Yellow Paper: Nebulas Rank

Nebulas Research

June 2018

Version:1.0.1

Conteúdos

1 Introdução

Hoje em dia, mais e mais cenários beneficiam de *descentralização*, que é o núcleo dos sistemas blockchain. Por exemplo, Bitcoin, a origem da blockchain, provou a sua significância relativa aos activos digitais, enquanto o Ethereum provou o quão importante a descentralização é para dApps. E existem mais e mais projectos na blockchain a explorar como tomar partido da descentralização.

Obviamente, a espinha dorsal da descentralização na blockchain é a sua abertura e características de anonimidade.

No entanto, abertura e anonimidade obstruem a emergência das medidas de valor [1]. Existem dois aspectos. Primeiro, é difícil inferir se uma conta pertence ao mesmo utilizador, o que significa que é difícil construír um mecanismo como HTTP Cookies [2], ou usar tecnologias de análise de dados tradicionais para entender características dos utilizadores. Segundo, a ertura da blockchain torna-a vulnerável a manipulação, especialmente medidas de valor. Atacantes podem facilmente obter todos os detalhes sobre as medidas de valor, e descobrir o ponto fraco do sistema. Isto difere dos métodos de medida de valor tradicionais que são fechados ou independentes.

Acreditamos que medidas de valor eficazes são a fundação da prosperidade da blockchain. Tanto a ineficácia como a falta de uma medida de valor podem restringir os usos da blockchain.

Primeiro, precisamos de uma metodologia para quantificar os valores dos dados, aplicações e contas nas blockchains. O problema raiz é que a cooperação na blockchain continua a escalar para cima, e os requisitos de eficiência continuam a aumentar. Sem medida de valor, tal colaboração pode ser afectada negativamente.

Segundo, blockchains encontram-se num estágio inicial, e o valor dos dados e activos nas blockchains estão ainda subterrados e à espera de ser encontrados. Medidas de valor eficazes irão desenterrar o seu valor e capacitar mais aplicações e cenários potenciais, por exemplo, empréstimos, crédito, pesquisa de dados, recomendações pessoais, e interacção cross-chain.

Terceiro, incentivos, baseados em médias de valor, são necessários para um ecossistema blockchain saudável. Sem medidas de valor eficazes, incentivos podem levar o sistema blockchain à corrupção, e colapso eventual.

Concluindo, uma medida de valor eficaz para a blockchain tem de ser

- **Verdadeira.** O rank (a classificação) tem de medir uma característica de um sistema blockchain, e, portanto, tem de ser fidedigno;
- Justa. Isto significa que a classificação tem de ser resistente a manipulação, e é o núcleo do algoritmo de classificação.

- Diversa. Irão existir vários requisitos de classificação para aplicações diferentes na blockchain, portanto um bom algoritmo de classificação deve cobrir cenários diferentes.

Nós acreditamos que o Nebulas Rank deve ser uma medida de valor eficaz para blockchains.

Para veracidade, definimos o Nebulas Rank como a quantificação da contribuição de uma conta no sistema blockchain depois da consideração de várias métricas.

Acreditamos que as criptomoedas devem ter os atributos do dinheiro, e as suas três funções: meio de troca, reserva de valor, e unidade de conta. Blockchains por si só são sistemas económicos e a teoria monetária clássica tem valor instrutivo. Mais, acreditamos que o valor das criptomoedas provém da sua liquidez. Especificamente, cada transacção entre utilizadores aumenta a liquidez das criptomoedas, e eventualmente dota um valor à criptomoeda. Por isso, transacções on-chain são fontes de dados naturais para uma medida de valor eficaz.

Para avaliar a eficácia do Nebulas Rank, calculámos a soma da classificação (rank) de todas as contas no Ethereum, e comparámo-las com a capitalização do mercado dada pelo coinmarketcap.com. A nossa avaliação mostra uma correlação forte entre eles, cerca de 0.84. O que significa que a Nebulas consegue medir a contribuição de contas num micro-nível, apesar de também ser capaz de medir o valor de blockchains num macro-nível.

Para justiça, involvemos uma função especial para resistir manipulação, e a nossa análise demonstra o seu desempenho em termos de resistência a manipulação.

Baseado na teoria do Nebulas Rank, dividímos o Nebulas Rank em Core Nebulas Rank e Extended Nebulas Rank para aplicações e cenários diferentes.

Core Nebulas rank define o algoritmo que calcula a contribuição de uma conta para o sistema blockchain inteiro durante um certo período de tempo, e o grau de entrada-e-saída de uma conta durante um período de tempo.

Extended Nebulas Rank é para aplicações e cenários diferentes, e é baseado no Core Nebulas Rank. Por exemplo, mostrámos como classificar smart contracts baseado no Core Nebulas Rank; também mostrámos como estender o Core Nebulas Rank para um vector multi-dimensional.

Além da teoria e metodologia do Nebulas Rank, também apresentámos a nossa consideração sobre como implementar o Nebulas Rank, incluindo se deveremos pôr pontuações das classificações on-chain, como actualizar o algoritmo do Nebulas Rank, e o nosso trabalho futuro no Nebulas Rank.

Dica especial: O conteúdo deste yellow paper pode ser diferente da descrição no nosso whitepaper (a versão 1.02 foi lançada em Abril de 2018) [3]. Isto é porque continuamos a desenvolver e a

verificar o algoritmo no nosso whitepaper, e agora sentimo-nos mais confiantes e capazes de o tornar mais rigoroso. Usamos um formato diferente (como este parágrafo) para enfatizar actualizações relevantes presentes neste yellow paper.

2 Fundo

Neste capítulo, introduzimos o fundo da blockchain e tecnologia associada. Devido à ausência de uma medida de valor, vamos discutir a implementação dos algoritmos de classificação típicos na área da blockchain, e as suas desvantagens.

2.1 O Estado do Desenvolvimento da Blockchain

Satoshi Nakamoto publicou o whitepaper da Bitcoin [4] em Outubro de 2008. Como a aplicação mais antiga de blockchain, Bitcoin é o exemplo mais marcante de um sistema criptomonetário descentralizado. A produção da bitcoin é dependente de computações massivas que executam um algoritmo especial, em vez de uma organização, o que garante a consistência num livro-razão descentralizado.

