Libro Amarillo: Nebulas Rank

Título original: ***Yellow Paper: Nebulas Rank***

Nebulas Research

June 2018
Version:1.0.3

Traducción: abril de 2019
Versión: 1.0.0

Tabla de contenidos

1 Introducción

A medida que las tecnologías blockchain evolucionan, más y más industrias se benefician de la *descentralización*, que es el corazón de los sistemas blockchain. Por ejemplo: Bitcoin, el primer proyecto blockchain en salir a la luz pública, ha demostrado su importancia para los activos digitales, mientras que Ethereum demostró cuán importante es la descentralización para las DApps. A medida que el tiempo corre, hay más y más proyectos blockchain estudiando cómo aprovechar este fenómeno.

Obviamente, la columna vertebral de la descentralización en blockchain reside tanto en su apertura y en su capacidad inherente de brindar anonimato.

Aun así, el anonimato y la apertura obstaculizan la emergencia de mediciones de valuación [1]. Existen dos aspectos que contribuyen a esta obstrucción. En primer lugar es difícil inferir si un grupo de cuentas pertenecen a la misma persona, haciendo casi imposible construir un mecanismo similar al de las cookies HTTP [2] o utilizar tecnologías tradicionales de análisis de datos para comprender las características de los usuarios. En segundo lugar, la apertura de los blockchains los hace vulnerables a la manipulación, en especial a la medición de valor. Un atacante podría fácilmente obtener detalles sobre los mecanismos de la medición de valor, y descubrir debilidades en el sistema. Esto difiere en gran medida de las mediciones de valor tradicionales, que son cerradas o independientes.

Creemos que la medición del valor efectivo es la base de la prosperidad de los blockchains. Tanto la falta de mediciones del valor como su ineficacia pueden limitar el potencial de los blockchains a sólo unos pocos usos prácticos.

En primer lugar, necesitamos una metodología para cuantificar el valor de los datos, las aplicaciones y las cuentas en los blockchains. La cooperación en los blockchains se sigue ampliando, y los requisitos de eficiencia siguen creciendo. Sin mediciones de valor, dicha colaboración puede verse afectada negativamente.

En segundo lugar, la tecnología de blockchains se encuentra en una fase muy temprana de desarrollo y uso, y el valor de los datos y activos en ellos todavía está bajo tierra y esperando ser encontrado. Las mediciones efectivas de valor permitirán potenciar más aplicaciones y crear más escenarios de uso; préstamos, crédito, búsqueda de datos, recomendaciones personalizadas e interacción entre blockchains.

En tercer lugar, los incentivos, que se basan en medidas de valor, son necesarios para mantener un ecosistema saludable en el blockchain. Sin mediciones efectivas de valor, los incentivos pueden llevar al blockchain a un esquema de corrupción, y a un

eventual colapso.

Como conclusión, una medida efectiva de valor que satisfaga las necesidades de los blockchains debe ser:

- **Veraz.** La valuación necesita medir con certeza algunas características del sistema blockchain, y por lo tanto, debe ser fiable;
- **Equitativa.** La medición necesita ser resistente a las manipulaciones;
- **Diversa.** Existen diferentes requerimientos de valuación para las distintas aplicaciones en el blockchain, de modo que un algoritmo de valuación de calidad debe ser capaz de cubrir distintos escenarios.

Creemos que el Nebulas Rank será una medida de valor efectiva para los blockchains.

En cuanto a veracidad, después de considerar muchas métricas diferentes, elegimos Nebulas Rank como la cuantificación de la contribución de una cuenta al sistema de blockchains.

Creemos que las criptodivisas deben tener los mismos atributos que el dinero; en particular, funcionar como medio de cambio, como depósito de valor y como unidad de contabilidad. Los blockchains en sí son sistemas económicos y la teoría monetaria clásica todavía tiene vigencia. Además, creemos que el valor de las criptodivisas proviene de su liquidez. Específicamente hablando, cada transacción entre usuarios aumenta la liquidez de las criptodivisas, y las dota de valor eventualmente. Por lo tanto, las transacciones en un blockchain son fuentes de datos efectivas y naturales para una medición efectiva del valor.

Para evaluar la efectividad de Nebulas Rank, calculamos la suma del valor NR de todas las cuentas en Ethereum, y lo comparamos con la capitalización de mercado dada por `coinmarketcap.com`. Nuestra evaluación muestra una fuerte correlación entre ellos, aproximadamente 0.84. Esto significa que Nebulas es eficaz para medir la contribución de las cuentas a nivel micro, mientras que también es capaz de medir el valor de los sistemas blockchain a nivel macro.

En cuanto a equidad, desarrollamos una función especial para generar resistencia a la manipulación; nuestros análisis demostraron que su performance es resistente a ellas.

Basándonos en la teoría de Nebulas Rank, podemos dividir Nebulas Rank a su vez en Core Nebulas Rank y Extended Nebulas Rank, con el fin de cubrir distintos escenarios y aplicaciones.

Core Nebulas Rank se define como el algoritmo que calcula la contribución de una cuenta al sistema blockchain entero durante un periodo de tiempo dado. Tal cálculo

involucra dos factores: la participación media de una cuenta durante ese periodo, y el grado de entrada y salida de la cuenta durante ese lapso.

Extended Nebulas Rank es adecuado para diferentes aplicaciones y escenarios, y se basa estrechamente en Core Nebulas Rank. Por ejemplo, podemos mostrar cómo valuar contratos inteligentes basándonos en Core Nebulas Rank; también podemos mostrar cómo extender Core Nebulas Rank a un vector multidimensional.

Más allá de la teoría y la metodología de Nebulas Rank, también presentamos nuestra consideración sobre cómo implementar Nebulas Rank, lo que incluye de qué manera se introducen los puntajes de valuación en el blockchain, cómo actualizar su algoritmo, y los planes a futuro para el mismo.

> Nota: el contenido de este libro amarillo podría diferir de las descripciones vertidas en nuestro libro blanco (concretamente de la versión 1.02, lanzada en abril de 2018) [3]. Esto es así debido a que el algoritmo descripto está sometido a un permanente desarrollo y mejora. Ahora tenemos más confianza y capacidad para hacerlo más riguroso. Utilizamos un formato distinto (como este párrafo) para enfatizar las actualizaciones relevantes presentadas en este documento.

2 Antecedentes

En este capítulo presentamos los antecedentes del blockchain y la tecnología asociada. Debido a la ausencia de mediciones de valor, discutiremos la implementación de algoritmos de valuación tradicionales en el área de blockchain, como así también sus desventajas.

2.1 Estado de desarrollo de blockchain

Satoshi Nakamoto publicó su libro blanco de Bitcoin [4] en octubre de 2008. Como una de las primeras aplicaciones de la tecnología blockchain, Bitcoin es el ejemplo más impactante del concepto de un *sistema de criptodivisa descentralizada*. La producción de Bitcoin depende de la ejecución de un algoritmo especial por parte de una gran cantidad de computadoras, en contraposición a cualquier otra organización, lo que garantiza la consistencia del sistema de contabilidad distribuida.

Mediante el uso de un lenguaje específico de *scripting*, Bitcoin puede ser utilizado para realizar pagos a terceros, como un sistema eficiente de micropagos, y más. En tiempos más recientes, emergió una ola de experimentos con origen en la plataforma Bitcoin, que incluyeron características más complejas que la primitiva criptodivisa

p2p. Por ejemplo: Namecoin [5] creó un sistema DNS distribuido, y Open Assets [6] implementó el concepto de *monedas coloreadas*; en ambos casos se introduce el concepto de activos inteligentes siguiendo la trazabilidad de Bitcoin.

Desafortunadamente, el lenguaje de *scripting* de Bitcoin tiene muchos defectos de diseño que dificultad su aplicabilidad, como la falta de instrucciones y el hecho de no ser Turing-completo, algo que limita su utilidad.

Con el desarrollo de la tecnología de blockchain, se han unido más sucesores, quehan tratado de ampliar las funciones relacionadas a distintas aplicaciones. El caso más significativo es el de Ethereum [7], que introduce el concepto de contratos inteligentes y Turing-completos, lo que abre una nueva dimensión para el campo de las aplicaciones.

Los contratos inteligentes son contratos ejecutados mediante métodos técnicos en el sistema blockchain. El contrato inteligente de la red Ethereum corre en la máquina virtual Ethereum (EVM), que no depende de ninguna autoridad centralizada; así, la EVM garantiza la consistencia de sus resultados, así como el de los contratos inteligentes, mediante un algoritmo de consenso.

