

PROPUESTA PARA MODIFICAR EL CONSENSO DE SATOSHI PARA MEJORAR LA PROTECCIÓN ANTE LOS ATAQUES DEL 51%

Un Sistema de Penalización por Entrega tardía de bloque



INTRODUCCIÓN

La regla de la cadena más larga o el Consenso de Satoshi, funcionó bien en el entorno relativamente descentralizado en el que se introdujo en 2009. Desde entonces, los recursos mineros se han estado concentrando, produciendo una disminución de costos de renta, de tal manera que la estrategia inicial que había planteado Satoshi ya no es válida para todas las cadenas de bloque de prueba de trabajo (PoW) que dependen de la regla de cadena más larga. Como los eventos recientes han demostrado, en algunas circunstancias puede ser económicamente factible lanzar un ataque del 51% contra las redes públicas operativas de blockchain. Este documento propone un nuevo ajuste al Consenso de Satoshi que hace que sea exponencialmente más costoso y por lo tanto menos probable, lanzar ataques para cualquier sistema de criptomonedas minable de prueba de trabajo (PoW).

El método más común para realizar un ataque de doble gasto es el siguiente:

- Ejecutar una transacción T₁ que envía monedas desde la dirección A a una dirección de centro cambiario en la actual cadena de bloques pública.
- Minar en privado un bloque en una cadena bifurcada en paralelo a la pública que contiene una transacción T₂ que envía monedas de la dirección A a otra dirección.
- Esperar a que T₁ sea confirmado por el centro cambiario. Mientras se continua minando de manera privada la cadena paralela a un ritmo más rápido que la cadena pública.
- Cambiar las monedas confirmadas en el centro cambiario, luego retirar los fondos a la dirección privada B
- Transmitir o anunciar a la red la cadena privada que es más larga que la pública.
- En este punto, la red adoptará la cadena privada de atacantes como la nueva cadena pública (ya que es más larga). Los mineros comenzarán a minar en la cadena pública recientemente reorganizada.
- T₁ ya no es válida y el atacante ya usó las monedas fraudulentamente

En resumen, estos ataques son posibles porque el sistema permite "sobrescribir" la vista actual del historial de la cadena de bloques del nodo con una nueva cadena más larga, después de que se haya aceptado una transacción específica (por ejemplo, después de que el centro cambiario esperó el tiempo de confirmación). Esto obedece a los principios de Satoshi que estableció en el libro blanco de Bitcoin e implementados por la mayoría de las criptomonedas de prueba de trabajo

(PoW). La generación de bloques en un consenso de prueba de trabajo (PoW) es un proceso estocástico y los mineros que son honestos pueden también generar bloques en paralelo a la misma altura de la otra cadena (dependiendo del tiempo de generación de bloques y retrasos de red), para lo cual el consenso de Satoshi tiene un método simple para solucionar la presencia de dos cadenas escogiendo a la cadena con el mayor trabajo acumulado. Por lo tanto, cortando ramas de la cadena corta con menos trabajo acumulado. Esto ha sido una forma eficiente de mantener una secuencia lineal de bloques en estos sistemas distribuidos.

El libro blanco de Satoshi se basa en la suposición de que la mayoría del poder de cómputo está controlado por nodos que son honestos (el principio de "una CPU por cada voto"), dentro de esta suposición es casi imposible crear una rama adversaria de longitud razonable para implementar el ataque de doble gasto. El método heurístico convencional consiste en la idea de que es suficiente esperar varios bloques de confirmación para obtener una probabilidad muy baja de cancelación de la transacción.

Muchas cosas cambiaron desde la publicación del libro blanco de Bitcoin. Algunos de los cambios más importantes que ponen en peligro la regla de la cadena más larga son la aparición de los circuitos integrados ASIC y otras técnicas de cómputo que rompen por completo el principio de "una CPU por cada voto". Muchas criptomonedas comparten el mismo algoritmo de minería, pero tienen diferencias muy marcadas en el hashrate , lo que permite que el poder computacional de un grupo de minería (Mining Pool) pueda ser utilizado para atacar otra cadena.

Por lo tanto, vemos que las suposiciones de Satoshi sobre la mayoría del poder computacional honesto y la imposibilidad de que existan largas ramas adversarias ya no son validas en el entorno actual, evidenciado por los últimos ataques del 51% en varias criptomonedas. Necesitamos un sistema más avanzado y más completo que satisfaga los requerimientos y condiciones actuales. El consenso de prueba de trabajo (PoW) central requiere correcciones para proporcionar servicios seguros, al mismo tiempo que permite la posibilidad de que mineros honestos generen bloques conflictivos y legitimar la sincronización retrasada de la red.



