia ragionabile aspettarsi la migrazione di almeno il 20% di tutti i REP esistenti verso il Vero esito durante il periodo di reporting di un fork, e noi rappresentiamo ciò con S ≥ 1/5. Inoltre, siamo disposti ad accomodare l'open interest parassita grande quanto il 50% dell'open interest nativo lasciando così $I_a \geq 2I_p$.

Tramite queste assunzioni, Il Teorema 1 ci dice che il protocollo di forking è integro ogniqualvolta che la capitalizzazione di mercato di REP sia almeno 7.5 volte rispetto all'open interest nativo.[25]

C. Spinte alla Capitalizzazione di Mercato

Augur ottiene le informazioni sul prezzo di REP nello stesso modo con il quale ottiene altre informazioni dal mondo reale: attraverso un mercato Augur. Ciò dà ad Augur l'abilità di computare l'attuale capitalizzazione di mercato di REP. Augur può anche misurare l'attuale open interest nativo, e pertanto può determinare quale capitalizzazione di mercato dovrebbe essere presa di mira al fine di soddisfare le condizioni di integrità di Augur. Ogni universo inizia con una commissione di reporting dell'1%. Se la capitalizzazione attuale del mercato è inferiore a quella target, allora le commissioni di reporting aumentano automaticamente (ma non sarà mai più grande del 33%), mettendo pressione al rialzo al prezzo di REP e/o pressione al ribasso sull'open interest nativo. Se la capitalizzazione di mercato attuale è al di sotto del target, allora le commissioni di reporting diminuiscono automaticamente (ma non saranno ami più basse dello 0.01%) così che i trader non devono pagare più di quanto richiesto per mantenere il sistema sicuro. Le commissioni di reporting sono determinate come segue. Sia r la commissione di reporting del precedente intervallo, sia t la capitalizzazione di mercato target e sia c la capitalizzazione di mercato attuale. Allora la commissione di reporting per l'intervallo attuale è data da max $\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10{,}000}\right\}$

D. Sfruttare la Minaccia di un Fork

Come menzionato precedentemente, i fork sono perturbanti e rallentano la finalizzazione dei mercati.

Invece di usare il processo di forking per risolvere ogni mercato, Augur sfrutterà la *minaccia* di un fork per risolvere efficientemente i mercati.

25. Vedi l'appendice B per alcune supposizioni alternative e le loro conseguenze.

Ricorda che ogni stake contestato con successo in favore del risultato finale del mercato riceverà il 50% di ROI sullo stake contestato.[26] In caso di fork, qualsiasi REP messo in staking su un qualsiasi Falso risultato del mercato dovrebbe perdere tutto il suo valore economico, mentre qualsiasi REP messo in staking sul Vero risultato del mercato viene ricompensato con il 50% in più di REP nell'universo figlio che corrisponde al Vero risultato del mercato (indipendentemente dal risultato del fork). Di conseguenza, se spinti a un fork, I titolari di REP che contestano risultati falsi in favore del Vero risultato ne verranno sempre fuori, mentre i titolari di REP che scommettono su risultati falsi vedranno i loro REP perdere valore economico. Crediamo che questa situazione sia sufficiente per garantire che tutti i falsi risultati provvisori verranno contestati con successo.

III. POTENZIALI PROBLEMI & RISCHI

A. Mercati Parassiti

Ricorda che il mercato parassita è un qualunque mercato che non paga le commissioni di reporting ad Augur, ma si risolve in conformità alla risoluzione di un mercato nativo di Augur. Poiché i mercati parassiti non hanno alcun reporter pagante, possono offrire lo stesso servizio di Augur con commissioni inferiori. Ciò potrebbe avere gravi conseguenze per l'integrità del protocollo di forking di Augur. In particolare, se dei mercati parassita attraggono l'interesse dei trader da Augur, allora i reporter di Augur riceverebbero meno in commissioni di reporting. Ciò eserciterebbe una pressione verso il basso sulla capitalizzazione di mercato di REP. Se la capitalizzazione di mercato di REP scende troppo, l'integrità del protocollo di forking è messa in pericolo (Teorema 1). Di conseguenza, i mercati parassiti hanno il potenziale per minacciare la viabilità a lungo termine di Augur e quindi dovrebbero essere contrastati con veemenza. La nostra migliore difesa contro i mercati parassiti è di rendere il trading sulla piattaforma di Augur il più economico possibile (mantenendo allo stesso tempo l'integrità dell'oracolo), al fine di minimizzare la ricompensa derivante dall'esecuzione di un mercato parassita.

B. Volatilità dell'Open Interest

Grandi, improvvisi e inaspettati aumenti nell'open interest – come quelli visti durante un evento di sport popolare – risultano in rapidi aumenti dei requisiti della capitalizzazione di mercato per l'integrità del protocollo di forking (Teorema 1). Quando li requisito di capitalizzazione di mercato eccede la capitalizzazione di mercato, c'è il rischio che gli attaccanti economicamente razionali causino un fork per risolvere incorrettamente. Mentre Augur tenta di spingere la capitalizzazione di mercato al rialzo durante queste situazioni (vedi Sezione II C), queste spinte sono reazionarie e sono aggiustate solo una volta per un intervallo di pagamento di 7 giorni.

Vale la pena notare, tuttavia, che gli speculatori che assistono all'improvviso aumento dell'open interest potrebbero acquistare REP in previsione della spinta reazionaria della capitalizzazione di mercato, guidando di conseguenza la capitalizzazione di mercato di REP verso l'alto. Forse verso un punto dove l'integrità del protocollo di forking non è più minacciata. Quindi il lasso temporale durante il quale l'oracolo è vulnerabile potrebbe non essere abbastanza lungo per un attaccante per poter sfruttare con successo la vulnerabilità.

