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 Economic Model

Cryptocurrencies are endowed with economic significance, either as a kind of trading medium or intelligent asset. Therefore, a reasonable economic model can help us to establish a value measurement standard on the blockchain, which is also the objective of Core Nebulas Rank. This chapter first introduces the mathematical representation of cryptocurrency, and then analyzes cryptocurrency with a simple but well-recognized monetary model. During this analysis, we introduce the Core Nebulas Rank as an important argument.

3.1 Representation of Cryptocurrency

The biggest difference between cryptocurrency and traditional economy is that all cryptocurrency transactions are traceable. This provides crucial data sources for us to analyze the impact of each transaction on the greater economic system.

In general, a cryptocurrency system can be defined as a pair $(\mathcal{L},\mathcal{U})$, where $\mathcal{L}$ denotes the ledger system, and $\mathcal{U}$ is the set of cryptocurrency users. Further, the ledger system can be described as a triple as below:

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

where $\mathcal{A}$ represents the set of accounts, $\mathcal{D}$ is the set of initial balances of each account, and $\mathcal{T}$ is the set of transactions. Each transaction can be recorded as a tetrad as below:

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

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

where $a \to d$ represents the balance d corresponding to the account a (d is a positive real number, in other words, we do not takes the accounts with zero balance into consideration). s, t, w and τ represents the source account, target account, amount and time of a transaction respectively.

An account is controlled by a relevant user, who can propose a transaction with the account, which can be denoted as:

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

On one hand, a user can control multiple accounts, represented as:

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

On the other hand, an account can only be controlled by a single user, shown as:

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

Note that the model described above is a reasonable simplification of any cryptocurrency system. In this model, we do not distinguish the on-chain data from off-chain data, and do not introduce either transaction price or invocations of smart contracts and so on. In addition, the accounts of exchanges are type-specific. Generally speaking, the transactions in an exchange can be divided as two categories: normal transactions that will be recorded on the chain, and intra-exchange transactions that will not be recorded in a centralized database of the exchange. This leads to an outcome where we will lose the intra-exchange transactions if we only obtain the data from the chain. However, if the intra-exchange transactions can be obtained with the cooperation of the exchange, we can further map an exchange account into multiple accounts, so as to use the model outlined above.

3.2 Model of Cryptocurrency

Although cryptocurrency differs largely from traditinal commodity currency and fiat money, the classical monetary theory still has the practical leading meaning nowadays. As a modern form of money borne out of a new economic entity [21], cryptocurrency is born with the attributes of traditional money and retaining its three necessary features: medium of exchange, store of value, and unit of account.

Hereby, we establish both a simple and classic monetary model assist in understanding the physical significance of Nebulas Rank.

First of all, we try to give the indicator to measure the *velocity factor* within the cryptocurrency ecosystem.

Another essential concept needed to be differentiated from the *velocity factor* in

the economics is *liquidity*. *Liquidity* describes the difficulty level in exchanging the assets for the medium of exchange. As money itself is a medium of exchange in economics, money is the assets with the best *liquidity*.

> In the Nebulas Technical White Paper [**?**], we used the word *liquidity* frequently. However, there is no rigid definition of *liquidity*, whose meaning is very broad even in economics. For example, the entries to explain the *liquidity* includes three totally different aspects in *The New Palgrave: A Dictionary of Economics*. R. S. Kroszner pointed out that there were 2795 independent papers mentioning *liquidity* during the past 6 months, each of which raised a typically different statement though [22]. The *liquidity* in this yellow paper is referred to as the **velocity of money**, meaning the turnover times of a monetary unit over a certain period of time.

We use the velocity of money to represent the turnover rate of cryptocurrency [23], namely the turnover of a monetary unit over a certain period of time (one day in this paper), which is represented with V. According to the classical quantity theory of money, the equation is expressed as below:

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

where M, V, P and Y represent the total monetary amount of the economic system, the velocity of money, the price level (measured by the money of unit economical output, thus the money price is $\frac{1}{P}$), and real economical output (real GDP) respectively. The equation illustrates that the product of monetary amount and velocity of money equals the product of price of goods and their output.

