Augur: Zdecentralizowana Wyrocznia i Platforma Predykcji Rynków

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander
Fundacja Forecast
(Dated: May 24, 2018)

Augur jest zdecentralizowaną wyrocznią i platformą predykcji rynków, która nie wymaga zaufanych uczestników rynku. Wyniki predykcji rynków sa ustalane przez użytkownikow, którzy posiadają natywny dla Augura token reputacji. Użytkownicy stawiają swoje tokeny na rzeczywisty wynik predykcji i otrzymują w zamian prowizję naliczaną po rozliczeniu kontraktu rynkowego. Struktura zachęcająca do korzystania z Augur'a została zaprojektowana w taki sposób, że dokładne i uczciwe raportowanie wyników predykcji jest zawsze najbardziej dochodową opcją dla użytkowników posiadających tokeny reputacji. Posiadacze tokenów mogą emitować obligacje proporcjonalnie duże do stanu posiadania tokenów w celu rozstrzygnięcia proponowanych wynikówch rynkowych. Jeżeli wartość wyemitowanych obligacji osiągnie wymagany pułap, reputacja zostaje rozbita na tyle wersji wyniku rynkowego, ile jest możliwych wyników rynkowych, po jednej na każdy możliwy wynik; posiadacze tokenów muszą następnie wymienić swoje Tokeny Reputacji na jedną z powyższych wersji wyniku. Wersje reputacji, które nie są powiązane z prawdziwym wynikiem staną się bezwartościowe z powodu braku chętnych na udział w predykcji do momentu ustalenia pewności na prawidłowy wynik. Z tego względu posiadacze tokenów będą wybierali wyłącznie tą wersję reputacji, która będzie miała wartość, czyli wersja która odnosi się do rzeczywistego wyniku.

Augur jest zdecentralizowaną wyrocznią i platformą predykcji rynków, nie wymagającą zaufanych uczestników rynku. W rynkach predykcji osoby mogą spekulować na temat wyników przyszłych wydarzeń; osoby, które prawidłowo przewidzą wynik, wygrywają pieniądze, a osoby, które źle przewidzą wynik, tracą pieniądze. [1–3]. Cena ustalona przez predykcję rynku może służyc jako precyzyjny, dobrze skalibrowany wskaźnik prawdopobieństwa pojawienia się danego wydarzenia. [4–7].

Augur umożliwi ludziom wzięcie udziału w rynkach predykcji przy znikomych kosztach. Jedynym znacznym wydatkiem, którzy uczestnicy muszą wziąć pod uwagę jest wynagrodzenie wypłacane twórcom rynku i użytkownikom raportującym rzeczywisty wynik po zajściu danego wydarzenia rynkowego. Dzięki temu powstaje rynek predykcji, w którym wymogi zaufania uczestnikom, spory oraz opłaty są na tyle niskie, na ile pozwalają konkurencyjne siły rynku.

Historycznie rynki predykcji były scentralizowane. Najprostszym sposobem na zebranie w jednym miejscu transakcji rynku predykcji jest utrzymwanie rejestru transakcji przez zaufaną jednostkę; podobnie, najprostszym sposobem na ustalenie wyniku zdarzeń i dystrybucję wypłat handlowcom jest zrobienie tego za pomocą bezstronnego, zaufanego sędziego. Jednakże scentralizowane rynki predykcji posiadają ryzyko i ograniczenia: nie pozwalają na globalne uczestnictwo, ograniczają typy rynków, które mogą być tworzone i handlowane i wymagają ufania operatorowi rynku, że nie ukradnie funduszy i prawidłowo ustali wynik rynków.

Augur ma na celu ustalenie rynków w całkowicie zdecentralizowany sposób. Zdecentralizowane, nie wymagające zaufania sieci, takie jak Bitcoin[8] i Ethereum[9], eliminują ryzyko prywatnych interesów przekształcających się w korupcję lub kradzież. Jedynym zadaniem deweloperów Augura jest publikowanie smart kontraktów w sieci Ethereum. Kontrakty Augura są całkowicie zautomatyzowane: deweloperzy nie mają możliwości wydania pieniędzy, które są trzymane w kontraktach escrow, nie kontrolują wyniku rynkowego, nie zatwierdzają ani nie odrzucają transakcji kupna/sprzedaży ani żadnych innych transakcji w sieci, nie są w stanie cofać transakcji, modyfikować ani kasować zleceń, itp. *Wyrocznia* Augura pozwala na migrację informacji ze świata rzeczywistego do technologii blockchain bez potrzeby polegania zaufanym pośrednikom. Augur będzie pierwszą na świecie zdecentralizowaną wyrocznią.

I. ZASADA DZIAŁANIA AUGURA

Rynki Augura postępują cztero-etapowo: *utworzenie*, *handel*, *raportowanie*, oraz *rozliczenie*. Każdy może stworzyć rynek bazujący na jakimkolwiek zdarzeniu w rzeczywistym świecie. Handel rozpoczyna się natychmiast po utworzeniu rynku i wszyscy użytkownicy mogą handlować na dowolnym rynku. Po zajściu zdarzenia na którym bazuje dany rynek, wynik zdarzenia jest zdeterminowany przez wyrocznię Augura. Po określeniu wyniku, handlujący mogą zamknąć swoje pozycje i otrzymać swoje wypłaty.

Augur posiada token REP (Reputacja) natywny dla platformy. REP jest potrzebny osobom tworzącym rynek i raportującym wynik zdarzenia opartego na rynku utworzonym na platformie Augura. Osoby raportujące raportują dany rynek przez *umieszczenie* ich REP na jednym z możliwych wyników. Przez ten proces, raportujący deklaruje, że wynik na którym tokeny zostały umieszczone, odpowiada prawdziwemu wynikowi zdarzenia zachodzącego w danym rynku. Konsensus osiągnięty przez raportujących rynku, jest uważany za "prawdę" w celu ustalenia wyniku zdarzenia rynkowego. Jeżeli raport raportującego nie pasuje do konsensusu osiągniętego

przez pozostałych raportujących, Augur przydziela tokeny REP umieszczone na tym raporcie raportującym, którzy zaraportowali zgodnie z konsensusem.

Dzięki posiadaniu tokenów REP i uczestniczeniu w dokładnym raportowaniu wyników zdarzeń, osoby posiadające tokeny są uprawnione do otrzymania części opłat platformy. Każdy postawiony token REP uprawnia jego właściciela do otrzymania równej porcji opłat platformy Augura. Im więcej tokenów REP posiada reporter, i raportuje prawidłowo, tym więcej opłat zarobi za swój wkład i pracę utrzymującą platformę bezpieczną.

Pomimo tego, że token REP odgrywa centralną rolę w operacjach Augura, nie jest używany do handlowania w rynkach Augura. Handlujący nie będą nigdy potrzebowali posiadać tokenów REP ani ich używać, ponieważ nie jest wymagane uczestnictwo w procesie raportowania.

A. Tworzenie Rynku

Augur umożliwia dowolnym osobom utworzyć rynek o dowolnym przyszłym zdarzeniu. *Twórca rynku* ustawia *zdarzenie i jego czas* i wybiera *wyznaczonego raportującego* aby zaraportował wynik zdarzenia. Wyznaczony reporter nie decyduje jednostronnie o wyniku rynku; społeczność zawsze ma szansę na spór i korektę raportu przedstawionego przez wyznaczonego raportującego.

Następnie twórca rynku wybiera *źródło rezolucji* które powinno zostać użyte przez raportujących do określenia wyniku. Źródłem rezolucji może być po prostu "wiedza powszechna", lub konkretne źródło informacji, takie jak "Departament Energii USA", bbc.com, lub adres szczególnego punktu końcowego API.[1] Ustalają również *opłatę twórcy*, która jest opłatą dla tworzącego rynek przez handlujących, którzy rozliczają kontrakt rynkowy (patrz Sekcja I D aby uzyskać szczegółowe informacje na temat opłat). Ostatecznie, twórca rynku publikuje dwie obligacje: *obligacja ważności*, oraz *obligacja nie przedstawienia wyznaczonego raportu* (również dla skrócenia określanej jako *obligacja no-show*).

Obligacja ważności jest płatna w tokenie ETH i zwracana do tworzącego rynek w przypadku, gdy rynek decyduje się na wynik inny niż *nieważny*.[2] Obligacja ważności zachęca tworzących rynki, aby tworzone rynki były na dobrze zdefiniowanych zdarzeniach z obiektywnymi i niedwuznacznymi rezultatami. Wielkość obligacji ważności jest ustalana dynamicznie, bazuje na odsetku nieważnych wyników w ostatnich rynkach.[3]

Obligacja no-show składa się z dwóch części: *obligacji no-show rozliczanej w jednostkach gas* (płatnej w tokenie ETH) oraz *obligacji no-show rozliczaniej w REP* (płatnej w REP). Powyższe obligacje są zwracane do tworzącego rynek, jeżeli raportujący wyznaczony przez rynek przedstawi raport w ciągu trzech dni po *końcu czasu zdarzenia*. Jeżeli wyznaczony raportujący nie przedstawi raportu w ciągu przydzielonego 3-dniowego okna, tworzący rynek traci obligację no-show i jest ona przeznaczona dla *pierwszego publicznego raportującego* który zaraportuje na danym rynku (patrz Sekcja I C 6). Zachęca to tworzącego rynek do wybierania rzetelnych wynaczonych raportujących, którzy będą w stanie szybko decydować o danym rynku.

Obligacja no-show gas jest utworzona w celu pokrycia kosztów w jednostkach gas pierwszego publicznego raportującego. Zapobiega to zajściu sytuacji, w której koszty zaraportowania są zbyt wysokie dla raportującego, aby raport był opłacalny. Wielkość obligacji no-show gas jest ustawiana na dwukrotność średnich kosztów raportowania podczas poprzedniego okna opłat.

W przypadku, gdy wyznaczony reporter nie przedstawi raportu, obligacja no-show REP jest przekazywana pierwszemu publicznemu reporterowi w formie kwoty postawionej na wyniku przez niego zaraportowanego, tak że pierwszy publiczny reporter otrzymuje obligację no-show REP wtedy i tylko wtedy, gdy zaraportuje prawidłowo. Podobnie jak z obligacją ważności, rozmiar obligacji no-show REP jest dostosowywany proporcjonalnie do wyznaczonych reporterów, którzy nie zaraportowali podczas poprzedniego okna opłat.[4]

Twórca rynku tworzy rynek i publikuje wszystkie konieczne obligacje za pomocą jednej transakcji Ethereum. Po zatwierdzeniu transakcji, rynek jest otwierany i rozpoczyna się handel.

B. Handel

Uczestnicy rynku przewidują wyniki zdarzeń handlując *akcjami* danych zdarzeń. *Całkowity zbiór akcji* jest kolekcją akcji, która składa się z jednej akcji na każdy możliwy wypłacalny wynik zdarzenia [10]. Zbiory całkowite są tworzone przez silnik Augura, który dopasowuje kontrakty w celu zakończenia handlu.

Przykładowo, weźmy pod uwagę rynek z dwoma możliwymi wynikami zdarzenia, A i B. Alicja jest skłonna zapłacić 0.7 ETH za akcję A natomiast Bob jest skłonny

[1] Na przykład, jeżeli rynek oparty jest na "Wysokiej temperaturze (w skali Fahrenheita) w dniu 10 kwietnia 2018 roku na lotnisku w San Francisco, jak zaraportowane przez serwis "Weather Underground", określa źródło rezolucji https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html, raportujący odwiedziliby stronę www i wpisali najwyższą temperaturę wyświetloną na stronie w swoim raporcie.

[2] *Nieważnym rynkiem* jest określany rynek, który został tak zdefiniowany przez raportujących z powodu, że żaden z wyników podanych przez tworzącego rynek jest prawidłowy, lub sformułowanie rynku jest dwuznaczne lub subiektywne; patrz Sekcja III F na rozwinięcie tematu.

[3] Patrz Aneks E 1 aby uzyskać dalsze szczegóły.

[4] Patrz Aneks E 2 aby uzyskać dalsze szczegóły.

Figure 1. Uproszczony zarys życia rynku predykcji.

zapłacić 0.3 ETH za akcjęB.[5] Po pierwsze, Augur dopasowuje zlecenia i pobiera sumarycznie kwotę 1 ETH od Alicji i Boba.[6] Następnie Augur tworzy kompletny zbiór akcji, przyznając Alicji akcję A a Bobowi akcję B. W ten sposób tworzone są akcje. Po utworzeniu akcji, mogą być one dowolnie wymieniane na wolnym rynku.

Kontrakty handlowe Augura utrzymują rejestr zleceń dla każdego rynku utworzonego na platformie. Każdy może utworzyć nowe zlecenie lub zrealizować istniejące zlecenie w dowolnym momencie. Zlecenia są realizowane za pomocą automatycznego algorytmu, który jest zaimplementowany w smart kontraktach Augura. Żądanie zakupu lub sprzedaży akcji jest spełniane natychmiastowo, jeżeli istnieje pasujące zlecenie po stronie przeciwnej w rejestrze zleceń. Może zostać spełnione przez zakup akcji lub sprzedaż akcji innym uczestnikom rynku, co może oznaczać emisję nowych kompletnych zbiorów akcji lub zamykanie istniejących. Algorytm Augura dopasowujący zlecenia zawsze sekwestruje, czyli przechowuje minimalną liczbę akcji i/lub gotówki potrzebnej do pokrycia wartości objętej ryzykiem. Jeżeli nie istnieje zlecenie przeciwstawne, lub zlecenie może być wykonane tylko częściowo, pozostałość jest umieszczana w rejestrze zleceń jako nowe zlecenie.

Zlecenia nie są nigdy wykonywane w cenie gorszej niż limit ceny ustalonej przez handlującego, ale może zostać wykonane po cenie lepszej niż zakładana. Niewykonane lub częściowo wykonane zlecenia mogą zostać usunięte z rejestru zleceń w dowolnym momencie przez tworzącego zlecenie. Opłaty są płacone przez handlujących wyłącznie wtedy, gdy kompletne zbiory akcji są sprzedane; opłaty rozliczenia transakcji są opisane szczegółowo w Sekcji I D.

