Augur: Un Oráculo Descentralizado y Plataforma de Mercados Predictivos

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander
Forecast Foundation
(Dated: 30 de abril de 2018)

Augur es un oráculo descentralizado, que no requiere confiar en un tercero para su funcionamiento, y una plataforma de mercados predictivos. Los resultados de las predicciones de los mercados de Augur son elegidos por los usuarios que poseen el token nativo de Augur llamado Reputación, quienes apilan sus tokens en base al resultado actual observado y reciben en retorno las comisiones resultantes de la liquidación de los mercados. La estructura de incentivos de Augur está diseñada para asegurar que el reporte de los resultados de forma honesta y exacta sea siempre la opción más rentable para los poseedores de los token de Reputación. Los poseedores de los token pueden vincular montos de fianza más grandes de Reputación de forma progresiva para disputar los resultados de los mercados propuestos. Si la cantidad de estos montos de fianza alcanza un determinado límite, los tokens de Reputación se dividen en múltiples versiones, una para cada posible resultado en el mercado disputado. Los poseedores de los tokens deben entonces cambiar sus token de Reputación por una de estas versiones. Las versiones de los token de Reputación que no se correspondan con el resultado correcto del mundo real perderán todo su valor, ya que nadie participará en las predicciones de los mercados a menos que estén seguros que los mercados se resolverán correctamente. Por tanto, los poseedores de los token seleccionarán la única versión de Reputación que sepan que continuará teniendo valor: la versión que se corresponde con la realidad.

Augur es un oráculo descentralizado, que no requiere confiar en un tercero para su funcionamiento, y una plataforma de mercados predictivos. En un mercado predictivo, los individuos pueden especular sobre los posibles resultados de los eventos. Aquellos que los predicen correctamente ganan dinero y aquellos que no pierden dinero [1–3]. El precio de un mercado predictivo puede servir como un indicador preciso y bien calibrado de cuan probable el evento vaya a ocurrir [4–7].

Usando Augur, la gente tendrá la habilidad de tradear en los mercados predictivos con un coste muy bajo. Los únicos gastos significativos que asumen los participantes es la compensación a los creadores de los mercados y a los usuarios que reportan los resultados de los mercados una vez que el evento tiene lugar. El resultado es una predicción de mercado donde los requerimientos de confianza, fricción y comisiones serán todo lo bajas que las fuerzas competitivas de los mercados puedan llevar a cabo.

Históricamente, los mercados predictivos han estado centralizados. La manera más simple de agregar trades en un mercado predictivo es a través de una entidad confiable que mantenga los registros contables. Igualmente, la forma más simple de determinar el resultado de un evento y distribuir los montantes pagaderos a los traders es a través de un juez imparcial y confiable que determina los resultados de los mercados. Sin embargo, los mercados predictivos centralizados tienen muchos riesgos y limitaciones: No permiten participación global, limitan los mercados que pueden ser creados o tradeados, y requieren a los traders que confíen en el operador de mercado para que sus fondos no sean robados y que los mercados se resuelvan correctamente.

Augur ambiciona resolver los mercados de forma totalmente descentralizada. Las redes descentralizadas y que no requieren de un tercero para su funcionamiento, como Bitcoin [8] y Ethereum[9], eliminan el riesgo de que el propio interés individual desemboque en corrupción o robo. El único rol de los desarrolladores de Augur es publicar contratos inteligentes para la red de Ethereum. Los contratos de Augur están totalmente automatizados, los desarrolladores no tienen la habilidad de gastar los fondos que están depositados bajo el paraguas de los contratos, no controlan como se resuelven los mercados, no aprueban o rechazan los trades u otras transacciones en la red, no pueden retroceder los trades, modificar ni cancelar órdenes, etc. El oráculo de Augur permite que la información sea migrada del mundo real al blockchain sin necesidad de un intermediario confiable. Augur será el primer Oráculo Descentralizado del mundo.

I. COMO FUNCIONA AUGUR

Los mercados de Augur siguen una progresión de 4 fases: *Creación,* , *trading*, *reporting*, y *liquidación*. Cualquiera puede crear un mercado basado en cualquier evento del mundo real. El trading empieza inmediatamente después de la creación del mercado, y todos los usuarios son libres de tradear en cualquier mercado. Después de que el evento sobre el que el mercado ha sido creado ha ocurrido, el resultado del evento se determina a través del oráculo de Augur. Una vez se determina el resultado, los traders pueden cerrar sus posiciones y recoger sus montantes resultantes.

Augur tiene un token nativo, Reputación (REP). Los creadores de mercado y los reporteros necesitan REP cuando reportan sobre el resultado de un evento creado en la plataforma de Augur. Los reporteros apilan REP sobre uno de los posibles resultados del mercado para reportar. Haciendo esto, el reportero declara que el resultado donde apila su REP es el que ha ocurrido en el mundo real. El consenso de los reporteros de los mercados

es considerado la "verdad" para determinar el resultado del mercado. Si un reportero reporta un resultado distinto al consenso alcanzado por los demás, Augur redistribuye el REP apilado en el resultado fuera del consenso de este reportero a los demás reporteros del consenso.

Por poseer REP y participar en los reportes de los eventos de forma precisa, los poseedores de los tokens tienen derecho a una porción de las comisiones de la plataforma. Cada REP apilado da derecho a su poseedor a una parte proporcional de las comisiones del mercado de Augur. Cuanto más REP posea un reportero, y reporte correctamente, más comisiones ganarán por su trabajo para mantener la plataforma segura.

Aunque REP juega un papel central en las operaciones de Augur, no se usa para tradear en los mercados de Augur. Los traders no necesitarán poseer REP o usar REP, ya que no son requeridos para participar en el proceso de reporte.

A. Creación del Mercado

Augur permite a cualquier persona crear un mercado acerca de cualquier evento pendiente de acontecer. El *creador del mercado* establece *cuando finaliza el evento* y elige un *reportero designado* para reportar el resultado del evento. El reportero designado no decide unilateralmente sobre el resultado del evento; la comunidad siempre tiene la oportunidad de disputarlo y corregir el resultado reportado por el reportero designado.

A continuación, el creador del mercado elige la *la fuente de resolución* que el reportero designado usará para determinar el resultado. La fuente puede ser simplemente "conocimiento común" o puede ser una fuente específica, como "El Departamento de Energía de Estados Unidos", `bbc.com`, , o la dirección de una API particular.[1] También crea la *comisión del creador*, que es la comisión que se paga al creador del mercado por los traders que liquidan con el contrato del mercado (ver la sección I D para los detalles sobre las comisiones). Finalmente, el creador del mercado define dos montantes más a modo de fianza: la de *validación*, y la del *reportero designado que no acude a reportar* (también definida como la de *no acudir* para abreviar).

El montante de la fianza de validación se paga en ETH y se devuelve al creador del mercado si el mercado se resuelve con cualquier resultado que no sea *inválido*.[2] El montante de la fianza de validación incentiva a los creadores de mercados a crear mercados basados en eventos bien definidos con un objetivo y resultado preciso y no ambiguo. El tamaño del monto de la fianza se establece de forma dinámica, basado en la proporción de resultados inválidos de los mercados recientes.[3]

El montante de la fianza por no acudir a reportar por parte del reportero designado consiste en dos partes: El *montante de la fianza del gas por no acudir* (pagadero en ETH) y el *montante de la fianza de no acudir de REP* (pagadero en REP). Esos montantes de fianza son retornados al creador del mercado si el reportero designado reporta durante los primeros tres días tras la finalización del evento. *event end time*. Si el reportero designado no reporta en este intervalo de tiempo, entonces el creador del mercado pierde el derecho sobre el monto de la fianza de no acudir y se le entrega al *primer reportero público* que reporte sobre ese mercado (ver la sección I C 6). Esto incentiva al creador del mercado a elegir a un reportero designado de confianza, que debería ayudar a que los mercados queden resueltos rápidamente.

El montante de la fianza del gas por no acudir está pensado para cubrir los costes de gas en los que el primer reportero público incurra. Esto se hace para prevenir el escenario en el que los costes de gas del primer reportero público sean muy altos para que el reporte sea rentable. El monto de la fianza del gas por no acudir se establece como el doble del coste medio del reporting durante la ventana de comisiones anterior.

En el caso que el reportero designado no reporte, el montante de la fianza REP de no aparecer se entrega al primer reportero público y se queda apilado junto a su resultado reportado, por lo que el reportero público recibe el REP de no acudir si y solo si reporta correctamente el resultado. De igual forma que el montante de la fianza de validación, el montante de la fianza de no aparecer de REP se ajusta de forma dinámica basado en la proporción de reporteros designados que no reportaron a tiempo durante la ventana de comisiones anterior. [4]

El creador del mercado crea el mercado y postea todos los montantes de las fianzas requeridos a través de una única transacción en Ethereum. Una vez la transacción queda confirmada, el mercado pasa a estar activo y la fase de trading comienza.

B. Trading

Los participantes del mercado predicen los resultados de los eventos tradeando las *participaciones* de esos resultados de los mercados. Un *set completo de participaciones*

[1] Por ejemplo, si un mercado sobre "El pico alto de temperatura (en grados Fahrenheit) el 10 de Abril, 2018 en el Aeropuerto Internacional de San Francisco, reportado por la Weather Underground", especifica una fuente de resolución a través de `https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html`, los reporteros pueden simplemente ir a dicha URL e introducir como resultado el pico alto de temperatura marcado en este reporte.

[2] Un *mercado inválido* es un mercado determinado de esta forma por los reporteros porque ninguno de los resultados enumerados por el creador del mercado es correcto, o porque el enunciado del mercado es ambiguo o subjetivo; ver la sección III F para discusión.

[3] Ver apéndice E 1 para detalles.

[4] Ver apéndice E 2 para detalles.

Figura 1. Esquema simplificado del ciclo de vida de una predicción de mercado.

es un grupo de participaciones consistentes en una participación de cada posible resultado válido del evento. [10]. Los sets completos son creados por el motor de contratos de Augur que los junta como sea requerido para completar los trades.

Por ejemplo, consideremos un mercado con dos posibles resultados, `A` y `B`. Alicia está dispuesta a pagar 0.7 ETH por una participación del resultado `A` y Bob está dispuesto a pagar 0.3 ETH por una participación de `B`.[5] Primero, Augur junta estas órdenes y recoge un total de 1 ETH por las participaciones de ambos, entregando a Alicia su participación en A y a Bob su participación en B. [6] Entonces Augur crea un set completo de participaciones, dando a Alicia la participación de `A` y a Bob la participación de `B`. Así es como las participaciones de los resultados pasan a existir. Una vez las participaciones son creadas, pueden ser tradeadas libremente.

Los contratos de trading de Augur mantienen un libro de órdenes para cada mercado creado en la plataforma. Cualquier persona puede crear una nueva orden o cruzar la orden con una existente en todo momento. Las órdenes son cruzadas por un motor de cruce automático que existe como parte de los contratos inteligentes de Augur. Las peticiones de compra venta de participaciones son cruzadas inmediatamente si hay una orden ya puesta que coincida en el libro de órdenes. Pueden ser cruzadas a través de la compra o venta de participaciones de otros participantes, que pueden involucrar la emisión de nuevos sets de participaciones o el cierre de sets completos existentes. El motor automático de cruce de órdenes de Augur aísla la cantidad mínima de participaciones y el efectivo necesario para cubrir el valor en riesgo. Si no hay ninguna orden que se cruce, o la petición solo puede ser parcialmente cruzada, el remanente es puesto en el libro de órdenes como una nueva orden.