Com uma linguagem de programação de script específica, Bitcoin pode ser usada para fazer pagamentos de terceiros, micro-pagamentos eficientes, e mais. Logo, uma onda de experiências proveniente da Bitcoin emergiu, e adicionou características mais complexas do que as propriedades monetárias básicas. Por exemplo, Namecoin [5] representa um DNS distribuído e outros como o Open Assets baseados em colored coins, ambos cópias de activos inteligentes que imitam a rastreabilidade da Bitcoin.

Infelizmente, a linguagem de script da Bitcoin tem muitas falhas de concepção, como a falta de instruções e fala falha do teste de Turing completude, limitando a sua utilidade.

Com o desenvolvimento de tecnologia relativa à blockchain, mais sucessores apareceram e tentaram estender as funções relativas a aplicaçõe diferentes. A mais significativa foi o Ethereum [7], fornecendo smart contracts com Turing completude, o que criou novas possibilidades para as aplicações.

Smart contracts são contractos executados por um método técnico num sistema de blockchain. O smart contract Ethereum é executado na EVM (Ethereum Virtual Machine), que não está sob o controlo de nenhuma entidade, e garante a consistência do output, e do smart contract por si só, através do seu algoritmo de consenso.

As pessoas podem desenvolver aplicações distribuídas (dApp) com funções complexas baseadas no smart contract do Ethereum. Estas dApps fornecem soluções para vários campos além de transacções básicas, como votação, financiamento colaborativo, empréstimos, direitos de propriedade, e mais. No entanto, mesmo que o Ethereum aumente as possibilidades das aplicações na blockchain, não existem apps matadoras na sua plataforma devido à falta de uma medida de valor.

Para um sistema que suporte smart contracts, existem dois tipos de conta. Contas de propriedade externa (EOA) e contas smart contract, e ambas carecem de uma medida de valor razoável. Ao mesmo tempo, informação inestimável é ocultada durante o processo de invocação do smart contract. A informação tem mais dimensões comparada com os dados de transacção tradicionais, e não pode ser avaliada com medidas de avaliação clássicas.

Em inícios de 2015, Chris Skinner concebeu a idea de value web [8], notando que o valor de um ecossistema deve conter trocas de valor, reservas de valor e sistemas de avaliação de valor. Chris nota também que há uma diferença clara entre uma plataforma de uma criptomoeda e uma sociedade tradicional, em termos de avaliação de valor, o que representa um desafio para classificar e medir o valor dos dados e a informação na plataforma da criptomoeda.

2.2 Algoritmos de Classificação de Nós Baseados em Grafos

A nova geração de projectos de blockchain como o Ethereum constroem ecossistemas complexos, são mais do que uma plataforma de criptomoeda. No entanto, não há um método razoável para avaliar o valor da entidade na cadeia/blockchain. Por exemplo, não fazemos a menor ideia sobre a qual tem a maior contribuição para o sistema de blockchain, ou como medir essas contribuições.

Aqui, iremos introduzir o algoritmo PageRank [9], uma medida de reputação típica, uma das primeiras na internet. Tão antiga como o algoritmo central da Google, PageRank era suposto resolver o problema de classificação em análise de web links. Com o desenvolvimento do PageRank, este tem sido usado em vários campos e tido muitos usos, como a classificação da importância de papers académicos, web crawlers, extração de palavras chave, classificação da reputação de utilizadores em redes sociais, etcetera.

Alguma investigação foca-se em usar o PageRank em blockchains. Fleder, Kester, Pillai et al. usaram o PageRank para descobrir endereços de contas na Bitcoin e analisar as suas actividades [10]. No entanto, a metodologia usada foi trabalho analítico manual com a ajuda do PageRank.

Como o algoritmo de classificação clássico, criado na web 2.0, PageRank sofre de limitações em classificação de reputação online.

Mais investigação em melhorar o PageRank tem emergido, e um dos mais famosos chama-se LeaderRank [11]. LeaderRank melhora a probabilidade de transição ao introduzir um nó base e arestas bidimensionais em vez de usar a mesma probabilidade de transição do PageRank, o que faz com que os nós tenham uma probabilidade de transição diferente, dentro e fora. Mas existem limites: o LeaderRank conta a classificação da reputação iterativamente e apenas considera a ligação entre os nós, ignorando a avaliação das actividades dos utilizadores.

Note que estes tipos de algoritmos de PageRank não são resistentes a aataques Sybil [12], que é uma estratégia onde um adversário subverte um sistema de reputação numa rede simétrica ao criar um grande número de pseudónimos.

O trabalho mais relevante do Nebulas Rank é o NEM [13]. Diferente do Proof-of-Work da Bitcoin, e da estratégia de consenso Proof-of-Stake do Ethereum, NEM adopta o protocolo de consenso Proof-of-Importance (prova de importância) e o NCDawareRank [14] como o seu algoritmo de classficação. O NCDawareRank tira partido do efeito de agrupamento da topologia da rede usando um algoritmo de alocalão (clustering) baseado no algoritmo de SCAN [15][16][17]. Apesar de haver uma estructura comunitária no grafo de transação e de ter utilidade contra os nós de spam, não garante que todos os nós na blockchain controlados por uma entidade no mundo real sejam mapeados num só grupo, o que deixa muito a desejar em termos de manipulação.

2.3 Resistência à Manipulação

A capacidade de resistir à manipulação, ou seja, veracidade, é o objectivo mais desafiante e significativa do Nebulas Rank.

Hopcroft et al. descobriram que o PageRank falha a avaliar a reputação de um utilizador sob manipulação [18]. Zhang et al. notam que um adversário pode diminuir o número da reputação de utilizadores não-Sybil eficazmente mesmo que o índice de avaliação da reputação do nó tenha sido construído [19].

Isto ocorre porque os algoritmos do PageRank funcionam baseados em topologia de rede, enquanto que um adversário pode obter uma pontuação de pontuação igual ou superior criando uma imagem da rede [20][21].

Em sistemas blockchain, alguns métodos de manipulação são:

1. Loop transfer. O atacante transfere através de um laço, o que permite o mesmo dinheiro flua sobre as mesmas arestas repetidamente. Assim um atacante espera aumentar o peso das arestas relacionadas.
2. Transferência para endereços aleatórios, para que o grau de foro do nó sybil aumente, e também a propagação do fundo;
3. Formação de um componente de rede independente com endereços controlados pelo atacante, para que este possa aparentar ser o nó central;
4. Interacção frequente com endereços do serviço de troca autoritativo, ex. transferência repetida do mesmo dinheiro entre o serviço e o atacante, para que este possa obter uma melhor posição estructural na rede.
Devemos ter isto em conta, de modo a garantir a justiça no Core Nebulas Rank, durante o estágio inicial.

