

# Prioridades en la Blockchain

## Abstract

*El bitcoin y la tecnología blockchain se proclama como un fenómeno disruptivo a nivel mundial, solo comparable con el auge de las .com o de internet mismo. Por ello es de vital importancia entender su funcionamiento, sus consecuencias y su futuro. Su gran limitación de escalabilidad son las demoras y las comisiones que se deben pagar para que las transacciones sean procesadas en poco tiempo. Por ello en este paper analizaremos las colas de espera de las transacciones antes de ser procesadas en la blockchain. El objetivo de este paper es comprender la naturaleza con la que se generan los famosos "cuellos de botella" y establecer un criterio objetivo para medir la eficiencia de la cantidad de colas de espera. Para ello se utilizará la técnica de Simulación (modelo dinámico) para obtener el tiempo de atención aproximado en cada cola.*

## Palabras Clave

Bitcoin, blockchain, simulación, colas de espera, bloque, prioridad, procesamiento, transacciones, comisión.

## Introducción

La blockchain es una base de datos pública, inhackeable y consensuada en donde se almacena información sobre las transacciones de bitcoins. Cuando alguien quiere realizar una transacción debe publicarla en la red blockchain para que algún nodo la procese. Las colas de espera se provocan debido a que la cantidad de nodos y transacciones es variable. Los usuarios pueden pagar una comisión para que los nodos procesen antes su transacción, dándole de esta forma prioridades a dichas colas. Este modelo presenta como problema principal que algunas transacciones de prioridad baja tardan demasiado en ser procesadas. Esto se volvió evidente en diciembre del 2017 donde las esperas eran muy altas y las comisiones subieron un 500% [1]. Por ello este proyecto analizará la composición de dichas colas de prioridad midiendo la

eficiencia mediante la comparación de la diferencia de tiempo entre las colas con mayor y menor tiempo promedio de espera. Se utilizó como único puesto de atención la blockchain y como tiempo de permanencia en el sistema el tiempo que permanece cada transacción en la cola hasta entrar a un bloque. Cabe destacar que los nodos suelen funcionar como uno solo, ya que pertenecen a un pool de minería, por ello se decidió utilizar un solo puesto de atención[2].

## Elementos del Trabajo y metodología de Simulación Evento a Evento

Se calculó una f.d.p que predice el tiempo de atención de cada transacción. Para calcularla se utilizó el software EasyFit utilizando como datos la media de los tiempos de atención de las transacciones del periodo 10/04/2017 - 10/04/2018[3]. Para saber el tiempo de arribo de las transacciones se estimó otra f.d.p tomando el promedio del periodo 13/04/2018 - 13/05/2018 [4]. Se trabajó con décimas de segundo ya que el intervalo de arribo de transacciones al sistema es de 4 décimas de segundo. Para determinar a qué cola asignar cada transacción se utilizó una función equiprobable con valores entre 0 y la cantidad de colas de la simulación en conjunto con la distribución de bitcoins[5]. Para simular la realidad de mejor manera se estableció como fee máximo 5 satoshis por byte[6], dividiéndolo por la cantidad de colas y ,luego, uniformemente entre ellas. Por ejemplo en el caso de tener 2 colas una proceso las transacciones con fees entre 0-2.5 satoshis y otra proceso las transacciones con un fee de 2.5-5 satoshis. Se le dio mayor prioridad a las colas que procesaban los fees más altos. Cada transacción al ingresar al sistema fue distribuida según la comisión que pagó. El

tiempo de procesamiento de cada cola se estableció como una función random cuyo máximo fueron 10 minutos. Este tiempo de procesamiento es análogo al tiempo de emisión de un bloque en la blockchain. Se utilizó la metodología evento a evento, con múltiples colas, con prioridad y vaciamiento. Se calculó el tiempo promedio de espera en cada cola y el porcentaje de transacciones en cada cola con respecto al total.

### Elementos del Trabajo y metodología de Simulación Delta T constante

En la metodología delta T constante se utilizó como intervalo de tiempo 10 minutos, ya que es el lapso que tarda en crearse un nuevo bloque y verificarse las transacciones que esperan en cola.[7]

Se utilizaron como eventos propios la entrada de transacciones y la salida de las mismas de las colas.