As for the monetary amount M, Nebulas is similar to Ethereum in that the monetary amount maintains steady growth (the additional issuance percentage of Nebulas money (NAS) is set as 4% at present), which is different from Bitcoin in that the total monetary amount of latter will be stable once the total at 21 million coins have been mined. The velocity of money V can be described as the ratio of the circulated monetary amount and the monetary supply. As a result, the Ecuación 7 can be further expressed as:

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

where Δm is the additional monetary supply.

In terms of price level P, it is acceptable that the value of price is determined by the relationship between the monetary supply and demand, both by classical theories of money and New Keynesian Models. In the long term, the total price level will be adjusted to ensure monetary supply and demand remain at the equilibrium point.

However, the total price level does not always remain at the equilibrium point between monetary supply and demand in the short term. In a healthy economical system, the growth rate in price is traditionally smaller than that of velocity of money. By increasing the monetary supply (in other words by reducing interest rates), both the price level P and goods/service demands Y will increase in the meantime. On the other side, the increase speed of price level should be controlled, to prohibit the users from holding the cryptocurrency for a long time, thus reducing the velocity. The rationale for the users to hold the cryptocurrency is that they expect over time the price of cryptocurrency will rise.

With regard to real economic output Y, it is traditionally represented by economists as real GDP, namely *a monetary measure of the market value of all final goods and services produced in a period of time*. We believe that the value of cryptocurrency is based on its velocity, namely each transaction contributes to the total economic aggregate to a certain extent. In other words, once a transaction takes place, it both increases the velocity of cryptocurrency and individual's approval and belief of cryptocurrency to some degree. As a result, we think that Y in the Ecuación 8 is consisted of each transaction. Given that the subjects of a economic system are accounts, we can also explain Y as the transactions issued by each account as below:

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

where $\mathcal{C}(a)$ represents the contributions made by account a to total economic output, namely Core Nebulas Rank.

The development of cryptocurrency relies upon continued community development. Therefore, we consider that quantifying the contribution made by each account is the basis of designing the reasonable incentive mechanism. Based on this, the economic system can create either explicit incentives (e.g., Proof of Devotion in Nebulas technical white paper) or implicit incentives (e.g., the sorted search results provided by search engines). The directive and primitive incentives in the cryptocurrency refers to the additional issuance of money, which is a differentiating factor from that in traditional monetary theories.

4 Core Nebulas Rank

Core Nebulas Rank is used to measure the contributions of a user in reference to the entire economy **over a certain period of time**. The precise calculation is relatively complicated, so we propose an approximation algorithm for its calculation. In this approximation algorithm, we consider two critical factors, the coinage and the account position information in the transaction network. The evaluation section below provides evidence of the accuracy of our approximation algorithm.

We use the transaction history on the mainnet over a certain time period as the data source of Core Nebulas Rank. All the transactions in a period of time $[t_0 - T,\ t_0]$, can be specified as a set:

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

Based on $\Theta(t_0)$, we can define a weighted directed graph, the node refers to the address of the account, the edge from node s to node d represents one transaction, the weight of the edge is w, the time of the edge is τ.

For account $a \in \mathcal{A}$, the calculation of Core Nebulas Rank $\mathcal{C}(a)$ is based on $\Theta(t_0)$, which can be represented as:

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

$\beta(a)$ is the median stake of account a in a certain period; $\gamma(a)$ is the in-and-out degree of account a in a certain period.

Different from the method we calculate the Core Nebulas Rank in Nebulas white paper [**?**], we have made some updates detailed below:
1. We no longer use the top K highest transaction amount as the weight when building the transaction graph;
2. We no longer rely on the weight of nodes in LeaderRank to attain the importance of the node.
First, we remove the transaction loops before we calculate the in-and-out degree β, so it can resist a loop attack. At the same time we still consider the strength of the edge. For some cases of homogeneous topology graph, PageRank and some other symmetric function (such as LeaderRank) has been proved to not be able to resist sybil attack [20]. In this yellow paper, we no longer use the Topology-like ranking strategy. We propose an asymmetric calculation Ecuación 21 which is effective for reducing the rewards by faking the low stake nodes in § 4.3.

Below, we discuss three issues in Ecuación 11: Median Account Stake $\beta(a)$, In-and-Out Degree $\gamma(a)$, and selection of function Ω and Ψ.