Oczekuje się, że większość handlu akcjami będzie miała miejsce przez rozliczeniem rynku, ale akcje mogą być wymieniane w dowolnym momencie po utworzeniu rynku. Wszystkie aktywa Augura – włączając akcje w wynikach zdarzeń rynkowych, tokeny partycypacji, akcje w obligacjach kwestii spornych i nawet własność rynków jako takich – są zbywalne w dowolnym momencie.

[5] Początkowo, handel w rynkach Augura będzie używał tokena Ether (ETH) natywnego dla Ethereum. Kolejne wersje Augura będą obejmowały również wsparcie dla rynków denominowanych w dowolnych tokenach wyemitowanych na sieci Ethereum, włączając w to akcje innych rynków, jak również tokeny trwale powiązane z walutami, tzw. ("stablecoins"), jeżeli/gdy będą one dostępne.

[6] Kwota 1 ETH została wybrana, aby ułatwić dyskusję. Rzeczywisty koszt kompletnego zestawu akcji jest o wiele mniejszy; patrz docs.augur.net/#number-of-ticks aby uzyskać dalsze szczegóły.

C. Raportowanie

Po zajściu zdarzenia, na którym opiera się rynek, wynik musi zostać określony aby rynek mógł zostać sfinalizowany i aby rozpocząć rozliczenie. Wyniki sa ustalane przez wyrocznię Augura, która składa się z raportujących motywowanych zyskiem, którzy po prostu raportują rzeczywisty wynik danego zdarzenia. Każdy właściciel tokena REP może uczestniczyć w raportowaniu i rozwiązywaniu kwestii spornych. Raportujący, których raporty są zgodne z konsensusem są wynagradzani finansowo, natomiast raportujący, których raporty nie są zgodne z konsensusem są finansowo karani (patrz Sekcja I D 3).

1. *Okna opłat*

System raportowania Augura działa w 7-dniowych cyklach *okien opłat*. Wszystkie opłaty zbierane przez Augura w ciągu danego okna są dodawane do *puli opłat reporterów* dla danego okna opłat. Po zakończeniu okna opłat, pula opłat reporterów jest wypłacana do posiadaczy tokenów REP, którzy brali udział w procesie raportowania. Reporterzy otrzymują nagrody proporcjonalne do ilości tokenów REP, które postawili w ciągu danego okna opłat. Uczestnictwo obejmuje: stawianie podczas początkowego raprotu, rozwiązywania kwestii spornej niepewnego wyniku, lub zakup *tokenów partycypacji*.

2. *Tokeny Partycypacji*

W czasie trwania dowolnego okna opłat, posiadacze tokenów REP mogą zakupić dowolną liczbę tokenów partycypacji za jeden attorep[7] każdy. Po zamknięciu okna opłat, mogą zrealizować swoje tokeny partycypacji za jeden attorep każdy, dodatkowo do propocjonalnej części opłat zawartej w *puli okna opłat*. W przypadku gdy nie było żadnych wydarzeń (*np.*, przedstawienia raportu lub rozwiązanie kwestii spornej raportu wysłanego przez innego użytkownika) które potrzebowały reportera, reporter może zakupić tokeny partycypacji aby zaznaczyć, że był obecny podczas okna opłat. Podobnie, jak w przypadku postawionych tokenów REP, tokeny partycypacji

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

mogą być zrealizowane przez ich właścicieli *proporcjonalnie* do części opłat w danych oknie opłat.

Jak przedstawiono w Sekcji II, ważne jest, aby posiadacze tokenów REP byli gotowi na uczestnictwo w ustalaniu rynku podczas zdarzenia rozwidlenia sieci. Tokeny partycypacji dostarczają bodziec dla posiadaczy tokenów REP do monitorowania platformy przynajmniej raz w tygodniu, i tym samym, byli gotowi do wzięcia udziału jeżeli zaistnieje potrzeba. Nawet posiadacze tokenów REP, którzy nie chcą brać udziału w procesie raportowania są motywowani do sprawdzania Augura raz podczas 7-dniowego okna opłat aby kupować tokeny partycypacji i otrzymywać opłaty. To regularne, aktywne meldowanie się, zapewni, że posiadacze tokenów będą zaznajomieni ze sposobem używania Augura, będą świadomi rozwidlenia sieci w przypadku ich zaistnienia i tym samym będą gotowi na uczestnictwo w rozwidleniach sieci, jezeli zaistnieją.

3. Progresja Stanu Rynku

Rynki Augua po utworzeniu, mogą znajdować się w jednym z siedmiu stanów. Potencjalne stany, lub "fazy", rynku Augura są jak następuje:

- Pre-raportowanie
- Wyznaczenie raportowania
- Otwarte Raportowanie
- Oczekiwanie na otwarcie kolejnego okna opłat
- Seria rozwiązywania kwestii spornych
- Rozwidlenie
- Zakończony

Związek pomiędzy poszczególnymi stanami jest przedstawiony na wykresie 2.

4. Pre-raportowanie

Faza *pre-reportowania* lub *handlowania* (Diag. 1) jest okresem czasu, który rozpoczyna się po rozpoczęciu handlu w danym rynku, ale zanim wydarzenie na którym opiera się dany rynek przeminęło. Zwykle, jest to najbardziej aktywny okres handlu dla dowolnego rynku Augura. Po zajściu wydarzenia, rynek wkracza w fazę *wyznaczenia raportowania* (Wykres 2a).

5. Wyznaczenie raportowania

Przy tworzeniu rynku, twórcy rynku muszą wybrać wyznaczonego raportującego i opublikować obligację no-show. Podczas fazy wyznaczonego raportowania (Wykres 2a) wyznaczony raportujący ma czas do trzech dni na zaraportowanie wyniku wydarzenia. Jeżeli wyznaczony raportujący nie zdoła zaraportować w ciągu wyznaczonego czasu trzech dni, twórca rynku traci obligację no-show i rynek automatycznie wkracza w fazę *otwartego raportowania* (Wykres 2b).

Jeżeli wyznaczony raportujący przedstawi raport na czas, obligacja no-show jest zwracana twórcy rynku. Wyznaczony raportujący musi opublikować wielkość postawioną dla wyznaczonego raportującego[8] na zaraportowany wynik, który straci, jeżeli rynek zakończy się wynikiem innym niż zaraportowany.[9] Jak tylko wyznaczony raportujący przedstawi swój raport, rynek wkracza w fazę *oczekiwania na otwarcie kolejnego okna opłat* (Wykres 2c), i zaraportowany wynik staje się *tymczasowym wynikiem.*

6. Otwarte Raportowanie

Jeżeli wyznaczony raportujący nie przedłoży raportu w ciągu przydzielonych trzech dni, twórca rynku traci obligację no-show i rynek natychmiastowo wkracza w fazę *otwartego raportowania* (Diag. 2b). Jak tylko rynek wejdzie w fazę otwartego raportowania, każdy może zaraportować wynik zdarzenia rynkowego. Jeżeli wyznaczony raportujący nie zdoła zaraportować, pierwszy raportujący który przedstawi raport na wynik zdarzenia, zostaje nazwany *pierwszym publicznym raportującym.*

Pierwszy publiczny raportujący rynku otrzymuje utraconą obligację no-show bond w formie udziału na wybrany wynik, w związku z tym może rościć sobie prawo do obligacji no-show REP wyłącznie, gdy jego zaraportowany wynik zgadza się z końcowym wynikiem rynkowym. Otrzymuje także obligację no-show gas po zakończeniu rynku wyłącznie gdy zaraportowany wynik zgadza się finalnym wynikiem rynku.

Pierwszy publiczny raportujący *nie* potrzebuje przekazać udziałów na jakikolwiek z własnych tokenów REP podczas raportowania wyniku zdarzenia rynkowego. W ten sposób, jakikolwiek rynek którego wyznaczony raportujący nie zdoła przedstawić raportu, oczekuje się na zaraportowania wyniku przez *kogokolwiek* bardzo szybko po przejściu rynku w fazę otwartego raportowania.

Po tym, jak *raport początkowy* został otrzymany przez pierwszego raportującego (niezależnie czy był to wyznaczony reporter, czy pierwszy publiczny reporter), zaraportowany wynik staje się tymczasowym wynikiem rynku, i rynek wkracza w fazę oczekiwania na otwarcie kolejnego okna opłat (Wykres 2c).

---

[8] Patrz aneks E 3 w celu szczegółow na temat wielkości udziału dla wyznaczonego raportującego.

[9] Stracony udział jest dodawany do puli opłat raportowania w danym oknie opłat, i zostaje użyty do wynagrodzenia uczciwych raportujących i osób pomagających rozwiązać kwestie sporne; patrze Sekcja I D 3 aby uzyskać dalsze szczegóły.

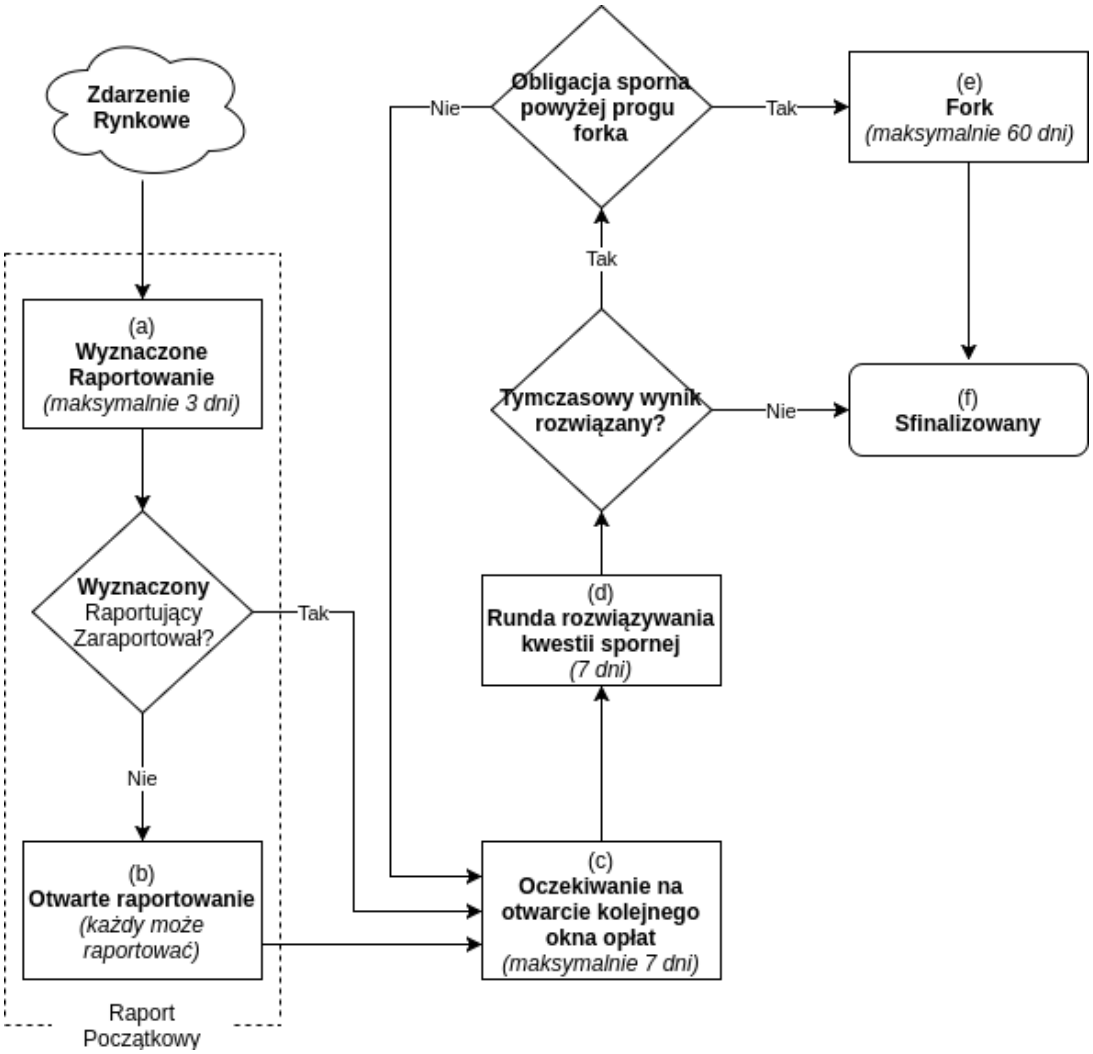

Figure 2. Diagram sekwencji raportowania.

7. *Oczekiwanie na Otwarcie Kolejnego Okna Opłat*

Po tym, jak rynek otrzyma raport początkowy, wkracza w fazę oczekiwania na otwarcie kolejnego okna opłat (Wykres 2c). Podczas tej fazy, raportowanie rynku jest wstrzymane do zamknięcia bieżącego okna opłat. Po otwarciu kolejnego okna opłat, rynek wkracza w fazę *serii rozwiązywania kwestii spornych.*

8. *Seria rozwiązywania kwestii spornych*

Seria rozwiązywania kwestii spornych (wykres 2d) jest 7-dniowym okresem podczas którego każdy posiadacz tokenów REP ma szansę na rozwiązania *niepewnego wyniku rynku.*[10] (Na początku serii, niepewny wynik rynku jest wynikiem, który będzie finalny, jeżeli nie zostanie skutecznie rozwiązany przez posiadaczy tokenów REP.) Rozwiązanie różnicy zdań składa się z *postawienia udziałów tokenów* REP (nazywane *udziałami spornymi* w tym kontekście) na wynik *inny niż* bieżący niepewny wynik rynku. Rozwiązanie sporu jest *skuteczne* jeżeli całkowita kwota udziałów spornych na dany wynik jest równa *kwocie obligacji spornej* wymaganej w bieżącej serii. Kwota obligacji spornej jest obliczana jak następuje.

