

EL PROTOCOLO ÁNGEL

Las tecnologías de transacciones digitales hacen posibles nuevos esquemas de redistribución que permiten flujos continuos de liquidez a través de todos los participantes de la economía, especialmente esenciales para la reactivación de la demanda.

La siguiente es una descripción de uno de estos esquemas. Inspirado en el protocolo de resiliencia de Johan Nygren, el cual está basado en dos mecanismos: el debilitamiento de enlaces transaccionales y la distribución de tasas voluntarias; sólo que en este nuevo protocolo estas tasas se acumulan en cuentas paralelas antes de ser distribuidas.

[Sé lo complicado que pareció eso, y sí, lo es un poco...]

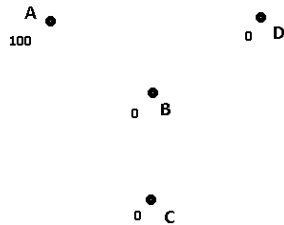
I. Debilitamiento de enlaces transaccionales

Originalmente los enlaces transaccionales son una idea de la criptomoneda Ripple desde la perspectiva de liquidación créditos. Así que sirven como una guía para volver a un estado inicial del sistema.

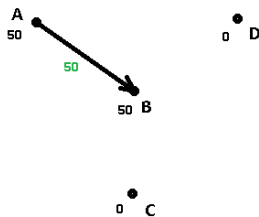
Con algunos diagramas veamos cómo funcionarán para este protocolo:

[Sé que los siguientes diagramas NO ayudan para decir que todo esto NO es una pirámide.]

Digamos que existen cuatro cuentas A, B, C, D donde inicialmente el balance de A es 100 y el de las demás es 0.



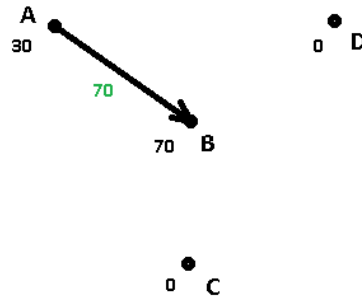
Digamos entonces que A hace una transacción a B de 50:



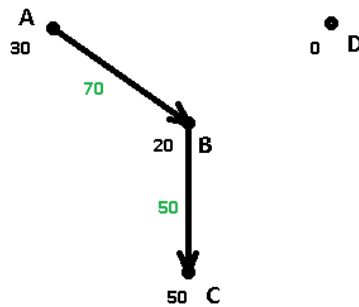
Así se genera un enlace transaccional unidireccional entre A y B por el valor de la transacción (verde).

[¡El balance del sistema sigue siendo 100! $A: 50 + B: 50 = 100$. Sólo que existe un enlace que permitiría volver a la situación inicial.]

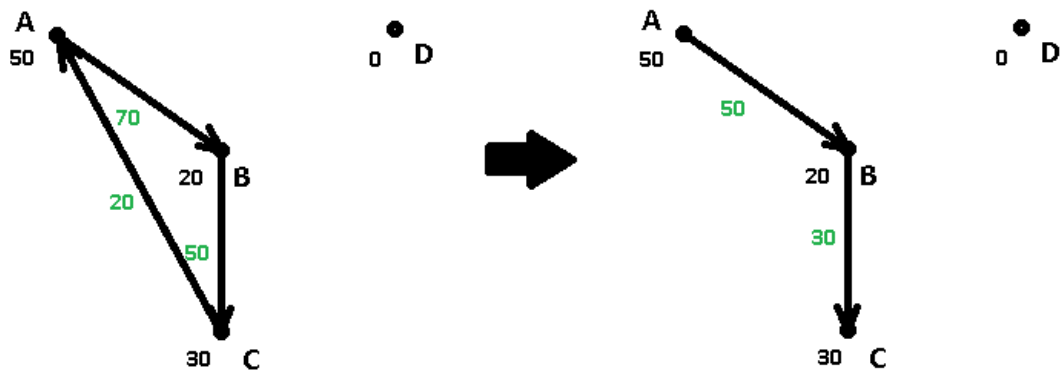
Si A hace de nuevo una transacción hacia B se refuerza el enlace. Digamos que A envía 20 a B:



Luego digamos que B hace una transacción a C de 50:



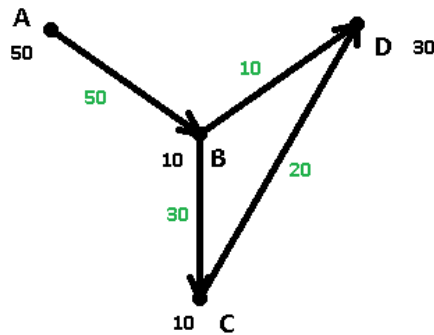
Cuando una transacción forma un lazo cerrado, se debilitan todos los enlaces del enlace por el valor de la transacción. Por ejemplo digamos que C envía 20 a A:



Es posible que se formen lazos anidados.