Las órdenes nunca se ejecutan a un precio peor que el límite de precio establecido por el trader, pero pueden ser ejecutadas a un mejor precio. Las ordenes no cruzadas y las parcialmente cruzadas pueden ser retiradas del libro de órdenes por el creador del mercado en cualquier momento. Las comisiones son pagadas por los traders solo cuando sets completos de participaciones son vendidas; la liquidación de las comisiones son discutidas en mayor detalle en la sección I D.

Se espera que la mayor parte del trading de participaciones ocurra antes que el mercado se liquide, pero las participaciones se pueden tradear en cualquier momento tras la creación del mercado. Todos los activos de Augur – incluyendo las participaciones en los resultados de los mercados, las comisiones de tokens en las ventanas, las participaciones en la disputa de los montantes de las fianzas, e incluso la propiedad de los mercados como tales – son transferibles en todo momento.

C. Reporting

Una vez el evento relacionado con el mercado creado ocurre, el resultado debe ser determinado para que el mercado finalice y comience el proceso de liquidación. Los resultados son determinados por el oráculo de Augur, que consiste en reporteros movidos por la consecución de beneficio, que simplemente reportan el resultado del hecho actual en el mundo real del evento. Cualquier poseedor de REP puede participar en el reporting y disputar los resultados. Los reporteros cuyos reportes son consistentes con el consenso son recompensados financieramente, mientras si sus reportes no son consistentes con el consenso serán penalizados financieramente. (ver Sección I D 3).

1. Ventanas de Comisiones

El sistema de reporting de Augur corre sobre un ciclo de ventanas de comisiones de 7 días consecutivos. *fee windows*. Todas las comisiones recogidas por Augur durante esta ventana de comisiones son añadidas al *montante total de comisiones* de esta ventana. Al final de la ventana de comisiones, el montante total de comisiones se reparte entre los poseedores de REP que han participado en el proceso de reporting. Los reporteros reciben las recompensas en proporción a la cantidad de REP que apilaron durante la ventana de comisión. La participación incluye: Apilar REP durante el reporte inicial, disputar un resultado tentativo o comprar *tokens de participación*.

[5] Inicialmente, los trades en los mercados de Augur usarán la moneda de la plataforma de Ethereum como moneda nativa, el Ether (ETH). En futuras versiones de Augur, se incluirá soporte para mercados denominados en una variedad de tokens dentro de la red Ethereum, incluyendo participaciones de otros mercados así como tokens indexados a monedas fiat (las "monedas estables"), si estuviesen disponibles y cuando lo estuviesen.

[6] La figura de 1ETH se utiliza aquí para facilitar la discusión. El coste actual de un set completo de participaciones es mucho más pequeño que esto; ver `docs.augur.net/#number-of-ticks` para detalles.

2. Tokens de Participación

Durante cualquier ventana de comisiones, los poseedores de REP pueden comprar cualquier número de tokens de participaciones por un attorep [7] cada uno. Al final de cada ventana de comisiones, pueden redimir sus tokens de participación por un attorep cada uno, que se suma a la parte proporcional de las comisiones generadas en la *ventana de comisiones*. Si no hay ninguna acción que el reportero necesite realizar (*por ejemplo*, reportar o disputar un reporte de otro usuario) el reportero puede comprar tokens de participación que indica que se han personado para esa ventana de comisiones. Al igual que cuando apilan REP, los tokens de participación pueden ser redimidos por sus propietarios por una porción *pro rata* de las comisiones en esa ventana de comisiones.

Según lo discutido en la Sección II, es importante que los tenedores de REP estén preparados para participar en la resolución de los mercados en el caso de una bifurcación (fork). Los tokens de participación sirven de incentivo a los tenedores de REP para monitorear la plataforma al menos una vez por semana, y adicionalmente estar dispuestos a participar si se necesitase. Incluso los tenedores de REP que no quieren participar en el proceso de reporting están incentivados a meterse en la plataforma de Augur una vez en cada ventana de comisiones de 7 días para comprar tokens de participación y recoger comisiones. Esta forma de acudir activa y regularmente en la plataforma les permitirá familiarizarse con el manejo y uso de Augur, y estarán al tanto de las bifurcaciones cuando ocurran y además estarán más preparados para participar en ellas cuando sucedan.

3. La Progresión del Estado del Mercado

Los mercados de Augur pueden estar en siete estados diferentes una vez han sido creados. Los potenciales estados o "fases" de un mercado de Augur son los siguientes:

- Pre-reporting
- Reporting designado
- Reporting abierto
- En espera del inicio de la siguiente ventana de comisiones
- En disputa
- En bifurcación (fork)
- Finalizados

La relación entre estos estados puede verse en la Figura. 2.

[7] Un *attorep* es 10^{-18} REP.

4. Pre-reporting

La fase de *pre-reporting* o *trading* (Fig. 1) es el periodo de tiempo que empieza después que el trading ha empezado en el mercado, pero antes que el evento del mercado haya acontecido. Generalmente, este el periodo más activo de trading para cualquier mercado de Augur. Una vez la fecha del evento ha pasado, el mercado entra en la fase del *reportero designado* (Figura 2a).

5. Reporting designado

Cuando creamos un mercado, los creadores necesitan elegir un reportero designado y postear un montante de fianza por no acudir a reportar. Durante la fase de reporting designado (Figura 2a) el reportero designado del mercado tiene hasta tres días para reportar sobre el resultado del evento. Si el reportero designado no reporta dentro de este periodo, el creador de mercado pierde el montante de la fianza por no acudir, y el mercado automáticamente entra en la fase de *reporting abierto* (Figura 2b).

Si el reportero designado envía el reporte a tiempo, entonces el montante de la fianza de no acudir se retorna al creador del mercado. El reportero designado requiere de apilar su monto [8] sobre el resultado que quiera reportar, que perderá si el mercado finaliza de forma diferente a la que ha reportado.[9] Tan pronto como el reportero designado mande su reporte, el mercado entra en la fase de *espera para el comienzo de la siguiente ventana de comisiones* (Figura 2c), y el reporte enviado se convierte en el *resultado tentativo* a partir de ese momento.

6. Reporting Abierto

Si el reportero designado no acude a reportar dentro de los tres días, el creador de mercado pierde el montante de la fianza de no acudir, y el mercado inmediatamente entra en la fase de *reporting abierto* (Figura 2b). Tan pronto como el mercado entra en la fase de reporting abierto, cualquiera puede reportar sobre el resultado del mercado. Cuando el reportero designado no ha reportado, el primer reportero que reporta sobre el resultado de un mercado es denominado el *primer reportero público*.

El primer reportero público recibe el monto de la fianza por no acudir del reportero designado que se apila junto al resultado reportado, por lo que pueden reclamar el REP de no acudir solo si su resultado reportado coincide

[8] Ver apéndice E 3 para los detalles sobre el tamaño del monto a apilar por el reportero designado.

[9] El monto renunciado es añadido al monto total de las comisiones de reporting de la ventana de comisiones asignada, y se usa para recompensar a los reporteros honestos y a los que disputen correctamente; ver la Sección I D 3 para detalles.

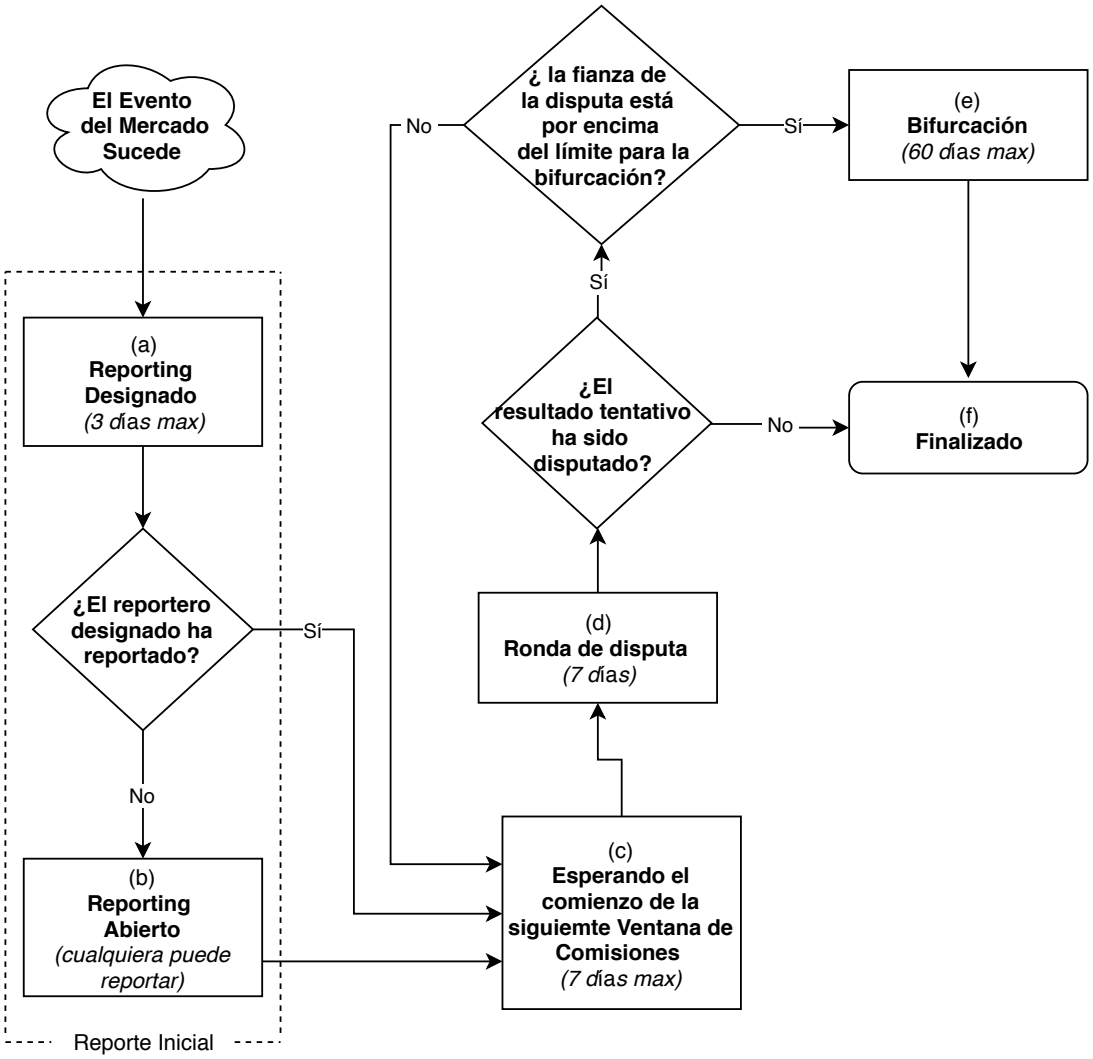

Figura 2. Flujo del Reporting.

con el resultado final del mercado. Solo reciben el montante de la fianza de no acudir una vez el mercado ha finalizado solo si su resultado reportado coincide con el resultado final del mercado.

El primer reportero público *no* necesita apilar su REP cuando reporte el resultado del mercado. De esta forma, cualquier mercado cuyo reportero designado no acude a la hora de reportar se espera que su resultado se reporte muy rápido por *alguien* durante la fase de reporting abierto.

Una vez el *reporte inicial* ha sido recibido (o bien por el reportero designado o el primer reportero público), el reporte de este resultado se convierte en el resultado tentativo del mercado, y el mercado entra en la fase de espera para el comienzo de la siguiente fase de ventana de comisiones (Figura. 2c).

7. *Fase de Espera del Comienzo de la Siguiente Ventana de Comisiones*

Una vez el mercado recibe el reporte inicial, entra en la fase de espera del comienzo de la siguiente ventana de comisiones (Figura 2c). Durante esta fase, el reporting del mercado está en modo espera hasta el final de la ventana actual de comisiones. Una vez que la siguiente ventana de comisiones se abre, el mercado entra en la fase de *disputa*.