Cada persona es libre de crear aplicaciones distribuidas (DApps) con funciones complejas basadas en el contrato inteligente de Ethereum. Estas DApps proporcionan soluciones a varios campos más allá de las transacciones básicas como el voto, el *crowdfunding*, los préstamos, los derechos de propiedad, etc. Sin embargo, incluso cuando Ethereum extiende las posibles aplicaciones de blockchain, no existen aplicaciones revolucionarias en la plataforma Ethereum debido a la falta inherente de capacidad de medición de valor.

Para todo sistema que da soporte a contratos inteligentes existen dos tipos de cuentas: cuentas de propiedad externa (EOA) y cuentas de contratos inteligentes, y ambas carecen de un sistema de medición de valor razonable. Mientras tanto, existe información de gran valor escondida en el proceso de invocación de un contrato inteligente. Esa información contiene más dimensiones que los datos transaccionales tradicionales, y no es posible evaluarla mediante mediciones de valor clásicas.

A principios de 2015, a Chris Skinner se le ocurrió la idea de una *web de valor* [8], señalando que un ecosistema de valor debería incluir intercambios de valor, almacenes de valor y sistemas de gestión de valor. Skinner señaló que existen claras diferencias entre las plataformas de criptodivisas y la sociedad tradicional en cuanto a medición del valor, lo que plantea un desafío para evaluar el valor de los datos y la información en las plataformas de criptodivisas.

2.2 Algoritmos de valuación de nodos basados en grafos

La nueva generación de proyectos blockchain, tales como Ethereum, construyeron un ecosistema complejo, que fue más allá de una simple plataforma de criptodivisas. No obstante, no hay un método razonable para valuar las entidades dentro del blockchain. Por ejemplo, no podemos decir con certeza qué entidad posee la mayor contribución al sistema blockchain, ni tampoco sabemos a ciencia cierta cómo medir ese parámetro.

El algoritmo PageRank [9] es una medida típica de reputación en internet. Como algoritmo principal de Google, PageRank fue propuesto para resolver el problema de clasificación en el análisis de enlaces web; luego de realizar investigaciones basadas en él, fue ampliamente utilizado en diversos campos tales como evaluar la importancia de *papers* académicos, en *web crawlers*, en la extracción de palabras clave, en la evaluación de la reputación de usuarios en redes sociales, etcétera.

Algunas investigaciones ponen el foco en el posible uso de PageRank en blockchains. Fleder, Kester, Pillai, et al. demostraron que PageRank se puede utilizar para el descubrimiento de cuentas Bitcoin y para analizar la actividad de dichas cuentas[10]. Sin embargo, el método que plantean es sencillamente trabajo analítico manual con la asistencia de PageRank.

Tal como el algoritmo de valuación original creado para su uso en la web 2.0, PageRank sufre de limitaciones inherentes para la evaluación de la reputación *online*.

Desde entonces han surgido más investigaciones que mejoran PageRank, siendo una de las más famosas *LeaderRank*. Este algoritmo mejora la probabilidad de transición introduciendo nodos *ground* y enlaces bidireccionales ponderados en lugar de utilizar la misma probabilidad de transición en PageRank, lo que hace que los nodos tengan una probabilidad de transición diferente tanto dentro como fuera. Sin embargo, sigue habiendo limitaciones: LeaderRank cuenta la reputación de forma iterativa tomando únicamente en consideración la relación entre los nodos, mientras carece de la capacidad de evaluar las actividades de los usuarios.

También es importante destacar que los algoritmos PageRank no son resistentes a los ataques Sybil[12], que es la estrategia por la cual un adversario subvierte el sistema de reputación dentro de una red simétrica creando un gran número de identidades seudónimas.

El trabajo más relevante con Nebulas Rank es NEM [13]. A diferencia de los algoritmos de consenso como Prueba de Trabajo (*Proof-of-Work* o PoW) o Prueba de Participación (*Proof-of-Stake* o PoS), NEM adopta el protocolo de consenso llamado Prueba de Importancia (*Proof-of-Importance*, o PoI) y, además, NCDawareRank [14] como su

algoritmo de clasificación. NCDawareRank hace uso del efecto de clusterización de la topología de red con un algoritmo de clusterización basado en el algoritmo SCAN [15] [16] [17].

Aunque la estructura de la comunidad está representada en el grafo de transacciones y debería ser útil para manejar los nodos de spam, esto no garantiza que todos los nodos de la cadena de bloques controlados por una entidad en el mundo real estén mapeados en un solo cluster, lo que da lugar a la manipulación.

2.3 Resistencia a la manipulación

La habilidad de resistir la manipulación, (veracidad), es la meta más significativa —y la que representa un mayor desafío— para Nebulas Rank.

Hopcroft et al. hallaron que PageRank falla al evaluar la reputación de un usuario sometido a manipulación [18]. Zhang et al. señalan que un adversario puede reducir efectivamente la reputación de los usuarios no-Sybil aún si se construye un índice de evaluación de la reputación del nodo.[19].

Esto se debe en gran medida a que los algoritmos de PageRank funcionan en base a la topología de la red, mientras que al adversario le basta con crear una imagen de la red para obtener la misma reputación, o una mayor. [20] [12].

En cuanto a los sistemas blockchain, los métodos más comunes de manipulación incluyen:

1. Transferencia en lazo. El atacante realiza transferencias a lo largo de una topología lazo, lo que permite que el mismo dinero circule repetidamente sobre las mismas aristas. Al hacerlo, el atacante espera incrementar la ponderación de las aristas relacionadas;

2. Transferencia a direcciones aleatorias, de tal forma que como resultado se incrementen los egresos del nodo Sybil y la propagación de sus fondos;

3. Formar un componente de red independiente con direcciones controladas por el atacante, de tal modo que éste pretenda ser un nodo central;

4. Interactuar frecuentemente con direcciones de casas de cambio importantes, es decir, transferir los mismos fondos una y otra vez con una dirección perteneciente a una casa de cambios importante, con el fin de que el atacante logre una mejor posición estructural en la red.

Tomamos en cuenta estos y otros métodos para garantizar la equidad de Core Nebulas Rank durante la etapa de diseño.

3 Modelo económico

Las criptodivisas están dotadas de importancia económica, ya sea como medios de transacción o como activos inteligentes. Por lo tanto, un modelo económico razonable nos puede ayudara establecer un estándar de medición de valor en el blockchain, lo que es también el objetivo de Core Nebulas Rank.

Este capítulo presenta en primer lugar la representación matemática de las criptodivisas y luego las analiza mediante un modelo monetario simple pero reconocido. Durante el análisis, presentaremos Core Nebulas Rank como una parte importante de la argumentación.

3.1 Representación de las criptodivisas

La mayor diferencia entre las criptodivisas y la economía tradicional es que todas las transacciones con criptodivisa poseen trazabilidad. Esto provee fuentes de datos cruciales para que podamos analizar el impacto de cada transacción sobre el sistema económico en su conjunto.

En general, un sistema de cripptodivisa se puede definir como un par $(\mathcal{L}, \mathcal{U})$, donde $\mathcal{L}$ denota el sistema contable, y $\mathcal{U}$ es el conjunto de sus usuarios. Más aún, el sistema contable puede ser descripto como una tripla, de este modo:

$$\mathcal{L} = (\mathcal{A}, \mathcal{D}, \mathcal{T}) \tag{1}$$

donde $\mathcal{A}$ representa el conjunto de cuentas, $\mathcal{D}$ es el conjunto de balances iniciales de cada cuenta, y $\mathcal{T}$ es el conjunto de transacciones. Cada transacción se puede registrar como un cuaternión de esta forma:

$$\mathcal{D} = \{a \to d, a{\in}\mathcal{A}, d{\in}R^*\} \tag{2}$$

$$\mathcal{T} = \{(s, t, w, \tau)\} \tag{3}$$

donde $a \to d$ representa el balance d correspondiente a la cuenta a (d es un número real positivo; en otras palabras, no tomamos en consideración las cuentas con balance cero). s, t, w y τ representan la cuenta origen, la cuenta destino, el monto y el tiempo de una transacción. respectivamente.

Una cuenta está controlada por un usuario relevante, quien propone una transacción con otra cuenta, lo que se puede escribir como:

$$u \texttt{ dom } a. \quad u \in \mathcal{U}, a \in \mathcal{A} \tag{4}$$

Por un lado, un usuario puede controlar múltiples cuentas:

$$A(u) = \{\forall a \in \mathcal{A} : u \texttt{ dom } a\} \tag{5}$$

Por otro lado, una cuenta sólo puede ser controlada por un único usuario:

$$\forall u_1, u_2 \in \mathcal{U} : A(u_1) \cap A(u_2) = \phi \tag{6}$$

Nótese que el modelo descrito arriba es una simplificación razonable de cualquier sistema de criptodivisas.