3 Modelo económico

Criptomoedas são dotadas de significância económica, ora como meio de troca, ora como activo inteligente. Logo, um modelo económico razoável pode ajudar a estabelecer uma medida de valor padrão na blockchain, que é o objectivo do Core Nebulas Rank. Este capítulo começa por introduzir a representação matemática de uma criptomoeda, e depois analiza a criptomoeda com um modelo monetário simples e bem reconhecido. Durante a análise, iremos introduzir o Core Nebulas Rank como um argumento importante.

3.1 Representação de Criptomoedas

A maior diferença entre criptomoedas e a economia tradicional é que todas as transacções de uma criptomoeda são rastreáveis. Este facto fornece fontes de dados, com as quais analisamos o impacto de cada transacção no sistema económico.
De modo geral, um sistema de criptomoeda pode ser definido pelo par $(\mathscr{L}, \mathscr{U})$, onde $\mathscr{L}$ é o sistema livro-razão, e $\mathscr{U}$ é o conjunto de utilizadores da criptomoeda. Adicionalmente, o sistema livro-razão pode ser descrito como o trio abaixo descrito:

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

onde A é o conjunto das contas, D é o conjunto dos balancetes iniciais, e T é o conjunto das transacções. Cada transacção pode ser gravada como o tétrade abaixo:

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

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

onde $a \to d$ representa o balancete d correspondente à conta a (d é um número real positivo, o que quer dizer que não temos contas com balancete igual a zero em consideração). s, t, w e τ representam a conta do remetente, a conta do destinatário, quantidade e tempo da transacção, respectivamente.

Uma conta é controlado por um utilizador, que pode propor uma transacção com uma conta, que pode ser denotado como:

$$u \text{ dom } a \,.\, u \in \mathscr{U}, a \in \mathscr{A} \tag{4}$$

Por outro lado, um utilizador pode controlar várias contas, representado por:

$$A(u) = \{\, \forall a \in \mathscr{A} : u \text{ dom } a\} \tag{5}$$

Também, uma conta pode apenas ser controlado por um único utilizador, representado por:

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

Noote que o modelo acima descrito é uma simplificação razoável de qualquer sistema de uma criptomoeda. No modelo, não fazemos distinção entre dados on-chain e off-chain, e não introduzimos nem preços de transacção, nem invocações de smart contracts. Adicionalmente, as contas de uma bolsa (economia) são específicas do tipo. De forma geral, as transacções numa bolsa podem ser divididas em duas categorias: transacções normais que serão guardadas na chain, ou transacções intra-bolsa que não serão guardadas na base de dados centralizada da bolsa. O resultado

é que perdemos as transacções intra-bolsa se apenas conseguimos obter dados da blockchain. No entanto, se se os puder obter através de cooperação da bolsa, podemos mapear uma conta de bolsa em várias contas, para utilizar o modelo acima descrito.

3.2 Modelo da Criptomoeda

Apesar de criptomoedas serem vastamente diferentes das tradicionais moedas de comodidade e dinheiro fiat, a teoria monetária clássica ainda tem valor. Como dinheiro de uma nova entidade económica [21], as criptomoedas nascem com os atributos do dinheiro e têm as três funções do dinheiro: meio de troca, reserva de valor, e unidade de conta.

Por este meio, estabelecemos então um modelo monetário simples e clássico para nos ajudar a perceber a importância física do Nebulas Rank.

Antes de tudo, tentamos dar um indicador para medir o *factor de velocidade* num sistema criptomonetário.

Outro conceito a ser diferenciado do *factor de velocidade* em economia é a liquidez. Liquidez é usada para descrever o nivel de dificuldade da troca de activos num meio de troca. Como o dinheiro em si é o meio da troca em economia, dinheiro é o activo com maior liquidez.

No Livro Branco Técnico da Nebulas [3], usamos a palavra *liquidez*. No entanto, não há uma definição rígida de liquidez, cujo significad é muito amplo, mesmo em economia. Por exemplo, a definição de liquidez no *The New Palgrave: A Dictionary of Economics* inclui três aspectos completamente diferentes. R.S. Kroszner salientou que cerca de 2796 papers independentes a mencionar liquidez foram publicados nos últimos 6 meses, e cada um levantou uma questão diferente [22]. Liquidez neste livro amarelo refere-se à **velocidade do dinheiro**, ou seja, a rotatividade de uma unidade monetária durante um certo período de tempo.

Usamos a velocidade do dinheiro para representar a variação da rotatividade durante um certo período de tempo (um dia neste paper), que é representada por um V. De acordo com a teoria quantitativa da moeda, a equação é exprimida como indicada abaixo:

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

onde M, V, P e Y representam respectivamente: o valor monetário total do sistema económico, a velocidade do dinheiro, o nível de preços (medido pela produção económica, logo o preço do dinheiro é $\frac{1}{p}$), e a produção económica real (PIB real). A equação ilustra que o producto da quantidade monetária e da velocidade do dinheiro são iguais ao producto do preço de bens e a sua produção económica.

Quanto à quantidade monetária M, Nebulas é semelhante ao Ethereum na medida em que a quantidade monetária mantém um crescimento contínuo (a percentagem da emissão adicional de Nebulas está em 4% de momento), o que é diferente da Bitcoin visto que a quantidade total monetária irá estabilizar quando chegar a 21 biliões, por fim. A velocidade do dinheiro V pode ser descrita como a razão entre a quantidade monetária em circulação e a oferta monetária. Como tal, a equação [7] pode ser expressa mais por:

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

onde Δm é a oferta monetária adicional.

Em termos do nível de preço P, é aceitável que o valor do preço seja determinado pela relação entre a oferta monetária e a procura, ambos dados pela teoria clássica do dinheiro e pelos novos Modelos Keynesianos. A longo prazo, o nível de preço total será ajustado para tornar a oferta monetária e a procura iguais.

No entanto, a curto prazo, os níveis de preço nem sempre nos dá um equilíbrio entre procura e oferta monetária. Num sistema económico saudável, a taxa de crescimento dos níveis de preço é frequentemente menor do que a velocidade do dinheiro. Ao aumentar a oferta monetária (reduzir as taxas de juro, por outras palavras), tanto os níveis de preço P e a oferta de bens/serviços Y vão aumentar. Por outro lado, o aumento da velocidade de crescimento dos níveis de preço deve ser controlado, de modo a desmotivar utilizadores de acumularem criptomoedas durante um período de tempo longo, o que diminuiria a velocidade. A razão pela qual os utilizadores acumulam criptomoedas é a esperança que o preço da moeda irá subir.