8. *Ronda de Disputa*

La ronda de disputa (Figura 2d) es un periodo de 7 días durante el cual cualquier poseedor de REP tiene la oportunidad de disputar el *resultado tentativo del mer-*

cado.[10] (Al inicio de una ronda de disputa, el resultado tentativo del mercado es el resultado que se convertirá en el resultado final del mercado si no se disputa de forma exitosa por parte de los poseedores de REP.) Una disputa consiste en *apilar* REP (referido a la *pilar de REP en disputa* en este contexto) sobre un resultado *distinto al* resultado tentativo reportado. Una disputa tiene *éxito* si el monto total apilado sobre la disputa de un resultado cumple con *el tamaño total* requerido dentro de la ronda actual. El montante total de la fianza de disputa se computa como sigue.

A_n es el monto total apilado sobre los resultados de este mercado al inicio de la ronda de disputa n. ω es cualquier resultado del mercado *diferente* al resultado tentativo reportado al inicio de la ronda de disputa. $S(\omega, n)$ es el montante total apilado sobre el resultado ω al inicio de la disputa n. Entonces el tamaño de la *disputa*que se necesita para disputar exitosamente el actual resultado tentativo en favor del nuevo resultado ω durante la ronda n se denomina $B(\omega, n)$ y se expresa de la siguiente forma:

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

Los tamaños del monto de fianza son escogidos de esta forma para asegurar un retorno de la inversión (ROI) de un 50 % para los reporteros que exitosamente disputen los falsos resultados (ver Sección II D).

El monto de la fianza en la disputa no necesita ser pagado enteramente por un único usuario. La plataforma de Augur permite a los participantes aunar la suma del monto total de la fianza de la disputa a través del sistema de crowdsource. Cualquier usuario que ve un resultado tentativo incorrecto puede disputar este resultado apilando REP en un resultado diferente al tentativo reportado. Si cualquier resultado (que no sea el tentativamente reportado) acumula suficiente monto total de disputa para satisfacer el montante total de fianza requerido, el resultado tentativo será disputado de forma exitosa.

En caso de una disputa exitosa, el mercado puede entrar en una nueva ronda de disputa o entrara en un estado de *bifurcación* (Figura 2e). Si el tamaño total del monto disputado es inferior al 2.5 % de todo el REP, entonces el nuevo resultado elegido se convierte en el nuevo resultado tentativo, y el mercado se encamina a otra nueva ronda de disputa.

Todo el montante disputado hasta este momento queda retenido durante la durante la ronda de disputa. Si el montante de la fianza de la disputa no prospera, entonces el montante disputado es retornado a sus propietarios al final de la ronda de disputa. Si no hay ninguna disputa exitosa durante los 7 días de la ronda de disputas, el mercado entra en la fase *finalizada* (Figura 2f), y su resultado tentativo es aceptado como *resultado final*. El resultado final de un mercado es el resultado tentativo que pasa a través de una ronda de disputa sin ser exitosamente disputado, o es determinado a través de una bifurcación (fork). Los contratos de Augur tratan a los resultados finales como la *verdad* y pagan de acuerdo a ello.

Todos los montos de las disputas sin éxito se retornan a sus propietarios originales al final de cada ronda de disputas. Todos los montos de las disputas exitosas se aplican al resultado sobre el cual se han apilado y quedan ahí hasta que el mercado se finaliza (o hasta que una bifurcación ocurre en algún mercado de Augur). Todos los montos por disputas (tanto las exitosas como las no exitosas) recibirán la porción de las *comisiones totales* [11] del reporting de la ventana de comisiones actual.

9. Bifurcación

El estado de bifurcación (Figura 2e) es un estado especial que dura hasta 60 días. La bifurcación es el método para la resolución del mercado como último recurso; es muy proceso muy disruptivo y la intención es que ocurra muy remotamente. La bifurcación se produce cuando hay un mercado con un resultado con un monto total de fianza disputado exitosamente de al menos un 2.5 % de todo el REP. Este mercado es lo que se conoce como *mercado bifurcado*.

Cuando una bifurcación se inicia, el periodo de 60 días [12] *periodo de bifurcación* comienza. La disputa de otros mercados no finalizados se congela hasta el final del periodo de la bifurcación. El periodo de la bifurcación es mucho más largo que el periodo usual de las ventanas de comisiones porque la plataforma necesita proveedor un intervalo temporal amplio para los poseedores de REP y los proveedores de servicios (como los monederos y los exchanges) para prepararse. El resultado final tras la bifurcación no puede ya ser disputado más.

Cada mercado de Augur y todos los token REP existen en un determinado *universo*. Los tokens REP pueden ser utilizados para reportar sobre los resultados (y por tanto ganar comisiones) *solo* para los mercados que existan en el mismo universo que los tokens REP. Cuando Augur se lance por primera vez, todos los mercados y los tokens REP existirán conjuntamente en un mismo universo de la *genesis inicial*.

---

[10] El hecho que la ronda de disputa coincida con la ventana de comisiones es por pura conveniencia; por principio, las rondas de disputa y la duración de las ventanas de comisiones podrían ser diferentes.

[11] Cualquier liquidación de comisiones y montos de fianza de validación durante la ventana de comisiones se añaden al monto total de comisiones de la ventana. Al final de dicha ventana de comisiones, el monto total de comisiones se paga a los usuarios en proporción a la cantidad de REP apilada en la ventana de comisiones.

[12] Los periodos de bifurcación pueden ser más cortos de 60 días: Un periodo de bifurcación termina o bien cuando los 60 días hayan pasado o cuando más del 50 % de todos los REP originales de la génesis han migrado a un universo infantil determinado.

Cuando un mercado se bifurca, se crean nuevos universos. La bifurcación crea un nuevo *universo infantil* para cada posible resultado del mercado bifurcado (incluyendo el `inválido`, como lo discutido en la Sección I D 2). Por ejemplo, un mercado "binario" tiene tres posibles resultados; `A`, `B`, e `Inválido`. Por tanto, un mercado "binario" bifurcado creará tres nuevos universos infantiles: universo `A`, universo `B`, y universo `Inválido`. Inicialmente, estos tres universos recién creados están vacíos: no contienen ningún mercado ni ningún token REP.

Cuando se inicia la bifurcación, el *universo padre* se *bloquea* permanentemente. En un universo bloqueado, ningún mercado nuevo puede crearse. Los usuarios pueden continuar tradeando las participaciones en los mercados bloqueados, y los mercados bloqueados pueden recibir todavía sus reportes iniciales. Sin embargo, no se paga ninguna recompensa por reportar y los mercados bloqueados no pueden ser finalizados. Para que los mercados o los token REP en el mercado bloqueado puedan ser útiles, tienen que migrarse primero al universo infantil.

Los poseedores de tokens REP en el universo paterno pueden migrar sus tokens al universo infantil de su elección. Esta elección tiene que someterse a una profunda consideración, porque la migración una vez se realiza no puede revertirse. Los tokens no se pueden enviar de un universo hermano a otro. *La migración representa un compromiso permanente de los token REP sobre un determinado resultado para un mercado.* Los REP que migran a universos infantiles diferentes deben ser considerados tokens enteramente separados, y los proveedores de servicios como los monederos y los exchanges deben listarlos como tales.

Cuando se inicia una bifurcación, todos los REP apilados en todos los mercados restantes que no han sido bifurcados se *desapilan* de tal forma que son libres para migrar al universo infantil durante el periodo de bifurcación.[13]

El mercado infantil que recibe un mayor número de tokens REP migrados al final del periodo de la bifurcación se convierte en el mercado ganador, y su resultado correspondiente se convierte en el resultado final del mercado bifurcado. Los mercados no finalizados en el universo padre pueden ser migrados solamente al universo ganador y, si han recibido un reporte inicial, serán reseteados a la fase de espera para el comienzo de la próxima ventana de comisiones.

No hay un límite de tiempo para migrar los tokens desde el universo paterno al universo infantil. Los tokens pueden ser migrados después del periodo de la bifurcación, pero no contarán en la determinación del universo ganador. Para incentivar una mayor participación, durante el periodo de bifurcación, todos los poseedores de tokens que migren sus REP dentro de los 60 días del comienzo de la bifurcación recibirán un 5 % adicional de REP en el mercado infantil al que migren.[14]. Esta recompensa es pagada mediante la emisión de nuevos tokens.[15]

Los reporteros que hayan apilado REP en uno de los resultados del mercado bifurcado no pueden cambiar su posición durante la bifurcación. El REP que se ha apilado sobre un resultado en el universo padre puede migrarse solamente al universo infantil que corresponda a este resultado. Por ejemplo, si un reportero ayudó a disputar exitosamente un monto de fianza a favor de un resultado `A` durante una ronda de disputa, entonces el REP apilado sobre el resultado `A` solo puede ser migrado al universo `A` durante la bifurcación.

Los mercados hermanos están totalmente desligados. Los token REP que existen en un universo no pueden ser utilizados para reportar sobre eventos o ganar recompensas de mercados en otro universo. Como los usuarios presumiblemente no van a querer crear o tradear mercados en un universo cuyo oráculo no es confiable, los REP que existen en un universo que no corresponde a la realidad objetiva es improbable que puedan generar comisiones a sus propietarios, y además no deberían poseer ningún valor significativo. Por tanto, los token REP migrados a un universo que no corresponde con la realidad objetiva no deberían tener valor, sin perjuicio que el universo objetivamente falso acabe siendo el universo ganador tras la bifurcación. Esto tiene consecuencias importantes en cuanto a la seguridad, que discutimos en la Sección II.

10. Finalización

Un mercado entra en su fase de finalización (Figura 2f) si pasan los 7 días de la ronda de disputa sin que su resultado tentativo haya sido disputado con éxito, o cuando se ha completado una bifurcación. El resultado de una bifurcación no puede ser disputado y se considera final siempre al final del periodo de la bifurcación. Una vez el mercado es finalizado, los traders pueden liquidar sus posiciones directamente en el mercado. Cuando el mercado entra en estado finalizado, nos referimos a su resultado elegido como el*resultado final.*

---

[13] La única excepción es la del REP apilado por parte del reportero inicial cuando realiza el primer reporte. Ese REP se mantiene apilado en el resultado reportado inicial y es automáticamente migrado al universo infantil que gana la bifurcación.

[14] Esto ocurre incluso cuando el periodo de bifurcación ha finalizado prematuramente debido a que el 50 %de todos los REP han migrado a un determinado universo infantil

[15] El efecto de esta adición de REP es pequeño. Por ejemplo, si un 20 % de todo el REP existente es migrado durante un periodo de bifurcación, este bonus incrementaría un 1 % el montante total de REP. Además, se espera que las bifurcaciones solo se den en ocasiones muy excepcionales.

D. Liquidación del Mercado

Un trader puede cerrar su posición de dos formas: O bien vendiendo las participaciones que han adquirido a otro trader por dinero, o bien liquidando sus participaciones en el mercado. Recordemos que toda participación viene a existir como parte de un set total cuando un total de 1 ETH ha sido apartado a través de Augur. [6] Para que se aparten estos 1 ETH, los traders deben dar a Augur un set completo de participaciones, o si el mercado ha finalizado, una participación del resultado ganador. Cuando este intercambio ocurre decimos que los traders están *liquidando con el contrato del mercado.*

Por ejemplo, consideremos un mercado no finalizado con los resultados posibles `A` y `B`. Supongamos que Alicia tiene una participación en el resultado `A` que quiere vender por 0.7 ETH y Bob tiene una participación el resultado `B` que quiere vender por 0.3 ETH. Primero, Augur hace coincidir estas órdenes y recoge las participaciones de `A` y `B` de los participantes. Entonces Augur le da 0.7 ETH (menos comisiones) a Alicia y 0.3 ETH (menos comisiones) a Bob.