En este modelo no distinguimos los datos dentro del blockchain de los datos fuera del mismo, y no introducimos ni el precio de transacción ni las invocaciones de contratos inteligentes, etc. Además, las cuentas de las casas de cambio son de un tipo específico. En términos generales, las transacciones en una casa de cambio se pueden dividir en dos categorías: transacciones normales que se registran en el blockchain y transacciones internas que se registrarán en una base de datos centralizada y propietaria. Esto nos lleva a un resultado en el que no disponemos de las transacciones internas de la casa de cambio si sólo obtenemos los datos del blockchain.

Sin embargo, si las transacciones internas son accesibles con la cooperación de la casa de cambio, podemos mapear la cuenta de una casa de cambio en múltiples cuentas, de modo de utilizar el modelo descrito anteriormente.

3.2 Modelo de criptodivisa

A pesar de que las criptodivisas difieren de la moneda comercial y el dinero fiduciario, la teoría monetaria clásica sigue teniendo un significado práctico hoy en día. Como una forma moderna de dinero nacida de una nueva entidad económica [21], las criptodivisas nacieron con los atributos del dinero tradicional tres de sus funciones: sirven como medio de cambio, como ahorro, y como unidades de contabilidad.

En virtud de ello, estableceremos un modelo monetario simple y clásico que ayude

a comprender el significado físico de Nebulas Rank.

Primero, trataremos de brindar un indicador para medir el *factor de velocidad* dentro del ecosistema de las criptodivisas.

Otro concepto esencial que necesita ser diferenciado del *factor de velocidad* en la economía es la *liquidez*.

La *Liquidez* describe el nivel de dificultad que existe en cambiar los activos por otro medio de cambio. Como en economía el dinero en sí mismo es un medio de cambio, podemos definir el dinero como uno de los activos con mayor *liquidez*.

> En el Libro Blanco Técnico de Nebulas [**?**], utilizamos la palabra *liquidez* frecuentemente. No obstante, no existe una definición rígida para tal concepto, cuyo significado es muy amplio incluso en Economía. Por ejemplo, en *The New Palgrave: A Dictionary of Economics* las entradas que explican la *liquidez* incluyen tres aspectos totalmente distintos. R. S. Kroszner indica que se crearon 2795 papers independientes que mencionan la palabra *liquidez* durante los últimos seis meses, cada uno de los cuales, sin embargo, planteó una declaración diferente [22]. El concepto de *liquidez* en este libro amarillo se refiere a la **velocidad del dinero**, queriendo significar con esto *los tiempos de rotación de una unidad monetaria durante un determinado período de tiempo*.

Utilizamos el concepto de *velocidad del dinero* para representar la tasa de rotación de las criptodivisas [23], es decir, el volumen de negocios de una unidad monetaria durante un determinado período de tiempo (un día en este documento), que se representa con el símbolo V. Según la teoría cuantitativa clásica del dinero, la ecuación se expresa de la siguiente manera:

$$M \times V = P \times Y \tag{7}$$

donde M, V, P y Y representan la cantidad monetaria total del sistema económico, la velocidad del dinero, el nivel de precios (medido por el dinero de la producción económica unitaria, por lo tanto el precio del dinero es $\frac{1}{P}$), y la producción económica real (PBI real) respectivamente. La ecuación muestra que el producto de la cantidad monetaria y la velocidad del dinero es igual al producto del precio de los bienes y su producción.

En cuanto a la cantidad monetaria M, Nebulas es similar a Ethereum en cuanto a que la cantidad monetaria mantiene un crecimiento constante (el porcentaje adicional

de emisión de dinero de Nebulas —NAS— se establece en el 4% en la actualidad), que es diferente al caso de Bitcoin en que su cantidad monetaria total será estable una vez que el total de 21 millones de monedas hayan sido creadas. La velocidad del dinero V puede ser descrita como la relación entre la cantidad monetaria circulante y la oferta monetaria. Como resultado, el Ecuación **??** puede expresarse más adelante como:

$$(M + \Delta m) \times \frac{\sum_{(s,t,w,\tau)\in\mathcal{T}} w}{M} = P \times Y \tag{8}$$

where Δm is the additional monetary supply.

En términos de nivel de precios P, es aceptable que el valor del precio esté determinado por la relación entre la oferta y la demanda monetaria, tanto por las teorías clásicas del dinero como por los Nuevos Modelos Keynesianos. A largo plazo, el nivel total de precios se ajustará para garantizar que la oferta y la demanda monetarias se mantengan en el punto de equilibrio.

Sin embargo, el nivel total de precios no siempre se mantiene en el punto de equilibrio entre la oferta y la demanda monetaria a corto plazo. En un sistema económico sano, la tasa de crecimiento del precio es tradicionalmente menor que la de la velocidad del dinero. Al aumentar la oferta monetaria (en otras palabras, al reducir las tasas de interés), tanto el nivel de precios P como las demandas de bienes y servicios Y aumentarán mientras tanto. Por otro lado, la velocidad de aumento del nivel de precios debe ser controlada, para impedirle a los usuarios retener en su poder la criptodivisa durante mucho tiempo, reduciendo así la velocidad. La razón por la que los usuarios retienen en su poder la criptodivisa es que esperan que, con el tiempo, el precio de la misma se incremente.

Con respecto a la producción económica real, los economistas la representan tradicionalmente como PBI real, es decir, *como medida monetaria del valor de mercado de todos los bienes y servicios finales producidos en un período de tiempo*. Creemos que el valor de la criptodivisa se basa en su velocidad, es decir, que cada transacción contribuye en cierta medida al agregado económico total. En otras palabras, una vez que una transacción tiene lugar, aumenta la velocidad de la criptodivisa, la aprobación de los usuarios y hasta cierto punto, la lealtad de estos para con aquella. Como resultado, pensamos que Y en el Ecuación 8 se compone de cada transacción. Dado que los sujetos de un sistema económico son las cuentas, también podemos explicar Y como las transacciones emitidas por cada cuenta como se indica a continuación:

$$Y = \sum_{a \in \mathcal{A}} \mathcal{C}(a) \tag{9}$$

donde $\mathcal{C}(a)$ representa la contribución hecha por una cuenta a al producto económico total, a saber, Core Nebulas Rank.

El desarrollo de las criptodivisas depende del desarrollo continuo de la comunidad. Por lo tanto, consideramos que la cuantificación de la contribución de cada cuenta es la base para diseñar un mecanismo de incentivos razonable. Basándonos en este hecho, el sistema económico puede crear incentivos explícitos (por ejemplo, *Prueba de Devoción* tal como se define en el Libro Blanco Técnico de Nebulas) o incentivos implícitos (por ejemplo, los resultados de búsqueda ordenados proporcionados por los motores de búsqueda). La directiva y los incentivos primitivos de la criptodivisa se refieren a la emisión adicional de dinero, que es un factor que las diferencia de las teorías monetarias tradicionales.

4 Core Nebulas Rank

Core Nebulas Rank se utiliza para medir las contribuciones de un usuario en referencia a la economía en su conjunto **durante un periodo de tiempo dado**.

El cálculo preciso es relativamente complicado, por lo que proponemos un algoritmo de aproximación para lograrlo. En este algoritmo de aproximación consideramos dos factores críticos: la *acuñación* y la información de la posición de la cuenta en la red de transacciones. La siguiente sección de evaluación proporciona evidencia de la precisión de nuestro algoritmo de aproximación.

Utilizamos el historial de transacciones de la *mainnet* durante un cierto período de tiempo como fuente de datos de Core Nebulas Rank.

Todas las transacciones durante un periodo de tiempo $[t_0 - T,\ t_0]$ pueden ser especificadas como un conjunto:

$$\Theta(t_0) = \{(s, t, w, \tau) \mid t_0 - T \leq \tau \leq t_0\ \wedge\ w > 0 \wedge s \neq t\} \tag{10}$$

Con base en $\Theta(t_0)$, podemos definir un grafo dirigido ponderado; el nodo hace referencia a la dirección de una cuenta, la arista que conecta el nodo s con el nodo d representa una transacción, la ponderación de la arista es w, el tiempo de la arista es τ.

Para una cuenta $a \in \mathcal{A}$, el cálculo de Core Nebulas Rank $\mathcal{C}(a)$ se basa en $\Theta(t_0)$, que se puede representar como:

$$\mathcal{C}(a) = \Omega(\beta(a)) \times \Psi(\gamma(a)) \tag{11}$$

$\beta(a)$ es la media de la participación (*stake*) de la cuenta a en un periodo dado; $\gamma(a)$ es la valuación de ingresos y egresos de la cuenta a en un periodo dado.