4.1 Median Account Stake $\beta(a)$

In time period of $[t_0 - T, t_0]$, there are n blocks in the blockchain system, marked as:

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

B_i refers to the parent block of B_{i+1}. For account $a \in \mathcal{A}$, the balance of the account at end of each block is

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

We can get a new list by sorting the items in ascending order:

$$d_{(0)}^a, d_{(1)}^a, \ldots, d_{(n)}^a$$

where $d_{(i)}^a < d_{(i+1)}^a, 0 \leq i \leq n-1$, thus, the $\beta(a)$ can be expressed as:

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

The median account stake represents the coinage in a certain way, that means the account need to hold the stake for more than half of the time period.

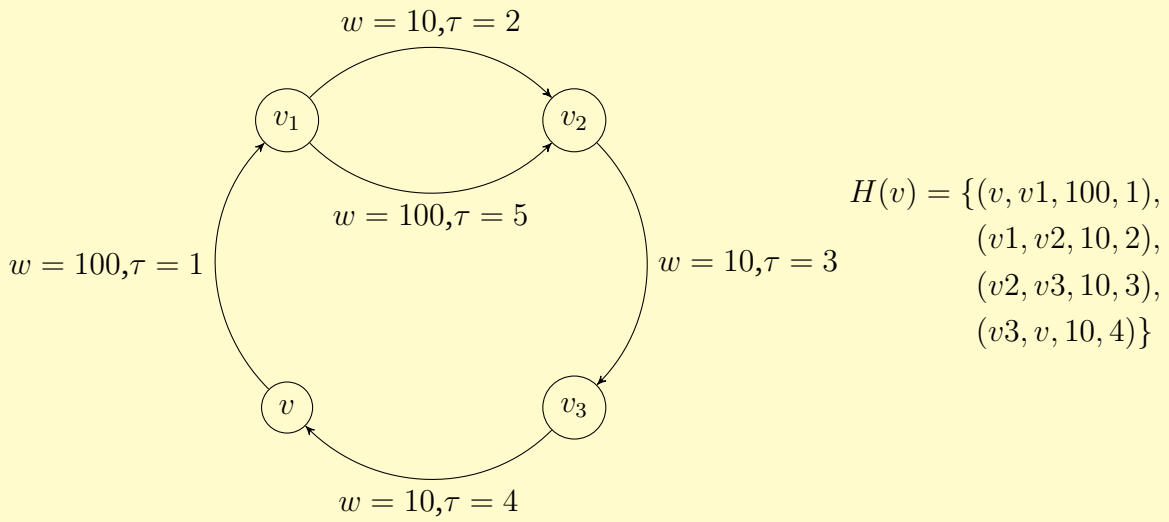

Figure 1: Forwarding loop in a transaction

4.2 In-and-Out Degree $\gamma(a)$

Consider the adversary would increase the in-and-out degree by utilising a loop attack. To avoid this situation we must to remove the forwarding loop before we calculate the In-and-Out degree for the transaction graph. The forwarding loop is a loop of transaction in a sequence of time. It starts and ends on same node v, which is a set of edges in the transaction graph. A forwarding loop can be marked as $H(v)$, which is

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

where $\forall 1 \leq i \leq n : \tau_i \leq \tau_{i+1}$. As shown in Fig. 1, there is a forwarding loop, and note that transaction $(v_1, v_2, 100, 5)$ is not included within the forwarding loop.

After figuring out the forwarding loop, we need to remove the loop before use it. Assuming that there are n forwarding loops in the system, and the forwarding loops are listed by the sequence of occurrence as below:

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

The minimal amount of the transaction in $H^i(v_i)$ is $(s^i_m, t^i_m, w^i_m, \tau^i_m)$, and

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

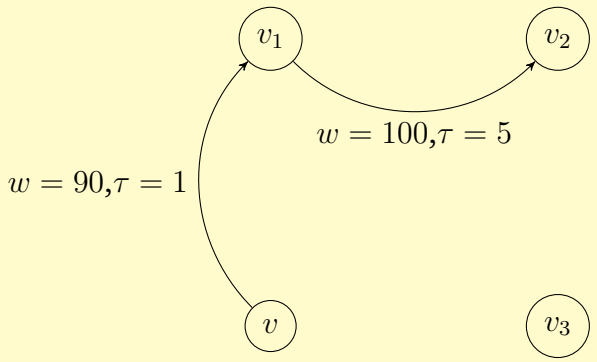

Figure 2: The transaction graph after removing forwarding loop in Fig. 1

Then, for each transaction in $H^i(v_i)$, we need ot minus the minimum transaction amount w_m^i accordingly and remove this transaction if the latest transaction amount is 0, which is

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

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

Fig. 2 shows the non-loop transaction graph after removing the forwarding loop in Fig. 1.