Niech A_n oznacza całkowity udział wszystkich wyników danego rynku na początku serii rozwiązywania kwestii spornych n. Niech ω oznacza dowolny wynik rynku *różny od* niepewnego wyniku rynku na początku danej serii. Niech $S(\omega, n)$ oznacza całkowitą ilość udziałów na wynik ω na początku serii n. Wtedy kwota *obligacji spornej* wymaganej do skutecznego rozwiązania

[10] Fakt, że serie rozwiązywania kwestii spornych zbiegają się z oknami opłat jest czystym udogodnieniem; w zasadzie, serie rozwiązywania kwestii spornych i czas trwania okien opłat mogłyby być różne.

bieżącego niepewnego wyniku na korzyść nowego wyniku ω podczas serii n jest oznaczona $B(\omega, n)$ i jest obliczana przez:

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

Kwoty obligacji są wybierane w taki sposób, aby zapewnić stały zwrot inwestycji na poziomie 50% dla raportujących którzy skutecznie rozwiązują spory dotyczące błędnych wyników (patrz Sekcja II D).

Obligacje sporne nie muszą być opłacone w całości przez jednego użytkownika. Platforma Augura pozwala użytkownikom na pozyskanie od społeczności funduszy na obligacje sporne. Każdy użytkownik, który widzi nieprawidłowy niepewny wynik może zapoczątkować spór przez przekazanie udziałów tokenu REP na wynik różny niż bieżący tymczasowy wynik. Jeżeli jakikolwiek wynik (różny od wyniku tymczasowegu) zgromadzi wystarczają liczbę udziałów spornych aby pokryć obligację sporną, spór dotyczący bieżącego wyniku tymczasowego zostanie skutecznie rozwiązany.

W przypadku skutecznego rozwiązania kwestii spornej, rynek przejdzie przez kolejną serię rozwiązywania sporu, lub przejdzie w fazę *rozwidlenia* (Wykres 2e). Jeżeli kwota wykupionej obligacji spornej jest większa niż 2.5% wszystkich tokenów REP, rynek wejdzie w fazę rozwidlenia. W przypadku, gdy kwota wykupionej obligacji spornej jest mniejsza niż 2.5% wszystkich tokenów REP, nowo wybrany wynik staje się nowym wynikiem tymczasowym i rynek przechodzi przez kolejną rundę dysputy.

W trakcie rozwiązywania sporu udział sporny znajduje się w całości na rachunku powierniczym. Jeżeli obligacja sporna jest nieudana, wtedy udział sporny jest zwracany właścicielom po zakończeniu serii dysputy. W przypadku, gdy żaden spór nie zostanie rozstrzygniety podczas 7-day rundy spornej, rynek wkracza w fazę *zakończoną* (Wykres 2f), a jego tymaczowy wynik zostaje zaakceptowany jako *wynik finalny*. Finalny wynik rynku jest tymczasowym wynikiem, który przejdzie przez rundę sporną bez skutecznego sporu, lub jest zdeterminowany przez rozwidlenie. Kontrakty Augura traktują finalny wynik jako *prawdziwy* i wypłacają zgodnie z tym wynikiem.

Wszystkie udziały nieskutecznego sporu są zwracane właścicielom na końcu każdej serii rozstrzygania sporu. Wszystkie udzały skutecznego sporu są przekazywane wynikowi, który został uznany za prawdziwy i pozostają tam do momentu sfinalizowania rynku (lub do momentu zajścia rozwidlenia w innym rynku Augura). Wszystkie udziały sporne (niezależnie czy skutecznych sporów, czy nie) otrzymają część *puli opłat reporterów*[11] z bieżącego okna opłat.

[11] Jakiekolwiek opłaty za rozliczenie i obligacje ważności zebrane w ciągu otwartego okna opłat są dodawane do powyższej puli opłat reporterów. Po zamknięciu okna opłat, pula opłat reporterów jest wypłacana użytkownikom proporcjonalnie do ilości tokenów REP, które zaryzykowali podczas tego okna opłat.

9. Rozwidlenie (Fork)

Stan rozwidlenia (ang. fork) (Wykres 2e) jest specjalnym stanem, który trwa do 60 dni. Rozwidlenie jest ostatnią deską ratunku na ustalenie wyniku rynku; jest to bardzo destruktywny proces i jest zamierzone, aby pojawiał się rzadko. Rozwidlenie jest spowodowane, gdy istnieje rynek z wynikiem korzystnie wykupionej obligacji spornej o kwocie równej przynajmniej 2.5% wszystkich tokenów REP. Ten rynek jest określany jako *rynek rozwidlający*.

Gdy rozwidlenie zostanie zainicjalizowane, rozpoczyna się 60-dniowy[12] *okres rozwidlenia*. Rozstrzyganie sporów dla wszystkich innych niezakończonych rynków zostaje wstrzymane do końca okresu rozwidlenia. Okres rozwidlenia jest o wiele dłuższy niż zwykłe okno opłat, ponieważ platforma musi zapewnić dostatecznie dużo czasu posiadaczom tokenów REP i dostawcom usług (takim jak portfele i giełdy) aby się na to przygotować. Ostateczny wynik rozwidlenia nie może być rozstrzygany za pomocą sporu.

Każdy rynek Augura i wszystkie tokeny REP istnieją w pewnym *uniwersum*. Tokeny REP mogą zostać użyte do raportowania (i tym samym zarabiać opłaty) *wyłącznie* dla rynków, które istnieją w tym samym uniwersum co tokeny REP. W momencie pierwszego uruchomienia platformy Augura, wszystkie rynki i wszystkie tokeny REP będa umieszczone w tym samym *początkowym uniwersum*.

W przypadku rozwidlenia rynku, tworzone są nowe uniwersa. Rozwidlenie tworzy nowe *uniwersum potomne* dla każdego możliwego wyniku rozwidlającego się rynku (włączając w to Nieprawidłowe, jak omówione w Sekcji I D 2). Przykładowo, "binarny" rynek ma 3 możliwe wyniki: A, B, oraz Nieprawidłowy. W związku z tym, rozwidlający się rynek binarny utworzy trzy nowe uniwersa potomne: uniwersum A, uniwersum B, oraz uniwersum Nieprawidłowe. Początkowe, wszystkie nowe uniwersa są puste: nie zawierają rynków ani tokenów REP.

Gdy rozwidlenie zostaje zainicjalizowane, *uniwersum macierzyste* zostaje permanentnie *zablokowane*. W zablokowanym uniwersum nie można tworzyć nowych rynków. Użytkownicy mogą kontynuować handel akcjami w rynkach w zamkniętych uniersach, i rynki w zamkniętych uniwersach mogą w dalszym ciągu otrzymywać swoje raporty początkowe. Jednakże nie są wypłacane żadne nagrody finansowe za raportowania i rynki w zablokowanych uniwersach nie mogą być sfinalizowane. Aby rynki i tokeny REP w zablokowanym uniwersum były użyteczne, muszą zostać migrowane do uniwersum potomnego.

[12] Okres rozwidlenia może wynosić mniej, niż 60 dni: okres rozwidlenia kończy się w przypadku gdy minęło 60 dni lub więcej niż 50% wszystkich początkowych tokenów REP zostało zmigrowanych do pewnego potomnego uniwersum.

Posiadacze tokenów REP w uniwersum macierzystym mogą migrować swoje tokeny do uniwersum potomnego, który wybiorą. Wybór powinien być starannie przemyślany, ponieważ migracja jest procesem jednokierunkowym; nie może zostać odwrócona. Tokeny nie mogą być przesłane między równoległymi uniwersum, mającymi wspólne uniwersum macierzyste. *Migracja jest nieodracalnym zobowiązaniem tokenów REP na konkretny wynik rynku.* Tokeny REP, które migrują do różnych uniwersum powinny być uważane za całkowicie odseparowane tokeny, a dostawcy usług tacy jak portfele i giełdy powinny je traktować osobno.

Gdy rozwidlenie zostaje zainicjalizowane, wszystkie tokeny REP postawione na wszystkie nie-rozwidlające się rynki zostają *zwrócone* tak aby można było je dowolnie migrować do uniwersum potomnego podczas okresu rozwidlenia.[13]

Którekolwiek uniwersum potomne otrzyma najwięcej zmigrowanych tokenów REP do końca okresu rozwidlenia, staje się *wygrywającym uniwersum*, i jego analogiczny wynik zostaje finalnym wynikiem rozwidlającego się rynku. Nie-sfinalizowane rynki w uniwersum macierzystym mogą zostać zmigrowane wyłącznie do wygrywającego uniwersum i jeżeli otrzymały początkowy raport, są resetowane ponownie do fazy oczekując na kolejne okno opłat.

Nie ma ograniczeń czasowych związanych z migrowaniem tokenów z uniwersum macierzystego do potomnego. Tokeny mogą zostać zmigrowane po okresie rozwidlenia, ale nie będą miały wpływu na ustalenie wygrywającego uniwersum. Aby zachęcić do większego udziału podczas okresu rozwidlenia, wszyscy właściciele tokenów REP, którzy zmigrują swoje tokeny w trakcie 60 dni od rozpoczęcia rozwidlenia otrzymają 5% dodatkowych tokenów REP w uniwersum potomnym, do którego zmigrują[14]. Nagroda ta jest wypłacana przez wykopanie nowych tokenów REP .[15]

Reporterzy, którzy postawili swoje tokeny REP na jeden z wyników rozwidlającego się rynku nie mogą zmienić pozycji podczas rozwidlania. Tokeny REP, które zostały postawione na wynik w uniwersum potomnym mogą zostać zmigrowane wyłącznie do uniwersum potomnego, który odpowiada danemu wynikowi. Przykładowo, jeżeli reporter pomógł ustalić korzystną obligację sporną na korzyść wyniku A podczas pewnej serii spornej, wtedy tokeny REP, które postawili na wynik A mogą zostać zmigrowane wyłącznie do uniwersum A podczas rozwidlenia.

Uniwersa równoległe są całkowicie niezależne. Tokeny REP, które istnieją w jednym uniwersum nie mogą zostać użyte do raportowania zdarzeń lub zarabiania na rynkach innego uniwersum. Ponieważ użytkownicy prawdopodobnie nie będą chcieli tworzyć rynków lub handlować na rynkach w uniwersum, które mają niezaufane wyrocznie, tokeny REP, istniejące w uniwersum, które nie zgadza się z obiektywną rzeczywistością są mało prawdopodobne do zarabiania pieniędzy swoim właścicielom i tym samym nie powinny posiadać znaczącej wartości rynkowej. W związku z tym, tokeny REP zmigrowane do uniwersum, które nie odpowiada obiektywnej rzeczywistości nie powinny posiadać wartości rynkowej, niezależnie od tego, czy obiektywnie fałszywe uniwersum wygra rozwidlenie. Ma to ważne konsekwencje kwestii bezpieczeństwa, które omawiamy w Sekcji II.

10. Zakończony

Rynek wchodzi w fazę końcową (Diag. 2f) jeżeli przejdzie 7-dniowy okres serii dysputy bez skutecznego wyniku tymczasowego, który został podważony, lub po przejściu rozwidlenia. Wynik rozwidlenia nie ma możliwości podważenia i jest zawsze uważany za ostateczny po zakończeniu okresu rozwidlenia. Po zakończeniu rynku, handlujący mogą rozliczyć swoje pozycje bezpośrednio na rynku. Po przejściu rynku w stan zakończenia, wybrany wynik jest określany *finalnym wynikiem.*

D. Rozliczenie Rynku

Handlujący mogą zamknąć pozycję na dwa sposoby: przez sprzedaż akcji, które posiadają, innemu uczestnikowi rynku w zamian za walutę, lub przez rozliczenie swoich akcji z rynkiem. Przypomnijmy, że każda akcja powstaje jako część kompletnego zestawu gdy sumarycznie 1 ETH został zdeponowany w Augurze.[6] Aby otrzymać z powrotem 1 ETH z depozytu, handlujący muszą przekazać Augurowi całkowity zbiór akcji, lub po zakończeniu rynku, część z wygranego wyniku. Gdy ta wymiana następuje, określa się to jako *rozliczanie z kontraktem rynkowym.*

Na przykład, rozważmy nie zakończony rynek z możliwymi wynikami A oraz B. Załóżmy, że Alicja posiada część akcji obstawiając na wynik A które chce sprzedać za sumę 0.7 ETH, a Bob posiada część akcji obstawiając na wynik B, które chce sprzedać za 0.3 ETH. Początkowo Augur dopasowuje te zlecenia i pobiera akcje A oraz B od uczestników. Następnie Augur przekazuje 0.7 ETH (minus opłaty) Alicji oraz 0.3 ETH (minus opłaty) dla Boba.

Jako drugi przykład, rozważmy zakończony rynek, którego wygrywającym wynikiem jest A. Alicja posiada

[13] Jedynym wyjątkiem są tokeny REP ustawione przez początkowego reportera po przedstawieniu początkowego raportu. Te tokeny REP pozstają umieszczone na początkowym zaraportowanym wyniku i są automatycznie migrowane do uniwersum potomnego, które wygra rozwidlenie.

[14] Zachodzi to również w przypadku, gdy okres rozwidlenia skończył się wcześniej z powodu większej ilości niż 50% wszystich tokenów REP zmigrowanych do pewnego uniwersum.

[15] Efekt zwiększenia podaży pieniądza jest mały. Przykładowo, jeżeli 20% wszystkich istniejących tokenów REP zostało by zmigrowanych podczas okresu rozwidlenia, bonus spowodowałby 1% wzrost podaży tokenów REP. Co więcej, oczekuje się, że rozwidlenia będa nadzwyczaj rzadkimi zdarzeniami.

akcje A i chce je zamienić na gotówkę. Wysyła więc swoją część A do Augura i w zamian otrzymuje 1 ETH (minus opłaty).

1. Opłaty za Rozliczenie

Jedynym przypadkiem, gdy Augur pobiera jakiekolwiek opłaty, jest czas rozliczania się z rynkiem przez uczestników rynku. Augur pobiera dwa rodzaje opłat podczas rozliczania: opłata twórcy, oraz opłata raportującego. Obie opłaty są proporcjonalne do sumy która jest wypłacana. Zatem w przypadku rozliczenia przez zakończeniem rynku z przykładu powyżej, gdzie Alicja otrzymuje 0.7 ETH, a Bob otrzymuje 0.3 ETH, Alice zapłaciłaby 70% z kwoty opłat, natomiast Bob zapłaciłby 30%.