> A diferencia de los métodos de cálculo para Core Nebulas Rank definidos en el Libro Blanco Técnico de Nebulas [3], hemos hecho algunas actualizaciones que detallamos a continuación:
> 1. Dejamos de utilizar los montos de las transacciones K más altas como factor de ponderación al construir los grafos de transacciones;
> 2. Ya no dependemos de la ponderación de los nodos de LeaderRank para obtener la importancia del nodo.
>
> Primero, eliminamos los bucles de transacción antes de calcular la valuación de los ingresos y egresos β, de modo que resistir un ataque de transacciones cíclicas o en bucle. Al mismo tiempo aún tomamos en cuenta la fuerza de la arista. Para ciertos casos de grafos de topología homogénea, PageRank y otras funciones simétricas (como LeaderRank) han probado no ser capaces de resistir ataques Sybil [20]. En este libro amarillo ya no utilizamos la estrategia de valuación de tipo topológica; en su lugar, proponemos un cálculo asimétrico Ecuación 21 que es efectivo para reducir las recompensas fingiendo los nodos de baja participación en § 4.3.

Abajo discutiremos tres problemas en Ecuación 11: Participación Media de Cuenta $\beta(a)$, Valuación de Ingresos y Egresos $\gamma(a)$, y la selección de la función Ω y Ψ.

4.1 Participación Media de Cuenta $\beta(a)$

En el periodo de tiempo de $[t_0 - T, t_0]$, existen n bloques en el sistema blockchain, marcados como:

$$B_0, B_1, \ldots, B_n$$

B_i se refiere al bloque padre de B_{i+1}. Para la cuenta $a \in \mathcal{A}$, el balance de la cuenta al final de cada bloque es:

$$d_0^a, d_1^a, \ldots, d_n^a$$

Podemos obtener una nueva lista ordenando los elementos en orden ascendente:

$$d^a_{(0)}, d^a_{(1)}, \ldots, d^a_{(n)}$$

donde $d^a_{(i)} < d^a_{(i+1)}, 0 \leq i \leq n-1$, de esa forma, $\beta(a)$ se puede expresar como:

$$\beta(a) = \begin{cases} d^a_{(k)} & \text{for} \quad n = 2 \times k, k = 1, 2, 3, \ldots \\ (d^a_{(k)} + d^a_{(k+1)})/2 & \text{for} \quad n = 2 \times k + 1, k = 1, 2, 3, \ldots \end{cases} \tag{12}$$

La participación media de la cuenta representa la acuñación de una cierta forma, lo que significa que la cuenta necesita mantener su participación por más de la mitad del periodo de tiempo.

4.2 Valuación de Ingresos y Egresos $\gamma(a)$

Considerando que un atacante podría incrementar su valuación de ingresos y egresos utilizando un ataque de bucle. Para evitar esta situación debemos remover el bucle de transacciones antes de calcular la valuación de ingresos y egresos para el grafo de transacciones. El bucle de transacciones es un ciclo dentro de un intervalo de tiempo. Éste comienza y termina en el mismo nodo v, que es un conjunto de aristas en el grafo de transacciones. Un ciclo de transacciones puede ser denotado como $H(v)$:

$$H(v) = \{(v, v_1, w_1, \tau_1), (v_1, v_2, w_2, \tau_2), \ldots, (v_i, v_{i+1}, w_i, \tau_i), \ldots, (v_n, v, w_{n+1}, \tau_{n+1})\}$$

donde $\forall 1 \leq i \leq n : \tau_i \leq \tau_{i+1}$. Como se muestra en Fig. 1, hay un bucle de transacciones; nótese que la transacción $(v_1, v_2, 100, 5)$ no está incluida dentro de ese bucle.

Luego de determinar la existencia de estos bucles es necesario removerlos. Asumiendo que hay n bucles en el sistema, y que éstos están listados por la secuencia que sigue:

$$H^1(v_1), H^2(v_2), \ldots, H^n(v_n)$$

La cantidad mínima de transacciones en $H^i(v_i)$ es $(s^i_m, t^i_m, w^i_m, \tau^i_m)$, y

$$\forall (s^i, t^i, w^i, \tau^i) \in \mathcal{T} : w^i \geq w^i_m$$

Así, por cada transacción en $H^i(v_i)$, necesitamos reducir el monto mínimo de transacción w^i_m de forma acorde y eliminar esta transacción si el monto de la última transacción

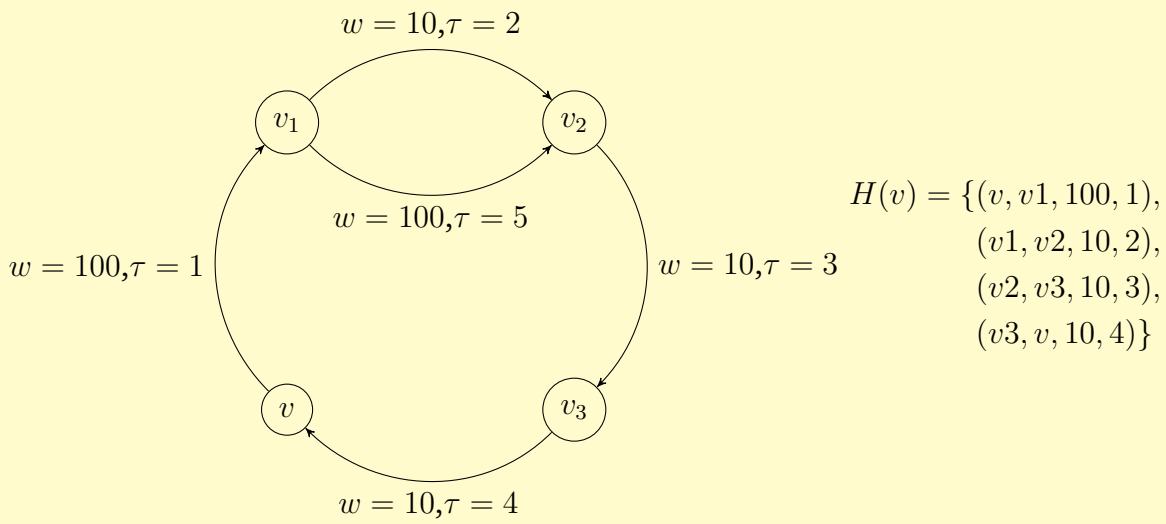

Figure 1: Forwarding loop in a transaction

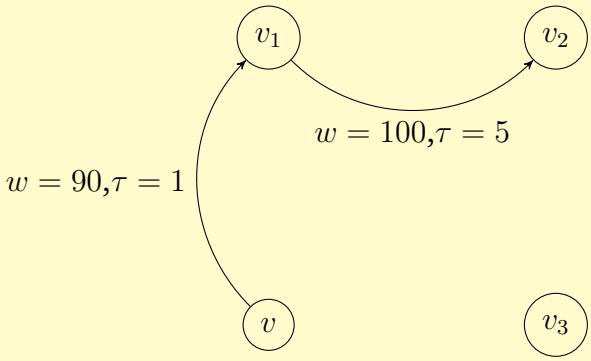

Figure 2: The transaction graph after removing forwarding loop in Fig. 1

es 0:

$$\mathcal{E}((s,t,w,\tau),w_m) = \begin{cases} (s,t,w-w_m,\tau) & \text{if} \quad w \neq w_m \\ \phi & \text{if} \quad w = w_m \end{cases}$$

$$\Theta'(t_0) = \Theta(t_0) - H^i(v) \cup \{\mathcal{E}(t), t \in H^i(v_i)\} \quad i = 1,2,\ldots,n \tag{13}$$

La Fig. 2 nos muestra el grafo de la transacción sin bucles luego de remover el bucle de transacciones en Fig. 1.

Fijamos el monto de ingreso al nodo v como $p(v)$, entonces

$$p(v) = \sum_{(s_i,v,w_i,\tau_i)\in\Theta'(t_0)} w_i \tag{14}$$

Similarmente, fijamos el monto de egreso del nodo v, que es

$$q(v) = \sum_{(v,t_i,w_i,\tau_i)\in\Theta'(t_0)} w_i \tag{15}$$

En este caso, para el nodo v, su valuación de ingresos y egresos $\gamma(v)$ es

$$\mathcal{G}(v) = (p(v) + q(v)) \cdot e^{-2\sin^2(\frac{\pi}{4} - \arctan\frac{q(v)}{p(v)})} \tag{16}$$

$$\gamma(v) = (\frac{\theta \cdot \mathcal{G}(v)}{\mathcal{G}(v) + \mu})^{\lambda} \tag{17}$$

donde θ, μ, λ son los parámetros a ser determinados.

Y la Fig. 3 muestra la curva de la Ecuación 14.

4.3 Función Wilbur

Es extremadamente complicado calcular Core Nebulas Rank si consideramos los distintos usos posibles y sus propiedades. Sin embargo, es posible proveer una función más general para Nebulas Rank.