Para lograr este objetivo, hemos identificado una área de oportunidad que aumentaría significativamente los recursos necesarios para un ataque exitoso de doble gasto (sin cambios en la hashrate de mineros honestos). Esta modificación cambiaría el costo de un ataque para que no tenga sentido económico realizarlo. Además, el aumento de los recursos necesarios para realizar un ataque exitoso causaría que las partes receptoras y los centros cambiarios no tengan que modificar sus ajustes de cantidad de confirmaciones para liberar una transacción.

EL ENFOQUE DE PENALIZACIÓN POR ENVÍO RETRASADO

Considerando que la minería privada es la fuente de un ataque de doble gasto, para hacerlo menos efectivo, introducimos una penalización en forma de un retraso de aceptación de bloque en relación con la cantidad de tiempo que el bloque ha estado oculto de la red pública. El tiempo se mide en intervalos de bloques, no se medirá temporalmente con una estampa de tiempo.

Supongamos que se tiene el siguiente escenario de recepción de bloque en la cadena:

BN_i = Bloque Normal

BM_i = Bloque Malicioso

BN100 - BN101 - BN102 - BN103 - BN104 - [...] - BN116 - BN117 - BN118 - BN119 - BN120

 BM100

 BM101

 BM102

 [...]

 BM119 - BM120 - BM121 - BM122

Tiempo →

Figura 1

En el sistema actual, los bloques BN117, BN118, BN119, BN120 no serán minados porque tan pronto como la red recibió el bloque BM119, la cadena maliciosa se convierte en la activa y la red comenzará a minar desde el bloque BM119 abandonando la cadena original.

Para evitar esto, presentamos un retraso de aceptación de una bifurcación de la cadena de bloque actual, proporcional a la cantidad de tiempo que la bifurcación se haya ocultado de la red pública.

Este retraso representa el número de bloques para los cuales se pospondrá la adopción de la nueva cadena. Para un atacante, significa que tendrá que seguir minando la bifurcación de la cadena de bloques maliciosa incluso después de revelarlo hasta el momento en que el retraso haya terminado.

Por ejemplo, consideremos la siguiente función de retraso FR. Para definir FR primero presentamos el parámetro RB_i que representa el retraso de recepción de bloque mediante una diferencia entre la altura actual de la cadena principal y la altura del bloque recibido (Ejemplo: $RB_{BM100} = 16$, $RB_{BM101} = 15$, ..., $RB_{BM115} = 1$, $RB_{BM116} = 0$, $RB_{BM117} = -1$, $RB_{BM118} = -1$) o -1 en caso de que la altura del bloque recibido sea mayor que la altura actual de la cadena principal.

La función de retraso FR en este caso para toda la cadena bifurcada se representará como la SUMA de valores RB_{BMi} , donde i representa los índices de los bloques en la cadena bifurcada. En el siguiente ejemplo de la Figura 2, el valor de FR ($MB100, \dots, MB119$) = $16 + 15 + 14 + 13 + 12 + \dots + 0 - 1 - 1 - 1 = 136 - 3 = 133$ bloques. Por lo tanto, el atacante tendrá que seguir minando su bifurcación después de que se haya hecho pública por otros 133 bloques para que pueda ser aceptada por otros nodos como la cadena principal.

BN100 - BN101 - BN102 - BN103 - BN104 - [...] - BN116 - BN117 - BN118 - BN119 - BN120

BM100

BM101

BM102

[...]

BM119 - BM120 - BM121 - BM122

Pmb

133 - 132 - 131 - 130

Tiempo



Figure 2.

Con la función de retraso presentado anteriormente, si suponemos, que se adoptara un tiempo de confirmación de 20 bloques, un castigo de demora de 21 bloques sería $21 * (21 + 1) / 2 = 231$, que significa que el número mínimo de bloques que se tendrán que minar para poder realizar el ataque serían $231 + 21 = 252$ bloques.

Tenga en cuenta que el tiempo de confirmación no puede comenzar hasta que una bifurcación esté en progreso.

El ajuste adecuado de la función de retardo complicará un ataque hasta el punto de que no sea factible ya que requerirá una cantidad de recursos significativamente mayor y también dará una oportunidad adicional de reaccionar en la bifurcación de la cadena de bloques antes de su adopción final. La red se enterará sobre la bifurcación paralela y el atacante deberá seguir minando hasta reducir la función de retardo completamente ($DF = 0$) antes de que la red adopte la cadena paralela como la más larga. Durante este período, los participantes de la red, como los centros cambiarios, pueden congelar depósitos potencialmente fraudulentos hasta que se resuelva el problema. Supongamos que el intento de cadena fraudulenta se abandona, o se ha conducido con éxito el tiempo de retraso ($DF = 0$) a través de la fuerza bruta. Los mineros honestos continuarán agregando a la cadena activa mientras el tiempo de retraso se consume.

