Tarea 9

Cruz Perez Ramon -315008148

January 5, 2021

1. **¿Cual es el problema de implementar un detector de fallas en redes arbitrarias (osea no completas)**

   Como no son completa hay procesos que no estan conectados entre ellos, por lo que algunos procesos necesitan de otros procesos para saber informacion, y es dificil saber cual es la mas reciente. Ademas debido a que la mayoria de los detectores son eventuales osea que requiere tiempo para que funcione.
   Por lo que en algunos casos, se necesitara ese tiempo para terminar el algoritmo, sabiendo que se puede hacer un poco mas rapido.

2. **¿Por que se pueden colapsar las 8 clases de detectores en solo 4?**

   Como en 4 detectores se cumple integrida debil y en otros 4 integridad fuerte, en una clase demostramos que se puede usar un algoritmo para hacer que el detector que cumple integridad debil pueda cumplir la fuerte y viceversa, por lo que estas se podrian colapsar y decir que son 4 detectores.

3. **¿Cual es el problema del doble gasto?**

   Se trata que una moneda digital puede ser gastada mas de una vez.(aprovechando un bug). Pero bitcoin usa un base datos distribuida que ayuda a ver si el dinero no es gastado mas de dos veces.

4. **¿Que es la prueba de trabajo?**

   Es una parte del minado, cada minero debe intentar resolver un acertijo criptografico.

Se debe crear un hash de un bloque satisfaga alguna restriccion.
Pues como deben satisfaser la restriccion, a la primera no sale el hash correcto, por lo que los mineros deben crear varias veces el hash hasta dar con la que mejor se acomode.

5. **¿Como se utiliza la prueba de trabajo para tratar de lograr consenso sobre que bloque añadir a la cadena?**

   Pues cada vez que un minero genera un bloque debe cumplir la dificulatad objetivo, si no cumple con el objetivo se vuelve a calcular el hash, si si cumple el objetivo, se envia el bloque "ganador" a todos los demas, entonces los otros mineros verifican que se cumpla la difcultad objetivo y asi lo propagan hasta realizar el acuerdo, si hay mas de un bloque ganador se hace un fork.

6. **¿Que es un fork? ¿Como se solucionan los forks?**

   Fork: Cuando se generan dos bloques ganadores, hacen que la cadena se divida en dos ramas distintas.

   Solucion: Con el tiempo los mineros escojen la rama con la cadena mas larga, pues tiene mas dificultad y la mas corta la olvidan. (por eso se deben espera un tiempo promedio de 10 min. o unos 2016 bloques para verificar que la transaccion sea añadida en la base de datos).

7. **¿Cuando se sabe que una transaccion ya se hizo efectiva en una blockchain?**

   Cuando se añade un bloque se debe esperar a que se añadan nuevos bloques.(esperar a ver si no hay forks)
   Si no hay fork. Listo termino la transaccion.
   Si si hay forks entonces, como se obtienen mas bloques eventualmente los participantes se daran cuanta que tienen historias diferentes.
   La solucion es que se toman la cadena sufijo mas larga, a partir de donde se genero el fork.
   (Por eso hay que esperar 10 min. aprox.)

8. **¿Que es lo que mas te parecio importante o interesante del seminario de blockchains?¿Por que?**

   Lo interesante para mi al principio fue la base de datos distribuida.
   Pues como era posible que cada vez que se realizara una transaccion

todos los integrantes iban a saber es ella, despues conforme la tiempo nos explican que se realiza un propagracion y el consenso para verificar que todos los datos sean correctos.