C. Fonti di Risoluzione Incoerenti o Malevole

Durante la creazione del mercato, i creatori dei mercati scelgono la fonte di risoluzione che i reporter dovrebbero utilizzare per determinare il risultato dell'evento in questione. Se il creatore di mercato sceglie una fonte di risoluzione incoerente o malevola, i reporter onesti potrebbero perdere del denaro. Ad esempio, Supponiamo che il mercato in questione ha i possibili esiti A e B, e che il creatore del mercato, Serena, ha scelto il suo sito web, attacker.com, come fonte di risoluzione. Dopo il momento finale del mercato, Serena – che è anche la reporter designata per il mercato – riporta l'esito A e aggiorna attacker.com per indicare che l'esito B è l'esito corretto. I reporter onesti che hanno controllato attacker.com vedranno che il report iniziale è incorretto e che durante il primo round di disputa dovrebbe essere contestato con successo il risultato provvisorio in favore dell'esito B. Serena Aggiornerebbe attacker.com per indicare che il risultato A è l'esito corretto e che il mercato dovrebbe entrare nel suo secondo round di disputa. Di nuovo, i reporter che hanno controllato attacker.com vedranno che l'esito provvisorio (il risultato B) è incorretto e che potrebbe essere contestato con successo. Serena può ripetere questo comportamento fino alla risoluzione del mercato, non importa come il mercato si risolve, alcuni reporter onesti perderanno il loro denaro. Esistono parecchie versioni di questo attacco. Ignorare semplicemente i mercati con fonti di risoluzione dubbie non è sufficiente, nel caso che un evento del genere causi un fork al mercato, tutti i possessori di REP dovranno scegliere un universo figlio verso il quale migrare i loro REP. I reporter dovrebbero rimanere vigilanti contro marcati con fonti di risoluzione dubbie. Tali mercati dovrebbero essere identificati pubblicamente in modo tale che i reporter possano coordinarsi per essere sicuri di rendere invalida la finalizzazione di questi mercati.

D. Query dell'Oracolo Autoreferenziali

I mercati che negoziano sul futuro comportamento dell'oracolo di Augur potrebbero avere un effetto indesiderato sull'oracolo stesso [11]. Ad esempio, si consideri un mercato che fa trading sulle domande, "il reporter designato fallirà nel consegnare un rapporto durante il periodo di reporting di 3 giorni prima del 31 dicembre 2018?" Le scommesse piazzata sul risultato No potrebbero agire come incentivo perverso per i reporter designati di fallire intenzionalmente nel consegnare il report. Se un reporter designato può comprare abbastanza azioni Si a un prezzo sufficientemente basso da compensare le perdite del no-show bond,

26. Misurato in REP che esiste in un universo che corrisponde al risultato finale del mercato; Vedi il teorema 3 dell'Appendice A.

potrebbe intenzionalmente fallire nel report. Se la capitalizzazione di mercato di REP è grande abbastanza (Teorema 1) allora le query autoreferenziali dell'oracolo non minacceranno l'integrità del protocollo di forking. Tuttavia, potrebbero intaccare negativamente le performance di Augur causando ritardi nelle finalizzazioni dei mercati. Mentre i mercati dovrebbero finalizzare correttamente, questa sorta di comportamento è perturbante e indesiderato.

E. Partecipazione Incerta al Fork

Non possiamo sapere in anticipo quanti REP verranno migrati verso il Vero universo durante il periodo di forking di un fork, perciò non possiamo sapere in anticipo se la capitalizzazione di mercato sia grande abbastanza per l'integrità dell'oracolo (Teorema 1). La nostra convinzione è che l'integrità del protocollo di forking potrebbe non essere forte abbastanza quanto la nostra convinzione nelle nostre supposizioni a proposito del limite inferiore della partecipazione onesta durante un periodo di forking. Presupponiamo che almeno il 20% di tutti i REP verrà migrato verso il Vero universo figlio durante il periodo di forking di un fork, ma non siamo in grado di garantirlo. I fork di Augur sono differenti dai fork delle blockchain in un unico aspetto importante: dopo il fork di una blockchain, un utente che ha posseduto una moneta sulla chain principale possederà adesso una moneta per entrambi i fork. Ignorando gli attacchi di replay, i fork delle blockchain comportano un piccolo rischio per gli utenti. Dopo un fork di Augur, tuttavia, un utente che possiede un token REP nell'universo genitore può migrare questa moneta solo verso un unico universo figlio. Se l'utente migra i suoi token verso un qualunque universo diverso dall'universo di consenso, c'è la probabilità che i suoi token perdano tutto il loro valore. Perciò migrare REP durante il periodo di forking di un fork, prima che sia chiaro quale universo ha ottenuto il consenso, espone l'utente a dei rischi. Questi rischi possono scoraggiare la partecipazione durante il periodo di forking del fork contestato. Nel tentativo di compensare questi rischi e incoraggiare la partecipazione durante il periodo di forking, tutti i possessori del token che migrano i loro REP entro 60 giorni dall'inizio del fork riceveranno il 5% in più di REP nell'universo figlio verso il quale hanno migrato (vedi Sezione I C 9). Tuttavia, non possiamo sapere in anticipo se il 5% di bonus sia abbastanza per compensare i rischi e incentivare la partecipazione durante il periodo di forking.

F. Mercati Soggettivi o Ambigui

Solo eventi che hanno esiti oggettivamente conoscibili sono idonei all'uso nei mercati di Augur. Se i reporter Credono che un mercato non sia idoneo alla risoluzione da parte della piattaforma – ad esempio, perché è ambiguo, soggettivo o l'esito non è conosciuto alla data finale dell'evento – dovrebbero riportare il mercato come Invalido. Se il mercato si risolve come Invalido, i trader vengono pagati con lo stesso valore per tutti i possibili risultati; Per mercati scalari, i trader sono pagati a metà strada tra il prezzo minimo e il prezzo massimo del mercato.