Como segundo ejemplo, consideremos un mercado finalizado cuyo resultado ganador es A. Alicia tiene una participación en `A` y quiere hacerla efectiva. Manda su participación de `A` a Augur y recibe en retorno 1 ETH (menos comisiones).

1. *Liquidación de comisiones*

El único momento en el que Augur grava con comisiones es cuando los participantes del mercado están liquidando contra el contrato de mercado. Augur grava dos tipos de comisiones durante la liquidación: la comisión de creación de mercado y la comisión del reporting. Ambas comisiones son proporcionales a la cantidad que está siendo pagada. Así, en el ejemplo anterior de la liquidación antes de la finalización, donde Alicia recibe 0.7 ETH y Bob recibe 0.3 ETH, Alicia pagaría un 70 % de las comisiones y Bob pagaría el restante 30 %.

La comisión de la creación del mercado la define el creador del mercado durante el proceso de creación del mercado, y se paga al creador del mercado en la liquidación. La comisión de reporting se establece de forma dinámica (ver Sección II C) y se paga a los reporteros que participan en el proceso de reporting.

2. *Liquidación de los Mercados Inválidos*

En el caso que un mercado se resuelve como `Inválido`, los traders que liquidan contra el contrato del mercado reciben una cantidad igual de ETH por cada participación en cada resultado. Si el mercado tiene N posibles resultados (no incluyendo el resultado `Inválido`), y el coste de un set completo de participaciones era C ETH, entonces los traders recibirán C/N ETH por cada participación liquidada en el contrato de mercado.[16]

3. *Redistribución de la Reputación*

Si un mercado finaliza sin iniciarse una bifurcación, todo el REP apilado en un resultado diferente al resultado final queda confiscado y se distribuye a los usuarios que han apilado en el resultado final del mercado en proporción al REP que hayan apilado. El tamaño del monto de fianza es escogido de tal forma que cualquiera que dispute de forma exitosa un resultado a favor del resultado final del mercado se recompensa con un 50 % de retorno de la inversión (ROI) sobre su montante disputado. [17] Este es un fuerte incentivo para que los reporteros disputen falsos resultados tentativos.

II. INCENTIVOS Y SEGURIDAD

Hay una fuerte relación entre la capitalización de mercado de REP y la confianza en el protocolo de bifurcación de Augur. Si la capitalización de mercado de REP es suficientemente grande [18], y los atacantes son racionales desde una perspectiva económica, entonces el resultado que gana en la bifurcación debería corresponder al de la realidad objetiva. De hecho, sería posible para Augur funcionar de forma adecuada sin usar reporteros designados y rondas de disputa. Usando *solamente* el proceso de bifurcación el oráculo reportaría la verdad.

Sin embargo, las bifurcaciones son procesos disruptivos y que consumen mucho tiempo. Una bifurcación tarda hasta 60 días en resolver un mercado individual, y solo puede resolver un mercado a la vez. Durante los 60 días en los que el mercado bifurcado se está resolviendo, todo el resto de mercados no finalizados se congelan. [19] Los proveedores de servicios tienen que realizar actualizaciones y los poseedores de REP tienen que migrar su REP a uno de los nuevos universos infantiles. Por tanto, las bifurcaciones deberían ser usadas solamente cuando son absolutamente necesarias. Las bifurcaciones son la opción nuclear.

Afortunadamente, una vez se ha establecido la confianza en las bifurcaciones para determinar la verdad, los

---

[16] Los trades no se pueden deshacer si el mercado se declara `Inválido` debido a limitaciones técnicas. Las participaciones de los resultados son solamente tokens, que se pueden tradear directamente entre usuarios; el ETH y las participaciones no están bajo el control de Augur y no se pueden devolver al propietario si el mercado finaliza como `Inválido`.

[17] Ver el Teorema 3 en el Apéndice A.

[18] Ver Sección II A para más detalles.

[19] Los traders pueden continuar tradeando en aquellos mercados, pero aquellos mercados no pueden finalizar hasta el final del periodo de bifurcación.

incentivos pueden ser usados para incentivar a los participantes a comportarse de forma honesta sin tener que iniciar una bifurcación de facto. *Es la amenaza creíble de una bifurcación y la creencia que una bifurcación se va a resolver correctamente las claves del sistema de incentivos de Augur.*

A continuación vamos a discutir las condiciones sobre las cuales una bifurcación puede ser de confianza para determinar la verdad. Discutiremos entonces el sistema de incentivos y como incita a la rápida y correcta resolución de todos los mercados.

A. Integridad del Protocolo de Bifurcación

Aquí vamos a discutir la solidez del proceso de bifurcación y las condiciones bajo las cuales pueden ser confiables. Para facilitar la discusión, cuando nos referimos a las bifurcaciones, nos referiremos al universo infantil que corresponda a la realidad objetiva como el universo `Verdadero`, ay cualquier otro universo infantil como un`Falso` universo. Nos referiremos al universo infantil que reciba más REP migrado durante el proceso de la bifurcación como el universo ganador y los otros universos infantiles serán los universos perdedores.

Naturalmente, nosotros siempre queremos que el universo `Verdadero` sea el universo ganador, y que los`Falsos` universos sean los universos perdedores. Decimos que el protocolo de bifurcación ha sido atacado de forma exitosa cuando un universo `Falso` falso acaba siendo el universo ganador de la bifurcación, - resultando por tanto incorrectos los pagos en el mercado bifurcado (y potencialmente todos los mercados no finalizados).

Nuestro enfoque para asegurar el oráculo es arreglar las cosas de tal forma que el máximo beneficio para un atacante exitoso sea menor que el coste mínimo de realizar el ataque. Formalizamos esto como sigue.

1. *Máximo beneficio para el atacante*

Un atacante que de forma exitosa ataque el oráculo podría causar que todos los mercados no finalizados migrasen al `Falso` universo. Si el atacante controla la mayoría del REP en el `Falso` universo, el atacante podría forzar todos los mercados no finalizados para resolverse como quisiera. En el caso más extremo, podría además recoger todos los fondos apartados en todos esos mercados. [20]

Definition 1. Definimos como I_a, el *interés abierto nativo* de Augur como el valor de la suma de todos los fondos apartados en los mercados no finalizados.[21]

Definition 2. Definimos un *mercado parásito* como cualquier mercado que no pague comisiones de reporting a Augur, pero que se resuelva de acuerdo a la resolución del mercado nativo de Augur.

Definition 3. Definimos como I_p, el *interés abierto del mercado parásito* como el valor de la suma de todos los fondos decomisados en todos los mercados parásitos que se resuelvan de acuerdo a los mercados no finalizados nativos de Augur.

En el caso más extremo, un atacante podría ser capaz de hacerse con todos los fondos de todos los mercados parásitos que se resuelven de acuerdo a los mercados no finalizados nativos de Augur.

Observation 1. El máximo beneficio (bruto) de un atacante que ataque exitosamente el oráculo es $I_a + I_p$.

2. *El interés abierto parásito es desconocido*

Augur puede precisa y eficientemente medir I_a. Sin embargo, I_p cno puede ser conocido en general, ya que pueden existir arbitrariamente muchos mercados parásitos fuera del sistema de Augur, cada uno con una cantidad aleatoria grande de interés abierto. Como el máximo posible beneficio de un atacante incluye la cantidad conocida I_p, uno no puede nunca estar objetivamente cierto que el oráculo es seguro contra los atacantes racionales desde el punto de vista económico.

Sin embargo, si queremos afirmar que I_p está racionalmente delimitado en la práctica, entonces podemos definir las condiciones sobre las que podemos asegurar que un oráculo es seguro.

3. *Mínimo coste para un ataque exitoso*

A continuación, consideramos el coste del ataque al oráculo. Denominamos P como el precio de REP. Denominamos un attorep como ϵ [22]. Denominamos a M como la cantidad existente de REP (el "suministro"de REP). Denominamos a S como la proporción de M que migrará al universo verdadero durante la bifurcación

Así el producto de SM representa la cantidad absoluta de REP migrada al universo verdadero durante el periodo de bifurcación de la bifurcación, y el producto de PM es la capitalización de mercado de REP.

Deinifimos P_f como el precio del REP migrado al`Falso` universo del atacante. Si $P \leq P_f$ entonces el oráculo no sería seguro contra atacantes económicamente racionales, porque sería al menos igual de rentable migrar las REP al falso universo que no migrar las REP en absoluto.

[20] Esto requeriría al atacante capturar *todas* las participaciones sobre un determinado resultado, y entonces forzar el mercado a finalizar con este resultado.

[21] Esto incluye mercados externos que pagan comisiones de reporting a Augur.

[22] Un *attorep* es 10^{-18} REP.

4. Integridad

Assumption 1. *Los reporteros que no son atacantes nunca migrarán REP a un universo* `Falso` *durante la bifurcación.* [23]

Debido al diseño, un ataque exitoso al oráculo requiere más REP a migrar al `Falso` universo que al `Verdadero` universo durante el periodo de bifurcación de la bifurcación. Se supone que solo el atacante migrará REP al universo`Falso`. La cantidad de REP migrada al universo `Verdadero` durante el periodo de reporting se denomina SM. Así, para que un atacante tenga éxito, tienen que migrar al menos $SM+\epsilon$ REP. Para simplificar, ignoraremos ϵ como despreciable, y diremos que un ataque exitoso requiere migrar al menos SM REP, que tiene un valor de SMP antes de la migración, a un `Falso` universo.

Si un atacante migra SM REP durante el periodo de reporte de una bifurcación, recibirán SM REP en el universo infantil al que migren[24] Si el atacante migra a un `Falso` universo entonces el valor de esas monedas se convierte en SMP_f. Así, el coste mínimo para el atacante es $(P-P_f)SM$.

Observation 2. La cantidad mínima de REP que un atacante exitoso debe migrar a un `Falso` universo durante una bifurcación es SM, que le cuesta al atacante $(P-P_f)SM$.

Nótese que si $S > \frac{1}{2}$ entonces el ataque es *imposible* porque no existe suficiente REP fuera del universo `Verdadero` para que cualquier `Falso` universo se convierta en universo ganador.

Dirigido en contra de los atacantes económicamente racionales, el oráculo se resolverá con resultados que se correspondan con la realidad objetiva si el máximo beneficio para un atacante es menor que el coste mínimo del ataque. Observando 1 & 2 podemos ver que esto ocurre cuando $S > \frac{1}{2}$ or $I_a + I_p < (P-P_f)SM$. Esto nos da la definición formal de integridad.

Definition 4. (Propiedad de la Integridad) El protocolo de bifurcación es *integro* cuando $S > \frac{1}{2}$ o cuando $I_a+I_p < (P-P_f)SM$.

La desigualdad anterior puede ser resuelta por PM para ver la relación entre la integridad del protocolo de bifurcación y la capitalización de mercado de REP.

Theorem 1. *(Teorema de la Seguridad de la Capitalización de Mercado) El protocolo de bifurcación es íntegro si y solo si:*

1. $S > \frac{1}{2}$, *o*
2. $P_f < P$ *y la capitalización de mercado de REP es mayor que* $\frac{(I_a+I_p)P}{(P-P_f)S}$.

Demostración. Supongamos que el protocolo de bifurcación es íntegro. Entonces por definición, $S > \frac{1}{2}$ or $I_a + I_p < (P-P_f)SM$. Supongamos que $I_a + I_p < (P-P_f)SM$. Como $I_a + I_p \geq 0$ and $SM > 0$, entonces sabemos que $P_f < P$. Entonces, resolviendo que $I_a+I_p < (P-P_f)SM$ para PM, vemos que $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Así, la primera dirección queda probada.