No que diz respeito à produção económica Y, é normalmente representada como o PIB real por economistas, nomeadamente *uma medida monetária do valor do mercado de todos os bens finais e serviços produzidos num certo período de tempo*. Acreditamos que o valor de uma criptomoeda é

baseado na sua velocidade, nomeadamente cada transacção que contribui para o agregado económico de alguma forma. Portanto, pensamos que o Y na equação [8] consiste em cada transacção. Dado que os sujeitos de um sistema económico são contas, também podemos definir Y como as transacções emitidas por cada conta como abaixo:

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

onde $C(a)$ representa as contribuições feitas pela conta a para a produção económica, nomeadamente o Core Nebulas Rank.

O desenvolvimento de uma criptomoeda depende do desenvolvimento da sua comunidade. Logo, consideramos que a quantificação das contribuições feitas por cada conta é a base para engendrar uma mecanismo de incentivos razoável. Baseado nisto, o sistema económico pode então criar incentivos explícitos (ex. Proof of Devotion no Livro Branco Técnico da Nebulas), ou incentivos implícitos (ex. A ordenação dos resultados fornecidos pelos motores de busca). A directiva e incentivos primitivos numa criptomoeda é a emissão adicional da moeda, que é diferente da teoria monetária tradicional.

4 Core Nebulas Rank

Core Nebulas Rank é usado para medir as contriubuições de um utilizador para a economia **durante um certo período de tempo**. Calcular a contribuição precisamente é bastante complicado, portanto fornecemos um algoritmo de aproximação para esse propósito. Neste algoritmo de aproximação considerámos dois factores críticos: a cunhagem e a informação da posição da conta na rede de transacção. Na secção abaixo iremos provar a eficácia deste algoritmo de aproximação.

Usamos o histórico de transacções na mainnet durante um certo período como a fonte de dados do Core Nebulas Rank. Todos as transacções num certo período de tempo $[t_0 - T, t_0]$ podem ser definidos como o conjunto:

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

Baseado em $\Theta(t_o)$, podemos definir um grafo direccionado com pesos, o nó do endereço da conta, a aresta do nó s para o nó d representa uma transacção, o grau da aresta é d, e o tempo da aresta é τ. Para uma conta $a \in A$, o cálculo do Core Nebulas Rank $C(a)$ é baseado em $\Theta(t_o)$, que pode ser representado como:

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

$\beta(a)$ é a aposta mediana da conta a durante um certo período de tempo; $\gamma(a)$ é o grau de entrada-e-saída da conta a durante um certo período.

Diferente da maneira como calculámos o Core Nebulas Rank no livro branco da Nebulas [3], fizémos algumas actualizações abaixo:
1. Não usamos o valor K mais alto da maior transacção na construção do grafo de transacção;
2. Não dependemos do grau dos nós do LeaderRank para obter a importância do nó.
Primeiro, removemos os laços de transacção antes de calcular o grau de entrada-e-saída B, para resistir a um ataque de laço. Ao mesmo tempo, consideramos a força da aresta. Para alguns casos em grafo de topologia homogénea, PageRank e outras funções simétricas (como o LeaderRank) não foram capazes de resistir ataques sybil [20]. Neste livro amarelo, não usamos estratégias de classificação topológicas. Propomos uma função de cálculo assimétrica [21] que é eficaz a reduzir as recompensas ao falsificar nós de baixa aposta em S4.3.
Abaixo iremos discutir três problemas da equação 11: Aposta Mediana da Conta B(a), Grau de Entrada-e-Saída Y(a), e selecção da função Q e VI.

4.1 Aposta Mediana da Conta $\beta(a)$

Durante o período de tempo $[t_0 - T, t_o]$, existem n blocos no sistema da blockchain, marcados or:

$$B_o, B_1, \ldots, B_n$$

B_i é o bloco parente de B_{i+1}. Para uma conta $a \in A$, o balancete da conta no fim de cada bloco é

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

Podemos obter uma nova lista ao ordenar os items de forma crescente

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

onde $d_{(i)}^a < d_{(i+1)}^a$,$0 \leq i \leq n-1$, $\beta(a)$ pode ser definido por:

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

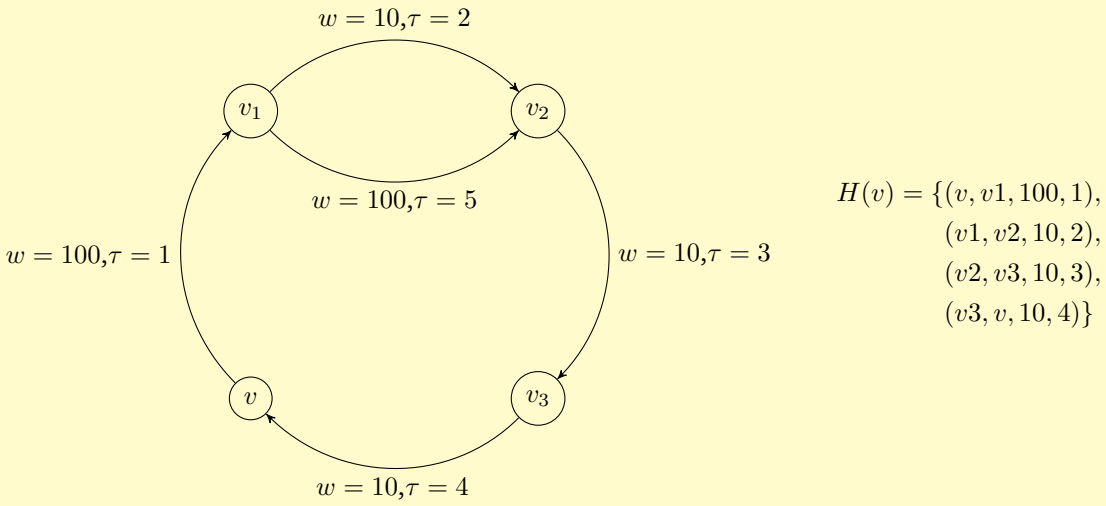


Figura 1: laço do remetente de uma transacção

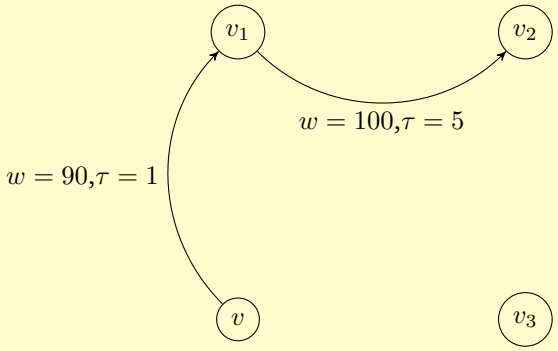


Figura 2: O grafo de transacção depois da remoção do laço do remetente na Fig. 1

A aposta mediana da conta representa a cunhagem de certa forma, o que significa que a conta tem de manter a aposta por mais de metade do período de tempo.