Opłata twórcy jest ustalana przez tworzącego rynek podczas tworzenia rynku, i jest mu wypłacana w trakcie rozliczania rynku. Opłata raportującego jest ustalana dynamicznie (patrze Sekcja II C) i jest wypłacana raportującym, którzy biorą udział w procesie reportowania.

2. Rozliczanie Nieważnych Rynków

W przypadku, gdy rynek zostanie określony jako Nieważny, handlujący, którzy rozliczają kontrakt rynkowy otrzymują równą liczbę ETH za akcje za każdy możliwy wynik. W przypadku, gdy rynek ma N możliwych wyników (pomijając wynik Nieważny), i koszt całkowitego zestawu akcji wynosił C ETH, wtedy handlujący otrzymają C/N ETH za każdą akcję rozliczoną z kontraktem rynkowym.[16]

3. Redystrybucja Tokenów Reputacji (REP)

Jeżeli rynek zostanie zakończony bez zainicjalizowania rozwidlenia, wszystkie tokeny REP postawione na wynik inny niż finalny dla danego rynku zostają utracone przez właścicieli i dystrybuowane użytkownikom, którzy postawili na finalny wynik rynku proporcjonalnie do liczby tokenów REP, które zaryzykowali. Rozmiary obligacji spornych są wybierane w taki sposób, aby każdy kto skutecznie rozwiąże spór na korzyść finalnego wyniku rynkowego jest wynagradzany 50% ROI od liczby swoich tokenów REP, które postawili na rozwiązanie sporu.[17] Jest to duża inicjatywa dla reporterów, aby pomóc w rozwiązaniu kwestii spornej na wyniki tymczasowe.

[16] Transakcje nie mogą być cofnietę gdy rynek zostanie zakwalifikowany jako Nieważny z powodów ograniczeń technicznych. Akcje są po prostu tokenami, które mogą być wymieniane bezpośrednio pomiędzy użytkownikami; zatem tokeny ETH i akcje nie są pod kontrolą Augura i nie mogą być zwrócone do pierwotnego właściciela w przypadku zakwalifikowania rynku jako Nieważny.

[17] Patrz Twierdzenie 3 w Aneksie A.

II. BODŹCE FINANSOWE I BEZPIECZEŃSTWO

Istnieje silny związek pomiędzy kapitalizacją rynkową tokenów REP i wiarygodnością protokołu rozwidlenia sieci Augura. Jeżeli kapitalizacja rynkowa jest odpowiednio duża, [18], i osoby przeprowadzające atak wiedzą, że nie jest to dla nich zyskowne, wtedy wynik, który wygra fork, powinien odpowiadać obiektywnej rzeczywistości. Tak naprawdę, to Augur mógłby funkcjonować właściwie bez wyznaczonych raportujących i serii rozwiązywania kwestii spornych. Używając *wyłącznie* procesu rozwidlenia sieci, wyrocznia raportowała by zgodnie z prawdą.

Jednakże, rozwidlenia są dystruktywne dla platformy i zajmują wiele czasu. Jest to spowodowane tym, że fork zajmuje do 60 dni rozwiązując spór dla pojedyńczego rynku, i może rozwiązać tylko jeden spór w danym czasie. Podczas 60 dni gdy rynek jest rozwidlany, wszystkie inne nie zakończone rynki zostają odłożone na później.[19] Dostawcy usług muszą również uaktualnić swoje serwisy, a posiadacze tokenów REP muszą migrować swoje tokeny REP do jednego z nowych uniwersów potomnych. Z tego względu fork powinien zajść tylko wtedy, gdy jest to całkowicie konieczne. Można to rozważać jako opcję równoznaczną z atakiem jądrowym.

Na szczęście, po tym jak zostało przyjęte, że fork może zostać użyty do określenia prawdy, można użyć nagrodę finansową aby zachęcić uczestników do uczciwego zachowania bez konieczności zainicjalizowania forka. *To wiarygodne zagrożenie z tego, co niesie fork oraz wiara w to, że fork zakończy się sukcesem stanowią kamień węgielny systemu nagród w Augurze.*

Następnie zostaną omówione warunki, dzięki którym można zaufać systemowi rozwidleń do ustalenia prawdy. Po tym zostanie omówiony system nagradzania oraz sposób w jaki zachęca on do szybkiego i prawidłowego ustalania wszystkich rynków.

A. Spójność Protokołu Rozwidlania (Fork)

Rozważamy w tym miejscu rzetelność przeprowadzania procesu rozwidlania i warunków pod którymi można mu zaufać. W celu ułatwienia dyskusji, gdy mówimy o forku, mamy na myśli uniwersum potomne, które odniosi się do obiektywnej rzeczywistości jako Prawdziwe uniwersum, a każde inne uniwersum potomne jako Fałszywe uniwersum. Będzimy określali uniwersum potomne które otrzymuje najwięcej tokenów REP podczas migracji w ciągu okresu forka jako wygrywające uniwersum, a wszystkie inne uniwersa potomne jako przegrywające uniwersa.

Oczywiście, zawsze chcemy aby Prawdziwe uniwersum było wygrywające, a Fałszywe uniwersa były przegrywa-

[18] Patrz Sekcja II A aby uzyskać szczegóły.

[19] Handlujący mogą w dalszym ciągu uczestniczyć w wymianie, ale rynki nie mogą zostać sfinalizowane do zakończenia forka.

jące. Mówimy, że protokół rozwidlenia został skutecznie zaatakowany, kiedykolwiek Fałszywe uniwersum staje się wygrywającym uniwersum danego forka – w związku z tym kończy się rozwidlonym rynkiem (i potencjalnie także wszystkimi nie zakończonymi rynkami) które zostają nieprawidłowo wypłacone.

Nasze podejście do zabezpieczenia wyroczni jest osiągnięte przez organizację systemu w ten sposób, aby największa korzyść, którą może osiągnąć atakujący była mniejsza niż minimalny koszt przeprowadzenia ataku. Nadajemy temu formalny charakter poniżej.

1. Największa Korzyść dla Atakującego Wyrocznię

Atakujący, który skutecznie zaatakuje wyrocznię spowodowałby migrację wszystkich niezakończonych rynków do Fałszywego uniwersum. Jeżeli atakujący kontroluje większość tokenów REP w Fałszywym uniwersum, może wymusić zakończenie wszystkich niesfinalizowanych rynków na dowolny wynik. W najbardziej ekstremalnym przypadku, mogłby także przechwycić wszystkie fundusze przechowywane w depozytach tych wszystkich rynków.[20]

Definicja 1. Definiujemy i oznaczamy przez I_a, *liczbę otwartych pozycji* Augura jako sumę wszystkich depozytów przechowywanych w niezakończonych rynkach Augura.[21]

Definicja 2. Definiujemy *rynek pasożytniczy* jako jakikolwiek rynek, który nie płaci opłat reporterów Augurowi, ale kończy się zgodnie z wynikiem natywnego rynku Augura.

Definicja 3. Definiujemy i oznaczamy przez I_p, *pasożytniczą liczbę otwartch pozycji* jako sumę wszystkich depozytów przechowywanych we wszystkich rynkach pasożytniczych, których wynik jest zgodny z niesfinalizowanymi, natywnymi rynkami Augura.

W najbardziej ekstremalnym przypadku, atakujący byłby zdolny przechwycić wszystkie fundusze we wszystkich rynkach pasożytniczych, które zakończą się zgodnie z niesfinalizowanymi natywnymi rynkami Augura.

Obserwacja 1. Maksymalny zysk (całkowity) dla atakującego, który skutecznie przeprowadzi atak wynosi $I_a + I_p$.

2. Pasożytnicza Liczba Otwartych Pozycji jest Niepoznawalna

Augur może dokładnie i efektywnie mierzyć I_a. Jednakże, I_p nie może być ogólnie znana, ponieważ może istnieć dowolnie wiele autonomicznych rynków pasożytniczych, każdy z dowolnie dużą liczbą otwartych pozycji. Ponieważ maksymalny możliwy zysk dla atakującego zawiera niemożliwą do poznania wartość I_p, nie można być nigdy obiektywnie pewnym, że wyrocznia jest zabezpieczona przez atakującymi racjonalnymi ekonomicznie.

Jednakże, jeżeli jesteśmy zgodni stwierdzić, że I_p jest w praktyce racjonalnie ograniczone, możemy zdefiniować warunki, pod którymmi może stwierdzić, że wyrocznia jest zabezpieczona.

3. Minimalny Koszt Skutecznego Ataku

Następnie rozważmy koszt ataku na wyrocznię. Niech P oznacza cenę tokenów REP. Niech ϵ oznacza jeden attorep[22]. Niech M oznacza całkowitą sumą wszystkich istniejących tokenów REP ("podaż pieniądza" w REP). Niech S oznacza odsetek M który będzie zmigrowany do Prawdziwego uniwersum w trakcie przeprowadzania procesu forkowania.

Zatem iloczyn SM reprezentuje całkowitą liczbę tokenów REP zmigrowanych do Prawdziwego uniwersum w trakcie przeprowadzania forkowania, a iloczyn PM jest kapitalizacją rynkową tokenów REP.

Niech P_f oznacza cenę REP zmigrowanych do Fałszywego uniwersum wybranego przez atakującego. Zauważmy, że jeżeli $P \leqslant P_f$ wtedy wyrocznia nie byłaby bezpieczna przed atakującymi racjonalnymi ekonomicznie, ponieważ byłoby przynajmniej tak opłacalna migracja REP do Fałszywego uniwersum, jak nie migrowanie wcale.

4. Spójność

Assumption 1. *Reporterzy, którzy nie są atakującymi nigdy nie zmigrują tokenów REP do* Fałszywego *uniwersum podczas przeprowadzania forka.*[23]

Zgodnie z zamysłem, skuteczny atak na wyrocznię wymaga więcej tokenów REP zmigrowanych do pewnego Fałszywego uniwersum niż do Prawdziwego uniwersum podczas przeprowadzania procesu rozwidlenia. Załóżmy, że tylko atakujący zmigruje swoje tokeny REP do Fałszywego uniwersum. Suma tokenów REP zmigrowanych do Prawdziwego uniwersum podczas okresu raportowania jest oznaczona SM. Zatem, aby atakujący odniósł sukces, musi zmigrować przynajmniej $SM + \epsilon$ REP. Upraszczając, zignorujmy pomijalne ϵ, i można stwierdzić, że skuteczny atak wymaga zmigrowania co najmniej SM

[20] Wymagałoby to, aby atakujący przechwycił *wszystkie* akcje danego wyniku i następnie zmusił rynek, aby zakończył sie na dany wynik.

[21] Włączając w to zewnętrzne rynki, które płacą opłaty reporterów Augurowi.

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

[23] Mogą być przypadki, w których nieświadomi reporterzy przypadkowo lub lekkomyślnie migrują swoje tokeny REP do Fałszywego uniwersum. Jednakże, takie zachowanie jest w praktyce niemożliwe do rozróżnienia od współpracy z atakującym.

REP, które posiada wartość SMP przed migracją do pewnego Fałszywego uniwersum.

Jeżeli atakujący zmigruje SM REP podczas okresu raportowania forka, otrzyma SM REP w uniwersum potomnym do którego zmigruje tokeny.[24] Jeżeli atakujący zmigruje do Fałszywego uniwersum wtedy wartość tych tokenów staje się SMP_f. Zatem minimalny koszt dla atakującego wynosi $(P - P_f)SM$.

Obserwacja 2. Minimalna liczba REP, którą skuteczny atakujący musi zmigrować do Fałszywego uniwersum podczas forka wynosi SM, które kosztuje go $(P-P_f)SM$.

Zauważmy, że jeżeli $S > \frac{1}{2}$ wtedy atak jest *niemożliwy* ponieważ nie istnieje wystarczająco wiele REP poza Prawdziwym uniwersum dla przekształcenia dowolnego Fałszywego do wygrywającego uniwersum.

Konkurując z ekonomicznie racjonalnymi atakującymi, wyrocznia zostanie zdeterminowana na wyniki, które odnoszą się do obiektywnej rzeczywistości, jeżeli maksymalny zysk dla atakującego jest mniejszy, niż minimalny koszt przeprowadzenia ataku. Przez obserwacje 1 & 2 możemy stwierdzić, że taka sytuacja pojawia się, gdy $S > \frac{1}{2}$ lub $I_a + I_p < (P - P_f)SM$. Daje to nam formalną definicję spójności sieci.

Definicja 4. (Własność Spójności) Protokół rozwidlania jest *spójny* kiedykolwiek $S > \frac{1}{2}$ lub kiedykolwiek $I_a+I_p < (P - P_f)SM$.

Powyższa nierówność może być rozwiązana dla dowolnego PM aby obliczyć zależność między spójnością protokołu forkowania a kapitalizacją rynkową REP.

Twierdzenie 1. *(Twierdzenie o Bezpieczeństwie Kapitalizacji Rynkowej) Protokół rozwidlenia jest spójny wtedy i tylko wtedy, gdy:*

1. $S > \frac{1}{2}$, *lub*
2. $P_f < P$ *i kapitalizacja rynkowa REP jest większa niż* $\frac{(I_a+I_p)P}{(P-P_f)S}$.

Proof. Zakładając, że protokół rozwidlenia jest spójny, wtedy, przez definicję, $S > \frac{1}{2}$ lub $I_a + I_p < (P - P_f)SM$. Zakładając $I_a + I_p < (P - P_f)SM$. Ponieważ $I_a + I_p \geqslant 0$ i $SM > 0$, wiadomo, że $P_f < P$. Nastepnie, rozwiązując $I_a + I_p < (P - P_f)SM$ względem PM, widać, że $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Zatem pierwszy cel jest udowodniony.