Definimos la función de cálculo de Core Nebulas Rank como $f(x)$, a saber *Función Wilbur*[1], donde x es el factor de Core Nebulas Rank; éste puede ser una cuenta de

[1]El nombre *Ataque Sybil* deriva de una serie de TV de los años 1970 llamada Sybil, en la que una mujer joven es diagnosticada con un trastorno de personalidades múltiples y recibe su tratamiento con la doctora Cornelia Wilbur.

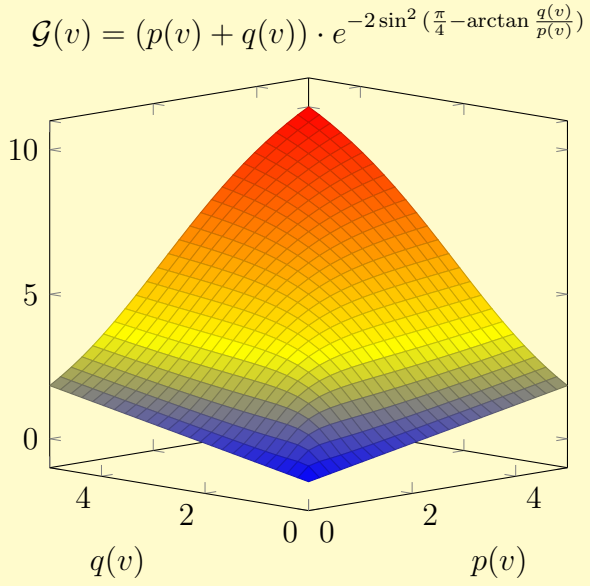

Figure 3: La curva de la función de valuación de ingresos y egresos

participación, una acuñación la valuación de ingresos y egresos. $f(x)$ satisface dos propiedades:

Propiedad 1. *Para dos variables cualesquiera x_1 y x_2, ambas mayores que 0, la suma de las dos funciones es menor que la función de suma de las dos variables.*

$$f(x_1 + x_2) > f(x_1) + f(x_2) \quad x_1 > 0, x_2 > 0 \tag{18}$$

Propiedad 2. *Para dos variables cualesquiera x_1 y x_2 cuyos valores son infinitos, la suma de las dos funciones es aproximadamente igual a la función de la suma de las dos variables.*

$$\lim_{x_1 \to \infty, x_2 \to \infty} f(x_1 + x_2) = f(x_1) + f(x_2) \quad x_1 > 0, x_2 > 0 \tag{19}$$

Las dos propiedades descritas arriba aseguran que, bajo determinadas conductas de transacción, el beneficio de dividir la participación en cuentas más pequeñas es comparativamente menor que mantenerlo dentro de una sola cuenta. Al mismo tiempo, cuando la participación es lo suficientemente grande, el costo de dividirla en cuentas más pequeñas puede ser ignorado.

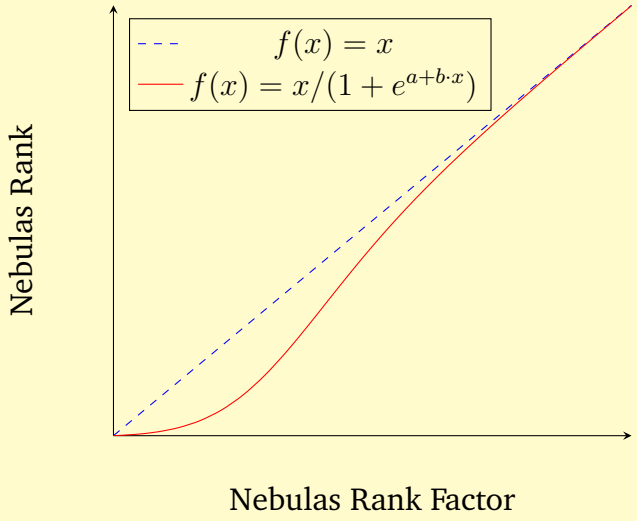

Figure 4: La curva de la función Nebulas Rank

Existe más de una función que satisface las dos propiedades descritas arriba. Aquí proveemos una función sucinta; la curva de esta función se muestra en Fig. 4.

$$f(x) = x/(1 + e^{a+b\cdot x}) \quad a > 1, b < 0 \tag{20}$$

La prueba detallada de la función se da en el anexo A

En síntesis, Ecuación 11 se puede expresar de este manera:

$$\mathcal{C}(v) = \frac{\beta(v)}{1 + e^{a+b\cdot\beta(v)}} \cdot \frac{\gamma(v)}{1 + e^{c+d\cdot\gamma(v)}} \tag{21}$$

donde a, b, c, d son parámetros a ser determinados.

Con el fin de verificar la efectividad de la función, calculamos el valor Core Nebulas Rank para todas las cuentas registradas en el blockchain Ethereum durante un período dado. Recogimos todos los registros de transacciones desde el primero de mayo de 2017 hasta el 30 de junio de ese mismo año (altura de bloque: desde 3629091 hasta 3955158), en suma, también recogimos el valor promedio diario de ETH (en dólares) y los volúmenes de transacciones [24].

La Fig. 5 muestra la tendencia entre la capitalización del mercado ETH y el valor Core Nebulas Rank para Ethereum, donde la línea sólida negra indica la capitalización de mercado para Ethereum (en dólares), mientras la línea sólida roja representa la suma de todas las cuentas Core Nebulas Rank basadas en Ecuación 21.

Podemos ver que Core Nebulas Rank refleja los cambios en la capitalización de

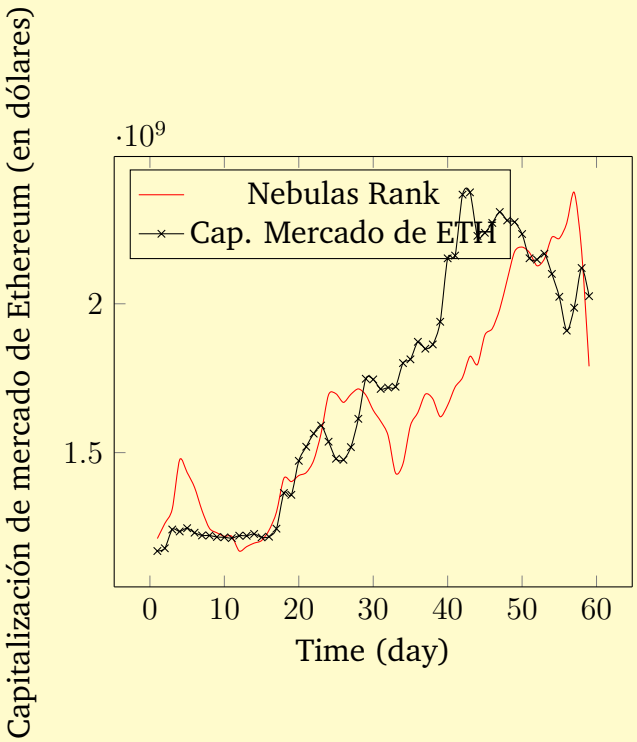

Figure 5: La capitalización de mercado y el valor Core Nebulas Rank de Ethereum

mercado de Ethereum de forma precisa. El coeficiente de correlación es de 0.84427, mientras que p (valor p, o significancia) es de $4.48 \times 10^{-17} < 0.001$. Esto significa que Ecuación 11 ilustra el éxito en describir las contribuciones de los usuarios al sistema económico en el blockchain, lo que demuestra tanto la validez y la precisión de Core Nebulas Rank.

5 Resistencia a la manipulación de Core Nebulas Rank

Este capítulo analiza la resistencia a la manipulación de Core Nebulas Rank, es decir, la equidad que ofrece Nebulas Rank.

Manipulación refiere a las acciones deshonestas de un atacante en beneficio propio. Las acciones que pueden tomar los atacantes incluyen: lanzar transferencias de activos, lo que implica hacer uso de activos y cuentas controladas por ellos y otros individuos deshonestos. Entre esas transferencias, el total de activos no excede los activos que el atacante posee; el origen de las transferencias puede ser el de cuentas controladas por el atacante y sus colaboradores, o algunas cuentas institucionales que sirven como casas de cambio. Usualmente, el beneficio que obtienen de esto está determinado por las cuentas cuyas claves privadas son conocidas por el atacante. Un

caso sencillo es aquel en el que el beneficio del atacante corresponde a la suma de la valuación (*ranking*) de todas estas cuentas. Por supuesto, se entiende que las claves privadas de las cuentas institucionales mencionadas anteriormente no están en poder de los atacantes.

El análisis de esta sección se basa en las acciones emprendidas y en el beneficio de los atacantes definidos anteriormente. En primer lugar, discutimos el límite superior para la mejora del puntaje de valuación de una única cuenta. Luego analizamos el límite superior para múltiples cuentas. Por último, se incluye la colusión y la discusión de la situación en la que interviene más de un atacante.