4.2 Grau de Entrada-e-Saída

Considere que o adversário irá aumentar o grau de entrada-e-saída ao usar um ataque de laço (loop ataque), portanto temos de remover o laço do remetente antes de calcular o grau de Entrada-e-Saída do grafo de transacção. O laço do remetente é um laço de uma transacção numa sequência de tempo. Começa e acaba no mesmo nó v que é um conjunto de arestas num grafo de transacção. Um laço do remetente pode ser denotado como $H(v)$, que é

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

onde $\forall 1 \leq i \leq n : \tau_1 \leq \tau_{i+1}$ Como demonstrado na Figura 1, há um laço do remetente, e note como a transacção $(v_1, v_2, 100, 5)$ não foi incluída no laço de transacção.
Depois de determinar o laço do remetente, temos de o remover antes de o usar. Pressupondo que existem n laços de remetente no sistema, e que estes estão listados pela sequência abaixo:

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

O valor mínimo da transacção em $H^i(v_i)$ é $(s_m^i, t_m^i, w_m^i, \tau_m^i)$, e

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

Logo, para cada transacção em $H^i(v_i)$ precisamos de subtrair a transacção mais pequena w_m^i, e remover esta transacção se o valor da última transacção é 0, que é

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

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

Fig. 2 mostra o grafo de transacção sem laços depois da remoção do laço do remetente da Fig. 1. Determine o valor da transferência para dentro do nó v como $p(v)$, depois

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

De forma semelhante, a transferência para foro do nó v é

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

Neste caso, para o nó v, o seu grau de entrada-e-saída $\gamma(v)$ é

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

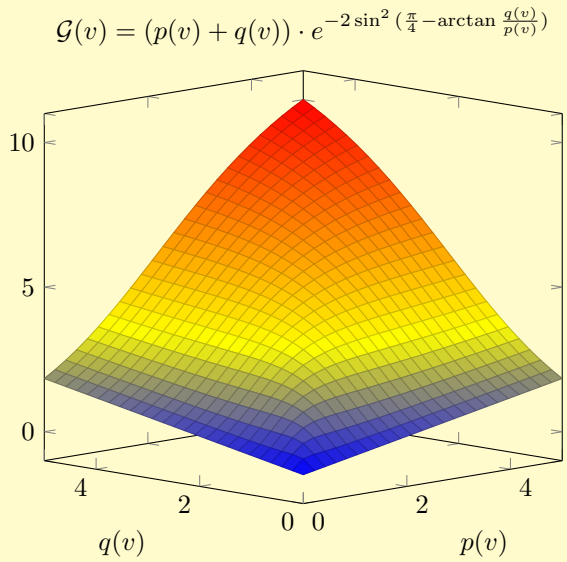


Figura 3: A função da curva do grau de Entrada-e-Saída

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

onde θ, μ, λ são parâmetros a ser determinados.
A Fig. 3 mostra a curva da função 14.

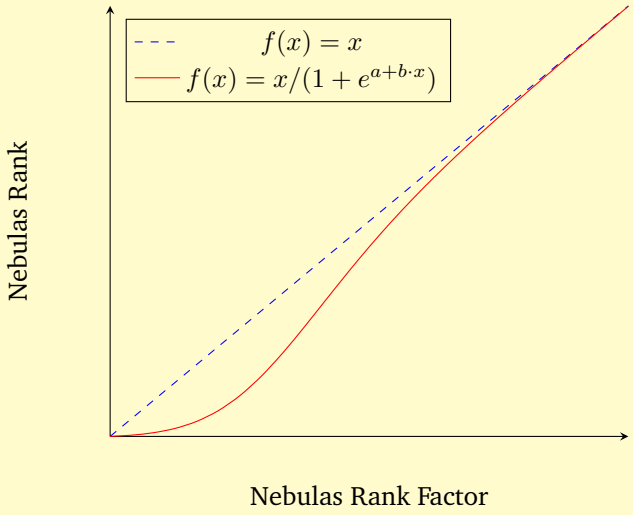
4.3 Função de Wilbur

Calcular o Core Nebulas Rank seria extremamente complicado se tivéssemos que considerar um cenário de caso de uso e as suas propriedades. No entanto, podemos fornecer uma função geral do Nebulas Rank.
Definimos a função $f(x)$ do cálculo do Core Nebulas Rank, nomeadamente, a função de Wilbur, onde x é o factor do Core Nebulas Rank, e pode ser a aposta (stake) da conta, a cunha, ou o grau de entrada-e-saída. $f(x)$satisfaz as seguintes propriedades:

1 O nome Ataque Sybil foi derivado da série televisiva Sybil, onde uma jovem é diagnosticada com transtorno de personalidade múltipla e recebe tratamento de um psiquiatra chamada Dr. Cornelia Wilbur.

Propriedade 1. *Para quaisquer duas variáveis a e b, onde ambas são maiores que 0, a soma das duas funções é maior do que a função da soma das duas variáveis.*

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



[FIGURE 4] – Factor do Nebulas Rank

Figura 4: A curva da função do Nebulas Rank

Propriedade 2. *Para quaisquer duas variáveis aproximando-se do infinito, a soma das duas funções é aproximadamente igual à função da soma das duas variáveis.*

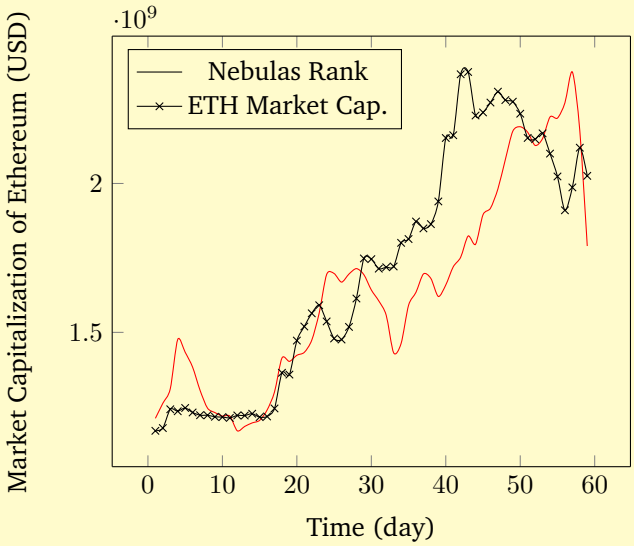
$$\lim_{x_1 \to \infty, x_2 \to \infty} f(x_1 + x_2) = f(x_1) + f(x_2) \quad x_1 > 0, x_2 > 0 \tag{19}$$

As propriedades descritas acima garantem, sob certos comportamentos transaccionais, que os benefícios da divisão de apostas em contas menores são mais pequenos do que os manter numa só conta. Ao mesmo tempo, quando a aposta é grande suficiente, o custo da divisão das apostas em contas mais pequenas pode ser ignorado.