La función de retraso también puede considerar la dificultad actual de minería (d) para proporcionar una mejor protección para las monedas con bajo índice de hashrate (por ejemplo, el aumento de la función de retraso se vería afectada de manera inversamente proporcional a la dificultad actual de minado). Tal factor de aumento se podría ver reflejado de tal manera: $DF' = DF * f(d)$ puede ignorarse estableciendo $f(d) = 1$, pero puede sustituirse acuerdo a las necesidades, mismo que tiene las propiedades de bajo impacto para el rango de bifurcación paralela de bloque honesta, también puede escalar exponencialmente fuera de cualquier rango razonable para los mineros deshonestos.

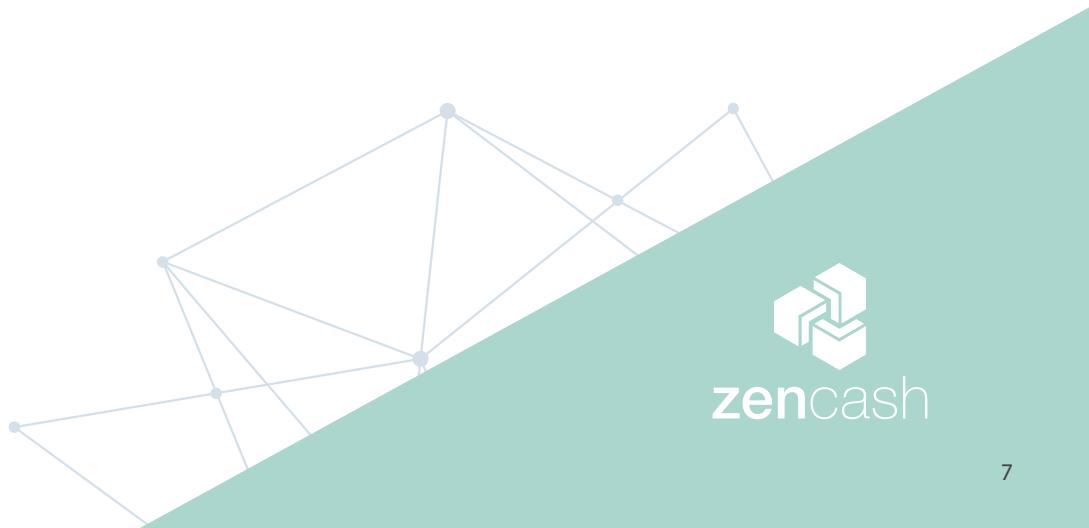
Aunque la característica introducida complica todo el espectro de ataques de minería (los que ejecutan minando bifurcaciones paralelas de manera privada), no impide que la red adopte una nueva cadena de bloques más larga en caso de una división natural (por ejemplo, cuando en algunas partes del mundo están completamente segregadas entre sí por algún tiempo determinado). El período de adopción de una cadena más larga será más prolongado que la regla del consenso de Satoshi, pero los mineros honestos trabajarán en la cadena paralela hasta conducir a $DF=0$.

Tenga en cuenta que si un adversario mina su cadena públicamente, no se aplicará la demora, pero en este caso todos pueden ver la bifurcación y tomar medidas preventivas (por ejemplo, los centros cambiarios aumentarán los períodos de confirmación, etc.).

CONCLUSIÓN

El entorno operativo para las criptomonedas ha cambiado significativamente desde sus orígenes en 2009, cuando la minería estaba mucho más descentralizada. El Consenso de Satoshi, o la regla de la cadena más larga, funcionó bien para adjudicar las bifurcaciones de cadenas naturales al simplemente adoptar la cadena con el mayor trabajo acumulado. Tanto las limitaciones técnicas como los incentivos económicos se combinan para hacer que la cadena más larga gobierne la estrategia dominante para cualquier minero, ya sea honesto o con malas intenciones. Este ya no es el caso y las cadenas de bloque públicas necesitan actualizar las reglas de consenso para que sea mucho más costoso tener éxito con los ataques de doble gasto.

Esta propuesta brinda uno de esos métodos que tiene una forma simple que, en sí misma, es bastante prometedora, pero que se puede generalizar con una función de escalado para que sea técnicamente inviable y económicamente desastroso para intentar el gasto doble. El método permite que los que minan de manera honesta puedan resolver bloques de manera paralela, así como en el caso de las fracturas de red legítimas que se resuelven con el tiempo. Ninguna estrategia de ataque debe considerarse neutralizada permanentemente, pero este método ciertamente hace menos probable un método común de ataque. La investigación adicional en estrategias de defensa en capas, como la introducción de esquemas de notarización de bloque de intervalo en la parte superior de este sistema de penalización podría hacer que el sistema sea aún más seguro y una investigación de implementación se debería de llevar acabo.



RECONOCIMIENTOS

AGRACEDIMIENTOS ESPECIALES A

el equipo y a la comunidad por contribuir:

@cronic, Peter Stewart, @ultimateblockage,
Rosario Pabst, Rowan Stone, Gustavo Fialho and Vitalik Demin.

Diseño: por Lucy Wang, Linda Baksija and Marko Orčić.

Traducido al Español por: @UANL91