Supongamos ahora que $S > \frac{1}{2}$, o que $P_f < P$ y $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Si $S > \frac{1}{2}$, entonces el protocolo de bifurcación tiene integridad por definición. Si $P_f < P$ y $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$, entonces, resolviendo la desigualdad para $I_a + I_p$, vemos que $I_a + I_p < (P-P_f)SM$, y que el protocolo de la bifurcación es íntegro. □

B. Nuestras Presunciones y sus Consecuencias

Creemos que los traders no querrán tradear en Augur en un universo donde los reporteros han mentido. También creemos que los creadores de mercado no pagarán para crear mercados en Augur en un universo donde no haya traders. En un universo sin mercados o trading, REP no renta a sus poseedores. Por tanto, creemos que el REP enviado a un `Falso` universo poseerá apenas valor de mercado y esto lo vamos a modelar asumiendo que $P_f = 0$.

Creemos que es razonable esperar que al menos un 20 % del REP existente migre al resultado verdadero durante el periodo de reporting de una bifurcación, y modelamos esto asumiendo que $S \geq \frac{1}{5}$. También estamos dispuestos a incluir un interés abierto parásito tan grande como un 50 % del interés abierto nativo, por lo que asumimos que $I_a \geq 2I_p$.

Bajo estos supuestos, el Teorema 1 nos dice que el protocolo de bifurcación tiene integridad cuando la capitalización de mercado de REP es al menos 7.5 veces su interés abierto. [25]

C. Los Impulsos de la Capitalización de Mercado

Augur toma información acerca del precio de REP del mismo modo que toma cualquier otra información sobre

[23] Puede haber casos donde reporteros sin malicia migren REP a un universo `Falso` accidentalmente o por descuido. Sin embargo, este comportamiento es, en la práctica, indistinguible de la colaboración genuina con el atacante.

[24] En la práctica, el atacante recibiría $1{,}05SM$ REP en el universo infantil por el 5 % de bonus de migrar durante los 60 días siguientes al inicio de una bifurcación. Ignoramos el 5 % de bonus aquí para facilitar la discusión. Para la discusión incluyendo el 5 % de bonus, ver el Apéndice C.

[25] Ver el apéndice B para presunciones alternativas y sus consecuencias.

el mundo real: a través de un mercado de Augur. Esto le da a Augur la habilidad para computar la capitalización de mercado actual de REP. Augur también puede medir el interés abierto nativo actual, y puede así determinar que capitalización de mercado debería ser marcada como objetivo para cumplir con los requisitos de integridad de Augur.

Cada universo empieza con una comisión de mercado por defecto de un 1 %. Si la capitalización de mercado actual está por debajo del objetivo, entonces las comisiones de reporting serán automáticamente incrementadas (pero nunca por encima de un 33.3 %), poniendo presión ascendente sobre el precio de REP y/o presión descendente sobre el nuevo interés abierto nativo. Si la capitalización de mercado actual está por encima del objetivo, entonces las comisiones de reporting bajarán automáticamente (aunque nunca por debajo de 0.01 %) para que los traders no paguen más de lo necesario para mantener el sistema seguro.

Las comisiones de reporting se determinan como sigue. Si r es el monto de comisión de la ventana de comisiones anterior, si t es la capitalización de mercado objetivo, y c be capitalización de mercado actual, entonces las comisiones de reporting para la ventana de comisiones actual será como máx $\left\{\text{mín}\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10{,}000}\right\}$.

D. Tomando ventaja de la Amenaza de una Bifurcación

Como se ha mencionado arriba, las bifurcaciones son disruptivas y una forma lenta para que los mercados alcancen su finalización. En vez de usar el proceso de bifurcación para resolver cada mercado, Augur toma ventaja de la amenaza de una bifurcación para resolver los mercados eficientemente.

Recordemos que cualquier monto que dispute de forma exitosa un resultado a favor del resultado final del mercado recibirá un 50 % de retorno de la inversión (ROI) sobre el monto disputado. [26] En el caso de una bifurcación, cualquier REP apilado sobre cualquier resultado falso del mercado debería perder todo su valor económico, mientras que el REP apilado sobre el resultado verdadero es recompensado con un 50 % más de REP en el universo infantil que se corresponda con el resultado verdadero del mercado (independientemente del resultado de la bifurcación). Por tanto, si se desencadena una bifurcación, los poseedores de REP que disputen los resultados falsos en favor de resultados verdaderos siempre saldrán victoriosos mientras que los poseedores de REP que apilaron sobre un resultado falso perderán todo su valor económico.

[26] Medido en el REP que existe en un universo que corresponde al resultado final del mercado; ver Teorema 3 en el Apéndice A.

Creemos que estas condiciones son suficientes para garantizar que todos los resultados tentativos falsos sean disputados con éxito.

III. PROBLEMAS Y RIESGOS POTENCIALES

A. Mercados Parásitos

Recordemos que un mercado parásito es cualquier mercado que no paga comisiones de reporting a Augur, pero que se resuelve de acuerdo con la resolución del mercado nativo de Augur. Como los mercados parásitos no tienen reporteros a los que pagar, pueden ofrecer el mismo servicio que Augur con comisiones menores. Esto puede tener serias consecuencias para la integridad del protocolo de bifurcación de Augur.

Concretamente, si los mercados parásitos atraen interés de trading hacia ellos en perjuicio de Augur, entonces los reporteros de Augur recibirán menos comisiones. Esto puede provocar presión a la baja en la capitalización de mercado de REP. Si la capitalización de mercado de REP baja mucho, la integridad del protocolo de bifurcación se pone en jaque (Teorema 1). Debido a esto, los mercados parásitos tienen el potencial de amenazar la viabilidad a largo plazo de Augur, y deberían ser rechazados con vehemencia. Nuestra mejor defensa contra los mercados parásitos es hacer que el trading en la plataforma de Augur sea los más barata posible (a la vez que mantenemos la integridad del oráculo), para minimizar la recompensa de correr un mercado parásito.

B. Volatilidad del interés abierto

Incrementos fuertes, repentinos y sorpresivos del interés abierto – como los que se podrían observar durante un evento deportivo popular – resultaría en un rápido incremento en los requerimientos de capitalización de mercado para la integridad del protocolo de bifurcación (Teorema 1). Cuando los requerimientos de capitalización de mercado exceden la capitalización de mercado, hay un riesgo que los atacantes racionales desde el punto de vista económico pueden causar una bifurcación que se resuelva incorrectamente. Mientras que Augur intenta poner presión al alza sobre la capitalización de mercado durante estas situaciones (ver Sección II C), estas presiones al alza son reactivas y se ajustan solamente una vez cada 7 días de la ventana de comisiones.

Merece la pena afirmar, sin embargo, que los especuladores que presencian el repentino incremento del interés abierto pueden comprar REP para anticipar la reacción de la capitalización de mercado al alza, por tanto subiendo la capitalización de mercado de REP, quizás a un punto donde la integridad del protocolo de bifurcación ya no se vea amenazada. El intervalo temporal durante el cual el oráculo es vulnerable puede no ser suficientemente largo para que un atacante se aproveche con éxito

de dicha vulnerabilidad.

C. Fuentes de Resolución Inconsistentes o Maliciosas

Durante la creación del mercado, los creadores del mercado escogen una fuente para su resolución que los reporteros deberían usar para determinar el resultado del evento en cuestión. Si el creador de mercado escoge una fuente inconsistente o maliciosa, los reporteros honestos pueden perder dinero.

Por ejemplo, supongamos que el mercado en cuestión tiene como resultados `A` y `B`, y que el creador del mercado, Serena, ha escogido su propia página web, `attacker.com`, como la fuente para la su resolución. Tras la finalización del evento del mercado, Serena – que es también la reportera designada para el reporte – reporta el resultado `A`, y actualiza `attacker.com` para indicar que el resultado`B` es el resultado correcto. Los reporteros honestos que chequean la página web `attacker.com` verán que el reporte inicial es incorrecto y, durante la ronda de disputa, deberían disputar con éxito el resultado tentativo a favor del resultado `B`. Serena actualizaría`attacker.com` para indicar que el resultado `A` es el correcto, y el mercado entraría entonces en su segunda ronda de disputa. Nuevamente, los reporteros que chequeen `attacker.com`podrán ver que el resultado tentativo (resultado `B`) es incorrecto, y pueden disputarlo exitosamente. Serena puede repetir este comportamiento hasta que el mercado se resuelva. No importa cómo se resuelva este mercado, algunos reporteros honestos perderán dinero.

Existen muchas variaciones de este ataque. Simplemente ignorando los mercados con fuentes de resolución dudosas no es suficiente, porque en caso de que este mercado cause una bifurcación, todos los poseedores de REP tendrán que escoger un universo infantil al cual migrar su REP. Los reporteros deben estar vigilantes contra los mercados con fuentes de resolución dudosas. Estos mercados deberían ser públicamente identificados para que los reporteros puedan coordinarse para asegurar que dichos mercados finalizan como inválidos.

D. Predicciones sobre el oráculo en sí mismo

Los mercados que se tradean sobre el futuro comportamiento del oráculo de Augur pueden tener efectos no deseados sobre el comportamiento del oráculo en sí mismo [11]. Por ejemplo, consideremos un mercado que se tradea en base a la siguiente pregunta, "¿Puede algún reportero designado no acudir a la hora de reportar durante los tres días siguientes anteriores al 31 de Diciembre del 2018?" Las apuestas sobre el resultado `No` en este mercado pueden actuar como un incentivo perverso para que los reporteros designados intencionalmente no acudan a reportar. Si un reportero designado puede comprar suficientes participaciones de `Si` a un precio suficientemente bajo para compensar la pérdida del monto de fianza por el no personarse, entonces pueden intencionalmente no acudir a reportar.

Si la capitalización de mercado de REP es suficientemente grande (Teorema 1) entonces estas peticiones sobre el propio oráculo pueden no ser amenaza para la integridad del protocolo de bifurcación. Sin embargo, pueden afectar negativamente el desempeño de Augur causando retrasos en la finalización de los mercados. Aunque los mercados finalicen correctamente, este tipo de comportamiento es disruptivo y no deseable.

E. Participación incierta en la bifurcación

No podemos saber por anticipado cuanto REP va a ser migrado al universo `Verdadero` durante el periodo de bifurcación de una bifurcación, por tanto no podemos saber anticipadamente si la capitalización de mercado es suficientemente grande para que oráculo tenga integridad (Teorema 1). Nuestra creencia en la integridad del protocolo de la bifurcación no puede ser más fuerte que nuestra creencia en nuestras presunciones sobre la participación honesta mínima requerida durante un periodo de bifurcación. Asumimos que al menos un 20 % del REP migrará al universo infantil`Verdadero` durante el periodo de bifurcación, pero no podemos garantizarlo.

Las bifurcaciones de Augur difieren de las bifurcaciones del blockchain en un importante aspecto: tras una bifurcación en una blockchain, el usuario poseedor de una moneda en la cadena paterna puede ahora tener una moneda en ambas bifurcaciones. Ignorando los ataques repetidos, las bifurcaciones de las blockchains tienen un riesgo pequeño para los usuarios. Tras una bifurcación de Augur, sin embargo, un usuario poseedor del token REP en el universo paterno puede migrar esa moneda únicamente a uno de los universos infantiles. Si el usuario migra su REP a cualquier otro universo diferente del consenso, su token puede perder todo su valor. Por tanto, migrar REP durante el periodo de bifurcación en un proceso de bifurcación, antes de que quede claro que universo infantil ha alcanzado consenso, expone al usuario a riesgo. Este riesgo puede desincentivar la participación durante el periodo de bifurcación de las bifurcaciones contenciosas.

