Problema de los generales Bizantinos adaptado a la tecnología Blockchain

Román Larrosa Lewandowska
ETSIIT, Universidad de Granada
romanlarrosa@correo.ugr.es

1 Introducción y aproximación al problema

El problema de los generales Bizantinos es un caso de problema de consenso. Los problemas de consenso son aquellos en los que N procesos (p_i) comienzan en un estado "indeciso" y proponen un valor (v_i). Los procesos comunican al resto su valor propuesto. Cada proceso establece una variable de decisión (d_i) entre todos los valores recibidos y su valor propuesto. Los requerimientos para un algoritmo de consenso son que las siguientes condiciones se mantengan para todas sus ejecuciones:

- Terminación: En algún momento cada proceso correcto establece su variable de decisión.
- Acuerdo: El valor de decisión de todos los procesos correctos es el mismo
- Integridad: Si los procesos correctos han propuesto el mismo valor, entonces cualquier proceso correcto en el estado "decidido" ha elegido ese valor.

El problema de los generales Bizantinos es una variante o concreción del problema de consenso, en cuya descripción informal, tres o más generales deben decidir si atacar. Uno, el comandante, emite una orden, el resto, subordinados al comandante, deben decidir si atacar o retirarse. Sin embargo, uno o más de los generales puede ser un traidor, o defectuoso. Si el general es el traidor, indica a un general ataca y al otro retirarse. Si un subordinado es el traidor, le dice a uno de sus compañeros que el comandante le ha dicho que ataque, y a otro compañero que el mensaje ha sido de retirada. La condición de integridad es, entonces: si el comandante es correcto (no es traidor), todos los procesos correctos deciden el valor que propone el comandante. Hay que notar que, para el problema de los generales Bizantinos, la integridad implica acuerdo cuando el comandante es correcto, pero no necesariamente es siempre así.

Asumimos que los procesos pueden experimentar fallos arbitrarios: un proceso defectuoso puede mandar cualquier mensaje con cualquier valor en cualquier momento, y puede omitir mandar cualquier mensaje. Hasta f de los N procesos pueden ser defectuosos. En el caso de la omisión de envío de mensajes, ésta puede ser detectada por los procesos correctos mediante un *timeout*.

Asumimos también que los canales entre los pares de procesos son opacos, es decir, solo son visibles para dicho par de procesos, puesto que en caso contrario sería fácil identificar a los procesos defectuosos o traidores. Para dar solución al problema con mensajes sin firmar, debe cumplirse que $N > 3f$, ya que, de otro modo, es imposible determinar una solución (consenso) debido a la incongruencia de mensajes recibidos. Las soluciones se encuentran en $f+1$ etapas de intercambio de mensajes. En el resto de

casos, se establece la solución mediante la mayoría de valores recibidos por cada proceso (general). Por ejemplo, para el caso de 4 generales y un solo traidor:

- En el caso en el que el traidor es el comandante, cada proceso recibe un valor diferente. Al hacer el intercambio de mensajes entre subordinados, cada uno recibe todos los valores diferentes que ha enviado el comandante, por lo que no hay consenso y se aborta.
- En el caso en el que el traidor es uno de los subordinados, cada uno recibe *N-2* mensajes. El valor enviado por el comandante es recibido N-3 veces y un valor falseado por el traidor. Por tanto, es fácil determinar cuál es el valor de consenso entre los procesos correctos.

2 Relación con Blockchain

La tecnología Blockchain (o de "contabilidad distribuida") es un protocolo de operaciones de intercambio entre pares que se producen, gestionan y comprueban de forma descentralizada, automatizada, compartida y segura [3], por tanto, basada en el consenso.

Blockchain usa el problema de los generales bizantinos para validar las transacciones que se realizan en todas las copias distribuidas en la red (pares), que actúan como generales. Hace uso de mensajes firmados para reducir el intercambio de mensajes cuando f puede ser mayor que 1, y por tanto habría un número de etapas muy superior al realizable. (Se pasa de una eficiencia del orden $O(N^{f+1})$ a una de orden $O(N^2)$).

Cuando se inicia una transacción, esta es indicada a todas las réplicas. Éstas se intercambian dicha transacción entre ellas, detectando por minoría al traidor, si existiese, incluso cuando es la réplica que inicia la transacción.

De esta manera se llega a un consenso en todas las réplicas, que mantienen un registro completo de las transacciones, y el cual es necesario para la validación de cualquier transacción. Es por ello que la tecnología Blockchain sustenta el funcionamiento de las criptomonedas y mantiene su seguridad mediante el problema de los generales bizantinos, sin el cual sería imposible mantener un conjunto descentralizado de réplicas idénticas para controlar los movimientos monetarios de manera que se garantice la integridad de las mismas en todo momento, de manera independiente a cualquier entidad, y únicamente basado en esta integridad entre la multitud de réplicas repartidas por la red.

Cualquier ataque que se quisiera efectuar sobre un blockchain debería de realizarse sobre al menos el 51% de las réplicas, algo que no es sencillo para nada y es por lo que el sistema se convierte cada vez más en el elegido por quien necesita un sistema distribuido y seguro.

3 Autoevaluación

1. ¿La explicación es clara y el contenido está estructurado? **SI**
2. ¿Queda reflejado que se han estudiado y entendido los algoritmos incluidos en la bibliografía proporcionada para las clases? **SI**

3. ¿Queda reflejado que se ha buscado suficiente bibliografía adicional y se ha comparado/contrastado la información entre las diferentes referencias encontradas (incluidas en el informe) y con la bibliografía proporcionada para las clases? **SI**

4. ¿La conclusión final a la que se ha llegado en el informe ha sido resultado de un estudio y análisis complejo y en profundidad de toda la bibliografía manejada sobre el tema abordado, lo cual ha requerido una aportación extra por mi parte? **SI**

5. ¿El informe realizado me ha llevado tiempo y servido para comprender la solución al problema abordado? **SI**

6. ¿Se ha realizado alguna aportación adicional más allá de lo que en esencia pedía este trabajo? **NO**

Dado que el trabajo considero que está lo suficientemente completo y que he llegado a entender ampliamente el problema y su solución, pero no he añadido nada extra, considero que la nota que me merezco un 9

Bibliografía y referencias

1. G. Coulouris.: “Distributed Systems: Concepts and Design” (5th Edition). Pearson.
2. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564.
3. Blockchain Services, http://www.blockchainservices.es/formacion/el-problema-de-los-generales-bizantinos/, última vez visitado 21 abril 2020.
4. Geeksforgeeks: https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/, última vez visitado 21 abril 2020.
5. R. Pass, L. Seeman, A. Shelat: Analysis of the blockchain protocol in asynchronous networks, 2017.
6. J. Kang et al., "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660-4670, June 2019.