5.1 Incremento del puntaje de valuación para una cuenta única

De acuerdo a Ecuación 21, para poder elevar el puntaje de valuación de una cuenta, éste debe estar positivamente correlacionado con la cantidad de activos y con el grado de movimientos de cuenta. La cantidad de activos en la cuenta, es decir, β, tiene un límite superior, esto es, no puede ser mayor que el total absoluto de activos en poder del atacante, lo cual está denotado por β_0. El grado de movimientos γ representa el volumen de transferencias, lo cual implica que el atacante necesita incrementar la cantidad de transferencias de una de sus cuentas tanto como le sea posible.

El aumento de la suma de la transferencia incluye dos partes: el aumento de la valuación de los ingresos y el aumento de la valuación de los egresos. El aumento de la valuación de los ingresos y egresos requiere dos cuentas participantes, una de las cuales es la cuenta de destino, cuyo objetivo es elevar su puntaje de valuación, y la otra cuenta podría estar o no controlada por el atacante. Si se trata de una cuenta no controlada por el atacante, el aumento de movimientos requiere realizar transacciones con otras personas; esta situación se discute en § 5.3. El otro caso se da cuando el atacante envía activos a extraños, lo cual es demasiado costoso para que se discuta en esta sección. Por ende, se podría definir que las acciones de los atacantes se centran principalmente en aumentar las transferencias entre las cuentas controladas por ellos mismos. Dado que los activos controlados por los atacantes son limitados y el período de tiempo para la valuación también es limitado, se desprende de ello que la valuación de una cuenta tiene un límite superior que se decide por la cantidad de activos que posee el atacante.

As analyzed above, we consider the scenario of transacting with accounts of the same owner. Based on the computation method Ecuación 21 as defined in § 4.3, the attacker's benefit will be reduced if it split the asset transfers into multiple ones. Thus

the attacker will attempt to make its transaction amount to be as high as possible, i.e. it tries to transfer all assets it owns into the account and then transfer it out all. Due to the cycle-removal algorithm, the attacker's asset cannot be transferred in again during this period.

Como se ha analizado anteriormente, consideramos un escenario de operaciones con cuentas del mismo titular. Basado en el método de cálculo Ecuación 21 como se define en § 4.3, el beneficio del atacante se reducirá si divide las transferencias de activos en múltiples transacciones. De este modo, el atacante intentará que el importe de la transacción sea lo más elevado posible, es decir, buscará transferir a una cuenta dada todos los activos que posee para luego re-enviarlos en su totalidad a la cuenta original. Debido al algoritmo de eliminación de ciclo, los activos del atacante no pueden ser transferidos nuevamente durante este período.

La valuación de los ingresos y egresos es $\gamma = 2\beta_0$. El puntaje de valuación es:

$$\mathcal{C} = \frac{2\beta_0^2}{(1 + e^{a+b\cdot\beta_0})(1 + e^{c+2d\cdot\beta_0})}. \tag{22}$$

Additionally, we consider a more advanced manipulation technique. Consider the case that an attacker manages to acquire the asset again somewhere else by transacting off-line. Then it could transfer the asset into the account again and the upper-bound of in-and-out degree is the asset amount times the number of off-line transactions. Since the ranking time period is limited, the upper-bound of the number of off-line transactions is a constant integer, i.e. γ is bounded by $2T\cdot\beta_0$, where T is a constant integer indicating the length of ranking time period. Therefore the upper-bound score is:

Adicionalmente, consideramos una técnica de manipulación más avanzada. Considérese el caso de que un atacante logra transferir nuevamente sus activos desde otra cuenta (tal vez mediante una transacción *offline*). De ese modo podría transferir los activos a la cuenta original, con lo que el límite superior de la valuación de los ingresos y egresos se transforma en el total de los activos multiplicado por el número de transacciones *offline*. Dado que el período de clasificación es limitado, el límite superior del número de transacciones *offline* es un número entero constante, es decir, γ está limitado por $2T \cdot \beta_0$, donde T es un número entero constante que indica la duración del período de clasificación. Por lo tanto, la puntuación máxima es:

$$\mathcal{C} = \frac{2T \cdot \beta_0^2}{(1 + e^{a+b\cdot\beta_0})(1 + e^{c+c\cdot d\cdot\beta_0})}. \tag{23}$$

5.2 Incremento del puntaje de valuación para cuentas múltiples (ataque Sybil)

El ataque Sybil hace referencia a una situación en la que un atacante obtiene un alto puntaje de valuación de carácter ilegítimo por medio de la creación de un gran número de pseudo-identidades con el fin de alterar el sistema de reputación de una red p2p [25].

Una entidad en una red p2p es una pieza de software a la que se le ha concedido acceso a recursos locales. Esa entidad se anuncia en la red p2p presentando una identidad. Una entidad puede tener más de una identidad. En otras palabras, el mapeo de identidades a entidades puede ser de muchos a uno. Las entidades en redes p2p utilizan múltiples identidades con el fin de lograr redundancia, intercambio de recursos, fiabilidad e integridad. En estas redes, la identidad se utiliza como una abstracción para que una entidad remota pueda llevar un registro de las identidades sin conocer necesariamente la correspondencia de las identidades con las entidades locales. Por defecto, se supone que cada identidad distinta corresponde a una entidad local distinta. En realidad, varias identidades pueden corresponder a la misma entidad local. Un adversario puede presentar múltiples identidades a una red p2p para verse y funcionar como múltiples nodos distintos. De este modo, el adversario puede adquirir un nivel desproporcionado de control sobre la red, por ejemplo, afectando los resultados de una votación [26].

Aquí asumimos que la recompensa del atacante es la suma de todas las cuentas que controla. Teniendo en cuenta la estrategia para mejorar el puntaje de valuación de una cuenta, que se analiza en la última subsección, el atacante podría aplicar la misma estrategia a varias cuentas: a partir de cualquiera de ellas, el atacante transfiere parte de su activo a la cuenta siguiente, formando finalmente un flujo de activos vinculado.

En este caso, dado que Core Nebulas Rank requiere que no haya más que la cantidad válida de activos en la cuenta durante un plazo no mayor a la mitad del período, el atacante no tiene manera de hacer que β sea la cantidad total de activos para más de una cuenta. Por lo tanto, el atacante debe adoptar otra estrategia en la que sus activos se distribuyan uniformemente en todas sus cuentas.

Supongamos que la longitud de las cuentas vinculadas es N, es decir, existen N cuentas controladas por el atacante, y para cada una de esas cuentas, $\beta = \frac{\beta_0}{N}$. El análisis de la valuación de los ingresos y egresos es el mismo que en el caso de § 5.1, el límite superior de γ es $K \cdot \beta$, donde $K = 2 \cdot N$ es un número entero constante. Por lo tanto, el límite superior de la suma de todas las cuentas de propiedad del atacante

es:

$$\mathcal{C} = N \cdot \frac{K\frac{\beta_0^2}{N}}{(1+e^{a+b\cdot\frac{\beta_0}{N}})(1+e^{c+K\cdot d\cdot\beta_0})} = \frac{K\beta_0^2}{(1+e^{a+b\cdot\frac{\beta_0}{N}})(1+e^{c+K\cdot d\cdot\beta_0})} \tag{24}$$

5.3 Manipulación en coalición

El resultado de la manipulación en coalición no difiere del caso en el que un atacante posee el total de activos de dos atacantes. En esta situación podemos analizar el ataque a través de las consecuencias del aumento de los activos de un solo atacante.

6 Implementación de Core Nebulas Rank

La implementación completa de Core Nebulas Rank está fuera del alcance de esta sección, de modo que nos limitaremos a introducir sus aspectos clave.

6.1 ¿Dentro o fuera del blockchain?

Tal como se explicó en capítulos anteriores, Core Nebulas Rank es una muestra de la contribución de cada cuenta al agregado económico global. Normalmente, cada nodo puede calcular la contribución de cualquier cuenta específica; sin embargo, es preciso plantear si es necesario colocar NR en el blockchain de forma periódica.

En nuestra opinión, es a la vez innecesario e inapropiado, debido a que:

- El tamaño de los datos generados por NR será inmenso, por lo que no será apropiado mantenerlos en el blockchain. Incluso para sistemas tales como IPFS o Genaro [27] [28] no sería apropiado almacenar el valor NR de cada cuenta periódicamente, incluso cuando son sistemas orientados a almacenar datos.

- Esto afectará negativamente la performance de la generación de bloques. La complejidad de cómputo de Core Nebulas Rank es alta, de modo que afectaría significativamente la generación de bloques y la performance de las validaciones y, eventualmente, afectaría también el valor de las transacciones por segundo (TPS).

En líneas generales, sugerimos que cada nodo calcule el valor Core Nebulas Rank de forma individual.