Teraz zakładając $S > \frac{1}{2}$, lub, że $P_f < P$ oraz $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Jeżeli $S > \frac{1}{2}$, wtedy protokół rozwidlenia przez definicję jest spójny. Jeżeli $P_f < P$ oraz $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$, wtedy, rozwiązując nierówność względem $I_a + I_p$, widać, że $I_a + I_p < (P - P_f)SM$, i protokół rozwidlenia jest spójny. □

[24] W praktyce, atakujący otrzymałby $1.05SM$ REP w jednym z uniwersów potomnych z powodu 5% premii za migrację w ciągu 60 dni od startu forka. Ignorujemy 5% premię aby ułatwić dalsze rozważania. Aby uzyskać dalsze szegóły na temat 5% premii, patrz Aneks **??**.

B. Nasze Założenia i Ich Konsekwencje

Wierzymy, że handlujący nie będą chcieli handlować na platormie Augur w świecie, w którym raportujący kłamali. Wierzymy także, że tworzący rynek nie zapłacą za tworzenie rynków Augurs w świecie, w którym nie ma handlujących. W świecie, w którym nie ma rynków ani handlu, REP nie dostarcza żadnej dywidendy dla posiadaczy tokenów. Zatem, wierzymy, że tokeny REP wysłane do Fałszywego uniwersum będą miały pomijalnie małą wartość rynkową i modelujemy to przez $P_f = 0$.

Uważamy, że jest racjonalne oczekiwać na to, że przynajmniej 20% istniejących REP zostanie zmigrowanych do Prawdziwego wyniku podczas okresu raportowania w procesie rozwidlania i modelujemy to przez oznaczenie $S \geqslant \frac{1}{5}$. Jesteśmy również skłonni przyznać, że pasożytnicza liczba otwartych pozycji jest na poziomie 50% natywnej liczby otwartych pozycji, co oznaczamy $I_a \geqslant 2I_p$.

Biorąc pod uwagę powyższe założenia, Twierdzenie 1 mówi, że protokół rozwidlenia jest spójny kiedykolwiek kapitalizacja rynkowa REP jest równa przynajmniej 7.5 raza liczbie otwartych pozycji.[25]

C. Kierunek Kapitalizacji Rynkowej

Augur otrzymuje informację o cenie REP w ten sam sposób, co jakąkolwiek inną informacją o rzeczywistym świecie: za pomocą rynku Augura. Daje to Augurowi możliwość obliczenia aktualnej kapitalizacji rynkowej tokenów REP. Augur może także mierzyć bieżącą liczbę otwartych pozycji i dzięki temu określić jak wielka kapitalizacja rynkowa jest konieczna do spełnienia wymagań dotyczących spójności protokołu.

Każde uniwersum startuje z domyślną opłatą raportujących na poziomie 1%. Jeżeli bieżąca kapitalizacja rynkowa jest poniżej wymaganego poziomu, wtedy opłaty raportujących zostają automatycznie podniesione (ale nigdy nie będą większe niż 33.3%), co powoduje presję wzrostową na cenę tokenów REP i/lub presję spadkową na nową liczbę otwartych pozycji. Jeżeli bieżąca kapitalizacja rynkowa jest powyżej wymaganego poziomu, opłaty raportujące są automatycznie zmniejszane (ale nigdy nie będą niższe niż 0.01%) tak, aby handlujący nie musieli płacić więcej niż trzeba za utrzymanie bezpiecznego systemu.

Opłaty raportujące są określane następująco. Niech r oznacza opłatę raportującą z poprzedniego okna raportowania, niech t oznacza wymaganą kapitalizację rynkową, i niech c oznacza bieżącą kapitalizację rynkową. Wtedy opłata raportująca w bieżącym oknie opłat wynosi $\max\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10,000}\right\}$.

[25] Patrz Aneks B aby poznać szczegóły alternatywnych założeń i i ich konsekwencji.

D. Korzystanie z Zagrożenia Rozwidleniem (Forka)

Jak stwierdzono powyżej, forki są destruktywne i spowalniają sfinalizowanie otwartych rynków. Zamiast używać rozwidlenia aby rozwiązać wynik każdego rynku, Augur korzysta z *zagrożenia* jakie niesie fork, aby efektywnie rozwiązywać rynki.

Przypomnijmy, że każda liczba tokenów postawiona na rozwiązanie konfliktu na rzecz finalnego wyniku otrzyma 50% ROI od liczby tokenów postawionej na wynik.[26] W przypadku zajścia rozwidlenia, jakiekolwiej REP postawione na fałszywe wyniki rynkowe powinny stracić całą wartość, a jakiekolwiek tokeny REP postawione na prawdziwy wynik są wynagradzane 50% więcej tokenów REP w uniwersum potomnym, które odpowiada prawdziwemu wynikowi (niezależnie od wyniku rozwidlenia). Z tego względu, jeżeli fork zostanie wymuszony, posiadacze tokenów REP którzy pomogą rozwiązać kwestię sporną na korzyść prawdziwych wyników będą zawsze wychodzili na plus, natomiast posiadacze tokenów, którzy postawią na fałszywy wynik stracą wartość swoich tokenów REP.

Wierzymy, że ta sytuacja jest wystarczająca, aby zagwarantować że wszystkie fałszywe potencjalne wyniki będa skutecznie rozwiązane.

III. POTENCJALNE PROBLEMY & RYZYKA

A. Rynki Pasożytnicze

Przypomnijmy, że rynkiem pasożytczniczym określamy dowolny rynek, który nie płaci opłat raportujących Augurowi, ale ma ten sam wynik, co natywny rynek Augura. Ponieważ rynki pasożytczne nie muszą płacić raportującym, mogą oferować te same usługi, co Augur, oferując mniejsze opłaty. Może to mieć poważne konsekwencja dla protokołu rozwidlania Augura.

W szczególności, jeżeli rynki pasożytniczne przyciągną zainteresowanie z dala od Augura, wtedy raportujący Augura otrzymają mniejsze wynagrodzenie z opłat raportujących. Spowodowałoby to presję spadkową na kapitalizację rynkową tokenów REP. Jeżeli kapitalizacja rynkowa REP spadnie zbyt nisko, spójność protokołu rozwidlenia zostaje wystawiona na niebezpieczeństwo (Twierdzenie 1). Wynikiem tego, rynki pasożytnicze mają potencjał, aby w dłuższej perpektywie zagrozić rentowności Augura i powinny być przedmiotem gorącego sprzeciwu.

Naszym najlepszym punktem obrony przed rynkami pasożytniczymi jest sprawienie, aby handel na platormie Augura był tak tani, jak to tylko możliwe (w dalszym ciągu utrzymując spójność wyroczni), aby zminimalizować zysk za uruchomienie rynku pasożytniczego.

B. Zmienność Liczby Otwartych Pozycji

Duży, nagły i nieoczekiwany wzrost liczy otwartych pozycji – przykładowo taki, który może być zaobserwowany podczas popularnego wydarzenia sportowego – skutkuje nagłym wzrostem wymaganej kapitalizacji rynkowej aby zachować spójność protokołu rozwidlania (Twierdzenie 1). Gdy wymagana minimalna kapitalizacja rynkowa przekracza wartość bieżącej kapitalizacji rynkowej, istnieje prawdopodobieństwo, że racjonalnie ekonomiczni atakujący spowodują zły wynik rozwidlenia. Pomimo tego, że Augur w takich sytuacjach próbuje podnieść kapitalizację rynkową przez interwencję na rynku (patrz Sekcja II C), wpływ na kapitalizację jest wyłącznie tymczasowy i dopasowywana raz na 7 dniowe okno opłat.

Warto jednakże zauważyć, że spekulanci, którzy będą świadkiem nagłego wzrostu liczby otwartych pozycji mogą kupować tokeny REP oczekując na interwencję kursu REP, i w związku z tym podnosząc kapitalizację rynkową REP, możliwie nawet do momentu, w którym spójność protokołu fork nie jest już zagrożona. Z tego względu okres czasu, w którym wyrocznia jest podatna na atak może nie być na tyle długi, żeby atakujący mogli skutecznie wykorzystać tą lukę.

C. Niespójne lub Celowo Złe Źródła Wyników

Podczas tworzenia rynków, twórcy rynku wybierają źródło wyniku, które powinno zostać użyte przez reporterów do zaraportowania wyniku zdarzenia, na którym opiera się handel. Jeżeli twórca rynku wybierze niespójne, lub celowo złe źródło wyniku, uczciwi reporterzy mogą stracić pieniądze.

Na przykład, weźmy pod uwagę rynek, który ma możliwe wyniki A i B, oraz twórca rynku, Serena, wybrała własny serwis internetowy, attacker.com, jako źródło wyniku. Po zajściu zdarzenia, na którym opierał się handel, Serena – która jest również wyznaczonym reporterem dla danego rynku – raportuje wynik A, i uaktualnia serwis attacker.com aby wzkazywał, że prawidłowy wynik to B. Uczciwi reporterzy, którzy sprawdzą serwis attacker.com zobaczą, że raport początkowy jest prawidłowy i podczas pierwszej serii rozwiązywania kwestii spornej dotyczącej wyniku, powinni skutecznie zatwierdzić niepewny wynik na korzyść wyniku B. Serena wtedy mogłaby uaktualnić serwis attacker.com aby wskazał, że to wynik A jest prawidłowym wynikiem, i rynek wkroczyłby w drugą serię rozwiązywania sporu. Ponownie, raportujący, którzy sprawdziliby serwis attacker.com zobaczyliby, że niepewny wynik (wynik B) jest nieprawidłowy i mogliby go skutecznie wskazać. Serena może powtarzać to w kółko do momentu ustalenia wyniku przez rynek. W tym przypadku niezależnie

[26] Mierzonej w tokenach REP które istnieją w uniwersum, które odpowiada finalnemu wynikowi rynku; patrz Twierdzenie 3 w Aneksie A.

jak rynek się ustali, niektórzy uczciwi reporterzy stracą pieniądze.

Istnieje kilka odmian tego typu ataku. Proste ignorowanie rynków z podejrzanymi źródłami wyniku nie jest wystarczające, ponieważ gdyby taki rynek wymusiłby rozwidlenie, wszyscy posiadacze tokenów REP musieliby wybrać uniwersum potomne, do którego mają migrować swoje tokeny. Raportujący powinni być czujni i bacznie obserwować rynki z podejrzanymi źródłami wyniku. Takie rynki powinny być zdentyfikowane publicznie, tak aby raportujący mogli skoordynować swoje działania i sprawić, aby taki rynek był sfinalizowany jako nieważny.

D. Zapytania Zwrotne do Wyroczni

Rynki, których handel bazuje na przyszłym zachowaniu wyroczni Augura może mieć niepożądany efekt na samej wyroczni [11]. Na przykład, weźmy pod uwagę rynek, który jest oparty na zapytaniu "Czy jakikolwiek wyznaczony raportujący nie przedstawi raportu podczas swojego 3-dniowego okresu raportowania przed 31 grudnia 2018?" Zakłady postawione na wynik Nie takiego rynku, mogą stanowić przewrotną inicjatywę dla wyznaczonych reporterów, aby celowo nie przedstawili swojego raportu. Jeżeli wyznaczony raportujący może kupić wystarczająco dużą część akcji na Tak w cenie wystarczająco niskiej na shares at a low enough price to wynagrodzenie straty obligacji no-show, mogliby celowo nie przedstawić swojego raportu, aby zarobić na tym pieniądze.

Jeżeli kapitalizacja rynkowa tokenów REP jest wystarczająco duża (Twierdzenie 1) wtedy te zapytania zwrotne do wyroczni nie zagroziłyby spójności protokołu rozwidlenia. Jednakże, mogą mieć negatywny wpływ na wydajność platformy Augura przez powodowanie opóźnień w finalizacji rynków. Pomimo tego, że rynki nadal finalizowałyby się prawidłowo, takie zachowanie jest destruktywne i niepożądane.

E. Niepewne Uczestnictwo w Forku

Nie możemy wiedzieć z góry, jaka liczba tokenów REP zostanie zmigrowana do Prawdziwego uniwersum podczas okresu forka i z tego względu nie wiemy z góry czy kapitalizacja rynkowa jest wystarczająco duża, aby wyrocznia zachowała spójność (Twierdzenie 1). Nasza wiara w spójność protokołu forkowania nie może być silniejsza niż wiara w założenia o dolnym ograniczeniu uczciwych uczestników rozwidlenia. Zakładamy, że przynajmniej 20% wszystkich tokenów REP zmigruje do Prawdziwego uniwersum potomnego podczas okresu rozwidlania danego forka, ale nie możemy tego zagwarantować.

Forki Augura różnią się od forków blockchain w jednym szczególnym względzie: po forku blockchain, użytkownik, który był właścicielem tokenów przed forkiem, zostanie właścicielem nowych tokenów i zachowa również stare. Pomijając ataki metodą powtórzenia (replay attacks), forki blockchainów nie stwarzają dużego zagrożenia użytkownikom. Jednakże po forku Augura, użytkownik, który posiada tokeny REP w uniwersum źródłowym, może je zmigrować wyłącznie do jednego z uniwersów potomnych. W przypadku, gdy użytkownik zmigruje swoje tokeny do uniwersum niezgodnego z konsensusem, jego tokeny mogą całkowicie stracić wartość. W związku z tym, migrowanie tokenów REP w okresie forka, zanim jest jasne które uniwersum osiągnie konsensus, wystawia użytkownika na ryzyko. To ryzyko może zniechęcić do udziału w rozwidleniu w okresie rozwidlania w trakcie kontrowersyjnych forków.

Aby zrekompensować to ryzyko i zachęcić do udziału w forku podczas okresu rozwidlania, wszyscy posiadacze tokenów REP, którzy zmigrują swoje tokeny w ciągu 60 dni od rozpoczęcia rozwidlania otrzymają dodatkową 5% premię REP w uniwersum potomnym do którego zmigrują swoje tokeny (patrz Sekcja I C 9). Jednakże, nie możemy wiedzieć z góry, czy ta 5% premia będzie wystarczająca do zrekompensowania ryzyka i zachęcenia ludzi do uczestnictwa w procesie forka podczas okresu rozwidlania.