È possibile immaginare mercati dove alcuni reporter sono certi che il risultato sia A e che altri siano certi che il risultato sia B. Ad esempio, nel 2006, TradeSports ha permesso ai suoi utenti di speculare se la Corea del Nord avrebbe lanciato un missile balistico che sarebbe atterrato fuori dal suo spazio aereo prima della fine di luglio 2006. Il 5 luglio, 2006 la Corea del Nord ha lanciato con successo un missile balistico che è atterrato al di fuori del suo spazio aereo e l'evento è stato ampiamente riportato dai media mondiali e confermato da molte fonti governative degli Stati Uniti. Tuttavia, il dipartimento di difesa degli Stati Uniti non ha commentato sull'evento, come era richiesto dal contratto di TradeSports. TradeSports ha concluso che le condizioni del contratto non erano state soddisfatte e ha emesso i pagamenti di conseguenza[27].

Questo è un caso in cui lo spirito del mercato – di predire il lancio del missile – era chiaramente soddisfatto, ma la lettera del mercato – di prevedere se il Dipartimento di Difesa degli Stati Uniti avrebbe confermato il lancio – non lo è stata. TradeSports, essendo un website centralizzato, è stato capace di dichiarare unilateralmente il risultato del mercato. Se tale situazione dovesse presentarsi in un mercato di Augur, i possessori di REP potrebbero avere opinioni differenti su come il mercato dovrebbe risolversi e scommetterebbero i loro REP di conseguenza. Nel peggiore dei casi, ciò potrebbe risultare in un fork dove i REP in più di un universo figlio mantengano un valore diverso da zero.

RICONOSCIMENTI

Ringraziamo Abraham Othman, Alex Chapman, Serena Randolph, Tom Haile, George Hotz, Scott Bigelow e Peronet Despeignes per i loro utilissimi feedback e suggerimenti.

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 mar-ket. 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.

27. Vedi https://en.wikipedia.org/wiki/Intrade#Disputes per i dettagli.

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 sys-tem. https://bitcoin.org/bitcoin.pdf, 2008.
9. V. Buterin. A next generation smart con-tract 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 Secu-rity, June 2014.
11. A. Othman and T. Sandholm. Decision rules and de-cision markets. In Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Sys-tems: 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 decentral-ized, open-source platform for prediction markets. arXiv:1501.01042v1 [cs.CR], 11 2014.

Appendice A: Tempo di Finalizzazione e Redistribuzione

Cominciamo con qualche notazione, definizione e osservazione.

Definizione 5. Per un dato mercato M, sia Ω_M lo spazio dei risultati (o set di risultati) di M.

Definizione 6. Per n ≥ 1 e ω ∈ Ω_M, sia S(ω, n) il numero totale di stake piazzato sul esito ω all'inizio del round di disputa n. Ciò include tutti gli stake provenienti da tutti i bond di disputa in favore di ω su tutti i precedenti round di disputa.

Definizione 7. Per n ≥ 1 e ω ∈ Ω_M, sia S(ω|, n) la quantità di stake su tutti gli esiti in Ω_M *eccetto per* ω all'inizio del round di disputa n:

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

Definizione 8. Per n ≥ 0, sia A_n lo stake totale di tutti gli esiti M all'inizio del round di disputa n:

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

Osservazione 3. Ne segue che $A_n - S(\omega, n) = S(\overline{\omega}, n)$

Definizione 9. Per n ≥ 1, sia $\hat{\omega}_n$ il risultato provvisorio all'inizio del round di disputa n. Ad esempio, $\hat{\omega}_1$ è il risultato riportato dal reporter iniziale.

Definizione 10. Per n ≥ 1 e $\omega \neq \hat{\omega}_n$ sia $B(\omega, n)$ la quantità di stake richiesta per eseguire con successo un bond di disputa in favore del risultato ω durante il round di disputa n.

Ricorda che la quantità di stake richiesto per eseguire con successo un bond di disputa in favore del risultato ω durante un round di disputa n, dove $\omega \neq \hat{\omega}_n$ è dato da Eq.1, $B(\omega, n) = 2A_n - 3S(\omega, n)$

Osservazione 4. Se un bond di disputa è eseguito con successo in favore del risultato ω durante il round di disputa n, allora $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. Cioè, lo stake della disputa è l'unico nuovo stake applicato al risultato ω alla fine del round di disputa n.

Osservazione 5. Per tutti $\omega \neq \hat{\omega}_n, S(\omega, n-1) = S(\omega, n)$
Cioè, se un bond di disputa non è interamente eseguito in favore del risultato ω, allora non viene aggiunto alcuno stake aggiuntivo al risultato ω all'inizio del prossimo round di disputa. Ciò è dovuto al fatto che tutto lo stake di disputa viene restituito agli utenti alla fine del round di disputa.

Osservazione 6. Per tutti $n \geq 2, A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$ cioè, l'ammontare totale di stake su tutti i risultati all'inizio del round di disputa è semplicemente lo stake totale dall'inizio del round di disputa precedente più lo stake dal precedente round di disputa. Tutti gli altri stake vengono restituiti agli utenti alla fine del round di disputa precedente.

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

Dimostrazione. Si supponga che un mercato entri nel round di disputa n, dove n ≥ 2. Durante il round di disputa n – 1 il risultato $\hat{\omega}_{n-1}$ è stato contestato in favore dell'outcome $\hat{\omega}_n$. Secondo Eq.1, la dimensione di questo bond di disputa è $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Utilizzando l'osservazione 3, può essere riscritto come:

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

Noi sappiamo che il bond di disputa è stato eseguito con successo durante il round n – 1. Usando l'osservazione 4, vediamo che $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. L'osservazione 5 ci dice che la quantità di stake su ω_n è invariata dal round n – 1 a n, $2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$. Pertanto, Eq.A1 si riduce a
$S(\hat{\omega}_n, n) = 2S(\hat{\omega}_n, n)$

Teorema 3. *Ogni possessore di REP che contesta con successo un risultato in favore del risultato finale del mercato riceverà il 50% di ROI sul suo stake in disputa (misurato in REP esistenti in un universo che corrisponde al risultato finale del mercato), a meno che il mercato non venga interrotto da qualche altro mercato che causando un fork*.