Set the transfer-in amount of node v as $p(v)$, then

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

Similarly, transfer-out amount of node v is

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

In this case, for node v, its in-and-out degree $\gamma(v)$ is

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

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

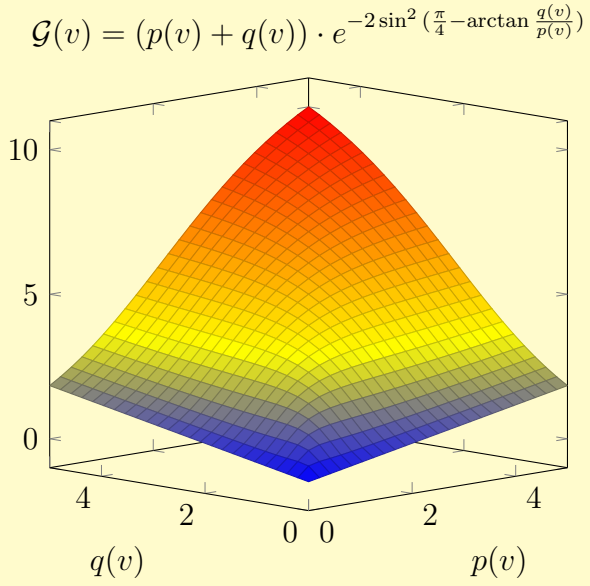

Figure 3: The curve of the In-and-Out degree function

where θ, μ, λ are the parameters to be determined.

And Fig. 3 shows the curve of the Ecuación 14.

4.3 Wilbur Function

It is extremely complicated to calculate Core Nebulas Rank if we consider an array of different usage case and its properities. However, we can provide a more general function for Nebulas Rank.

We define the Core Nebulas Rank calculation function as $f(x)$, namely *Wilbur Function*[1],where x is the factor of Core Nebulas Rank, it can be account stake, coinage or the in-and-out degree. $f(x)$ satisfies flowing two properties:

Propiedad 1. *For any two variables x_1 and x_2, which are both larger than 0, the sum of the two functions is smaller than the function of sum of two variables.*

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

Propiedad 2. *For any two variables x_1 and x_2 are infinity, the sum of the two functions is approximately equal to the function of the sum of the two variables.*

[1]The name *Sybil Attack* derives from 1970's TV mini-series Sybil, in which an young woman is diagnosed as suffering from muliple personalities and receives treatment from psychiatrist named Dr. Cornelia Wilbur.

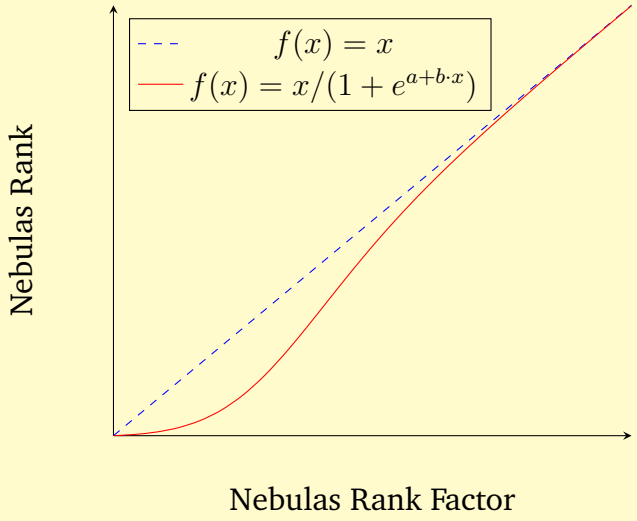

Figure 4: The curve of the Nebulas Rank function

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

These properties described above ensure, under given transaction behaviors, the benefit of splitting stakes into smaller accounts is comparatively smaller than keeping them within a single account. At the same time, when the stake is large enough, the cost of splitting the stakes into small accounts can be ignored.