Há mais do que uma função que satisfaz as duas propriedades acuna, Aqui, vamos fornecer uma função sucinta, a curva da funão está na Fig. 4.

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

Provas detalhadas da função são dadas no Apêndice A



[FIGURE 5] – A capitalização do mercado e o Core Nebulas Rank do Ethereum

Resumindo, a equação 11 pode ser exprimida como:

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

onde a, b, c, d são parâmetros a ser determinados.

De modo a verificar a eficácia da função, calculámos o Core Nebulas Rank de todas as contas do Ethereum durante um certo período de tempo. Coleccionámos todos os registos de transacções de 1 de Maio de 2017 até 30 de Junho de 2017 (altura do bloco: de 3629091 até 3955158), e também o preço médio diário de cada token ETH (em USD) e volumes transaccionais [24].

A Fig.5 mostra a tendência da capitalização de mercado de ETH e o Core Nebulas Rank de Ethereum, onde a linha preta indica a capitalização de mercado (em USD) do Ethereum, ao passo

que a linha vermelha representa a soma do Core Nebulas Rank de todas as contas baseada na função 21.

Podemos ver que o Core Nebulas Rank reflecte as variações da capitalização de mercado do Ethereum com precisão. O coeficiente de correlação é 0.84427, o p (valor p) é $4.48 \times 10^{-17} < 0.001$. Isso significa que a função 11 mostra o sucesso em representar as contribuições dos utilizadores para o sistema económico na blockchain, o que demonstra a validez do Core Nebulas Rank.

5 Resistência à Manipulação do Core Nebulas Rank

Este capítulo irá analisar como o Core Nebulas Rank resiste à manipulação, ex. a justiça do Nebulas Rank.

Manipulação é o facto que um atacante pode tomar acções específicas para obter mais benefícios. O espaço da acção de um atacante é a emissão de transferências de activos ao utiliar activos e contas controladas por eles e potenciais colaboradores. Entre as transferências, a quantidade dos activos não excede a quantidade dos activos possuídos pelo atacante; a fonte das transferências é ora o conjunto de contas possuído pelo atacante e os seus colaboradores, ou as contas de um instituto que servem de bolsa. Normalmente, o benefício adquirível é determinado pelas contas cuja chave privada está sob o controlo do atacante. Um caso simples é que o benefício do atacante é igual à soma das pontuações de todas as classificaçoes das suas contas. Claro, podem notar que as chaves privadas das contas dos institutos acima mencionadas não estão sob o controlo do atacante.

A análise desta secção é baseada no espaço de acção e benefícios dos atacantes no exemplo simples delineado acima. Primeiro, iremos discutir o limite superior do aprimoramento da pontuação da classificação de uma conta única. Depois iremos analisar o mesmo, para múltiplas contas. Por fim, colusão irá ser incluída, e iremos discutir a situação de mais de um atacante.

5.1 Aprimoramento da Pontuação da Classificação para Uma Conta

De modo a aumentar a pontuação da classificação para uma conta, de acordo com a fórmula 21, a pontuação da classificação de uma aconta está positivamente correlacionado com a quantidade de activos e com o grau de entrada-e-saída. A quantidade de activosna conta, ex. β, tem um limite

superior, ex. não é maior do que o número de activos possuídos pelo atacante, definidos por β_o. O grau de entrada-e-saída γ representa o volume de transferências, o que significa que o atacante tem de aumentar o número de transferências de uma conta o máximo possível.

O aumento do número de transferências inclui duas partes: aumentar o grau de entrada e o graude saída. Para aumentar o grau de entrada-e-saída são precisas duas contas, uma das quais será a conta alvo cujo objectivo é aumentar a pontuação da classificação. A outra conta pode ser controlada, ou não. Se não for, aumentar o grau significa transaccionar com outros, e esta situação é discutida em S5.3. O outro caso é que o atacante envia activos para terceiros incondicionalmente, mas isso é demasiado caro e não será discutido nesta secção. Logo, tipicamente, pode ser definido que as acções de atacantes focam-se principalmente no aumento das transferências entre contas controlados por eles mesmos. Visto que os activos controlados pelos atacantes são limitados e o período de tempo da classificação também é limitado, pode-se dizer que o grau de uma conta tem um limite superior que é decidido pelo número de activos possuídos pelo atacante.

Como analisado acima, consideramos o caso de transferir entre contas controlados pelo mesmo utilizador. Baseado no método de computação 21, definido em S4.3, o benefício do atacante irá diminuir caso este divida as transferências dos activos em múltiplas. Logo, o atacante vai tentar transferir o maior número possível de activos por transacção, ex. vai tentar transferir todos os activos que possui para uma conta, e depois de volta para a primeira. Devido ao algoritmo de remoçao de ciclos (cycle removal), os activos do atacante não podem ser transferidos de volta outra vez durante este período. O grau de entrada-e-saída é $\gamma = 2\beta_o$. A pontuação da classificação é:

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

Adicionalmente, pensamos numa maneira mais avançada de manipulação. Considere o caso em que o atacante consegue adquirir o activo outra vez noutro sítio ao transferi-lo off-line. Depois pode transferir esse activo de volta para a sua conta outra vez e o limite superior do grau de entrada-e-saída é igual ao número de activos vezes o número de transacções off-line. Visto que o tempo limite do período de classificação é limitado, o limite superior do número de transacções off-line é um número inteiro constant, ex. γ é limitado por $2T \cdot \beta_o$, onde T é um número inteiro constante indicando a duração do tempo de classificação. Logo, o limite superior da pontuação é:

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

5.2 Aprimoramento da Pontuação da Classificação para Multiplas Contas (Ataque Sybil)

Ataque Sybil refere-se a quando um atacante obtem uma pontuação de classificação elevada usando métodos desonestos, ao criar um número grande de pseudónimos para adulterar o sistema de reputação de uma rede P2P [25].