Dimostrazione. Durante un fork, a tutti gli utenti che hanno eseguito un bond di disputa con successo in favore del risultato finale del mercato in forking viene dato (tramite nuove monete coniate durante il fork) il 50% di ROI sul loro stake in disputa quando gli stessi migrano il loro stake in disputa verso l'universo figlio corrispondente. Pertanto, nel caso in cui il mercato in questione ha causato un fork, il teorema è immediatamente soddisfatto.

Adesso consideriamo il caso in cui il mercato in questione si risolva senza causare un fork e il reporting non viene interrotto da qualche altro mercato che causa un fork.

Denotiamo l'esito finale del mercato con ω_{Final} e supponiamo che il mercato si risolva alla fine del round di reporting n, dove n ≥ 2. Ciò significa che il risultato provvisorio n è ω_{Final} e che questo risultato non è stato contestato con successo durante il round n. in altre parole $\hat{\omega}_n = \omega_{\text{Final}}$. Allora per lemma 2, sappiamo che $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$. Poiché il mercato si risolve alla fine del round n con nessun stake aggiunto a un qualsiasi risultato, l'equazione precedente mostra la quantità finale di stake sul risultato finale del mercato, ω_{Final}, e la somma di tutti gli stake su tutti gli altri risultati del mercato $\overline{\omega_{\text{Final}}}$. Nota che c'è esattamente il doppio di stake nel risultato finale del mercato di quanto non c'è ne sia in tutti gli altri risultati messi insieme. Augur ridistribuisce tutti gli stake nel risultato non definitivo agli utenti che hanno lo stake su $\overline{\omega_{\text{Final}}}$ in proporzione all'ammontare di REP che hanno messo in stake. Perciò gli utenti che hanno eseguito correttamente un bond di disputa in favore di $\overline{\omega_{\text{Final}}}$. Successivamente, consideriamo il numero massimo di round di disputa necessari per risolvere il mercato. L'Eq.1 è minimizzata quando ω è scelto per essere il risultato non provvisorio che comincia il round di disputa con la maggiore quantità di stake.

Il lemma 2 implica che l'esito non provvisorio con la più grande quantità di stake è l'esito provvisorio del precede
Round di disputa. Perciò, il più piccolo bond di disputa possibile che può essere eseguito correttamente durante il round di disputa n, dove $n \geq 2$, is $B(\hat{\omega}_{n-1}, n)$.
In altri termini, la dimensione del bond di disputa cresce lentamente quando gli stessi due risultati di mercato vengono ripetutamente contestati in favore di un altro. Ne segue che il numero di round contestati richiesti per l'inizio di un fork è massimizzando quando 2 risultati uguali vengono ripetutamente contestati in favore in un altro. Di conseguenza, possiamo determinare il numero massimo di round di disputa che qualunque mercato potrebbe subire prima di iniziare un fork trovando il numero massimo di round di dispute che possono avvenire nel caso particolare in cui gli stessi due risultati di mercato sono ripetutamente contestati in favore di un altro. Questo caso verrà esaminato adesso.

Si supponga che ogni bond di disputa viene eseguito con successo in favore del risultato provvisorio del round di disputa precedente. Allora i due risultati provvisori che sono iterativamente contestati in favore di un altro sono $\hat{\omega}_1$ e $\hat{\omega}_2$.

Osservazione 7. Nel caso in cui gli stessi 2 risultati provvisori sono ripetitivamente contestati in favore di un altro $\hat{\omega}_n = \hat{\omega}_{n-2}$ per tutti gli n ≥ 3.

Definizione11. Sia *d* la quantità di stake piazzata su $\hat{\omega}_1$ durante il report iniziale. Siccome il risultato provvisorio per ogni round in questa situazione è conosciuto, possiamo semplificare la nostra notazione per le dimensioni del bond di disputa. Definiamo l'abbreviazione B_n per denotare la dimensione del bond necessario per il round n, così che B_1 = 2*d* e $B_n = B(\hat{\omega}_{n-1}, n)$ per tutti gli n ≥ 2. Ciò per una più facile lettura e comprensione.

Osservazione 8. Nel caso in gli stessi 2 risultati provvisori sono ripetutamente contestati in favore di un altro, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ for $n \geq 3$. . (Cioè, ogni altro bond di disputa corretto è aggiunto al medesimo risultato).

Lemma 4. *Se gli stessi 2 risultati provvisori sono ripetutamente contestati in favore di un altro, allora per tutte le n, dove n ≥ 3:*

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

Dimostrazione. (Per induzione su n)

Si supponga che gli stessi 2 risultati provvisori sono ripetutamente contestati in favore di un altro.

(Caso Base) Per definizione e Eq.1 facciamo le seguenti osservazioni.

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

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, quindi la parte 1 del dilemma vale per n = 3.
$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, così la parte 2 del dilemma vale per n = 3.
$B_3 = 6d = 3d2^{3-2}$, così la parte 3 del dilemma vale per n = 3.

Quindi il lemma, nella sua interezza, vale per il caso base in cui n = 3.

(Induzione) si supponga che il lemma sia Vero per tutte le n di questo tipo 3 ≤ *n* ≤ *k.* Vogliamo dimostrare che il lemma è Vero per n = k + 1. Cioè, vogliamo dimostrare che:

(a) $S(\hat{\omega}_k, k+1) = \frac{2}{3}B_k$
(b) $A_{k+1} = 2B_k$ and
(c) $B_{k+1} = 3d2^{k-1}$

Primo, proviamo la parte (a). Dall'osservazione 8:

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

Dall'osservazione 7 possiamo riscriverla come:

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

Dalle ipotesi di induzione, possiamo riscrivere $S(\hat{\omega}_{k-2}, k-1)$ come $\frac{2}{3}B_{k-2}$ sulla parte destra, ottenendo:

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

Dalle ipotesi di induzione, possiamo scrivere B_{k-2} come $3d2^{k-4}$ e B_{k-1} come $3d2^{k-3}$:

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

Applicando l'osservazione 7 sulla parte sinistra otteniamo:

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

Infine, nota che dall'equazione precedente e le ipotesi di induzione, $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$.
Ciò prova la parte (a).
In seguito, proviamo la parte (b). Dall'osservazione 6:

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

Dalle ipotesi di induzione, $A_k = 2B_{k-1}$:

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

Dalle ipotesi di induzione, $B_{k-1} = 3d2^{k-3}$ così la parte destra può essere semplificata in:

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

Dalle ipotesi di induzione, $B_k = 3d2^{k-2}$ possiamo riscrivere la parte destra come:

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

E la parte (b) è provata.

