


Implementación y evaluación de setchain*

Arivarasan Karmegam^{1,2}, Gabina Luz Bianchi³, Margarita Capretto³, Martín Ceresa³, Antonio Fernández Anta¹, and César Sánchez³

¹ IMDEA Networks Institute, Madrid, España

² Universidad Carlos III, Madrid, España

³ IMDEA Software Institute, Madrid, España

Resumen

La escalabilidad de los blockchains es un desafío que limita su adopción. Por ello se están desarrollando diversas técnicas para mejorar su rendimiento. Setchain [2] es un tipo de datos concurrente y distribuido que mejora la escalabilidad frente a un blockchain, al relajar el requisito de orden total entre las transacciones. Setchain implementa conjuntos distribuidos que solo crecen (*grow-only sets*) cuyos elementos (por ejemplo, transacciones) no están ordenados. En un setchain se pueden imponer barreras de sincronización para crear épocas. Cada época contiene un subconjunto, acordados por consenso, de los últimos elementos agregados. Aunque los elementos dentro de una época no están ordenados, los elementos entre diferentes épocas sí están ordenados según los números de época. Este tipo de “blockchain relajado” es adecuada para aplicaciones que no requieren un orden total entre las transacciones dentro del mismo bloque.

En una edición anterior de las JCSD [1], se presentaron tres algoritmos diferentes de setchain. En esta presentación comparamos el rendimiento y la escalabilidad de estos tres algoritmos: (a) *Vanilla*, una implementación básica; (b) *Compresschain*, que agrupa un conjunto de transacciones en un lote y comprime el lote antes de transmitirlo como una transacción; y (c) *Hashchain*, donde se emplea una función hash para convertir un lote de transacciones en un hash de longitud fija, facilitando así su transmisión. Para este tercer algoritmo, también proponemos una técnica de inversión de hash para recuperar el lote de transacciones original a partir del hash para su verificación. Tanto Compresschain como Hashchain utilizan un software intermedio llamado Collector, que agrega transacciones de clientes y genera los lotes.

Los tres algoritmos de Setchain han sido implementados en la plataforma de aplicación blockchain CometBFT dentro de un entorno Docker, donde cada nodo Docker opera un servidor y un cliente de CometBFT. Las implementaciones se han evaluado en escenarios que involucran cuatro, siete y diez nodos servidores de CometBFT, enfocándose en parámetros como el tamaño máximo del bloque y la tasa de envío. Los resultados demuestran que los algoritmos de setchain mejoran significativamente la escalabilidad de blockchain.

* Parte del proyecto PID2022-140560OB-I00 (DRONAC) financiado por MCIN/AEI /10.13039/501100011033/ y por ERDF, A way of making Europe.



Palabras clave: Blockchain, Setchain, rendimiento, escalabilidad, CometBFT.

Referencias

1. Bianchi, G.L., Capretto, M., Ceresa, M., Sánchez, C.: Hashchain: an efficient set-chain implementation built on top of tendermint (wip), unpublished manuscript. Presented at JCSD 2023.
2. Capretto, M., Ceresa, M., Fernández Anta, A., Russo, A., Sánchez, C.: Improving blockchain scalability with the setchain data-type. Distributed Ledger Technologies: Research and Practice (2023)

