PONTIFICIA
UNIVERSIDAD
CATÓLICA
DE CHILE

IIC2523 - Sistemas Distribuidos
Escuela de Ingeniería
Departamento de Ciencias de la Computación
2017-2

Análisis de sistemas Blockchain

Sebastián Amenábar - 14632233
Raimundo Herrera - 14632152

Heterogeneidad

Uno de los elementos claves de una tecnología como blockchain es la capacidad de ser utilizado por múltiples agentes. De esta forma, debe ser capaz de ejecutarse sin problemas en todos los nodos, sea cual sea el entorno de dicho nodo. En general las implementaciones de blockchain implementan distintas formas de acceder a la cadena y realizar modificaciones, y/o actualizaciones, sin embargo, todas ellas consideran la posibilidad de la multiplataforma, siendo por ejemplo posible realizar transacciones por programas para todos los SO o incluso por navegadores, por requests HTTP, entre otros.

Apertura (Openness)

Como tecnología, blockchain se puede considerar áltamente abierto, esto radica en la simpleza de su definición. En términos simples se considera a blockchain como una cadena de registros (bloques) encriptados que va creciendo gradualmente y cuyas actualizaciones quedan registradas de manera permanente luego de ser verificadas. Siguiendo esa noción, existen muchísimas implementaciones de blockchain que utilizan esta tecnología, y cada implementación difieren en muchas cosas pero no en lo central, que es la tecnología subyacente. En ese sentido, según lo visto en clases, la capacidad de agregar recursos y funcionalidades a un sistema blockchain es ilimitada, por lo tanto se puede considerar con un alto nivel de openness.

Seguridad

Todos los mecanismos populares que implementan blockchain cuentan con sistemas criptográficos, es decir, cada bloque de la cadena está encriptado y es seguro. Además, es resistente a ataques de denegación de servicio porque funciona de manera de que sigue siendo utilizable en caso de que muchos nodos estén desconectados. Además no importa que se caigan en un preciso instante porque las actualizaciones son “eventuales”, es decir la instantaneidad de los ataques DDOS por ejemplo, no tiene efecto útil en ellos porque la fortaleza de blockchain no está ahí. En cuanto a la integridad de los datos esta se mantiene ya que las copias de la cadena están distribuidas por todos los nodos, de modo que modificar la información de manera maliciosa o incorrecta es virtualmente imposible. Sin embargo, como se hablará en escalabilidad, si se centraliza demasiado, se puede volver más vulnerable.

Escalabilidad

Uno de los problemas de los sistemas blockchain tiene que ver con la escalabilidad, cuando la cadena es muy grande, y hay muchas transacciones, se puede volver costoso ser un nodo completamente capaz, ya que se requiere más espacio, ancho de banda, etc. Es por eso que sufre riesgo de centralización, ya que unos pocos nodos serían capaces de utilizar el potencial del sistema. Una posible solución que se utiliza es que algunos nodos tengan la cadena completa de transacciones, pero que los demás nodos sean nodos “livianos” y que solo tengan la última parte de las transacciones, de modo que ahí se vuelve muy escalable y se elimina dicha limitación de espacio.

Manejo de fallas

Como es una red de computadores, o nodos, donde muchos se encuentran ejecutando cálculos muy similares (sino idénticos), en el caso de que uno falle pueden ocurrir los siguientes eventos:

- ➔ Fallas, errores de código principalmente, se pueden ver en robo de *bienes* en la cadena, ataques en general pueden producir la caída de un nodo, pero no de toda la red.
- ➔ Error en el cálculo del bloque: al transmitir a otros nodos será rechazado luego no influye en la cadena.
- ➔ Bajo ciertos eventos se pueden forzar *rollbacks*, por medio de *hard-forks* que regresan la cadena a un estado anterior, como ocurrió con Ethereum y el robo a la DAO. Ésta decisión no es tomada por una persona o entidad, si no que los miembros de la cadena deben llegar a un consenso para realizar el *rollback.*

Concurrencia

En la cadena no se pueden agregar transacciones a medio realizar. En caso de divergencias en la cadena, se cuenta con mecanismos para llegar a un consenso. Como por ejemplo, cuando hay 2 transacciones distintas que envían todo el balance de una cuenta (solo se puede hacer una vez).

Transparencia

Los fallos principales son que ante una mayor carga de la red, no se puede simplemente aumentar la cantidad de *hashing* para procesar todas las solicitudes y demora más tiempo que las transacciones sean añadidas a la cadena.
Para lograr aumentar la capacidad de carga, que son la cantidad de transacciones por segundo, se deben integrar algoritmos y modificar la estructura.
Como todavía es una tecnología emergente, la conexión a nodos es más bien manual, por lo que si se está conectado a uno de forma remota, y este cae, se debe manualmente buscar otro nodo para establecer una nueva conexión.

Calidad de servicio (QoS)

Existen cadenas con largas demora para transacciones (sobre 15 minutos) y otras que dicen tardar pocos segundos. En situaciones de alto tráfico generalmente aumenta (varias veces) el tiempo que demora en hacerse la transacción e incluso puede llegar a no realizarse. En situaciones normales, si un nodo tiene problemas de conectividad, pero logra enviar exitosamente la transacción, entonces lo más probable es que sea añadida a la cadena (siempre que sea válida).