Infine, proviamo la parte (c). dall' Eq.1:

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

Dall'osservazione 8, possiamo scrivere $S(\hat{\omega}_k, k+1)$ come $S(\hat{\omega}_k, k-1) + B_{k-1}$:

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

Dall'osservazione 7, $\hat{\omega}_k = \hat{\omega}_{k-2}$

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

Dall'osservazione 6, $A_{k+1} = A_k + B_k$:

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

Dalle ipotesi di induzione, $A_k = 2B_{k-1}$ e $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$:

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

Dalle ipotesi di induzione, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ e $B_{k-2} = 3d2^{k-4}$. Facendo queste sostituzioni e semplificando:

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

Ciò prova la parte (c) e conclude la dimostrazione del lemma.

Teorema 5. *Se non interrotto da qualche altro mercato che causa un fork, un dato mercato potrebbe subite al massimo 20 round di dispute prima di finalizzarsi o causare un fork.*

Dimostrazione. Si supponga che un dato mercato non viene interrotto da qualche altro mercato che causa un fork. Allora, come mostrato precedentemente, sappiamo che il numero di round di disputa richiesto da un mercato per iniziare un fork è massimizzato quando gli stessi due risultati sono ripetutamente contestati in favore di un altro.

La parte 3 e la parte 4 del Lemma ci dice che, in questa situazione, la dimensione del bond di disputa necessaria che contestare con successo il risultato provvisorio durante il round n è data da $3d2^{n-2}$, dove *d* è la quantità di stake piazzato durante il report iniziale.

Sappiamo che i fork iniziano dopo la corretta esecuzione di un bond di disputa con una dimensione di almeno il 2,5% di tutti i REP esistenti, e sappiamo che ci sono 11 milioni di REP in esistenza. Pertanto un fork inizia quando la dimensione di un bond di disputa raggiunge i 275,000 REP. Sappiamo inoltre che $d \geq 0.35$ REP, perché la quantità minima di stake sul report iniziale è $d \geq 0.35$ REP.

Risolvendo $3(0.35)2^{n-2} > 275,000 \text{ for } n \in \mathbb{Z}$ è uguale a $n \geq 20$. Perciò, possiamo garantire che un mercato si risolverà o causerà un fork dopo al massimo 20 round di disputa.

Appendice B: Supposizioni Alternative e Conseguenze

Ricorda che:

- S, è la proporzione totale di REP migrata verso il Vero universo durante il periodo di fork.
- P, è il prezzo di REP nel Vero universo.
- P_f, è il prezzo di REP che è stato migrato verso un Falso universo scelto dall'attaccante.
- I_a, è l'open interest nativo di Augur.
- I_p, è l'open interest parassita.

Augur determina ipotesi su S, P_f, e I_p al fine di giungere alla capitalizzazione target del mercato. Nello specifico, Augur suppone che almeno il 20% di tutti i REP verranno migrati verso il Vero universo durante il periodo di forking di un fork, i REP migrati verso un Falso universo non avranno alcun valore significativo e l'open interest parassita sarà al massimo la metà dell'open interest nativo. In altre parole: $S \geq 0.2$, $P_f = 0$ e $I_a \geq 2I_p$. Sotto questi presupposti, il Teorema 1 ci dice che il protocollo di forking è integro ogniqualvolta la capitalizzazione di mercato di REP è maggiore di 7.5 volte dell'open interest nativo. Puoi fare le tue ipotesi su S, P_f, e I_p per arrivare alle tue proprie conclusioni su quanto grande la capitalizzazione di mercato deve essere per l'oracolo per avere integrità nella pratica. Elenchiamo qualche scenario alternativo per illustrazione.

Scenario 1. Più del 50% dei REP esistenti migrerà verso il Vero universo durante il periodo di forking. In questo caso P_f e I_p non hanno alcuna importanza. Siccome $S > 1/2$, il protocollo di forking è integro e non importa l'entità della capitalizzazione di mercato. Non esisterebbero sufficienti REP sul mercato perché l'attaccante possa avere successo.

Scenario 2. Il 48% dei REP esistenti migra verso il Vero universo durante il periodo di forking, non esiste alcun mercato parassita e i REP che vengono inviati a un Falso universo non hanno valore. In questo caso $S = 0.48$, $I_p = 0$, and $P_f = 0$. Sotto queste supposizioni, la capitalizzazione di mercato di REP deve essere maggiore del doppio dell'open interest nativo affinché il protocollo di forking abbia integrità.

Scenario 3. Il 20% di tutti i REP esistenti migra verso il Vero universo durante il periodo di forking, l'open interest parassita è uguale all'open interest nativo e i REP migrati verso un Falso universo rappresentano il 5% del valore dei REP migrati verso il Vero universo. In questo caso $S = 0.05$, $I_p = 2I_a$ e $P_f = 0.05P$. Sotto queste ipotesi, la capitalizzazione di mercato di REP deve essere maggiore di 10.5 volte dell'open interest nativo affinché il protocollo di forking abbia integrità.