Se utilizó el software EasyFit para calcular una f.d.p que predijo la cantidad de transacciones que arribaban por segundo, utilizando los datos del periodo 01/08/2018 - 01/09/2018 [8] y para saber la comisión que pagará cada transacción se calculó otra f.d.p utilizando como datos las comisiones de las transacciones del periodo 24/08/2018 - 01/09/2018[9].

Se tomó un tamaño de bloque igual al tamaño de bloque de Bitcoin, 1MB. Para conocer el tamaño de las transacciones que entrarán en dicho bloque se tomó el promedio de tamaño mensual de transacción[10].

A usos prácticos de la simulación, para determinar la comisión mínima y la máxima para cada una de las colas, se obtuvo la comisión máxima cada 10 minutos[11]. Luego se dividió dicha comisión uniformemente entre la cantidad de colas al igual que en la metodología evento a evento. También se les dio mayor prioridad a las colas que procesaban las comisiones más altas y se distribuyó cada transacción al ingresar al sistema según la comisión que pagó.

Se calculó la cantidad óptima de colas de espera, la cantidad de veces que el bloque no se llena al 100% y el promedio de espera en el sistema por cola.

### Criterio para la determinación de la cantidad óptima de colas de espera

Para obtener la cantidad óptima de colas con cada metodología se realizaron 50 simulaciones con diferentes cantidades de colas (desde una hasta treinta) y un periodo de una hora. Se utilizó como criterio de mejor cola la que menor diferencia tuvo entre los promedios de permanencia en el sistema (PPS).

### Lenguaje de Programación

Las simulaciones fueron realizadas en Java.

### Resultados

Al usar la metodología Evento a Evento el número óptimo de colas dio como resultado 3, con un 5% de transacciones en la cola con mayor prioridad y un 70% de transacciones en la cola con menor prioridad.

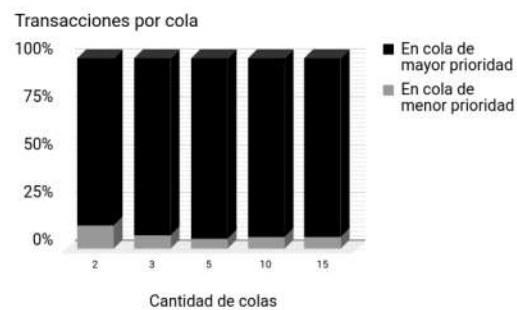


Figura 1 - Gráfica Comparativa de los porcentaje de transacciones en las colas de mayor y menor prioridad, utilizando la metodología Evento a Evento.

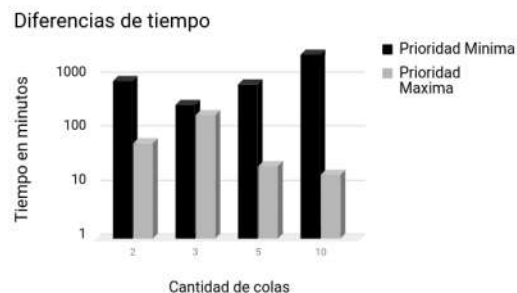


Figura 2 - Gráfica Comparativa de los tiempos de atención (en minutos) en las colas de mayor y menor prioridad, utilizando la metodología Evento a Evento.

Al utilizar la metodología Delta T constante, el número óptimo fue de 2 colas con un 60% de las transacciones en la cola de mayor prioridad y un 20% en la cola con menor prioridad.

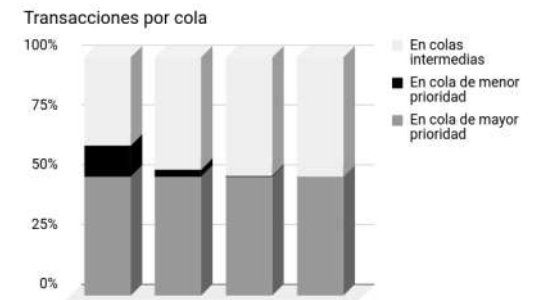


Figura 3 - Gráfica Comparativa de los porcentajes de transacciones en las colas de mayor y menor prioridad, utilizando la metodología Delta T constante.