En un esfuerzo para compensar por este riesgo e incentivar la participación durante los periodos de bifurcación, todos los poseedores de REP que migren sus REP durante los 60 días siguientes del comienzo del periodo de la bifurcación reciben un 5 % adicional de REP en el universo infantil al que hayan migrado (ver Sección I C 9). Sin embargo, no podemos saber de forma anticipada si este 5 % de bonus va a ser suficiente para compensar el riesgo e incentivar la participación durante el periodo de bifurcación.

F. Mercados Ambiguos o Subjetivos

Solo los eventos que tengan resultados objetivamente conocidos son adecuados para ser usados en los mercados de Augur. Si los reporteros creen que un mercado no es adecuado para su resolución por la plataforma – por ejemplo, porque es ambiguo, subjetivo, o el resultado nos es conocido a la fecha de la finalización del evento – deberían reportar el mercado como `Inválido`. Si un mercado se resuelve como `Inválido`, los traders son pagados de forma igual en todos los resultados posibles; para los mercados escalares, los traders son pagados en un punto medio entre el precio mínimo y máximo.

Es posible imaginar mercados donde algunos reporteros están seguros que el resultado es A y otros están seguros que el resultado es `B`. Por ejemplo, en el 2006 Tradesports dejo a sus usuarios especular sobre si Corea del Norte lanzaría un misil balístico que cayese fuera de su espacio aéreo antes del fin de Julio de 2006. El 5 de Julio, Corea del Norte lanzo un misil balístico de forma exitosa que cayo fuera de su espacio aéreo, y el evento fue ampliamente reportado por los medios de comunicación en todo el mundo y confirmado por numerosas fuentes de Estados Unidos. Sin embargo, el Departamento de Defensa de Estados Unidos, no confirmó este evento, como se requería en el contrato de Tradesports. Tradesports concluyó que las condiciones contractuales no se habían cumplido y pagó de acuerdo a esta conclusión.[27]

Este es un caso donde el espíritu del mercado – predecir el lanzamiento de un misil – fue claramente satisfecho, pero la letra del contrato del mercado – predecir si el Departamento de Defensa de Estados Unidos confirmaría este lanzamiento – no lo fue. Tradesports, siendo una website centralizada, fue capaz de declarar el resultado del mercado de forma unilateral. Si esta situación ocurriese en un mercado de Augur, los poseedores de REP podrían tener opiniones divergentes acerca de cómo este mercado debiera resolverse, y apilar su REP de acuerdo a esto. En el peor de los casos, esto podría desencadenar una bifurcación donde el REP en más de un mercado infantil mantendría un valor mayor que cero.

ACKNOWLEDGMENTS

Agradecemos a Abraham Othman, Alex Chapman, Serena Randolph, Tom Haile, George Hotz, Scott Bigelow, and Peronet Despeignes por su valioso feedback y sugerencias.

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

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

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

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

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

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

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

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

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

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

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

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

[27] Ver `https://en.wikipedia.org/wiki/Intrade#Disputes` para detalles.

Apéndice A: Tiempo de Finalización y Redistribución

Empezamos con algunas notaciones, definiciones y observaciones.

Definition 5. Para un determinado mercado M, Ω_M es el espacio del resultado (o set de resultados) de M.

Definition 6. Para $n \geq 1$ y $\omega \in \Omega_M$, $S(\omega, n)$ denota la cantidad total apilada en un resultado ω al inicio de la ronda de disputa n. Esto incluye la pila de todos los montantes de fianza disputados con éxito en favor de ω sobre todas las rondas de disputa previas.

Definition 7. Para $n \geq 1$ y $\omega \in \Omega_M$, $S(\overline{\omega}, n)$ denota la cantidad apilada en todos los resultados en Ω_M *excepto para* ω al inicio de la ronda de disputa n:

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

Definition 8. Para $n \geq 1$, A_n denota el montante total apilado en todos los resultados M al inicio de la ronda de disputa n:

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

Observation 3. Se sigue que $A_n - S(\omega, n) = S(\overline{\omega}, n)$.

Definition 9. Para $n \geq 1$, let $\hat{\omega}_n$ denota el resultado tentativo al inicio de la ronda de disputa n. Por ejemplo,$\hat{\omega}_1$ es el resultado reportado por el reportero inicial.

Definition 10. Para $n \geq 1$ y $\omega \neq \hat{\omega}_n$, $B(\omega, n)$ denota la cantidad requerida para disputar con éxito el montante de fianza del resultado ω durante la ronda de disputa n.

Recordemos que la cantidad requerida para disputar con éxito el montante de fianza del resultado ω durante la ronda de disputa n, donde $\omega \neq \hat{\omega}_n$ se da por la Ecuación 1, $B(\omega, n) = 2A_n - 3S(\omega, n)$.

Observation 4. Si un monto de fianza es disputado exitosamente en favor de un resultado ω durante la ronda de disputa n, entonces $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. Esto es, el monto de la disputa exitosa es el único nuevo monto aplicado al resultado ω al final de la ronda de disputa n.

Observation 5. Para todo $\omega \neq \hat{\omega}_n, S(\omega, n-1) = S(\omega, n)$. Esto es, si el monto de fianza de disputa no se completa con éxito a favor del resultado ω, entonces ninguna pila adicional se añade al resultado ω al inicio de la siguiente ronda de disputa. Esto es debido a que todo el montante de disputa no exitosa es devuelto a los usuarios al finalizar la ronda de disputa.

Observation 6. Para todo $n \geq 2, A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$. Esto es, el monto total sobre todos los resultados al inicio de la ronda de disputa es simplemente el monto total del inicio de la ronda de disputa previa más el monto exitoso disputado en la previa ronda de disputa. Todo el monto restante se retorna a los usuarios al finalizar la ronda previa de disputa.

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

Demostración. Supongamos que un mercado entra en una ronda de disputa n, donde $n \geq 2$. Durante la ronda de disputa $n-1$, el resultado $\hat{\omega}_{n-1}$ debe haberse disputado con éxito en favor del resultado $\hat{\omega}_n$. De acuerdo a la Ecuación 1, el tamaño del monto de la fianza de la disputa es $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Usando la observación 3, esto puede reescribirse como

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

Sabemos que el monto de fianza de la disputa fue exitosamente cubierto durante la ronda $n-1$. Usando la observación 4, vemos que $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. La observación 5 nos dice que la cantidad total apilada sobre $\overline{\hat{\omega}_n}$ no cambia de la ronda $n-1$ a la n, $2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$. Así, la Ecuación A1 se reduce a $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$. □

Theorem 3. *Cualquier poseedor de REP que disputa exitosamente un resultado a favor del resultado final de mercado recibirá un 50 % de retorno de la inversión (ROI) en su monto disputado (medido en REP que existe en un universo que corresponde al resultado final del mercado), a menos que el mercado sea interrumpido por otro mercado causando una bifurcación.*

Demostración. Durante una bifurcación, todos los usuarios que exitosamente cubran montos de fianza en las disputas a favor del resultado final del mercado se les otorga (a través de monedas acuñadas durante la bifurcación) un 50 % de retorno de su monto disputado cuando migran su pila al correspondiente universo infantil. Así, en el caso donde el mercado en cuestión ha causado una bifurcación, el teorema es inmediatamente verdadero.

Ahora consideremos el caso donde el mercado en cuestión se resuelve sin causar una bifurcación, y el reporting no es interrumpido por algún otro mercado que cause una bifurcación.

Denotamos al resultado final del mercado como ω_{Final} y suponemos que el mercado se resuelve al final de la ronda de reporting n, donde $n \geq 2$. Esto significa que el resultado tentativo para la ronda n es ω_{Final}, y que el resultado no está disputado con éxito en la ronda n. En otras palabras: $\hat{\omega}_n = \omega_{\text{Final}}$. Entonces por el Lema 2 sabemos que $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$.

Desde que el mercado queda resuelto al final de la ronda n sin ningún monto más añadido a ningún resultado, la ecuación de arriba nos muestra la cantidad final apilada en el resultado final del mercado, ω_{Final}, y la suma de todos los montos en todos los otros resultados del mercado $\overline{\omega_{\text{Final}}}$. Note that there is exactly twice as much stake

on the market's final outcome as there is on all other outcomes combined.

Augur redistributes all stake on the non-final outcomes to users who staked on ω_{Final}, en proporción a la cantidad de REP que apilaron. De esta forma, los usuarios que cubrieron con éxito una disputa del monto de fianza en favor de ω_{Final} obtienen un 50 % de ROI en su REP apilado. □

A continuación consideremos el máximo número de rondas de disputa requeridas para resolver un mercado. La Ecuación 1 es minimizada cuando ω es escogido para ser el resultado no tentativo que empieza la ronda de disputa con el mayor monto apilado. El Lema 2 implica que los resultados no tentativos con el monto mayor conforman el resultado tentativo de la ronda previa de disputa. De esta forma, la cantidad menor posible de disputa puede ser exitosamente cubierta durante la ronda de disputa n, donde $n \geq 2$, es $B(\hat{\omega}_{n-1}, n)$.

En otras palabras, el monto de disputa crece más *despacio* cuando los mismos dos resultados son disputados repetidamente uno en favor de otro. Se sigue que el número de rondas de disputa requeridas para que un mercado inicie una bifurcación se *maximiza* cuando los mismos dos resultados son repetidamente disputados uno a favor del otro. Por consiguiente, podemos determinar la máxima cantidad de rondas de disputa que cualquier mercado atraviesa antes de iniciar una bifurcación encontrando el máximo número de rondas de disputa que pueden ocurrir en el caso particular donde dos resultados de mercado son repetidamente disputados uno en favor de otro. Examinamos el caso a continuación.

Supongamos que toda ronda de disputa exitosa se cubre en favor del resultado tentativo de la ronda de disputa previa. Entonces los dos resultados tentativos que se disputan de forma iterativa uno a favor del otro son $\hat{\omega}_1$ y $\hat{\omega}_2$.

Observation 7. En el caso donde los mismos dos resultados tentativos son repetidamente disputados uno en favor de otro, $\hat{\omega}_n = \hat{\omega}_{n-2}$ para todo $n \geq 3$.

Definition 11. Denotemos d como la cantidad apilada en $\hat{\omega}_1$ durante el reporte inicial. Como el resultado tentativo de cada ronda es conocido en esta situación, podemos simplificar nuestra notación para el tamaño de la disputa. Definamos de forma sucinta B_n para denotar el tamaño del monto requerido para la ronda n, de forma que $B_1 = 2d$ and $B_n = B(\hat{\omega}_{n-1}, n)$ para todo $n \geq 2$. Esto hará más fácil su lectura y comprensión.

Observation 8. En el caso donde los mismos dos eventos tentativos son repetidamente disputados uno a favor del otro, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ for $n \geq 3$. (Esto es, cualquier otro monto de fianza exitosamente disputado se añade al mismo resultado)

Lemma 4. *Si los mismos dos resultados tentativos son repetidamente disputados uno en favor del otro, entonces para todo n donde $n \geq 3$:*

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

Demostración. (Por inducción sobre n)

Supongamos que los mismos dos resultados tentativos son repetidamente disputados uno a favor del otro.

(Caso de base) Por definición y Ecuación 1 hacemos las siguientes observaciones.

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

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, por lo que la parte 1 del lema se cumple para $n = 3$.

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, por lo que la parte 2 del lema se cumple para $n = 3$.

$B_3 = 6d = 3d2^{3-2}$, por lo que la parte 3 del lema se cumple para $n = 3$.

Por tanto, el lema, en su totalidad, se cumple para el caso de base case of $n = 3$.