Uma entidade numa rede peer-to-peer é uma peça de software que tem acesso a recursos locais. Uma entidade anuncia-se numa rede peer-to-peer ao apresentar uma identidade. Mais do que uma identidade podem corresponder a uma única entidade. Por outras palavras, o mapeamento das identidades para entidades é surjectiva, de várias para uma só. Entidades é redes peer-to-peer usam várias identidades devido a propósitos de redundância, partilha de recursos, confiança, e integridade. Em redes peer-to-peer, a identidade é usada como uma abstração de forma a que uma entidade remota possa estar cien das identidades sem necessáriamente saber qual a correspondência entre identidades e entidades locais. Por padrão, cada identidade distinta corresponde normalmente a uma entidade local distinta. Na realidade, várias identidades podem corresponder à mesma entidade. Um adversário pode ter várias identidades numa rede peer-to-peer de modo a aparentar e funcionar como vários nós distintios. O adversário pode então ser capaz de adquirir um nível de controlo desproporcional na rede, tal como afectar o resultado de votações [26].

Aqui assumimos que o lucro do atacante é a soma de todas as contas controladas por ele. Tendo a estratégia para aumentar a pontuação da classificação de uma conta em consideração, que foi analisada na última subsecção, o atacante pode aplicar a mesma estratégia usando várias contas: começando por qualquer uma delas, o atacante transfere parte dos seus activos para a próxima conta, finalmente formando um cadeia de fluxo de activos. Neste caso, visto que o Core Nebulas Rank requere que não mais do que um número válido de activos permaneça na conta por não mais do que metade do período de tempo, o atacante não pode de forma alguma fazer com que B de uma conta seja maior do que o número total de activos possuídos por ela. Logo, o atacante deve adoptar outra estratégia onde os seus activos estão distribuídos de forma homogénea por todas as contas. Suponha que o comprimento da cadeia é N, ex. existem N contas controlados, e por cada conta,

$\beta = \frac{\beta_o}{N}$. A análise do grau de entrada-e-saída é a mesma em S5.1, o limite superior de γ é $K \cdot \beta$, onde $K = 2 \cdot N$ é um número inteiro. Logo, o limite superior da soma de todas as contas possuídas pelo atacante é:

$$\mathscr{C} = N \cdot \frac{K\frac{\beta_0^2}{N}}{(1+e^{a+b\cdot\frac{\beta_0}{N}})(1+e^{c+K\cdot d\cdot\beta_0})} = \frac{K\beta_0^2}{(1+e^{a+b\cdot\frac{\beta_0}{N}})(1+e^{c+K\cdot d\cdot\beta_0})} \quad (22)$$

5.3 Manipulação de Coalição

O resultado da manipulação de coalição não é diferente do caso em que um atacante possui o número de activos de dois atacantes. Portanto podemos analisar este caso analisando as consequências do aumento dos activos de um atacante único.

6 Implementação do Core Nebulas Rank

A implementação completa do Core Nebulas Rank está fora do escopo desta proposta, portanto apenas iremos discutir pontos chaves da implementação.

6.1 On-chain ou não?

Como foi explicado em capítulos prévios, o Core Nebulas Rank mostra a contribuição de cada conta para o agregado económico. Normalmente, cada nó é capaz de calcular a contribuição de qualquer conta, no entanto, precisamos mesmo de por o NR na chain periodicamente?
Na nossa opinião, é desnecessário ou inadequado, porque:

- O tamanho dos dados do NR será enorme, e portanto não será conveniente metê-los na chain. Mesmo com IPFS, Genaro, etc [27][28], armazenar o NR de todas as contas periodicamente seria impróprio, mesmo sendo armazenamento de dados o seu foco.
- Irá afectar o desempenho da geração de blocos. A complexidade computacional do Core Nebulas Rank é elevada, portanto pode afectar o desempenho da geração e verificação de blocos significativamente e, eventualmente, as TPS também serão afectadas.

No geral, sugerimos que cada nó seja capaz de calcular o Core Nebulas Rank individualmente.
No entanto, se cada nó fizer o cálculo individualmente, como podemos garantir que o Core Nebulas Rank é confiável e durável? Por exemplo, um nó pode viciosamente alterar o resultado do cálculo do NR e atribuir um incentivo baseado nesse resultado. Para aplicações importantes, devemos verificar o resultado do cálculo do NR, para garantir justiça; por outro lado, para aquelas aplicações que não são importantes, o uso do resultado do cálculo NR deverá depender delas, tal como a verificação do resultado.
Outra situação importante que devemos considerar é: o nó pode recusar-se a calcular o NR devido a preocupações de poupança de energia. Pensando nisso, um serviço Core Nebulas Rank de confiança pode ser introduzido, para que cálculos repetidos possam ser evitados. Esse serviço pode ser oferecido de graça, ou podemos cobrar pelo número de vezes. A implementação e detalhes do serviço estão fora do escopo deste paper.

6.2 Actualização do Core Nebulas Rank

Como todos sabemos, o Core Nebulas Rank está associado à economia de uma criptomoeda digital. À medida que a economia muda, o algoritmo do Core Nebulas Rank também deverá ser modificado, especialmente os seus parâmetros. É importante explorar como podemos actualizar o algoritmo rapidamente. A nossa solução é: actualização do algoritmo de cálculo do Nebulas Rank através do Nebulas Force.
Mais detalhadamente, vamos actualizar a estructura dos dados do bloco, e a nova estructura irá incluir o algoritmo do Core Nebulas Rank e parâmetros (baseados no LLVM IR). A Nebulas Virtual Machine (NVM) irá ser o motor de execução do algoritmo: obtém o código do algoritmo e os parâmetros do bloco, executa o código, e eventualmente obtém o Core Nebulas Rank de dentro do nó.
Sempre que o algoritmo ou os parâmetros precisarem de ser actualizados, iremos trabalhar juntamente com a comunidade, para garantir que o novo algoritmo e parâmetros sejam incluídos nos novos blocos, para que a actualização seja atempada e suave, de modo a evitar potenciais bifurcações mais tarde.