F. Dwuznaczne lub Subiektywne Rynki

Wyłącznie te zdarzenia, które mają obiektywne wyniki, mają zastosowanie w rynkach Augura. Jeżeli raportujący wierzą, że dany rynek nie jest odpowiedni, aby jego wynik miał być rozwiązany przez platformę – przykładowo, gdy jest dwuznaczny, subiektywny lub wynik nie ma ustalonej daty końcowej – powinni zaraportować taki rynek jako Nieważny. Jeżeli rynek zostanie rozwiązany jako Nieważny, handlującym wypłaca się równe części za wszystkie możliwe wyniki; dla rynków bazujących na skalarach, liczbach rzeczywistych, handlujący są wynagradzani połową kwoty między ceną minimalną, a maksymalną dla danego rynku.

Można sobie wyobrazić rynki, w których część raportujących jest pewna, że wynikiem jest A a pozostali są pewni, że wynikiem jest B. Przykładowo w 2006 roku serwis TradeSports pozwolił użytkownikom na spekulację, czy Korea Północna odpali pocisk balistyczny, który wyląduje poza ich przestrzenią powietrzną przed końcem lipca 2006 roku. Dnia 5 lipca 2006 roku Korea Północna skutecznie wystrzeliła pocisk balistyczny, który wylądował poza ich przestrzenią powietrzną, a wydarzenie to było szeroko raportowane przez światowe media i potwierdzone przez wiele źródeł rządowych U.S.A. Jednakże, Departament Obrony U.S.A. nie potwierdził tego wydarzenia, a było to wymagane przez kontrakt serwisu TradeSports. Serwis TradeSports wywnioskował, że warunki kontraktu nie zostały spełnione, i wypłacił

wynagrodzenia zgodnie z tą wersją.[27]

Jest to przypadek, w którym postawa rynku – aby przewidzieć wystrzelenie pocisku balistycznego – była wyraźnie spełniona, ale komunikat rynku – aby przewidzieć, czy Departament Obrony U.S.A. potwierdzić wystrzelenie – zostało niespełnione. Serwis TradeSports, który jest scentralizowanym serwisem, mógł jednostronnie określić wynik zdarzenia rynku. Jeżeli taka sytuacja zaistnieje w rynku Augura, posiadacze tokenów REP mogą mieć różne opinie co do tego, jak dany rynek powinien się rozwiązać i postawić na to swoje tokeny REP. W najgorszym przypadku, mogłoby to spowodować rozwidlenie, gdzie tokeny REP w więcej niż jednym uniwersum posiadałyby niezerową wartość rynkową.

ACKNOWLEDGMENTS

Dziękujemy następującym osobom: Abraham Othman, Alex Chapman, Serena Randolph, Tom Haile, George Hotz, Scott Bigelow, oraz Peronet Despeignes za ich pomocne sugestie i opinie.

[1] J. Wolfers and E. Zitzewitz. Prediction markets. *Journal of Economic Perspectives*, 18(2):107–126, 2004.

[2] James Surowiecki. *The Wisdom of Crowds*. Anchor, 2005.

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

[4] D.M. Pennock, S. Lawrence, C.L. Giles, and F.A. Nielsen. The real power of artificial markets. *Science*, 291:987–988, 2001.

[5] C. Manski. Interpreting the predictions of prediction markets. *NBER Working Paper No. 10359*, 2004.

[6] J. Wolfers and E. Zitzewitz. Interpreting prediction market prices as probabilities. *NBER Working Paper No. 10359*, 2005.

[7] S. Goel, D.M. Reeves, D.J. Watts, and D.M. Pennock. Prediction without markets. In *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, pages 357–366. ACM, 2010.

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

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

[10] J. Clark, J. Bonneau, E.W. Felten, J.A. Kroll, A. Miller, and A. Narayanan. On decentralizing prediction markets and order books. In *WEIS '14: Proceedings of the 10^{th} Workshop on the Economics of Information Security*, June 2014.

[11] A. Othman and T. Sandholm. Decision rules and decision markets. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: Volume 1 - Volume 1*, AAMAS '10, pages 625–632. International Foundation for Autonomous Agents and Multiagent Systems, 2010.

[12] J. Peterson and J. Krug. Augur: a decentralized, open-source platform for prediction markets. *arXiv:1501.01042v1 [cs.CR]*, 11 2014.

[27] Patrz https://en.wikipedia.org/wiki/Intrade#Disputes aby uzyskać więcej szczegółów.

Appendix A: Czas Finalizacji & Redystrybucja

Zaczynamy od oznaczeń, definicji i obserwacji.

Definicja 5. Dla danego rynku M, niech Ω_M oznacza zbiór wszystkich zdarzeń elementarnych (lub zbiór wyników) M.

Definicja 6. Dla $n \geqslant 1$ oraz $\omega \in \Omega_M$, niech $S(\omega, n)$ oznacza całkowitą sumę postawioną na wynik ω na początku rundy n rozwiązywania kwestii spornej. Wlicza się w to wszystkie kwoty ze wszystkich skutecznych rund spornych rozwiązanych na korzyść ω w ciagu wszystkich poprzednich rund rozwiązywania kwestii spornej.

Definicja 7. Dla $n \geqslant 1$ oraz $\omega \in \Omega_M$, niech $S(\overline{\omega}, n)$ oznacza sumę całkowitą postawioną na wszystkie wyniki w Ω_M *z wyjątkiem* ω na początku rundy n rozwiązywania kwestii spornej:

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

Definicja 8. Dla $n \geqslant 1$, niech A_n oznacza całkowitą sumę po wszystkich wynikach M postawioną na początku rundy n rozwiązywania kwestii spornej:

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

Obserwacja 3. Z tego wynika $A_n - S(\omega, n) = S(\overline{\omega}, n)$.

Definicja 9. Dla $n \geqslant 1$, niech $\hat{\omega}_n$ oznacza tymczasowy wynik na początku rundy n rozwiązywania kwestii spornej. Przykładowo, $\hat{\omega}_1$ jest wynikiem zaraportowanym przez pierwszego raportującego.

Definicja 10. Dla $n \geqslant 1$ oraz $\omega \neq \hat{\omega}_n$, niech $B(\omega, n)$ oznacza wymaganą sumę postawioną na wydarzenie, aby skutecznie wykupić obligację sporną na korzyść wyniku ω podczas rundy spornej n.

Przypomnijmy, że wymagana suma potrzebna do wykupienia obligacji spornej na korzyść wyniku ω podczas rundy n rozwiązywania kwestii spornej, gdzie $\omega \neq \hat{\omega}_n$ jest dane przez równanie 1, $B(\omega, n) = 2A_n - 3S(\omega, n)$.

Obserwacja 4. Jeżeli obligacja sporna jest skutecznie wykupiona na korzyść wyniku ω podczas rundy n rozwiązywania kwestii spornej, wtedy $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. Oznacza to, że część postawiona na rozwiązanie sporu jest jedyną nową częścią zaaplikowaną do wyniku ω na końcu rundy spornej n.

Obserwacja 5. Dla wszystkich $\omega \neq \hat{\omega}_n, S(\omega, n-1) = S(\omega, n)$. Oznacza to, że jeżeli obligacja sporna nie zostanie całkowicie wypełniona na korzyść wyniku ω, wtedy nie jest konieczna żadna dodatkowa stawka do wyniku ω na początku kolejnej rundy rozwiązywania kwestii spornej. Jest to spowodowane tym, że wszystkie nieskuteczne stawki sporne są zwracane użytkownikom na końcu rundy spornej.

Obserwacja 6. Dla wszystkich $n \geqslant 2, A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$. Oznacza to, że całkowita stawka we wszystkich wynikach na początku rundy rozwiązywania kwestii spornej jest po prostu całkowitą stawką z początku poprzedniej rundy spornej plus stawka skutecznego rozwiązania spornu z poprzedniej rundy rozwiązywania kwestii spornej. Wszystkie pozostałe stawki są zwracane użytkownikom na końcu poprzedniej rundy spornej.

Lemat 2. *$S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$, dla $n \geqslant 2$.*

Proof. Przyjmijmy, że rynek wkracza w rundę n dysputy, gdzie $n \geqslant 2$. Podczas rundy $n-1$ dysputy, wynik $\hat{\omega}_{n-1}$ musiał zostać skutecznie rozwiązany na korzyść wyniku $\hat{\omega}_n$. Zgodnie z równaniem 1, rozmiar tej obligacji spornej wynosi $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Wykorzystując obserwację 3, można to przedstawić jako

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

Wiemy, że obligacja sporna została skutecznie wykupiona w trakcie rundy $n-1$. Przez obserwację4, widzimy, że $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. Obserwacja 5 mówi nam, że całkowity rozmiar stawki postawionej na $\overline{\hat{\omega}_n}$ nie zmienia się między rundami $n-1$ a n, $2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$. W związku z tym, równanie A1 zostaje uproszczone do $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$. □

Twierdzenie 3. *Każdy posiadacz tokenów REP skutecznie rozwiązujący spór na korzyść finalnego wyniku rynkowego otrzyma 50% ROI na swoją stawkę sporną (mierzoną w tokenach REP, które istnieją w uniwersum, któremu odpowiada finalny wynik rynkowy), chyba że rynek zostanie przerwany przez inny rynek, który spowoduje fork.*

Proof. Podczas rozwidlenia, wszyscy użytkownicy, którzy skutecznie wykupili obligację sporną na korzyść finalnego wyniku rozwidlającego się rynku otrzymują (przez tokeny wykopane podczas forka) 50% zwrot na swoją stawkę sporną gdy zmigrują swoje tokeny do odpowiedniego uniwersum potomnego. Z tego względu, w przypadku gdy rynek poddany w wątpliwość spowoduje rozwidlenie, twierdzenie jest automatycznie prawdziwe.

Teraz rozważmy przypadek, gdzie rynek poddany w wątpliwość zostaje rozwiązany bez zainicjalizowania forka, a raportowanie nie jest przerwane przez inny rynek powodujący rozwidlenie.

Oznaczmy finalny wynik rynku przez ω_{Final} i załóżmy, że rynek zostanie rozwiązany na końcu rundy n dysputy, gdzie $n \geqslant 2$. Oznacza to, że tymczasowy wynik dla rundy n wynosi ω_{Final}, i że ten wynik nie jest skutecznie rozwiązany podczas rundy n. Innymi słowy: $\hat{\omega}_n = \omega_{\text{Final}}$. Wtedy przez Lemat 2 wiadomo, że $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$.

Ponieważ rynek zostaje rozwiązany na końcu rundy n bez dalszych stawek dodawanych do któregokolwiek wyniku, powyższe równanie pokazuje końcową sumę stawki na finalny wynik rynku, ω_{Final}, i sumę wszystkich stawek na wszystkich innych wynikach rynkowych,

$\overline{\omega_{\text{Final}}}$. Zauważmy, że istnieje dokładnie dwa razy więcej stawek na finalny wyniku rynku niż na wszystkie pozostałe wyniki razem wzięte.

Augur redystrybuuje wszystkie stawki na niefinalne wyniki użytkownikom, którzy postawili na ω_{Final}, proporcjonalnie do liczby tokenów REP, które postawili. Z tego względu użytkownicy, którzy skutecznie wypełnili obligację sporną na korzyść ω_{Final} otrzymują 50% ROI za swoją stawkę REP. □

Następnie rozważmy maksymalną liczbę rund rozwiązywania kwestii spornej potrzebnej do rozwiązania rynku. Równanie 1 może zostać uproszczone gdy ω jest wybrane tak, aby być pewnym wynikiem który rozpoczyna rundę dysputy z największą możliwą stawką. Lemat 2 implikuje, że pewny wynik z największą możliwą stawką jest równy stawce niepewnego wyniku z poprzedniej rundy. Z tego względu, kwota najmniejszej możliwej obligacji spornej, która może być skutecznie wykupiona podczas rundy spornej n, gdzie $n \geqslant 2$, wynosi $B(\hat{\omega}_{n-1}, n)$.

Innymi słowy, kwota obligacji spornej wzrasta *najwolniej* gdy dwa takie same wyniki są wielokrotnie rozwiązywane na korzyść jednego z nich. Również kolejno liczba rund dysput wymaganych przez rynek do zainicjalizowania forka jest *zmaksymalizowana* jeżeli dwa takie same wyniki są wielokrotnie rozwiązywane na korzyść jednego z nich. Z tego względu można określić największą liczbę rund rozwiązywania kwestii spornej, którą jakikolwiek rynek może przejść przed zainicjalizowaniem forka, przez znalezienie maksymalnej liczby rund dysput, które mogą się pojawić w danym szczególnym przypadku, gdzie dwa te same wyniki są wielokrotnie rozwiązywane na korzyść jednego z nich. Zbadamy dokładnie ten przypadek poniżej.

Załóżmy, że każda skuteczna obligacja sporna jest wykupiona na korzyść poprzedniego niepewnego wyniku z poprzedniej rundy. Wtedy, dwa niepewne wyniki, które są na przemian rozwiązywane na korzyść jednego z nich to $\hat{\omega}_1$ oraz $\hat{\omega}_2$.

Obserwacja 7. W przypadku, gdzie te same dwa niepewne wyniki są na przemian rozwiązywane na korzyść jednego z nich, $\hat{\omega}_n = \hat{\omega}_{n-2}$ dla wszystkich $n \geqslant 3$.

Definicja 11. Niech d oznacza sumę stawki umieszczonej na $\hat{\omega}_1$ podczas początkowego raportu. Ponieważ niepewny wynik dla każdej rundy w takiej sytuacji jest znany, możemy uprościć oznaczenie kwot obligacji spornych. Zdefiniujmy skrót B_n aby oznaczyć kwotę obligacji wymaganej dla rundy n, takiej, że $B_1 = 2d$ oraz $B_n = B(\hat{\omega}_{n-1}, n)$ dla wszystkich $n \geqslant 2$. Ułatwi to czytanie i zrozumienie kolejnych twierdzeń.

Obserwacja 8. W przypadku, gdzie dwa takie same niepewne wyniki są na przemian rozwiązywane na korzyść jednego z nich, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ dla $n \geqslant 3$. (Oznacza to, że każda kolejna obligacja sporna jest dodawana do tego samego wyniku.)

Lemat 4. *Jeżeli dwa takie same niepewne wyniki są na przemian rozwiązywane na korzyść jednego z nich, wtedy dla wszystkich n gdzie $n \geqslant 3$:*

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

Proof. (Przez indukcję na n)

Załóżmy, że dwa takie same niepewne wyniki są na przemian rozwiązywane na korzyść jednego z nich.