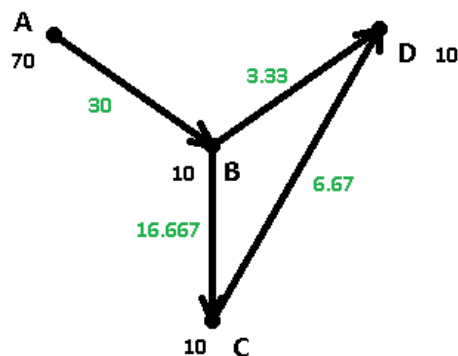
[Ok, en estos casos el debilitamiento se puede hacer de muchas maneras, este es el que sugiero, aunque puede parecer muy complicado:]

Por ejemplo digamos que se hacen las transacciones C a D de 20 y luego B a D de 10:



[En Ripple, la transacción BD hecha después de la transacción CD tomaría la ruta BCD reforzando los enlaces existentes sin crear el enlace directo BD... Pero para este protocolo necesitaremos los enlaces directos como BD, ya veremos porqué más adelante.]

Y entonces si D hace una transacción de 20 a A habría dos lazos anidados ABDA y ABCDA para debilitarlos, se va ponderando entre el enlace más débil de cada ruta única a debilitar. Para este caso las rutas únicas son BD y BCD. El enlace más débil de BCD es CD de 20. Se va a debilitar 20 entre las dos rutas, así: Por BD $6.67 = 20 * (10 / (10 + 20))$ [valor por el que se debilita = total a debilitar * (enlace más débil de la ruta / (suma de los enlaces más débiles de rutas distintas))] y por BCD $13.33 = 20 * (20 / (10 + 20))$ o $13.33 = 20 - 6.67$ [En la operación anterior hubo aproximación, así que sugiero usar el complemento].



[Hay muchas maneras más simples de hacer el debilitamiento de lazos anidados, por ejemplo, debilitar la ruta con el enlace más pequeño primero, pero considero que esta modula mejor y hace el proceso más 'justo'.]

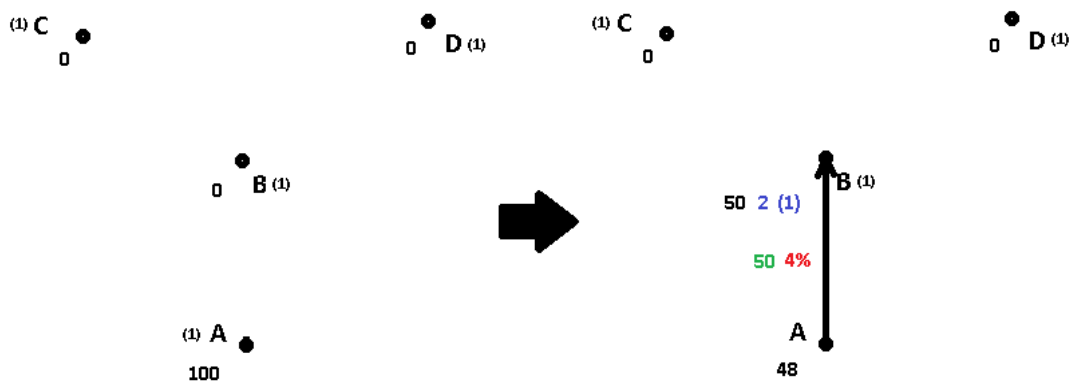
Haciendo las transacciones contrarias de los enlaces se regresa a la situación original [DC 6.67; DB 3.33; CB 16.67; BA 30]. También, haciendo transacciones que directamente regresen a los balances iniciales, los enlaces se debilitan a 0 [BA 10; CA 10; DA 10].

Así que de nuevo, los enlaces transaccionales sirven como una guía para volver a un estado inicial del sistema.

II. Distribución de tasas voluntarias acumuladas en cuentas paralelas

El segundo mecanismo consiste en acumular en una cuenta paralela a cada cuenta una tasa voluntariamente agregada a las transacciones y luego distribuir el acumulado ponderando los enlaces. [Con un ejemplo se verá más fácil:]