Scenario 4. Solo il 5% di tutti i REP esistenti migra verso il Vero universo durante il periodo di forking, l'interest parassita è grande il doppio dell'open interest nativo e i REP inviati a un Falso universo rappresentano il 5% del valore dei REP inviati al Vero universo. In questo caso $S = 0.05$, $I_p = 2I_a$, e $P_f = 0.05P$. Sotto queste ipotesi, la capitalizzazione di mercato di REP deve essere maggiore 63 volte quella dell'open interest nativo affinché il protocollo di forking abbia integrità.

Appendice C: L'effetto del Bonus di Migrazione sull'Integrità del Protocollo di Forking.

Per rendere la discussione semplice, abbiamo ignorato il 5% di bonus della migrazione e un piccolo termine durante la discussione dell'integrità del protocollo di forking. Qui rivisitiamo il Teorema 1 prendendo in considerazione queste due cose. Come in precedenza, la quantità di REP inviati verso il Vero universo durante la fase di reporting è denotata da SM. Pertanto affinchè un attaccante abbia successo, deve riuscire a migrare almeno SM + ε REP, che ha un valore di (SM + ε) P prima della migrazione verso un Falso universo. Se un attaccante migra SM + ε REP verso un Falso universo durante il periodo di reporting di un fork, riceverà 1.05(SM + ε) REP sull'universo figlio verso il quale ha fatto la migrazione. Per definizione di P_f il valore di queste monete è dato da 1.05(SM + ε) P_f. Perciò il costo minimo per l'attaccante è (SM + ε) P – 1.05(SM + ε) P_f, che può essere espresso come (SM + ε) (P – 1.05 P_f). Come in precedenza, il beneficio (lordo) massimo dell'attaccante è dato da I_a + I_p. Di conseguenza potremmo dire che il protocollo di forking è integro ogniqualvolta S > ½ o:

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

Risolvendo la disequazione per la capitalizzazione di mercato, PM, possiamo vedere che il protocollo di forking ha integrità se e solo se:

1. S > ½
2. 1.05 P_f < P e la capitalizzazione di mercato di REP è maggiore di $\frac{P(I_a+I_p-\epsilon(P-1.05P_f))}{S(P-1.05P_f)}$.

Come possiamo vedere, l'effetto del bonus di migrazione sulla capitalizzazione di mercato è alquanto piccolo.

Appendice D: L'effetto del Bonus di Migrazione sul Costo Minimo del Fork

Per incoraggiare una maggiore partecipazione durante un fork, tutti i titolari del token che migrano i propri REP entro 60 giorni dall'inizio del fork, riceveranno il 5% di REP in più nell'universo figlio verso il quale hanno migrato. Questa ricompensa è pagata tramite l'inflazione della moneta. Questo bonus può diventare un incentivo perverso se il costo nell'iniziare un fork è eccessivamente basso. Nello specifico, se un attaccante riesce a guadagnare più valore dal 5% di bonus in REP rispetto a quello che perderebbe iniziando un fork, allora ci aspetteremmo che i fork accadano il più spesso possibile. Questo attacco, al quale ci riferiamo come *inflation milking attack,* non dovrebbe risultare in un reporting incorretto dell'oracolo, ma dovrebbe risultare nell'accadimento frequente di fork perturbanti. Al fine di prevenire questo comportamento, Augur deve essere sicuro che il costo nell'iniziare un fork sia maggiore del valore massimo che può essere guadagnato dal 5% di bonus di inflazione. Qui, deriviamo un peso inferiore sul costo di inizio di un fork al fine di prevenire questo incentivo perverso.

Sia P_0 il prezzo di REP prima del fork e P_1 il prezzo di REP dopo il fork. Sia M_0 l'offerta di moneta prima del fork e M_1 l'offerta di monera successiva al fork. Sia S la proporzione di M_0 che migra verso il Vero universo durante il periodo di forking del fork. Sia *b* la quantità di REP che deve essere economicamente bruciata (cioè, messa in stake su un Falso outcome) al fine di iniziare un fork. Ipotizziamo che b > 1.

Per il fine di questa sezione, assumiamo conservativamente che tutti i REP che vengono migrati durante il periodo di forking sono controllati dall'attaccante. Ipotizzeremo successivamente (poiché minimizza il costo di questo attacco) che tutti i REP che migrano durante il periodo di forking sono migrati verso il Vero universo.

Con questa notazione, SM_0 è la quantità di REP migrata durante il periodo di forking, mentre (1 – S) M_0 è la quantità di REP non migrata durante il periodo di forking.

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

Quando il totale di SM_0 REP è migrato durante il periodo di forking, un totale di $0.05SM_0$ REP viene creato tramite inflazione:

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

Facendo attenzione solo sull'effetto dell'inflazione, e per ragioni di semplicità, ipotizziamo che la capitalizzazione dopo il fork sarà la stessa di quella prima del fork[28].

$$P_0M_0 = P_1M_1 \qquad \text{(D3)}$$

Sostituendo D1 e D2 in D3 e semplificando abbiamo:

$$P_1 = \frac{20P_0}{20 + S} \qquad \text{(D4)}$$

Il beneficio (lordo) per un attaccante nell'iniziare un fork e approfittare del bonus di migrazione è rappresentato dal valore dei suoi REP dopo la migrazione meno il valore degli stessi prima della migrazione:

$$1.05SM_0P_1 - SM_0P_0 \qquad \text{(D5)}$$

Sostituendo D4 in D5 otteniamo un'espressione alternativa per il beneficio (lordo) guadagnato dall'attaccante:

$$1.05SM_0\frac{20P_0}{20 + S} - SM_0P_0 \qquad \text{(D6)}$$

Ricorda che *b* è la quantità di REP che deve essere economicamente bruciata affinchè si possa iniziare un fork. Pertanto, il costo nell'iniziare un fork è Bp_0. Di conseguenza, pagare il costo per iniziare un fork al fine approfittare del bonus di migrazione è fruttuoso

---

[28] Pensiamo che sia conservativo. Nella pratica , ci aspettiamo che la capitalizzazione di mercato diminuisca dopo il fork.