There is more than one function that satisfies the two properties above. Here, we provide a succinct function, the curve of the function is shown in Fig. 4.

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

Detailed proofs for the function are given in Appendix A

In summary, Ecuación 11 can be expressed further as below:

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

where a, b, c, d are parameters to be determined.

In order to verify the effectiveness of the function, we calculate the Core Nebulas Rank for all accounts on the Ethereum blockchain over a certain time period. We collected all the transaction records from May 1st 2017 to June 30th 2017 (block

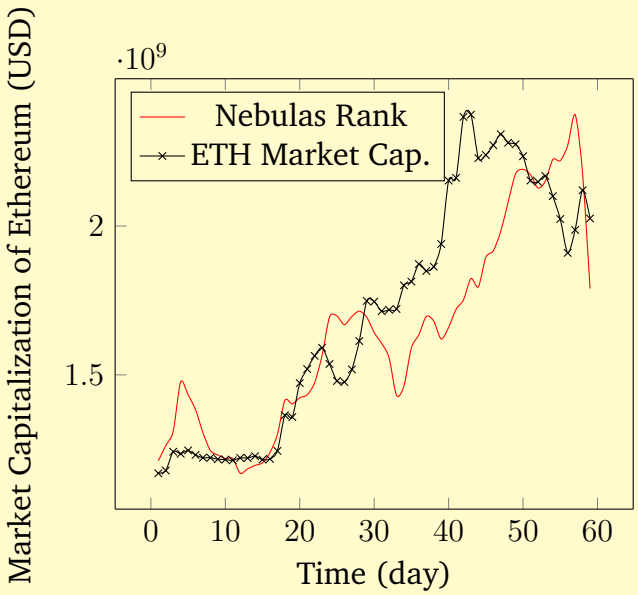

Figure 5: The market capitalization and Core Nebulas Rank of Ethereum

height: from 3629091 to 3955158), in addition, we also collected average daily ETH token price (in USD) and transaction volumes [24].

Fig. 5 shows the trend between ETH market capitalization and Core Nebulas Rank of the Ethereum, where the black solid line indicates Ethereum market capitalization (in USD), while the red solid line represents the summation of all accounts' Core Nebulas Rank based on Ecuación 21.

We can see that the Core Nebulas Rank reflects the market capitalization changes of Ethereum precisely. The correlation coefficient is 0.84427, p (p-value) is $4.48 \times 10^{-17} < 0.001$. That means, the Ecuación 11 illustrates the success in depicting the contributions of users to the economic system on chain, which demonstrates both the validity and accuracy of Core Nebulas Rank.

5 Manipulation-resistance of Core Nebulas Rank

This chapter is the analysis on how Core Nebulas Rank resists manipulation, i.e. the fairness of Nebulas Rank.

Manipulation refers to dishonest actions of an attacker for personal gain. Actions that may be undertaken by attackers include: launching asset transfers, this involves making use of assets and accounts controlled by them and their other dishonest individuals. Among the transfers, the amount of asset doesn't exceed the asset owned by the attacker; the source of transfer is either the accounts owned by the attacker

and its cooperators, or some institutes' accounts who serve as exchanges. Usually, the benefit obtainable is determined by the accounts whose private keys are known by the attacker. A simple case is that the attacker's benefit is the sum of all of these accounts' ranking scores. Of course, it could be noticed that the private keys of institutes' accounts mentioned before are not controlled by the attacker.

The analysis of this section is based on the actions undertaken and the attackers' benefit defined above. First, we discuss the upper-bound for a single account's ranking score enhancement. Then we analyze the upper-bound for multiple accounts. Last, collusion is included and we discuss the situation of more than one attacker.

5.1 Ranking Score Enhancement for One Account

According to Ecuación 21 in order to raise the ranking score for one account, the ranking score of the account is positively correlated with both the amount of assets and the in-and-out degree. The amount of assets in the account, i.e. β, has an upper bound, i.e. it is no more than the absolute total of the assets owned by the attacker, denoted by β_0. And in-and-out degree γ represents the volume of transfers, which means the attacker needs to increase the transfers amount of one controlled account as much as possible.