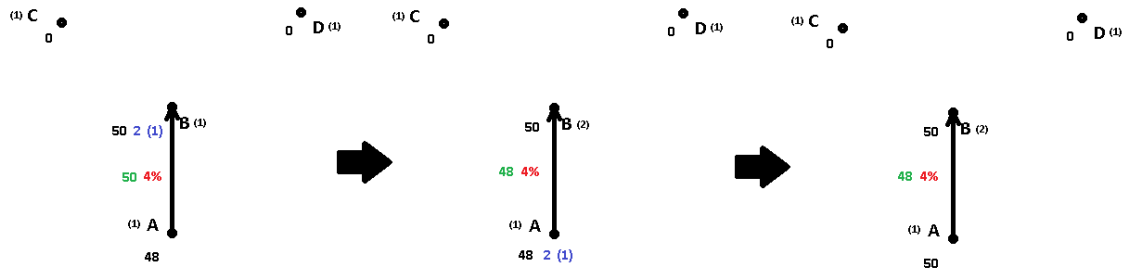
Supongamos que tenemos la situación inicial A 100 y B, C y D en 0. Luego A hace una transacción a B de 50 con una tasa adicional voluntaria del 4% [así A envía 52, pero el enlace registra 50, veremos que así se transferirá valor realmente con el adicional. 50 van a la cuenta principal y 2 a la cuenta paralela de B (azul)]:



[Check: A: 48 + (B: 50 + BII: 2) + C: 0 + D: 0 = 100 *los enlaces no entran en la suma]

La regla de distribución será esta: cuando el número de transacciones a la cuenta paralela alcance el número de enlaces entrantes +1 [número entre paréntesis] se distribuye hacia las cuentas paralelas de los enlaces entrantes y a la cuenta principal propia ponderando los pesos de los enlaces.

[nota: el número de enlaces se actualiza después de la distribución de un enlace nuevo (por lo que en este caso B distribuye):]

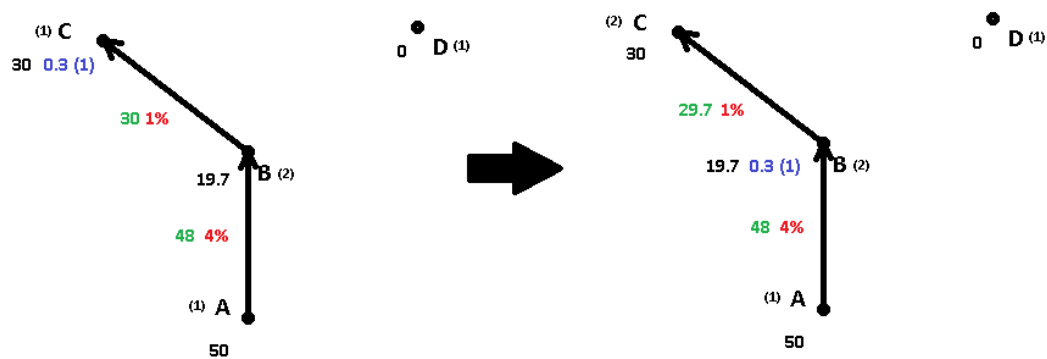


Como B no tiene enlaces salientes todavía, vemos que B distribuye el 100% de 2 a la paralela de A ¡y el enlace se debilita! También se actualiza el número de distribución de B a (2). Luego A distribuye, en este caso el 100% a sí mismo.

[Y así vemos, que A mandó a B 50 y es como si no hubiese pasado nada más. Pero, el enlace vale 48, así que si el enlace se lleva a 0 (lo que sería una transacción de B a A de 48 al 0%), no se volvería a la situación inicial sino a A con 98 y B con 2.]

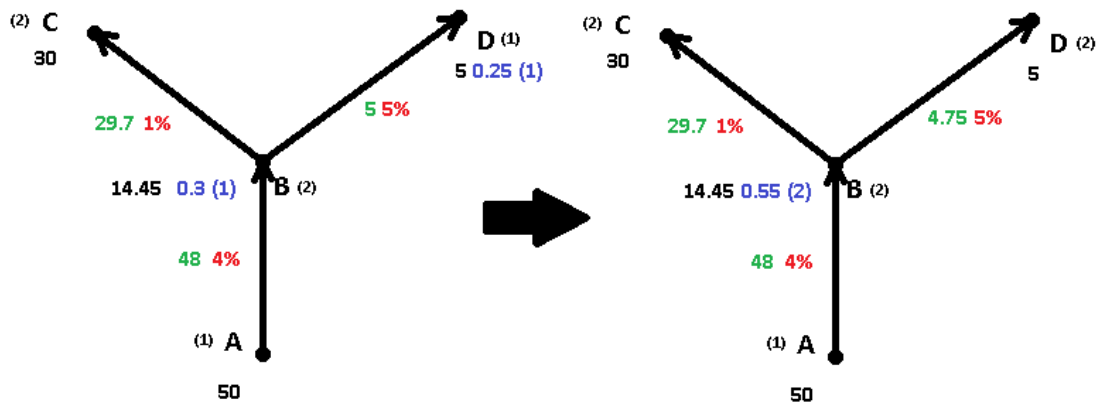
Veamos un par de transacciones más:

Primero B a C 30 al 1%:



Entonces, B envía 30.3 a C (30 a la principal, 0.3 a la paralela). Los 0.3 de la paralela se distribuyen de vuelta hacia la paralela de B debilitando el enlace, también se actualiza el número de distribución de C. Esta vez B no distribuye su paralela todavía.