No obstante, si cada nodo realiza el cómputo de forma individual, no hay seguridad alguna de que el valor calculado sea confiable. Por ejemplo, un modo podría modificar maliciosamente el cálculo NR basar en ellos los incentivos. Para las aplicaciones críticas se verificarán todos los cálculos NR con el fin de garantizar la equidad de los resultados. En contraste, para aquellas aplicaciones que no son tan importantes, dependerá de ellas mismas decidir si el uso que le dan al valor NR amerita o no una verificación.

Existe otra situación importante a tener en cuenta, que es que un nodo podría negarse a realizar el cómputo del valor NR basándose en el costo de la operación. Debido a esto, se considerará la creación de un servicio Core Nebulas Rank que evite la repetición innecesaria de los cómputos, que se podrá ofrecer de forma gratuita o bien a cambio de un pago, dependiendo del número de veces que se requiera realizar el cálculo. Los detalles de tal servicio, y su completa implementación, están fuera del alcance de este documento.

6.2 Actualización de Core Nebulas Rank

Core Nebulas Rank está asociado íntimamente a la economía de una criptodivisa. A medida que la economía cambia, el algoritmo de Core Nebulas Rank necesitará actualizaciones, especialmente sus parámetros. Es sumamente importante determinar la mejor manera de actualizar rápidamente el algoritmo. Nuestra propuesta es la de actualizar el algoritmo de Nebulas Rank mediante el uso de Nebulas Force.

Específicamente actualizamos la estructura de los bloques de datos, que incluirá el algoritmo de Core Nebulas Rank y sus parámetros (basados en LLVM IR). La máquina virtual de Nebulas (NVM) será el motor de ejecución del algoritmo: éste obtiene su código —junto con sus parámetros— desde el blockchain, ejecuta el código, y eventualmente obtiene el Core Nebulas Rank dentro del nodo.

Siempre que el algoritmo o sus parámetros requieran una actualización, el equipo de Nebulas trabajará junto a la comunidad, asegurando que esas modificaciones se incluyan en los nuevos bloques. Esto garantizará una actualización suave y oportuna, que impida la creación de *forks* en el futuro.

7 Extended Nebulas Rank

Core Nebulas Rank se utiliza para evaluar la contribución de una cuenta individual a la economía agregada, y es una parte vital tanto del algoritmo de consenso *Proof of Devotion* (PoD) como del *Developer Incentive Protocol* (DIP). No obstante, como

hemos notado, existen otros casos de uso que podrían requerir una metodología de evaluación diferente; para esos casos hemos diseñado *Extended Nebulas Rank* —que se basa en Core Nebulas Rank— para garantizar la continuidad de los incentivos en toda la economía de Nebulas y en todos los casos de uso posibles.

7.1 Extended Nebulas Rank orientado a contratos inteligentes

La valuación de contratos inteligentes juega un rol importante dentro de la economía. Por un lado ayuda a los usuarios a encontrar DApps de alta calidad; por otro lado también motiva a que los desarrolladores escriban DApps de esas características, con lo que la economía puede expandirse de forma estable y continua.

Ahora bien, esa valuación depende de dos factores: las llamadas que los usuarios —desde sus cuentas— realizan a los contratos inteligentes, y las llamadas entre diferentes contratos inteligentes. Las llamadas de usuarios a contratos reflejan el hecho de que desde esas direcciones (de usuarios) se está contribuyendo, de forma distribuida, a la economía agregada de todos los contratos inteligentes, ya que cada contrato inteligente tiene su propio valor NR asignado inicialmente. Las llamadas entre contratos inteligentes pueden ser tratadas también como un grafo acíclico dirigido. Por lo tanto, utilizamos el algoritmo de Page Rank para calcular el valor NR de cada contrato inteligente.

7.2 Extended Nebulas Rank multidimensional

Hemos visto también que algunas aplicaciones requieren datos multidimensionales para computar la correlación entre diferentes tipos de datos en el blockchain. Por ejemplo, en un sistema de publicidad basado en blockchain, es necesario obtener la correlación entre la publicidad y el usuario desde distintas dimensiones. En esa situación hacemos uso de Extended Nebulas Rank, ya que es multidimensional y se puede representar como un vector; en este caso, Core Nebulas Rank es una de sus dimensiones, y el resto de ellas dependen de cada aplicación en particular. Sin perjuicio de ello, los algoritmos de cálculo siempre podrán referenciar a aquellos del algoritmo Core Nebulas Rank.

Comenzando por un caso de uso real, diseñamos el algoritmo Extended Nebulas Rank para su uso por parte de contratos inteligentes; hemos descripto también un método de implementación de Extended Nebulas Rank. También hemos ilustrado con ejemplos el mecanismo de evaluación correspondiente a este algoritmo, y hemos

propuesto el sistema multidimensional Extended Nebulas Rank, que muestra la posibilidad de usar nuestro mecanismo de evaluación en otros casos de uso.

8 Trabajo futuro

El objetivo de Nebulas Rank es proporcionar una medida de valor necesaria para los blockchains, desde la perspectiva de proporcionar una evaluación justa basada en la contribución real de las direcciones de las cuentas de los usuarios a la economía agregada. Si bien es un trabajo en progreso, aquí sumarizamos nuestros planes, a ser implementados en un futuro cercano:

- Nebulas Rank inter-blockchain Podemos prever que habrá una gran demanda de transferencia de datos inter-blockchain en un futuro cercano. Por nombrar algunos pocos casos, podemos citar las interacciones de datos inter-blockchain y las transferencias de activos digitales, que ciertamente requieren una medida de valor en diferentes blockchains. Por ejemplo, cuando los desarrolladores migren sus DApps de un blockchain a otro, será necesario contar con un método para calcular el valor NR de dichas DApps, y también será necesario contar con una metodología única, que permita arribar a una medición estándar entre distintos blockchains.

- Otros indicadores de contribución basados en la economía agregada. Nebulas Rank se basa en la contribución a la economía agregada. No obstante, el crecimiento continuo del blockchain obliga a tener una comunidad en crecimiento. Por ello, en términos de economía agregada, no podemos ignorar la contribución de la comunidad. Así, la forma en que evaluamos las contribuciones —individuales o de una organización— en la comunidad, y cómo estas se ven reflejadas en Nebulas Rank, ciertamente tiene grandes implicaciones.

Referencias

[1] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*, pp. 127–140, ACM, 2013.

[2] "HTTP Cookie." `https://en.wikipedia.org/wiki/HTTP_cookie`.

[3] "Nebulas Technical White Paper." `https://nebulas.io/docs/NebulasTechnicalWhitepaper.pdf`. Accessed: 2018-04-01.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] "Namecoin." `https://namecoin.org`.

[6] "Openassets protocol." `http://github.com/OpenAssets/open-assets-protocol`.

[7] V. Buterin *et al.*, "Ethereum white paper," 2013.

[8] "Forget fintech – welcome to the valueweb." `http://thefinanser.com/2015/02/forget-fintech-welcome-to-the-valueweb.html/`.

[9] L. Page, S. Brin, R. Motwani, and T. Winograd, "The pagerank citation ranking: Bringing order to the web.," tech. rep., Stanford InfoLab, 1999.

[10] M. Fleder, M. S. Kester, and S. Pillai, "Bitcoin transaction graph analysis," *arXiv preprint arXiv:1502.01657*, 2015.

[11] Q. Li, T. Zhou, L. Lü, and D. Chen, "Identifying influential spreaders by weighted LeaderRank," *Physica A: Statistical Mechanics and its Applications*, vol. 404, pp. 47–55, 2014.

[12] A. Cheng and E. Friedman, "Manipulability of pagerank under sybil strategies," 2006.

[13] "NEM Technical Reference." `http://nem.io/NEM_techRef.pdf`. Accessed: 2017-08-01.

[14] A. N. Nikolakopoulos and J. D. Garofalakis, "NCDawareRank," *Proceedings of the sixth ACM international conference on Web search and data mining - WSDM '13*, no. February 2013, p. 143, 2013.

[15] X. Xu, N. Yuruk, Z. Feng, and T. A. Schweiger, "Scan: a structural clustering algorithm for networks," in *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 824–833, ACM, 2007.

[16] H. Shiokawa, Y. Fujiwara, and M. Onizuka, "Scan++: efficient algorithm for finding clusters, hubs and outliers on large-scale graphs," *Proceedings of the VLDB Endowment*, vol. 8, no. 11, pp. 1178–1189, 2015.

[17] L. Chang, W. Li, L. Qin, W. Zhang, and S. Yang, "pscan: Fast and exact structural graph clustering," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 2, pp. 387–401, 2017.

[18] J. Hopcroft and D. Sheldon, "Manipulation-resistant reputations using hitting time," in *International Workshop on Algorithms and Models for the Web-Graph*, pp. 68–81, Springer, 2007.