The increasing of transfer amount includes two parts: increasing in-degree and increasing out-degree. Increasing in-and-out degree needs two participating accounts, one of which is the target account whose goal is to raise their ranking score, the other account could either be a controlled account or an uncontrolled account. If it is an uncontrolled account, increasing degree means transacting with other people, this situation is discussed in § 5.3. The other case is that the attacker sends assets to strangers unconditionally, which is too costly that it won't be discussed in this section. Therefore typically, it could be defined that, the actions of attackers mainly focus on increasing the transfers among the accounts controlled by themselves. Since the assets controlled by attackers are limited and the time period for ranking is also limited, it holds that the degree of an account has an upper-bound which is decided by the amount of assets held by the attacker.

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. And the in-and-out degree is $\gamma = 2\beta_0$. The ranking score is

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

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

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

5.2 Ranking Score Enhancement for Multiple Accounts (Sybil Attack)

Sybil Attack refers to a situation whereby the attacker obtains falsely high ranking score by creating a large number of pseudo-identities to tamper the reputation system of P2P network [25].

An entity on a peer-to-peer network is a piece of software which has been granted access to local resources. An entity advertises itself on the peer-to-peer network by presenting an identity. More than one identity can correspond to a single entity. In other words, the mapping of identities to entities may be multiples to one. Entities in peer-to-peer networks utilise multiple identities for purposes of redundancy, resource sharing, reliability and integrity. In peer-to-peer networks, the identity is used as an abstraction so that a remote entity can be aware of identities without necessarily knowing the correspondence of identities to local entities. By default, each distinct identity is usually assumed to correspond to a distinct local entity. In reality, many identities may correspond to the same local entity. An adversary may present multiple identities to a peer-to-peer network in order to appear and function as multiple distinct nodes. The adversary may thus be able to acquire a disproportionate level of control over the network, such as by affecting voting outcomes [26].

Here we assume the attacker's payoff is the sum of all accounts controlled by the attacker. Considering the strategy to enhance ranking score for one account, which is analyzed at last subsection, the attacker could apply the same strategy to multiple

accounts: starting from any one account, the attacker transfer part of its asset into the next account, finally forming a linked asset flow. In this case, since Core Nebulas Rank requires that no more than valid amount of asset stays in the account for no more than half of the period, by no means the attacker could make β for more than one account to be the total amount of assets owned by it. Thus the attacker should adopt another strategy where its assets are evenly distributed into all its accounts. Suppose the length of link is N, i.e. there are N controlled accounts, and for every account, $\beta = \frac{\beta_0}{N}$. The in-and-out degree analysis is same with § 5.1, the upper-bound of γ is $K \cdot \beta$, where $K = 2 \cdot N$ is a constant integer. Therefore the upper-bound of the sum of all accounts owned by the attacker is:

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

5.3 Coalition Manipulation

The result of coalition manipulation is no different than the case where one attacker owns the original total assets of two attackers. In this situation we can analyze the case of coalition manipulation by analyzing the consequence of a single attacker's assets increasing.

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:

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

□

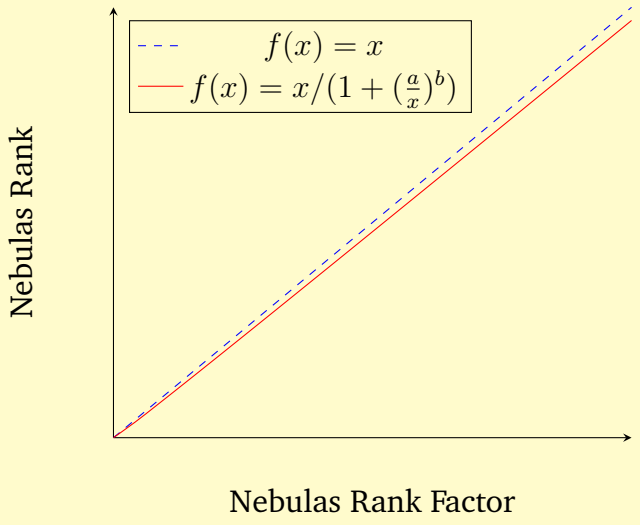

Figure 6: Curva de la función de Nebulas Rank

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.