



DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 2

Sistemas distribuidos

Sistemas Operativos
Primer Cuatrimestre de 2018

Integrante	LU	Correo electrónico
Nicolas Bukovits	546/14	nicko_buk@hotmail.com
Kevin Frachtenberg	247/14	kevinfra94@gmail.com
Laura Muiño	399/11	lauramuino2@gmail.com



Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
<http://www.fcen.uba.ar>

Resumen

En el siguiente trabajo práctico, se realizó una implementación de un protocolo de envío de mensajes entre procesos concurrentes. En el mismo se desarrolló un sistema de blockchain.

Índice

1. Analisis del protocolo	3
1.1. ¿Puede este protocolo producir dos o más blockchains que nunca converjan?	3
1.2. ¿Cómo afecta la demora o la pérdida en la entrega de paquetes al protocolo?	3
1.3. ¿Cómo afecta el aumento o la disminución de la dificultad del Proof-of-Work a los conflictos entre nodos y a la convergencia?	3

1. Analisis del protocolo

1.1. ¿Puede este protocolo producir dos o más blockchains que nunca converjan?

EL protocolo puede producir dos o más blockchains que nunca converjan. Si se tienen dos nodos A y B que cuando B comunica a A que encontró un bloque nuevo, y si A, antes de recibir el mensaje de B, encontró un bloque nuevo con el mismo índice que el nuevo bloque de B, entonces cuando A reciba el mensaje de B, va a descartar su bloque porque va a apostar por su propia cadena. Este esquema se puede repetir una cantidad de veces indeterminadas generando dos bifurcaciones que nunca converjen.

1.2. ¿Cómo afecta la demora o la pérdida en la entrega de paquetes al protocolo?

La demora en la entrega de paquetes puede producir dos bifurcaciones como lo mencionado en la pregunta anterior. La pérdida de mensajes puede producir que un nodo quede lo suficientemente desactualizado como para que el índice de su último bloque esté a una distancia mayor que la máxima diferencia tolerada de bloques generando nuevamente una bifurcación que podría no converjer.

1.3. ¿Cómo afecta el aumento o la disminución de la dificultad del Proof-of-Work a los conflictos entre nodos y a la convergencia?

La variación de la dificultad de *Proof-of-Work* está directamente relacionada con la convergencia del proceso de minar bloques, e inversamente con los conflictos producidos entre los nodos al competir por agregar bloques propios a la cadena. Es decir, a mayor dificultad, mayor el tiempo total del proceso y menor la cantidad de conflictos entre nodos.

Al aumentar dicha dificultad, observamos que los procesos tardan más en encontrar un hash que cumpla las condiciones de validez, haciendo menos probable que dos nodos encuentren un hash para un bloque de mismo índice. Todo lo contrario sucede si se disminuye la dificultad; el proceso tarda menos en llegar al tamaño máximo de la cadena y se producen más conflictos.

Para mostrar esto, se realizaron 40 ejecuciones con dificultad 8 y 15 (20 cada una), donde se buscaba alcanzar los 200 bloques en la cadena y la diferencia máxima aceptada entre cadenas era de 5 bloques. Los resultados obtenidos del experimento, se volcaron en el siguiente gráfico, el cual muestra la cantidad de conflictos promedio para cada dificultad.