[19] J. Zhang, R. Zhang, J. Sun, Y. Zhang, and C. Zhang, "Truetop: A sybil-resilient system for user influence measurement on twitter," *IEEE/ACM Transactions on Networking*, vol. 24, no. 5, pp. 2834–2846, 2016.

[20] A. Cheng and E. Friedman, "Sybilproof reputation mechanisms," in *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, pp. 128–132, ACM, 2005.

[21] M. Swan, *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 2015.

[22] R. S. Kroszner, "Liquidity and monetary policy," 2007.

[23] R. Selden, "Monetary velocity in the united states," 1956.

[24] "CoinMarketCap." `https://coinmarketcap.com/`.

[25] D. Quercia and S. Hailes, "Sybil attacks against mobile users: friends and foes to the rescue," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–5, IEEE, 2010.

[26] Wikipedia contributors, "Sybil attack — Wikipedia, the free encyclopedia," 2018. [Online; accessed 25-June-2018].

[27] "IPFS." `https://ipfs.io/`.

[28] "Genaro." `https://genaro.network/en/`.

Anexo A Pruebas

A.1 Prueba de propiedad 1

Proof. Para todo $x_1 > 0$, $x_2 > 0$ tenemos:

$$\begin{aligned} f(x_1 + x_2) &= \frac{x_1 + x_2}{1 + e^{a+b\cdot(x_1+x_2)}} \\ &= \frac{x_1}{1 + e^{a+b\cdot(x_1+x_2)}} + \frac{x_2}{1 + e^{a+b\cdot(x_1+x_2)}} \\ &= \frac{x_1}{1 + e^{b\cdot x_2} \cdot e^{a+b\cdot x_1}} + \frac{x_2}{1 + e^{b\cdot x_1} \cdot e^{a+b\cdot x_2}} \end{aligned}$$

En la ecuación 21 tenemos $b < 0$, de modo que $0 < e^{b\cdot x_1} < 1$, $0 < e^{b\cdot x_2} < 1$, por otra parte:

$$\frac{x_1}{1 + e^{b\cdot x_2} \cdot e^{a+b\cdot x_1}} > \frac{x_1}{1 + e^{a+b\cdot x_1}} = f(x_1)$$

$$\frac{x_2}{1 + e^{b\cdot x_1} \cdot e^{a+b\cdot x_2}} > \frac{x_2}{1 + e^{a+b\cdot x_2}} = f(x_2)$$

es, en realidad:

$$f(x_1 + x_2) > f(x_1) + f(x_2)$$

□

A.2 Prueba de propiedad 2

Proof. Para todo $x_1 > 0$, $x_2 > 0$ tenemos:

$$\begin{aligned} f(x_1 + x_2) - f(x_1) - f(x_2) &= \frac{x_1 + x_2}{1 + e^{a+b\cdot(x_1+x_2)}} - \frac{x_1}{1 + e^{a+b\cdot x_1}} - \frac{x_2}{1 + e^{a+b\cdot x_2}} \\ &= \left(\frac{x_1}{1 + e^{b\cdot x_2} \cdot e^{a+b\cdot x_1}} - \frac{x_1}{1 + e^{a+b\cdot x_1}}\right) \\ &\quad + \left(\frac{x_2}{1 + e^{b\cdot x_1} \cdot e^{a+b\cdot x_2}} - \frac{x_2}{1 + e^{a+b\cdot x_2}}\right) \end{aligned} \tag{25}$$

Aquí la función $g(x_1, x_2)$ representa —dentro del segundo miembro de 25— el primer término, y $h(x_1, x_2)$ el segundo término:

$$g(x_1, x_2) = \frac{x_1}{1 + e^{b\cdot x_2} \cdot e^{a+b\cdot x_1}} - \frac{x_1}{1 + e^{a+b\cdot x_1}} \tag{26}$$

$$h(x_1, x_2) = \frac{x_2}{1 + e^{b\cdot x_1} \cdot e^{a+b\cdot x_2}} - \frac{x_2}{1 + e^{a+b\cdot x_2}} \tag{27}$$

De modo que (25) para x_1 y x_2, sus límites pueden ser representados como:

$$\lim_{\substack{x_1\to\infty\\x_2\to\infty}}[f(x_1+x_2)-f(x_1)-f(x_2)]=\lim_{\substack{x_1\to\infty\\x_2\to\infty}}g(x_1,x_2)+\lim_{\substack{x_1\to\infty\\x_2\to\infty}}h(x_1,x_2)$$

tenemos

$$\begin{aligned}g(x_1,x_2)&=\frac{x_1}{1+e^{b\cdot x_2}\cdot e^{a+b\cdot x_1}}-\frac{x_1}{1+e^{a+b\cdot x_1}}\\&=\frac{x_1\cdot e^{a+b\cdot x_1}\cdot(1-e^{b\cdot x_2})}{(1+e^{b\cdot x_2}\cdot e^{a+b\cdot x_1})\cdot(1+e^{a+b\cdot x_1})}\\&<\frac{x_1\cdot e^{a+b\cdot x_1}\cdot(1+e^{a+b\cdot x_1})}{(1+e^{b\cdot x_2}\cdot e^{a+b\cdot x_1})\cdot(1+e^{a+b\cdot x_1})}=\frac{x_1\cdot e^{a+b\cdot x_1}}{1+e^{b\cdot x_2}\cdot e^{a+b\cdot x_1}}\\&<\frac{x_1\cdot e^{a+b\cdot x_1}}{1+e^{a+b\cdot x_1}}=\frac{x_1}{1+\frac{1}{e^{a+b\cdot x_1}}}\end{aligned}$$

Se calcula el límite para $\frac{x}{1+\frac{1}{e^{a+b\cdot x}}}$, de acuerdo a la regla de L'Hôpital:

$$\begin{aligned}\lim_{x\to\infty}\frac{x}{1+\frac{1}{e^{a+b\cdot x}}}&=\lim_{x\to\infty}\frac{1}{(e^{-a-b\cdot x})'}\\&=\lim_{x\to\infty}\frac{1}{-b\cdot e^{-a-b\cdot x}}\end{aligned}$$

En la ecuación 21 tenemos $b<0$, por lo que $\lim_{x\to\infty}-b\cdot e^{-a-b\cdot x}=\infty$; por otra parte,

$$\lim_{x\to\infty}\frac{x}{1+\frac{1}{e^{a+b\cdot x}}}=0$$

De acuerdo a A.1, tenemos $g(x_1,x_2)>0$, por lo que de acuerdo al teorema del emparedado:

$$\lim_{\substack{x_1\to\infty\\x_2\to\infty}}g(x_1,x_2)=0$$

Similarmente, podemos obtener:

$$\lim_{\substack{x_1\to\infty\\x_2\to\infty}}h(x_1,x_2)=0$$

Por lo que:

$$\lim_{\substack{x_1\to\infty\\x_2\to\infty}}[f(x_1+x_2)-f(x_1)-f(x_2)]=0$$

□

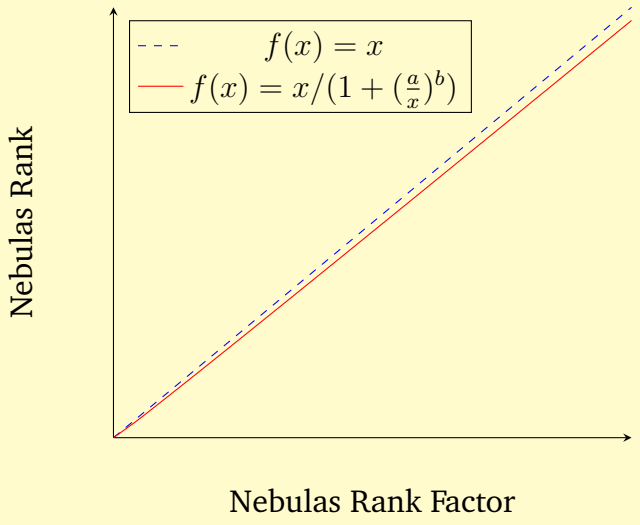

Figure 6: Curva de la función de Nebulas Rank

Anexo B Nueva función Wilbur

Se adopta una nueva función Wilbur para la versión 1.0 de Nebulas NOVA.

$$f(x) = x/(1 + (\frac{a}{x})^b) \quad a > 0, 0 < b < 1 \tag{28}$$

Como se muestra en la figura 6, es sencillo demostrar que la función satisface las dos propiedades 1, 2 y en § 4.3.

Anexo C Registro de cambios

- 1.0 Lanzamiento.
- 1.0.1 Se corrigen las descripciones matemáticas de las propiedades 1 y 2 en § 4.3 con el fin de evitar ambigüedades.
- 1.0.2 Se corrigen algunos errores de ortografía y gramática.
- 1.0.3 Se añade el apéndice B, que introduce la nueva función Wilbur en Nebulas Nova 1.0.