Ahora B a D 5 al 5%:

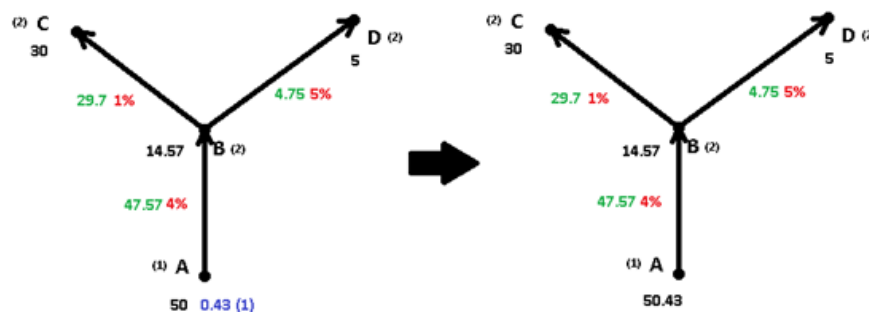


[Check: $A + (B + BII) + C + (D + DII) = 100$ *los enlaces no entran en la suma]

Hasta aquí, B envía 5.25, 0.25 llegan a la paralela de D que distribuye de vuelta a la paralela de B, debilitando el enlace, y que ahora cumple la regla de distribución. 0.55 se deben distribuir entre B y sus enlaces entrantes.

[Aquí viene una ponderación algo pesada:]

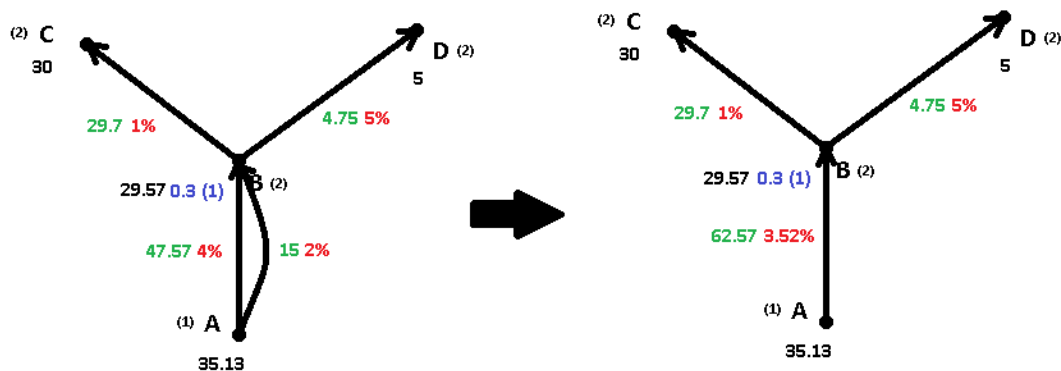
El peso de cada enlace en la ponderación está dado por su valor y su tasa, así BA pesa $1.92 = 48 * 4\%$, BC $0.297 = 29.7 * 1\%$ y BD $0.2375 = 4.75 * 5\%$. Luego se distribuye a cada enlace: BC $0.066 = 0.55 * (0.297 / (0.297 + 0.235 + 1.92))$ [distribución al enlace= valor a distribuir * (peso del enlace / suma de los pesos)], BD 0.54 y BA 0.43. Como BC y BA no son entrantes a B sino salientes, el valor calculado de ellos se acumula (0.12) y se suma a la cuenta principal de B. El valor calculado de BA va hacia la cuenta paralela de A, debilitando el enlace, y luego A distribuye a sí mismo:



[Check: $A + B + C + D = 100$]

A ya empezó a recuperar su transacción inicial de 50. La transacción inicial de A fue de 52, pero el enlace que se creó fue de 50, así que será lo máximo que recuperará *si los demás (B, C y D) continúan haciendo transacciones entre ellos*, y por efectos de la ponderación del peso del enlace que se hace cada vez más pequeño, la recuperación será cada vez más lenta.

Algo más, las transacciones con tasas diferentes al mismo destino cambian la tasa del enlace. Digamos que A hace una transacción a B de 15 al 2%:



[Check: $A + (B + BII) C + D = 100$ *los enlaces no entran en la suma]

La tasa del enlace directo cambia a: $3.52\% = (47.57 * 4\% + 15 * 2\%) / (47.57 + 15)$ [tasa del enlace = (valor anterior * tasa anterior + valor de transacción * tasa de transacción) / suma del valor anterior y el valor de transacción].

Este cambio en la tasa sólo es posible porque se tienen enlaces directos [como se mencionó antes, Ripple no cuenta con estos.]