Ogniqualvolta la seguente disequazione è soddisfatta:

$$0 < 1.05SM_0\frac{20P_0}{20+S} - SM_0P_0 - bP_0 \qquad \text{(D7)}$$

Osservando che $P_0 > 0$ e $S \neq 20$, risolviamo per *b,* e vediamo che l'attacco è profittevole quando:

$$b < \frac{21M_0S}{S+20} - M_0S \qquad \text{(D8)}$$

Al fine di prevenire l'incentivo perverso, Augur deve fare in modo che:

$$b > \frac{21M_0S}{S+20} - M_0S \qquad \text{(D9)}$$

Nulla che la S, è ristretta all'intervallo [0, 1], vediamo che il valore della parte destra della disuguaglianza D9 è massimizzata quando $S = 2\sqrt{105} - 20 \approx 0.4939$. Cioè, questo attacco è più redditizio per l'attaccante quando più o meno il 49,3% di tutti i REP esistenti viene migrato durante il periodo di forking. Essendo conservativi, usiamo questo valore per S[29]. Sostituendo S = 0.4939 in D9 otteniamo $b < 0.012297M_0$. Di conseguenza, se il costo nell'iniziare un fork richiede almeno 1.2197% di tutti i REP esistenti allora l'attacco *inflation milking* non è redditizio.

Ricorda che un fork inizia solo dopo l'esecuzione di un bond di disputa che è maggiore del 2,5% di tutti i REP esistenti. Supponendo che tale bond di disputa sia eseguito correttamente in favore dell'esito ω e un fork era già stato avviato. L'outcome ω è Vero o Falso.

Se l'outcome ω è Falso, allora almeno il 2.5% di tutti i REP esistenti sono stati messi in staking su un Falso risultato e perciò economicamente bruciati. Quindi l'inflation milking non è redditizio quando ω è Falso.

Se l'outcome ω è Vero, allora il Lemma 2 ci dice che almeno l'1.25% dei REP esistenti (in totale) è messo in staking su un Falso risultato e perciò economicamente bruciati. Quindi l'inflation milking è non redditizio anche quando ω è Vero.

È per questa ragione che iniziare un fork richiede l'esecuzione di un bond di disputa grande quanto almeno il 2.5% di tutti i REP esistenti.

Appendice E: Aggiustamenti della Dimensione del Bond

Lo stake del bond di validità, del no-show REP bond e del reporter designato viene dinamicamente aggiustato in base al comportamento dei partecipanti durante il precedente intervallo di pagamento. Qui descriviamo come vengono regolati questi valori.

Definiamo la funzione $f : [0,1] \to [\frac{1}{2}, 2]$, per:[30]

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

La funzione f è usata per determinare i multipli utilizzanti in questo aggiustamento, come descritto nella successiva sottosezione. In breve, se il comportamento indesiderabile avviene esattamente l'1% delle volte durante il precedente intervallo di pagamento, allora la dimensione del bond rimane la stessa. Se ciò fosse meno frequente, allora la dimensione del bond sarà ridotta almeno della metà. Se ciò fosse più frequente, allora la dimensione del bond verrà aumentata almeno del doppio.

1. Bond di Validità

Durante il primo vero intervallo, successivo al lancio, il bond di validità verrà fissato a 0.01 ETH. Poi, se più dell'1% dei mercati finalizzati nel precedente intervallo di pagamento era Invalido, il bond di validità verrà aumentato. Se meno dell'1% dei mercati finalizzati nel precedente intervallo di pagamento era Invalido, allora il bond di validità verrà diminuito (ma non sarà mai inferiore a 0.01 ETH).

Nello specifico, sia ν la proporzione dei mercati finalizzati invalidi nel precedente intervallo di pagamento, e sia b_v l'ammontare del bond di validità del precedente intervallo di pagamento. Allora il bond di validità per l'intervallo attuale è massimo di $\{\frac{1}{100}, b_v f(\nu)\}$

2. No-Show REP Bond

Durante il primo intervallo di pagamento, successivo al lancio, il no-show REP bond verrà impostato a 0.35 REP. Come per il bond di validità, il no-show REP bond è aggiustato verso l'alto o verso il basso, prendendo come obiettivo l'1% di tasso no-show con un minimo di 0.35 REP. Nello specifico, sia p la proporzione di mercati nel precedente intervallo di pagamento per i quali il reporter designato ha fallito nel consegnare il report in tempo, e sia b_r la dimensione del no-show REP bond del precedente intervallo di pagamento. La quantità del no-show REP bond per l'attuale intervallo di pagamento è massimo $\{0.35, b_r f(\rho)\}$.

3. Stake del Reporter Designato

Durante il primo intervallo di pagamento, successivo al lancio, la quantità di stake del reporter designato è dinamicamente aggiustata in base al numero di report designati incorretti (che hanno fallito nel coincidere con il risultato finale del mercato) durante il precedente intervallo di pagamento.

29. In pratica, l'attaccante non può ostacolare la migrazione dei REP degli altri partecipanti durante il periodo di forking, e perciò non può garantire che *S* non dovrebbe eccedere il suo valore ideale all'incirca di 0.4939. Tuttavia, siccome ci stiamo difendendo contro lo scenario peggiore possibile, usiamo S = 0.4939.

30. Questa formula potrebbe cambiare una volta ottenuti dati empirici da mercati reali.

Nello specifico, sia § la proporzione dei report designati che erano incorretti durante il precedente intervallo di pagamento, e sia b_d la quantità di stake del reporter designato durante l'intervallo di pagamento precedente, allora la quantità di stake del reporter designato per l'intervallo attuale è massimo $\{0.35, b_d f(\delta)\}$.

Appendice F: Cambi di Design

Siamo arrivati all'attuale design di Augur dopo 3 anni di ricerca e iterazioni. Il design emerso da questo processo si differenzia sostanzialmente dalla visione prevista dal nostro vecchio Whitepaper [12]. Qui, discutiamo di tre cambiamenti significativi tanto quanto la razionalità di questi cambiamenti.