(Inducción) Supongamos que el lema es verdadero para todo n en el que $3 \leq n \leq k$. Queremos mostrar que el lema se cumple para $n = k+1$. Esto es, queremos mostrar que:

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

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

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

Primero, probamos la parte (a). Por observación 8:

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

Por observación 7 podemos reescribir lo de arriba como:

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

Por la hipótesis de inducción, podemos reescribir $S(\hat{\omega}_{k-2}, k-1)$ como $\frac{2}{3}B_{k-2}$ en la parte derecha para obtener:

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

Por la hipótesis de inducción, podemos escribir B_{k-2} como $3d2^{k-4}$ y B_{k-1} como $3d2^{k-3}$:

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

Aplicando la observación 7 en la parte de la izquierda obtenemos:

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

Finalmente, notemos que la ecuación de arriba y la hipótesis de inducción, $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. Esto prueba la parte (a).

A continuación, probamos la parte (b). Por observación 6:

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

Por la hipótesis de inducción, $A_k = 2B_{k-1}$:

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

Por la hipótesis de inducción, $B_{k-1} = 3d2^{k-3}$, por lo que la parte derecha puede simplicarse como

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

Por la hipótesis de inducción, $B_k = 3d2^{k-2}$ para reescribir la parte derecha como

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

y queda probada la parte (b).

Finalmente probamos la parte (c). Por la Ecuación 1:

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

Por la observación 8, podemos escribir $S(\hat{\omega}_k, k+1)$ como $S(\hat{\omega}_k, k-1) + B_{k-1}$:

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

Por la observación 7, $\hat{\omega}_k = \hat{\omega}_{k-2}$:

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

Por la observación 6, $A_{k+1} = A_k + B_k$:

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

Por la hipótesis de inducción, $A_k = 2B_{k-1}$ y $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$:

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

Por la hipótesis de inducción, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ y $B_{k-2} = 3d2^{k-4}$. Haciendo estas substituciones y simplificando los campos:

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

Esto prueba la parte (c), y concluye la prueba del lema. □

Theorem 5. *Si no se interrumpe por otro mercado causando una bifurcación, un mercado dado puede atravesar por al menos 20 rondas antes de finalizar o causar una bifurcación.*

Demostración. Supongamos que un mercado dado no es interrumpido por otros mercados causando una bifurcación. Entonces, como hemos mostrado arriba, sabemos que el número de rondas de disputa requeridas para que un mercado inicie una bifurcación se maximiza cuando los mismos dos resultados se disputan repetidamente uno a favor del otro.La Parte 3 del Lema 4 nos dice que, en esta situación, el tamaño del monto de fianza requerido para disputar con éxito el resultado tentativo durante la ronda n es dado por $3d2^{n-2}$, donde d es la cantidad del monto total apilado durante el reporte inicial.

Sabemos que las bifurcaciones son iniciadas después de ser exitosamente completada una disputa con un monto total de al menos un 2.5 % de todos los REP existentes, y sabemos que hay 11 millones de REP en circulación. Por tanto, una bifurcación se inicia cuando el monto de fianza cubre con éxito la disputa de un tamaño de 275.000 REP. También sabemos que $d \geq 0{,}35$ REP, porque la cantidad mínima apilada en el reporte inicial es 0,35 REP[28].

Resolviendo $3(0{,}35)2^{n-2} > 275,000$ para $n \in \mathbb{Z}$ da como resultado $n \geq 20$. Por tanto, podemos garantizar que un mercado se resolverá o causará una bifurcación tras al menos 20 rondas de disputa. □

Apéndice B: Asunciones Alternativas & Consecuencias

Recordemos que:

- S es la proporción de REP total que es migrada al universo `Verdadero` en el periodo de bifurcación.
- P es el precio del REP en el universo `Verdadero`
- P_f es el precio del REP que ha sido migrado al universo `Falso` que ha elegido el atacante
- I_a es el interés abierto nativo de Augur
- I_p es el interés abierto parásito

Los mercados de Augur hacen determinadas asunciones sobre S, P_f, and I_p para llegar a definir una capitalización de mercado objetivo. En particular, Augur asume que al menos un 20 % de todo el REP va a migrarse al universo`Verdadero` durante el periodo de bifurcación de una bifurcación, el REP migrado a un `Falso` universo no tendrá un valor no despreciable, y el interés abierto parasito será como mucho la mitad del interés abierto nativo. En otras palabras: $S \geq 0{,}2$, $P_f = 0$, and $I_a \geq 2I_p$. Bajo esos supuestos, el Teorema 1 nos dice que el protocolo de bifurcación tiene integridad cuando la capitalización de mercado de REP es mayor que 7.5 veces su interés abierto nativo.

Puedes hacer tus propios supuestos sobre S, P_f, y I_p para llegar a tus propias conclusiones sobre cuán grande

[28] Ver apéndices E 2 y E 3

la capitalización de mercado debe ser para que el oráculo tenga integridad en la práctica. Enumeramos aquí algunos escenarios alternativos para tu conveniencia.

Scenario 1. Más del 50 % del REP existente migra al universo `Verdadero` durante el periodo de la bifurcación. En este caso P_f y I_p no importan en absoluto. Como $S > \frac{1}{2}$, el protocolo de bifurcación tiene integridad sin importar la capitalización de mercado. No existiría suficiente REP remanente para que un ataque fuese exitoso.

Scenario 2. El 48 % de todo el REP existente migra al universo `Verdadero` durante el periodo de bifurcación, no existen mercados parásitos y el REP migrado a un `Falso` universo no tiene valor. En este caso $S = 0{,}48$, $I_p = 0$, y $P_f = 0$. Bajo estos supuestos, la capitalización de mercado de REP tiene que ser mayor que cerca del doble del interés nativo abierto para que el protocolo de bifurcación tenga integridad.

Scenario 3. 20 % de todo el REP existente migra al universo `Verdadero` durante el periodo de bifurcación, el interés parasito abierto es igual que el interés abierto nativo y el REP migrado al universo `Falso` se tradea por un 5 % del valor del REP migrado al universo `Verdadero`. En este caso $S = 0{,}2$, $I_p = I_a$, y $P_f = 0{,}05P$. Bajo estos supuestos, la capitalización de mercado de REP debe ser más grande que cerca de 10.5 veces el interés abierto nativo para que el protocolo de bifurcación tenga integridad.

Scenario 4. Solo el 5 % del REP existente migra al universo `Verdadero` durante el periodo de bifurcación, el interés parasito es dos veces superior al interés abierto nativo y el REP enviado a un `Falso` universo se tradea a un 5 % del valor del REP enviado al universo `Verdadero`. En este caso, $S = 0{,}05$, $I_p = 2I_a$, y $P_f = 0{,}05P$. Bajo estas circunstancias, la capitalización de mercado de REP debe ser mayor que cerca de 63 veces el interés abierto nativo para que el protocolo de bifurcación tenga integridad.

Apéndice C: Los Efectos del Bonus de la Migración Temprana sobre la Integridad del Protocolo de Bifurcación

Para facilitar la discusión, ignoramos el 5 % de bonus por migración temprana y un término pequeño cuando discutimos la integridad del protocolo de la bifurcación. Aquí revisitamos el Teorema 1 tomando ambas cosas en consideración.

Como antes, la cantidad de REP enviada al universo `Verdadero` durante el periodo de reporting se denota como SM. De esta forma, para que un atacante tenga éxito deben migrar al menos $SM + \epsilon$ REP, que tiene un valor de $(SM+\epsilon)P$ antes de la migración, a un universo `Falso`.

Si un atacante migra $SM+\epsilon$ REP a un `Falso` universo durante el periodo de reporting de una bifurcación, recibirán $1{,}05(SM + \epsilon)$ REP en el universo infantil al que han migrado. Por definición de P_f, el valor de estas monedas viene dado por $1{,}05(SM+\epsilon)P_f$. Por tanto, el coste mínimo para el atacante es $(SM+\epsilon)P-1{,}05(SM+\epsilon)P_f$, que puede ser expresado como $(SM + \epsilon)(P - 1{,}05P_f)$.

Como antes, el máximo beneficio (bruto) para un atacante es dado por I_a+I_p. Por tanto, podemos decir que el protocolo de bifurcación tiene integridad cuando $S > \frac{1}{2}$ o:

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

Resolviendo la desigualdad anterior para la capitalización de mercado PM, podemos ver que el protocolo de bifurcación tiene integridad si y solo si:

1. $S > \frac{1}{2}$ or
2. $1{,}05P_f < P$ y la capitalización de mercado de REP es mayor que $\frac{P(I_a+I_p-\epsilon(P-1{,}05P_f))}{S(P-1{,}05P_f)}$

Como podemos ver, el efecto de una temprana migración del bonus sobre el requerimiento de capitalización de mercado es muy pequeño.

Apéndice D: El Efecto de una Migración Temprana del Bonus sobre el Coste Mínimo de una Bifurcación

Para incentivar una mayor participación durante una bifurcación, todos los poseedores de token que migren su REP durante los 60 días desde el inicio de una bifurcación recibirán un 5 % adicional de REP en el universo infantil al que hayan migrado. Esta recompensa se paga vía inflación de la moneda.

Este bonus puede convertirse en un incentivo perverso si el coste de iniciar una bifurcación es muy bajo. En particular, si un atacante puede ganar más valor del 5 % de bonus de REP del que perdería por iniciar una bifurcación, entonces cabría esperar que las bifurcaciones se sucediesen tan frecuentemente como fuese posible. Este ataque, al que nos referimos como el del ataque para *exprimir la inflación*, no resultaría en que el oráculo reportase incorrectamente, pero si resultaría en bifurcaciones disruptivas sucediendo frecuentemente.

Para prevenir este comportamiento, Augur necesita asegurar que el coste de iniciar una bifurcación es más alto que el máximo valor que puede ser ganado del 5 % del bonus de inflación. Aquí, vamos a derivar un límite bajo sobre el costo de iniciar una bifurcación para prevenir este incentivo perverso.

Vamos a denominar como P_0 al precio del REP antes de la bifurcación y P_1 el precio del REP tras la misma. Vamos a denominar como M_0 el suministro de moneda antes de la bifurcación y M_1 tras la misma. Vamos a denominar S como la proporción de M_0 migrado al universo `Verdadero` durante el periodo de la bifurcación de la bifurcación. Vamos a denominar b como la cantidad de REP que debe ser quemada económicamente (esto es,

apilada sobre un resultado `Falso`) para iniciar una bifurcación. Asumimos que $b > 1$.

Para el propósito de esta sección, hacemos una asunción conservadora que todo el REP migra durante el periodo de la bifurcación es controlado por el atacante. Asumimos además (porque minimiza el coste de este ataque) que todo el REP que migra durante el periodo de bifurcación se migra al universo `Verdadero`.

Bajo estos parámetros, SM_0 es la cantidad de REP migrada durante el periodo de la bifurcación, mientras que $(1 - S)M_0$ es la cantidad de REP *no* no migrada durante el periodo de bifurcación.

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

Cuando un total de SM_0 REP es migrado durante el periodo de bifurcación, un total de $0{,}05SM_0$ REP se crea vía inflación:

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

Enfocándonos solamente en los efectos de la inflación, y para simplificar, estamos asumiendo que la capitalización de mercado tras la bifurcación será la misma que la capitalización de mercado antes de la bifurcación[29]:

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

Substituyendo D1 y D2 en D3 y simplificando nos da:

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

El beneficio (bruto) de un atacante para iniciar una bifurcación y tomando ventaja de la migración temprana del bonus es el valor de su REP migrado tras la migración menos el valor de su REP migrado antes de la migración:

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

Substituyendo D4 en D5obtenemos una expresión alternativa del beneficio (bruto) para el atacante:

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

Recordemos que b es la cantidad de REP que debe ser económicamente quemada para empezar una bifurcación. Así, el coste de iniciar una bifurcación es bP_0. Por tanto, pagar el coste de iniciar una bifurcación aprovechar el bonus de migración temprana merece la pena cuando la siguiente ecuación se satisface:

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

[29] Creemos que esto es conservador. En la práctica, esperamos que la capitalización de mercado caiga tras una bifurcación.