(Wariant podstawowy) Przez definicję i równanie 1 przeprowadzamy następujące obserwacje.

- $S(\hat{\omega}_1, 1) = d$, $S(\hat{\omega}_2, 1) = 0$, $A_1 = d$, 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 $B_3 = 6d$

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, zatem część 1 lematu jest spełniona dla $n = 3$.

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, zatem część 2 lematu jest spełniona dla $n = 3$.

$B_3 = 6d = 3d2^{3-2}$, zatem część 3 lematu jest spełniona dla $n = 3$.

Zatem lemat, w całości, jest spełniony dla wariantu podstawowego $n = 3$.

(Indukcja) Załóżmy, że lemat jest prawdziwy dla wszystkich n takich, że $3 \leqslant n \leqslant k$. Chcemy udowodnić, że lemat jest spełniony dla $n = k+1$. Oznacza to, że chcemy pokazać, że:

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

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

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

Po pierwsze, udowadniamy część (a). Przez obserwację 8:

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

Przez obserwację 7 można przepisać powyższe jako:

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

Przyjmując hipotezę indukcyjną, można przyjąć $S(\hat{\omega}_{k-2}, k-1)$ jako $\frac{2}{3}B_{k-2}$ po prawej stronie, aby otrzymać:

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

Przyjmując hipotezę indukcyjną, można napisać B_{k-2} jako $3d2^{k-4}$ oraz B_{k-1} jako $3d2^{k-3}$:

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

Stosując obserwację 7 do lewej strony równania otrzymujemy:

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

Ostatecznie, zauważamy że za pomocą powyższego równanie i hipotezy indukcyjnej, $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. To udowadnia (a).

Następnie udowadniamy (b). Przez obserwację 6:

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

Przyjmując hipotezę indukcyjną, $A_k = 2B_{k-1}$:

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

Przyjmując hipotezę indukcyjną, $B_{k-1} = 3d2^{k-3}$, tak, że prawa strona równania może zostać uproszczona do

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

Przyjmując hipotezę indukcyjną, $B_k = 3d2^{k-2}$ można przepisać prawą stronę równania jako

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

co udowadnia część (b).

Ostatecznie, udowadniamy część (c). Korzystając z równania 1:

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

Przez obserwację 8, możemy napisać $S(\hat{\omega}_k, k+1)$ jako $S(\hat{\omega}_k, k-1) + B_{k-1}$:

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

Przez obserwację 7, $\hat{\omega}_k = \hat{\omega}_{k-2}$:

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

Przez obserwację 6, $A_{k+1} = A_k + B_k$:

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

Przyjmując hipotezę indukcyjną, $A_k = 2B_{k-1}$ oraz $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$:

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

Przyjmując hipotezę indukcyjną, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ oraz $B_{k-2} = 3d2^{k-4}$. Podstawiając te równania i upraszczając otrzymujemy:

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

To udowadnia część (c), i konkluduje dowód lematu. □

Twierdzenie 5. *Dany rynek może przejść co najwyżej 20 rund dysput zanim zostanie sfinalizowany lub spowoduje fork, jeżeli nie jest przerwany przez inny rynek, który spowoduje rozwidlenie.*

Proof. Załóżmy, że dany rynek nie jest przerwany przez inny rynek, który spowoduje fork. Wtedy, jak pokazano powyżej, wiemy, że liczba rund rozwiązywania kwestii spornej wymaganej do rozwiązania rynku jest zmaksymalizowana gdy dwa takie same wyniki są wielokrotnie rozstrzygane na korzyść jednego z nich. Część 3 Lematu 4 mówi nam, że w takiej sytuacji, rozmiar obligacji spornej wymaganej do skutecznego rozwiązania niepewnego rynku podczas rundy n wynosi $3d2^{n-2}$, gdzie d jest sumą stawki postawionej podczas raportu początkowego.

Wiemy, że forki są inicjalizowane po skutecznym wykupieniu obligacji spornej w kwocie równej przynajmniej 2.5% wszystkich istniejących tokenów REP, i wiemy że istnieje obecnie 11 milionów tokenów REP. Z tego względu fork zostaje zainicjalizowany, gdy obligacja sporna w kwocie 275,000 REP zostaje wykupiona. Wiemy także, że $d \geqslant 0.35$ REP, ponieważ minimalna stawka raportu początkowego wynosi 0.35 REP[28].

Rozwiązując $3(0.35)2^{n-2} > 275,000$ dla $n \in \mathbb{Z}$ daje $n \geqslant 20$. Z tego względu możemy zagwarantować, że rynek zostanie rozwiązany lub spowoduje fork po co najwyżej 20 rundach rozwiązywania kwestii spornej. □

Appendix B: Alternatywne Założenia & Konsekwencje

Przypomnijmy, że:

- S jest odsetkiem wszystkich tokenów REP które zostały zmigrowane do Prawdziwego uniwersum podczas okresu rozwidlania
- P jest ceną tokenów REP w Prawdziwym uniwersum
- P_f jest ceną tokenów REP które zostały zmigrowane do Fałszywego uniwersum wybranego przez atakującego
- I_a jest natywną liczbą otwartych pozycji Augura
- I_p jest pasożytniczą liczbą otwartych pozycji

Augur stawia pewne założenia o S, P_f, oraz I_p aby utrzymać się w docelowej kapitalizacji rynkowej. W szczególności, Augur zakłada, że przynajmniej 20% wszystkich tokenów REP zostanie zmigrowanych do Prawdziwego uniwersum w trakcie okresu rozwidlania, tokeny REP zmigrowane do Fałszywego uniwersum będą miały zaniedbywalną wartość, a pasożytnicza liczba otwartych pozycji będzie równa co najwyżej połowie natywnej liczbie otwartych pozycji. Ujmując inaczej: $S \geqslant 0.2$, $P_f = 0$, oraz $I_a \geqslant 2I_p$. Korzystając z powyższych założeń, Twierdzenie 1 mówi nam, że protokół rozwidlania

[28] Patrz aneksy E 2 i E 3

zachowuje spójność tak długo jak kapitalizacja rynkowa tokenów REP jest większa niż liczba otwartych pozycji razy 7.5.

Można stworzyć własne założenia dotyczące S, P_f, oraz I_p i dojść do swoich konkluzji jak duża musi być kapitalizacja rynkowa, aby w praktyce wyrocznia zachowała spójność. Dla ułatwienia przedstawiamy poniżej kilka alternatywnych scenariuszy.

Scenariusz 1. Więcej niż 50% wszystkich istniejących tokenów REP migruje do Prawdziwego uniwersum podczas okresu rozwidlenia. W tym przypadku P_f oraz I_p nie mają żadnego znaczenia. Ponieważ $S > \frac{1}{2}$, protokół rozwidlenia gwarantuje spójność niezależnie od kapitalizacji rynkowej sieci. Nie istnieje wystarczająco wiele pozostałych tokenów REP na rynku, aby atakujący odniósł sukces.

Scenariusz 2. 48% wszystkich istniejących tokenów REP migruje do Prawdziwego uniwersum podczas okresu rozwidlenia, nie istnieje żaden rynek pasożytniczy, oraz tokeny REP wysłane do Fałszywego uniwersum nie mają żadnej wartości. W takim przypadku $S = 0.48$, $I_p = 0$, oraz $P_f = 0$. Zgodnie z powyższymi założeniami, kapitalizacja rynkowa REP musi być większa niż około dwukrotność wartości liczby otwartych pozycji aby protokół rozwidlania zachował spójność.

Scenariusz 3. 20% wszystkich istniejących tokenów REP migruje do Prawdziwego uniwersum podczas okresu rozwidlenia, pasożytnicza liczba otwartych pozycji jest równa natywnej liczbie otwartych pozycji, oraz tokeny REP zmigrowane do Fałszywego uniwersum mają wartość 5% wartości tokenów REP zmigrowanych do Prawdziwego uniwersum. W takim przypadku $S = 0.2$, $I_p = I_a$, oraz $P_f = 0.05P$. Zgodnie z powyższymi założeniami, kapitalizacja rynkowa REP musi być większa niż około 10.5 raza wartości liczby otwartych pozycji aby protokół rozwidlania zachował spójność.

Scenariusz 4. Jedynie 5% wszystkich istniejących tokenów REP migruje do Prawdziwego uniwersum podczas okresu rozwidlania, pasożytnicza wartość liczby otwartych pozycji jest dwukrotnie większa od wartości natywnej liczby otwartych pozycji, a tokeny REP wysłane do Fałszywego uniwersum są warte 5% wartości tokenów REP wysłanych do Prawdziwego uniwersum. W takim przypadku $S = 0.05$, $I_p = 2I_a$, oraz $P_f = 0.05P$. Zgodnie z powyższymi założeniami, kapitalizacja rynkowa REP musi być większa niż około 63 razy wartość liczby otwartych pozycji aby protokół rozwidlania zachował spójność.

Appendix C: Wpływ Premii za Wczesną Migrację na Spójność Protokołu Rozwidlania

W celu ułatwienia rozważań, zignorowaliśmy 5% premię za wczesną migrację i wspomnieliśmy o niej podczas dyskusji o spójności protokołu rozwidlania i określiliśmy ją pokrótce podczas dyskusji o spójności protokołu rozwidlania. Powróćmy do Twierdzenia 1 rozważając te dwie sprawy.

Jak poprzednio, suma tokenów REP wysłana do Prawdziwego uniwersum podczas okresu raportowania jest oznaczona SM. Z tego względu, aby atakujący odniósł sukces, musi zmigrować przynajmniej $SM + \epsilon$ REP, które mają wartość $(SM + \epsilon)P$ przed migracją, do jednego z Fałszywych uniwersów.

Jeżeli atakując migruje $SM + \epsilon$ REP do Fałszywego uniwersum w ciągu okresu raportowania podczas rozwidlania, otrzymają $1.05(SM + \epsilon)$ REP w uniwersum potomnym, do którego zmigrowali. Przez definicję P_f, wartość tych tokenów jest dana przez $1.05(SM + \epsilon)P_f$. Z tego względu minimalny koszt dla atakujących wynosi $(SM + \epsilon)P - 1.05(SM + \epsilon)P_f$, co można określić jako $(SM + \epsilon)(P - 1.05P_f)$.

Jak poprzednio, maksymalny (całkowity) zysk dla atakującego jest oznaczany przez $I_a + I_p$. Z tego względu możemy powiedzieć, że protokół rozwidlania jest spójny, kiedykolwiek $S > \frac{1}{2}$ lub:

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

Rozwiązując powyższą nierówność względem kapitalizacji rynkowej, PM, widzimy, że protokół rozwidlania jest spójny wtedy i tylko wtedy, gdy:

1. $S > \frac{1}{2}$ or
2. $1.05P_f < P$ i kapitalizacja rynkowa REP jest większa niż $\frac{P(I_a+I_p-\epsilon(P-1.05P_f))}{S(P-1.05P_f)}$

Jak widać z powyższego, wpływ wczesnej migracji na wymóg kapitalizacji rynkowej jest bardzo mały.

Appendix D: Wpływ Premii za Wczesną Migrację na Minimalny Koszt Forku

Aby zachęcić do uczestnictwa podczas trwania forka, wszyscy posiadacze tokenów REP, którzy zmigrują swoje tokeny w ciągu 60 dni od startu rozwidlania otrzymają 5% dodatkowej premii REP w uniwersum potomnym do którego zmigrowali. Nagroda to jest płatna przez inflację waluty.

Premia ta może stać się przewrotną inicjatywą jeżeli koszt zainicjowania forka jest zbyt niski. W szczególności, jeżeli atakujący mogą zyskać większą wartość z 5% premii REP niż straciliby przy inicjalizacji forka, wtedy oczekiwalibyśmy, że forki przeprowadzane byłyby tak często jak to możliwe. Taki atak, który określamy jako *inflation milking attack*, nie miałby wpływu na nieprawidłowe raportowanie wyroczni, ale miałby wpływ na destruktywne forki, które często zdarzały by się.

Aby zapobiec takim wydarzeniom, Augur musi zapewnić, że koszt inicjalizacji forka jest większy niż maksymalny zysk, który może powstać z 5% premii inflacyjnej. Poniżej wyprowadzamy wzór na niższe ograniczenie kosztu inicjalizacji forku, aby zapobiec temu zjawisku.

Niech P_0 oznacza cenę tokenów REP przed forkiem, a P_1 oznacza cenę REP po zajściu forka. Niech M_0 oznacza podaż pieniądza przed forkiem, a M_1 oznacza podaż pieniądza po zajściu forka. Niech S oznacza odsetek M_0 migrujących do Prawdziwego uniwersum podczas okresu rozwidlania w trakcie trwania forka. Niech b oznacza ilość REP która musi zostać ekonomicznie spalona (co oznacza, postawiona na Fałszywy wynik) aby zainicjalizować fork. Zakładamy $b > 1$.

W celu dalszej dyskusji w tej sekcji, robimy konserwatywne założenie, że wszystkie REP, które migrują podczas okresu rozwidlania są kontrolowane przez atakujących. Dalej, zakładamy (ponieważ minimalizuje to koszt takiego ataku), że wszystkie tokeny REP, które migrują podczas okresu rozwidlania migrują do Prawdziwego uniwersum.

Korzystając z powyższych oznaczeń, SM_0 jest sumą REP zmigrowanych podczas okresu rozwidlania, natomiast $(1-S)M_0$ jest sumą tokenów REP *nie* zmigrowanych podczas okresu rozwidlania.