1. Commissioni di Reporting

Nel vecchio design, il creatore del mercato avrebbe stabilito una commissione di trading che avrebbe diviso 50/50 con i reporter. Nel design corrente, le commissioni del creatore del mercato e dei reporter sono indipendenti, e le commissioni dei reporter sono accordate dinamicamente da Augur stesso per mantenere il sistema sicuro. Le commissioni pagate ai reporter impattano sul prezzo di REP, che ha un effetto diretto sulla sicurezza del protocollo di forking (Teorema 1). Se le commissioni pagate ai reporter sono troppo basse, allora l'integrità dell'oracolo è messa a rischio. Se le commissioni pagate ai reporter sono troppo alte, allora la minaccia di mercati parassiti aumenta. Perciò, è importante che le commissioni pagate ai reporter si aggiuntino dinamicamente per mantenere la sicurezza di Augur, invece di essere decise arbitrariamente dai creatori dei mercati. Disaccoppiare le commissioni dei reporter dalle scelte dei creatori dei mercati garantisce inoltre che i reporter (e quindi, l'integrità del protocollo di forking) non siano danneggiati dalla competizione tra creatori dei mercati, e che la qualità del reporting dovrebbe essere misurata e compensata separatamente. La competizione dovrebbe essere permessa per guidare le commissioni dei creatori dei mercati verso lo zero, senza trascinare verso il basso anche le commissioni pagate ai reporter.

2. Commissioni di Trading

Nel vecchio design, le commissioni venivano raccolte dai trader su ogni trade. Nel nuovo design, le commissioni sono raccolte dai trader solo quando sono stabilite direttamente nel contratto di mercato. Questo cambio è stato fatto, in parte, perché Augur non può sorvegliare il trading offline. Le azioni del mercato degli outcome sono semplicemente dei token, che possono essere scambiate liberamente tra utenti. Siccome raccogliere le commissioni su ogni scambio è infattibile, Augur invece raccoglie le commissioni solo quando i trader risolvono direttamente i contratti di mercato di Augur. Un beneficio aggiunto di questo approccio è che riduce le commissioni medie pagate dai trader, e ciò dovrebbe rendere Augur maggiormente competitivo.

3. Universi

Nel vecchio design, c'era solo una "versione" di REP e la sua offerta totale era fissa. Nel design attuale, REP può subire dei fork in tante versioni differenti (universi), ognuno dei quali può ritrovarsi con più o meno REP in totale rispetto alla versione originale.

Se un fork è contestato, l'offerta di REP in ogni universo figlio dovrebbe essere solo una frazione dell'offerta totale dell'universo genitore. In un fork non contestato, il bonus di migrazione per i partecipanti al fork potrebbe risultare in un universo figlio che ha più REP in totale del suo universo genitore.

Le nuove versioni di REP generate da un fork sono token diversi tra loro, ognuno con il suo prezzo e la sua offerta totale e i fornitori di servizi dovrebbero trattarli come tali. Quando Augur verrà lanciato la prima volta, ci sarà un singolo universo (l'universo genesi) e un'unica versione di REP, proprio come esiste adesso. Tuttavia, non appena accade un fork, la singola versione di REP verrà divisa in molteplici versioni; Ad esempio, un mercato in forking con gli esiti A e B dovrebbe sfornare i nuovi token REP-A, REP-B e REP-Invalido. I wallet e gli exchange che supportano REP adesso dovrebbero avere 4 versioni differenti di REP che dovrebbero (in teoria) supportare – REP-genesis (la versione originale di REP, che adesso dovrebbe essere bloccata), REP-A, REP-B e REP-Invalido[31].

L'offerta totale di REP in ogni universo figlio dipende da quanto REP è stato migrato verso lo stesso e quando detta migrazione è avvenuta. Migrare REP durante un fork, prima che sia chiaro quale universo figlio ha ottenuto il consenso, espone l'utente a una piccola (ma non zero) quantità di rischio (vedi la Sezione III E), che potrebbe scoraggiare la partecipazione durante il periodo di forking del fork contestato. Al fine di incoraggiare la partecipazione durante un fork, gli utenti devono essere compensati adeguatamente per il rischio.

Gli utenti che non vogliono partecipare durante il periodo di forking di un fork potrebbero essere penalizzati perdendo una porzione dei loro REP, infatti, il vecchio design ha usato un meccanismo di tipo "usalo o perdilo", che penalizzava i non partecipanti come se fossero reporter che non avevano riportato correttamente. Tuttavia, punire gli utenti che non partecipano crea gravi problemi di usabilità. Punire gli utenti che non partecipano è problematico per i wallet e gli exchange che sono i custodi dei loro acquirenti di REP. Nel caso di un fork, gli exchange dovrebbero aver bisogno di migrare i REP dei loro clienti verso qualche universo figlio durante il periodo di forking o perdere una porzione dei loro REP[32]. Invece di penalizzare i non partecipanti, i partecipanti al fork che migrano i loro REP durante il periodo di forking vengono

---

31. Come questione pratica, i fornitori di servizi potrebbero trovare facile (e almeno perturbante per i loro utenti) l'incoraggiare i loro utenti a partecipare al fork e poi semplicemente supportare l'universo vincente una volta che il fork si è risolto.

32 Abbiamo inoltre trovato, come questione pratica, che il codice degli smart contract necessario per implementare le ricompense dei forking usando solamente la redistribuzione era esageratamente complesso. Il codice di contratti complessi è esso stesso un rischio alla sicurezza, così abbiamo provato a semplificare l'implementazione ogniqualvolta possibile.

Ricompensati da una coniazione del 5% di bonus nell'universo figlio verso il quale sono migrati. Se il 4.762% dei REP (o più) migra verso un universo perdente – nel quale dall'1.25% al 2.5%

È stato già impegnato come stake di disputa – allora tutti gli universi avranno un'offerta di moneta di REP inferiore a quella dell'universo genitore.