Observando que $P_0 > 0$, y $S \neq -20$, resolvemos para b y vemos que el ataque es rentable cuando:

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

Para prevenir el incentivo perverso, Augur debe arreglar las cosas de tal forma que:

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

Notemos que S se restringe al intervalo $[0, 1]$, vemos que el valor de la parte derecha de la desigualdad D9 se maximiza cuando $S = 2\sqrt{105} - 20 \approx 0{,}4939$. Esto es, este ataque tiene una rentabilidad máxima para el atacante cuando en torno al 49.39 % del REP existente se migra durante el periodo de la bifurcación. Siendo conservadores, usamos este valor para S.[30]

Substituyendo $S = 0{,}4939$ en D9 obtenemos que $b \geq 0{,}012197M_0$. Por tanto, si el coste de iniciar una bifurcación es al menos 1.2197 % del REP existente entonces el ataque de exprimir la inflación no es rentable.

Recordemos que la bifurcación se inicia solo cuando se completa una disputa exitosa del monto de fianza mayor que el 2.5 % del REP existente. Supongamos que este monto de fianza de disputa se completase a favor del evento ω y la bifurcación se iniciase. El resultado ω es verdadero o falso.

Si el resultado ω es falso, entonces al menos un 2.5 % del REP existente se apiló sobre un resultado falso, y por tanto se quemó económicamente hablando. Así que el exprimir la inflación no es rentable cuando ω es falso.

Si el resultado ω es verdadero, entonces el Lema 2 nos dice que al menos un 1.25 % del REP existente (en total) se apiló sobre resultados falsos, y por tanto se quemó económicamente. Así que el exprimir la inflación tampoco es rentable cuando ω es verdadero.

Es por esta razón que el inicio de la bifurcación requiere apilar al menos 2.5 % del REP existente de forma exitosa sobre el monto total de fianza de disputa.

Apéndice E: Ajustes en el Tamaño del Monto de Fianza

El monto de fianza de validación, el monto de fianza del no acudir y la pila acumulada del reportero designado son ajustados dinámicamente basados en el comportamiento de los participantes durante la ventana de comisiones previa. Aquí describimos como ajustamos aquellos valores.

[30] En la práctica, el atacante no puede prevenir que otros participantes migren su REP durante el periodo de bifurcación, y por tanto no puede garantizar que S no exceda su valor ideal de cerca de 0.4939. Sin embargo, desde que nos estamos defendiendo del peor de los escenarios, usamos $S = 0{,}4939$.

Definimos la función $f : [0, 1] \to [\frac{1}{2}, 2]$ como:[31]

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

La función f es usada para determinar el múltiplo usado en estos ajustes, como se describe en las subsecciones de abajo. De forma resumida, si la conducta no deseada ocurre exactamente en un 1 % del tiempo durante la ventana de comisiones previa, entonces el tamaño del monto de fianza queda igual. Si fue menos frecuente, entonces el tamaño del monto de fianza se reducirá hasta como mucho la mitad. Si fue más frecuente, entonces el tamaño del monto de fianza se incrementara hasta como mucho por un factor de 2.

1. Monto de Fianza de Validación

Durante la primera ventana de comisiones tras el lanzamiento, el monto de fianza de validación se establecerá en 0.01 ETH. Entonces, si más del 1 % de los mercados finalizados en la ventana de comisiones anterior son inválidos, el monto de fianza de validación se incrementará. Si menos del 1 % de los mercados finalizados en la ventana de comisiones previa son inválidos, entonces el monto de fianza decrecerá (pero nunca será menor que 0.01 ETH).

En particular, si definimos ν como la proporción de mercados finalizados en la ventana de comisiones previa que fueron inválidos, y b_v a la cantidad del monto de fianza de validación de la ventana de comisiones anterior. Entonces, el monto de fianza de validación para la ventana actual es como máximo máx $\left\{\frac{1}{100}, b_v f(\nu)\right\}$.

2. Monto de Fianza por No Acudir a Reportar

Durante la primera ventana de comisiones tras el lanzamiento, el monto de fianza por no acudir a reportar se establecerá en 0.35 REP. Al igual que el monto de fianza de validación, el monto de fianza por no acudir de REP se ajusta hacia arriba o hacia abajo, con un objetivo de un 1 % de ratio por no acudir con un suelo de 0.35 REP.

Específicamente, definimos ρ como la proporción de los mercados en la ventana de comisiones previa cuyos reporteros designados no acudieron a reportar a tiempo, y definimos b_r como la cantidad del monto de fianza por lo acudir de REP proveniente de la ventana de comisiones anterior. La cantidad de monto de fianza de no acudir de REP para la ventana actual es como máximo máx $\{0{,}35, b_r f(\rho)\}$.

[31] Esta fórmula puede cambiar una vez que se obtengan datos empíricos con los mercados en funcionamiento.

3. Monto del Reportero Designado

Durante la primera ventana de comisiones tras el lanzamiento, el monto de la pila del reportero designado se establecerá en 0.35 REP. El monto de la pila del reportero designado se ajusta dinámicamente de acuerdo a cuantos reportes designados fueron incorrectos (los que no coincidieron con el resultado final del mercado) durante la venta de comisiones previa.

En particular, si definimos δ como la proporción de reportes designados incorrectos durante la ventana de comisiones previa, y definimos b_d como el monto de la pila del reportero designado durante la ventana de comisiones previa, entonces el monto de la pila del reportero designado para la ventana actual es como máximo máx $\{0{,}35, b_d f(\delta)\}$.

Apéndice F: Cambios en el Diseño

Hemos llegado al diseño actual de Augur tras tres años de investigación e iteración. El diseño que ha emergido de este proceso difiere substancialmente de la visión expuesta en nuestro Whitepaper antiguo [12]. Aquí, discutimos tres cambios significativos así como la explicación de estos cambios.

1. Reporting Fees

En el diseño antiguo, el creador de mercado establecía una comisión de trading que se dividía al 50/50 entre reporteros. En el diseño actual, las comisiones para el creador de mercado y los reporteros son independientes, y las comisiones de los reporteros se ajustan dinámicamente por Augur para mantener el sistema seguro.

Las comisiones pagadas a los reporteros impactan en el precio de REP, lo cual tiene un efecto directo en la seguridad del protocolo de bifurcación (Teorema 1). Si las comisiones pagadas a los reporteros son muy bajas, entonces la integridad del oráculo está en riesgo. Si las comisiones pagadas a los reporteros son muy altas entonces la amenaza de mercados parásitos aumenta. Por tanto, es importante que las comisiones pagadas a los reporteros sean ajustadas de forma dinámica para mantener la seguridad de Augur, en vez de que sean decididas de forma arbitraria por los creadores de los mercados.

Separando las comisiones de los reporteros de las elecciones de los creadores de los mercados nos asegura también que los reporteros (y por tanto la integridad del protocolo de bifurcación) no sean dañados por la competencia entre los creadores de mercado para crear mercados con las comisiones más baratas posibles. Los mercados de calidad y los reportes de calidad tienen que ser medidos y recompensados por separado. La competencia debe permitir dirigir las comisiones del creador de mercado hacia cero, sin arrastrar a las comisiones pagadas a los reporteros también.

2. Comisiones de Trading

En el antiguo diseño, las comisiones se recogían por los traders en cada trade. En el nuevo diseño, las comisiones son recogidas por los traders solamente cuando se liquidan directamente con los contratos de los mercados.Este cambio fue hecho, en parte, debido a que Augur no puede actuar como un policía en el trading fuera de la plataforma. Las participaciones de los resultados de los mercados son simplemente tokens, que se pueden tradear libremente por parte de los usuarios. Como recoger las comisiones de cada trade no es factible, Augur las recoge solo cuando los traders liquidan directamente con los contratos de los mercados de Augur. Un beneficio añadido de este enfoque es que reduce las comisiones medias pagadas por los traders, lo cual debería hacer a Augur más competitivo.

3. Universos

En el antiguo diseño, solamente había una "versión" de REP, y el circulante total estaba fijado. En el diseño actual, REP puede bifurcarse en muchas versiones diferentes (universos), cada uno de los cuales puede acabar con más o menos REP total que la versión original. Si la bifurcación es contenciosa, el circulante de REP en cada universo infantil podría ser solo una fracción del circulante total en el universo paterno. En una bifurcación no contenciosa, la migración temprana del bonus a los participantes de la bifurcación podría resultar en un universo infantil que tenga más REP en total que su universo paterno.

Las nuevas versiones de REP engendradas por una bifurcación son todo tokens diferentes, cada uno con su propio precio y circulante, y los proveedores de servicios deberían tratarlos como tales.Cuando Augur se lance por primera vez, habrá un solo universo (el universo de génesis) y una sola versión de REP, como existe hoy en día. Sin embargo, tan pronto como ocurra una bifurcación, la versión única del REP se partirá en muchas otras versiones: por ejemplo, un mercado bifurcado con resultados `A` y `B` engendraría nuevos tokens REP-`A`, REP-`B`, y REP-`Inválido`. Los monederos y los exchanges que soporten REP tendrían ahora cuatro tipos de versiones diferentes de REP que podrían (en teoría) soportar: el – REP-`de la génesis` (el REP de la versión original, que ahora quedaría bloqueado), el REP-`A`, REP-`B`, y REP-`Inválido`.[32]

El circulante total de REP en cada universo infantil depende de cuánto REP haya migrado a él, y cuando ocurra esta migración. Migrar REP durante una bifurcación, antes que este claro que universo infantil haya alcanzado consenso, expone al usuario a una pequeña (pero no inexistente) cantidad de riesgo (ver Sección III E), que puede desincentivar la participación durante la bifurcación en periodos de bifurcación contenciosos. Para incentivar esta participación, los usuarios tienen que ser compensados por su riesgo.

Los usuarios que no quieran participar en el periodo de la bifurcación de una bifurcación pueden ser penalizados perdiendo una parte de los REP que poseen. De hecho, el viejo diseño tenía un mecanismo de "úsalo o piérdelo" que penalizaba a los no participantes como si fuesen reporteros que hubiesen reportado incorrectamente. Sin embargo, castigar a los usuarios que no participan crea problemas de usabilidad significantes. Los usuarios castigados que no participan son problemáticos para los monederos y los exchanges que son quienes custodian los REP de sus clientes. En caso de bifurcación, los exchanges deberían necesitar migrar los REP de sus clientes hacia algún universo infantil durante el periodo de la bifurcación, o perder alguna proporción de los REP que poseen.[33]

En vez de penalizar a los no participantes, los participantes de las bifurcaciones que migren durante el periodo de bifurcación son recompensados con la emisión de un 5 % de bonus en el universo infantil al cual han migrado. Si el 4.762 % del REP (o más) migran a un universo perdedor – del cual de 1.25 % a 2.5 % ya ha sido comprometido en el monto total de la disputa – entonces todos los universos tendrán un circulante total de REP menor que el del universo paterno.

---

[32] En términos prácticos, los proveedores de servicios pueden encontrar como lo más fácil (y menos disruptivo para sus clientes) el incentivar a participar en la bifurcación, y entonces simplemente soportar el universo ganador una vez la bifurcación se ha resuelto.

[33] También encontramos, en términos prácticos, que el código de programación de los contratos inteligentes requerido para implementar las recompensas del proceso de bifurcación usando solo un proceso de redistribución era inusualmente complejo. La complejidad de los códigos de los contratos es en sí mismo una amenaza para la seguridad, por lo que hemos intentando simplificar la implementación donde fuese posible.