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

Gdy całkowita liczba SM_0 REP jest zmigrowana podczas okresu rozwidlania, całkowita ilość $0.05SM_0$ REP jest tworzona przez inflację:

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

Koncetrując się jednynie na wpływie inflacji, w celu uproszczenia rozważań, zakładamy, że kapitalizacja rynkowa po forku będzie równa kapitalizacji rynkowej przed forkiem[29]:

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

Podmieniając D1 oraz D2 do D3 i upraszczając, otrzymujemy:

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

Ten (całkowity) zysk dla atakujących za inicjalizację forka i wykorzystanie wczesnej premii za migrację jest wartością ich zmigrowanych tokenów REP po migracji minus wartość tokenów REP przed migracją:

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

Podmieniając D4 do D5 otrzymujemy alternatywne wyrażenie określające (całkowity) zysk dla atakujących:

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

Przypomnijmy, że b jest sumą REP, która musi zostać ekonomicznie spalona, aby zainicjalizować fork. Z tego względu, koszt zainicjalizowania forka wynosi bP_0. Wynika z tego, że płacenie za koszt inicjalizacji forku, aby wykorzystać wczesną premię za migrację jest opłacalna, jeżeli poniższa nierówność jest spełniona:

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

Obserwując, że $P_0 > 0$, oraz $S \neq -20$, rozwiązujemy nierówność względem b i widzimy, że atak jest opłacalny, gdy:

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

Aby zapobiec przewrotnej inicjatywie, Augur musi następująco zorganizować sytuację, tak aby:

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

Zauważając, że S jest ograniczone do interwału $[0, 1]$, widzimy, że wartość prawej strony nierówności D9 jest maksymalna, gdy $S = 2\sqrt{105} - 20 \approx 0.4939$. Oznacza to, że taki atak jest najbardziej opłacalny dla atakujących, gdy około 49.39% wszystkich istniejących REP jest migrowanych podczas okresu rozwidlania. Zakładając konserwatywnie, używamy powyższą wartość za S.[30]

Podnieniając $S = 0.4939$ do D9 otrzymujemy $b \geqslant 0.012197M_0$. Z tego względu, jeżeli koszt inicjalizacji forka wynosi przynajmniej 1.2197% wszystkich istniejących REP wtedy atak wykorzystujący inflację nie jest opłacalny.

Przpomnijmy, że fork jest inicjalizowany tylko po skutecznej obligacji spornej, która jest wypełniona sumą większą niż 2.5% wszystkich istniejących REP. Załóżmy, że taka obligacja sporna byłaby wypełniona na korzyść wyniku ω i fork zostałby zainicjalizowany. Wynik ω jest prawdą lub fałszem.

Jeżeli wynik ω jest fałszem, wtedy przynajmniej 2.5% wszystkich istniejących REP było postawione na fałszywy wynik, i z tego względu tokeny stają się bezwartościowe. Zatem atak wykorzystujący inflację nie jest opłacalny, gdy ω jest fałszem.

Jeżeli wynik ω jest prawdą, wtedy Lemat 2 określa, że przynajmniej 1.25% istniejących REP (sumarycznie) jest postawionych na fałszywe wyniki, i z tego względu spalone ekonomicznie. Zatem atak wykorzystujący inflację również nie jest opłacalny gdy ω jest prawdą.

Z tego powodu start rozwidlenia wymaga skutecznego wykupienia obligacji spornej, która wynosi przynajmniej 2.5% istniejących REP.

---

[29] Uważamy takie podejście za konserwatywne. W praktyce, oczekujemy, że kapitalizacja rynkowa zmiejszy się po zajściu forka

[30] W praktyce, atakujący nie może zapobiec temu, że inni uczestnicy będą migrowali swoje tokeny REP podczas okresu rozwidlania i w związku z tym nie można zagwarantować, że S nie przekroczyłoby swojej idealnej wartości wynoszącej około 0.4939. Jednakże bronimy się przed najgorszym możliwym scenariuszem i używamy $S = 0.4939$.

Appendix E: Regulacja Kosztu Obligacji

Obligacja ważności, obligacja no-show oraz ilość postawiona dla wyznaczonego raportującego są regulowane dynamicznie bazując na zachowaniu uczestników w trakcie poprzedniego okna opłat. Poniżej opisujemy, jak regulowane są te wartości.

Zdefiniujmy funkcję $f : [0, 1] \to [\frac{1}{2}, 2]$ przez:[31]

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

Funkcja f jest użyta aby obliczyć wielokrotność użytą w tych obliczeniach, jak opisano w podsekcjach poniżej. Krótko mówiąc, jeżeli niepożądane zachowanie pojawiło się dokładnie 1% czasu poprzedniego okna opłat, wtedy rozmiar obligacji nie ulega zmianie. Jeżeli było mniej częste, rozmiar obligacji zostanie zredukowany maksymalnie do połowy. Jeżeli było bardziej częste, wtedy rozmiar obligacji zostanie zwiększony maksymalnie dwukrotnie.

1. Obligacja Ważności

Podczas pierwszego okna opłat po wprowadzeniu Augura na rynek, rozmiar obligacji ważności zostanie ustawiony na 0.01 ETH. Następnie, jeżeli więcej niż 1% zfinalizowanych rynków w poprzednim oknie opłat było nieważnych, obligacja ważności zostanie zwiększona. Jeżeli mniej niż 1% zfinalizowanych rynków w poprzednim oknie opłat było nieważne, wtedy obligacja ważności zostanie zmniejszona (ale nigdy jej wartość nie będzie mniejsza niż 0.01 ETH).

W szczególności, niech ν oznacza odsetek zfinalizowanych nieważnych rynków w poprzednim oknie opłat, a b_v oznacza sumę obligacji ważności z poprzedniego okna opłat. Wtedy obligacja ważności dla bieżącego okna wynosi $\max\left\{\frac{1}{100}, b_v f(\nu)\right\}$.

2. Obligacja No-Show

Podczas pierwszego okna opłat po wprowadzeniu Augura na rynek, obligacja no-show zostanie ustawiona na 0.35 REP. Podobnie jak z obligacją ważności, obligacja no-show jest regulowana w górę lub w dół, celując w wartość 1% no-show z najniższą wartością równą 0.35 REP.

W szczególności, niech ρ oznacza odsetek rynków w poprzednim oknie opłat, w których wyznaczeni raportujący nie przedstawili raportu na czas, i niech b_r oznacza sumę obligacji no-show z poprzedniego okna opłat. Rozmiar obligacji no-show dla bieżącego okna opłat wynosi $\max\{0.35, b_r f(\rho)\}$.

3. Stawka Wyznaczonego Raportującego

Podczas pierwszego okna opłat po wprowadzeniu Augura na rynek, rozmiar stawki dla wyznaczonego raportującego zostanie ustawiony na 0.35 REP. Rozmiar wyznaczonej stawki zostanie dynamicznie dostosowany w zależności od tego ilu wyznaczonych raportujących było nieprawidłowych (nie zdołali przyczynić się do finalnego wyniku rynku) podczas poprzedniego okna opłat.

W szczególności, niech δ oznacza odsetek wyznaczonych raportujących, którzy byli nieprawidłowi podczas poprzedniego okna opłat, oraz niech b_d oznacza sumę stawki wyznaczonego raportującego podczas poprzedniego okna opłat, wtedy suma stawki dla wyznaczonego raportującego w bieżącym oknie wynosi $\max\{0.35, b_d f(\delta)\}$.

Appendix F: Zmiany Projektowe

Bieżąca wersja projektu Augur została osiągnięta po trzech latach badań i iteracji wymiany zdań. Projekt, który pojawił się jako wynik tego procesu różni się znacznie od wizji, która została przedstawiona w naszej starszej wersji tego dokumentu [12]. Poniżej omawiamy trzy szczególnie znaczne zmiany, jak również racjonalne uzasadnienie tych zmian.

1. Opłaty za raportowanie

W starym projekcie, twórca rynku ustalał opłatę za handel, która była dzielona 50/50 z raportującymi. W obecnym projekcie, opłaty dla twórcy rynku i raportujących są niezależne, a opłaty dal reporterów są ustalane dynamicznie w taki sposób, aby utrzymać bezpieczeństwo systemu.

Opłaty płacone reporterom mają wpływ na cenę REP, co ma bezpośredni wpływ na bezpieczeństwo protokołu rozwidlania (Twierdzenie 1). Jeżeli opłaty płacone raportującym są zbyt niskie, wtedy spójność wyroczni jest wystawiona na ryzyko ataku. W przypadku, gdy opłaty są zbyt wysokie, wzrasta ryzyko pojawienia się rynków pasożytczniczych. Z tego względu ważne jest, aby opłaty płacone raportującym były automatycznie korygowane, aby zachować bezpieczeństwo Augura, zamiast dowolnie decydować o ich poziomie przez tworzących rynki.

Rozdzielenie opłat raportujących od opłat tworzących rynek również zapewnia, że raportującym (i w związku z tym spójności protokołowi rozwidlania) nie szkodzi rywalizacja z tworzącymi rynki, aby tworzyć rynki z możliwie najniższymi opłatami. Dobre jakościowo rynki i dobre jakościowo raportowanie powinno być osobno mierzone i wynagradzane. Rywalizacja powinna być umożliwiona,

[31] Powyższy wzór może ulec zmianie po otrzymaniu danych empirycznych z żywych rynków.

aby kierować opłaty dla tworzących rynki w kierunku zera, bez obniżania opłat płaconych raportującym.

2. Opłaty za Handel

W starym projekcie, opłaty były zbierane od handlujących od każdej wymiany. W nowym projekcie, opłaty są zbierane od handlujących wyłącznie podczas rozliczania się bezpośrednio z kontraktami rynkowymi. Ta zmiana została po części dokonana dlatego, że Augur nie jest w stanie nadzorować wymian zachodzących offline. Akcje wyników rynkowych są po prostu tokenami, które mogą być dowolnie wymieniane między użytkownikami. Ponieważ zbieranie opłat od każdej wymiany jest niewykonalne, Augur zamiast tego zbiera opłaty wyłącznie wtedy, gdy handlujący rozliczają się bezpośrednio z kontraktami rynkowymi Augura. Dodatkową korzyścią takiego podejścia jest zmniejszenie średnich opłat płaconych przez handlujących, co powinno sprawić, że Augur będzie bardziej konkurencyjny, niż inne rozwiązania.

3. Uniwersa

W poprzedniej architekturze, istniała tylko jedna "wersja" tokenów REP, i podaż tokenów była ustalona z góry. Obecnie REP może rozwidlać się w wiele wersji (uniwersa), z których każde może zawierać inną, mniejszą lub większą liczbę tokenów REP niż wersja pierwotna. Jeżeli fork jest sporny, podaż tokenów REP w każdym z uniwersów potomnych może zawierać tylko ułamek całkowitej podaży w uniwersum pierwotnym. W przypadku forka, który nie jest sporny, wczesna premia za migrację dla uczestników forka może spowodować wygenerowanie większej liczby tokenów, niż w uniwersum pierwotnym.

Nowe wersje tokenów REP powstałych przez rozwidlenie są całkiem różnymi tokenami, każdy ma własną cenę i podaż, i tak powinni traktować je dostawcy usług. Po pierwszym uruchomieniu Augura, będzie istniało tylko jedno uniwersum (uniwersum początkowe) i jedna wersja tokenów REP, tak jak to ma obecnie miejsce. Jednakże, zaraz po zajściu forka, wersja ta zostanie podzielona na wiele wersji: na przykład, rynek rozwidlający z wynikami A i B spowoduje powstanie nowych tokenów REP-A, REP-B, oraz REP-Invalid. Portfele i giełdy, które wspierają tokeny REP miałyby w tym przypadku cztery różne wersje tokenów REP, które (w teorii) mogłyby wspierać – REP-pierwotny (początkowa wersja REP, która byłaby zablokowana), REP-A, REP-B, oraz REP-Invalid.[32]

Całkowita podaż tokenów REP w każdym uniwersum potomnym zależy od tego, ile tokenów REP zostało do niego migrowanych, i zależnie od tego, kiedy nastąpiła migracja. Migrowanie tokenów REP podczas trwającego forka, zanim stanie się jasne, które uniwersum potomne osiągnie konsensus, wystawia użytkownika na małe (ale różne od zera) ryzyko (patrz Sekcja III E), co może zniechęcić do partycypacji podczas trwania forka w przypadkach spornych forków. Aby zachęcić do uczestnictwa w czasie trwania forka, użytkownicy muszą zostać wynagrodzeni za podjęcie ryzyka.

Użytkownicy, którzy nie biorą udziału w forku w czasie jego trwania, mogą być ukarani przez stratę części posiadanych tokenów REP. Właściwie, to stara wersja architektury posiadała mechanizm, który można by opisać jako "bierz albo trać", który karał nie biorących udziału w forku, traktując ich tak, jak gdyby byli raportującymi, którzy nie zaraportowali poprawnie. Jednakże karanie użytkowników, którzy nie biorą udziału tworzy znaczny problem z użytecznością platformy. Karanie użytkowników jest problematyczne zarówna dla portfeli jak i giełd, które przechowują tokeny zdeponowane przez swoich klientów. W przypadku forka, giełdy musiałyby migrować tokeny REP klientów do jednego z uniwersów potomnych, lub tracić część udziałów tokenów.[33]

Zamiast karać użytkowników, którzy nie biorą udziału w forku, uczestnicy którzy biorą w nim udział otrzymują nagrodę przez wygenerowanie 5% premii w uniwersum potomnym do którego migrują tokeny. Jeżeli 4.762% tokenów REP (lub więcej) zostanie migruje do uniwersum, które przegrywa – z którego 1.25% do 2.5% zostało już przeznaczone na rozwiązanie dysputy – wtedy wszystkie uniwersa będą miały mniejszą podaż tokenów REP niż uniwersum pierwotne.

---

[32] Ze względów praktycznych, dostawcom usług prawdpodobnie będzie najłatwiej (i najmniej zakłócając ich użytkowników) zachęcić użytkowników do wzięcia udziału w forku, i później po prostu wspierać uniwersum, które zostanie wybrane przez większość po zakończeniu forka.

[33] Odkryliśmy również, że kod smart kontraktów konieczny do implementacji nagród za uczestnictwo w forku używając wyłącznie redystrybucji tokenów był We also found, as a practical matter, that the smart contract code needed to implement forking rewards only using redistribution was nadmiernie skomplikowany. Złożoność kodu smart kontraktów jest obarczone ryzykiem wpływającym na bezpieczeństwo, zatem staraliśmy się upraszczać implementację tam, gdzie było to możliwe.