7 Extensão do Nebulas Rank

O Core Nebulas Rank é usado para avaliar a contribuição de uma conta individual para o agregado económico, e é deveras importante que o Proof of Devotion (PoD), o Developer Incentive Plan (DIP), e o Core Nebulas Rank correspondam aos seus casos de uso. No entanto, também reparámos que existem outros casos de uso que precisam de outra avaliação. Consequentemente, engendramos o Extended Nebulas Rank. O Extend Nebulas Rank é baseado no Core Nebulas Rank, para garantir incentivos contínuos para a comunidade inteira, mesmo para casos de uso diferentes.

7.1 Extensão do Nebulas Rank com Foco em Smart Contracts

Em toda a economia, a classificação de smart contracts tem um papel importante. Por um lado, ajuda o utilizador a encontrar dApps de alta qualidade, por outro, também motiva os desenvolvedores que criam essas dApps, portanto a economia pode crescer saudável e com estabilidade.

A classificação de smart contracts depende em dois factos: a comunicação de um endereço de um utilizador para um smart contract, e comunicações entre smart contracts diferentes. A comunicação do endereço do utilizador para o smart contract reflecte que a conta do utilizador ligada a esse endereço está realmente a distribuir activos e a contribuir para o agregado económico de todos os smart contracts, visto que cada smart contract tem o seu NR inicial. As comunicações entre smart contracts podem também ser tratadas como grafos orientados acíclicos. Portanto, usamos o algoritmo PageRank para calcular o NR de cada smart contract.

7.2 Extensão Multi-dimensional do Nebulas Rank

Também descobrimos que algumas aplicações precisam de dados multidimensionais para poder computar a correlação entre tipos de dados diferentes na chain. Por exemplo, num sistema publicitário baseado na blockchain, precisamos da correlação entre a publicidade e o utilizador. Nesta situação, o Extended Nebulas Rank é multidimensional, e podemos representá-lo como um vector, onde o Core Nebulas Rank constitui uma dimensão.

O extended Nebulas Rank é multidimensnal, com a excepção do Core Nebulas Rank, as outras dimensões dependem das aplicações em concreto. A forma de implementar essas dimensões também depende da aplicação em si. Porém, o algoritmo de cálculo pode sempre referenciar os cálculos do algoritmo do Core Nbulas Rank.

Partindo de um caso de uso real, engendrámos o Extended Nebulas Rank para smart contracts, e descrevêmos o método de implementação do Extended Nebulas Rank. Também ilustrámos o mecanismo de avaliação correspondente deste algoritmo, e propusemos o Extended Nebulas Rank multidimensional, o que mostra a possibilidade do nosso mecanismo de avaliação de ser usado em outros casos de uso.

8 Trabalho Futuro

O objectivo do Nebulas Rank é de dar uma medida de valor necessária à blockchain, da perspectiva de fazer uma avaliação da contribuição do endereço da conta de um utilizador para o agregado económico. Haverá mais trabalho ao longo deste percurso. Eis então o sumário do nosso itinerário para o futuro:

- Cross-chain Nebulas Rank. Podemos facilmente prever que irá haver muito demanda para transferência de dados entre cadeias (chains) num futuro próximo. Para dar alguns exemplos, interacção de dados entre cadeias e transferência de activos digitais irão certamente precisar de uma medida de valor em cadeias diferentes. Por exemplo, quando desenvolvedores transferem as suas dApps de uma chain para outra, o método do cálculo do Nebulas Rank das dApps irá ter que ser uma medida de valor única entre as cadeias diferentes.
- Mais indicadores de contribuições baseados no agregado da economia. O Nebulas Rank é baseado nas contribuições para o agregado da economia. No entanto, este tipo de desenvolvimento na indústria da blockchain precisa da sua comunidade. Portanto, em termos de agregado económico, não podemos ignorar as contribuições da comunidade. Logo, a forma como avaliamos a contribuição de um indivíduo ou organização, e como isto se reflecte no Nebulas Rank tem implicações tremendas.

Referências

[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 con- ference*, pp. 127–140, ACM, 2013.

[2] “Http cookie.” https://en.wikipedia.org/wiki/HTTP_cookie.

[3] “Nabulas 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. Lu¨, 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 *Proceed- ings 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/.

A.1 Prova da Propriedade 1

Prova. Para qualquer x1>0, x2>0, temos

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

Na fórmula 21, temos $b<0, 0<e^{(a+b)\cdot x_1}<1, 0<e^{b\cdot x_2<1}$, e mais,

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

é realmente:

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

A.2 Prova da Propriedade 2

Prova. Para qualquer $x_1>0, x_2>0$ temos

$$\begin{aligned} f(x_1+x_2)-f(x_1)-f(x_2) &= \frac{x_1+x_2}{1+e^{a+b\cdot(x_1+x_2)}} - \frac{x_1}{1+e^{a+b\cdot x_1}} - \frac{x_2}{1+e^{a+b\cdot x_2}} \\ &= \left(\frac{x_1}{1+e^{b\cdot x_2}\cdot e^{a+b\cdot x_1}} - \frac{x_1}{1+e^{a+b\cdot x_1}}\right) \\ &\quad + \left(\frac{x_2}{1+e^{b\cdot x_1}\cdot e^{a+b\cdot x_2}} - \frac{x_2}{1+e^{a+b\cdot x_2}}\right) \end{aligned} \tag{23}$$

Aqui usamos a função $g(x_1, x_2)$ que representa a parte esquerda, enquanto que $h(x_1, x_2)$ representa a parte direita:

$$g(x_1, x_2) = \frac{x_1}{1 + e^{b \cdot x_2} \cdot e^{a+b \cdot x_1}} - \frac{x_1}{1 + e^{a+b \cdot x_1}} \tag{24}$$

$$h(x_1, x_2) = \frac{x_2}{1 + e^{b \cdot x_1} \cdot e^{a+b \cdot x_2}} - \frac{x_2}{1 + e^{a+b \cdot x_2}} \tag{25}$$

Portanto 23 para x1 e x2, os seus limites podem ser representados como:

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

e temos

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

Calculamos o limite $\frac{x}{1 + \frac{1}{e^{a+b \cdot x}}}$ usando as regras de L'Hospital,

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

Na fórmula 21, temos $b < 0, \lim_{x \to \infty} -b \cdot e^{-a-b \cdot x} = \infty$, e mais,

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

De acordo com A.1, temos $g(x_1, x_2) > 0,$, portanto de acordo com o teorema do confronto:

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

Similarmente, temos:

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

Portanto,

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

Apêndice B Mudanças

- Lançamento 1.0.