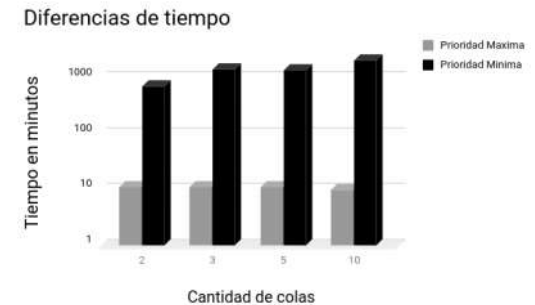


Figura 4 - Gráfica Comparativa de los tiempos de atención (en minutos) en las colas de mayor y menor prioridad, utilizando la metodología Delta T constante.

## Discusión

Luego de realizar las simulaciones se pudo apreciar ciertos patrones en los resultados. En el caso de la metodología evento a evento, la cola prioritaria tuvo el menor promedio de espera en cola y la cola con menor prioridad tuvo el mayor promedio de espera. También se pudo apreciar que el mayor porcentaje de transacciones estuvo en las penúltimas colas, esto se vuelve más evidente cuando aumenta el número de colas de prioridad.

Por otro lado en el caso de la metodología delta T constante, la cola de mayor prioridad siempre tuvo el menor promedio de espera en cola pero también tuvo el mayor porcentaje de transacciones. En contrapartida, las penúltimas colas fueron las que tuvieron mayor promedio de permanencia en el sistema y menor cantidad de transacciones.

## Conclusión

Aunque las simulaciones realizadas con ambas metodologías nos dieron resultados parecidos, la más adecuada a este problema es la metodología Delta T constante, ya que es la que mejor se adapta a la problemática. Al utilizar la metodología evento a evento realizamos muchas abstracciones para adaptar el modelo y por ende sus resultados son menos exactos, esto se vuelve evidente al ver los porcentajes de transacciones en cada cola y explica la diferencia en el resultado del número óptimo de colas. En la realidad lo que ocurre es similar a los resultados de nuestra simulación con metodología delta T constante, la diferencia de dinero actualmente es tan poca que la gente decide pagar un poco más para tener menos espera. También se pudo apreciar que en el caso de elegir un número de colas mayor a 15 dejaban de llegar transacciones a la cola con menor prioridad, esto se debe a que la gente no paga comisiones tan bajas porque sabe que su transacción podría no procesarse nunca.

En este trabajo se presentan las bases para una investigación académica posterior

sobre las colas de espera de la blockchain, sobre la cual se utilice esta misma metodología para investigar cómo afecta a las colas de espera el cambio en el tamaño del bloque como es el caso de Bitcoin Cash[12].

También se estableció un criterio de eficiencia para poder establecer el número óptimo de colas de espera en la blockchain.

[12]Javarone, M. A., & Wright, C. S. (2018). From Bitcoin to Bitcoin Cash: a network analysis. arXiv preprint arXiv:1804.02350.

## Referencias

- [1]Average Network Transaction Fees per Byte. Obtenido de <https://statoshi.info/dashboard/db/fee-estimates?panelId=3&fullscreen&from=1512137794231&to=1537539438289>
- [2] Hashrate Distribution. Obtenido de <https://www.blockchain.com/pools>
- Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is bitcoin a decentralized currency?. IEEE security & privacy, 12(3), 54-60.
- Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS (Vol. 2013, p. 11).
- [3]Median confirmation time. Obtenido de <https://blockchain.info/es/charts/median-confirmation-time>
- [4]Transaction Rate. Obtenido de <https://www.blockchain.com/es/charts/transactions-per-second>
- [5]Bitcoin rich list. Obtenido de <https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html>
- [6]Bitcoin Satoshi to USD. Obtenido de <http://www.btc Satoshi.com>
- [7]Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- [8]Transactions Accepted Per Second. Obtenido de <https://statoshi.info/dashboard/db/transactions?panelId=6&fullscreen&from=1533134615310&to=1535813015310>
- [9] Average Network Transaction Fees per Byte. Obtenido de <https://statoshi.info/dashboard/db/fee-estimates?from=1535120194231&to=1535811438289&panelId=3&fullscreen>
- [10]Avg transaction size. Obtenido de <https://blockchain.info/q/avgtxsize/4500>
- [11] High fee per KB. Obtenido de <https://api.blockcypher.com/v1/btc/main>