Mesa Redonda
Blockchain, retos técnicos y soluciones

Ramón Martínez, BAES Lab, Alicante
Salvador Roca, Universitat de València
Carlos Turró, Universitat Politècnica de València

Modera: José M. Claver, Universitat de València

TOPOLOGÍA DE LA RED

La red es una red P2P en estrella con tres tipos de nodo diferenciados:

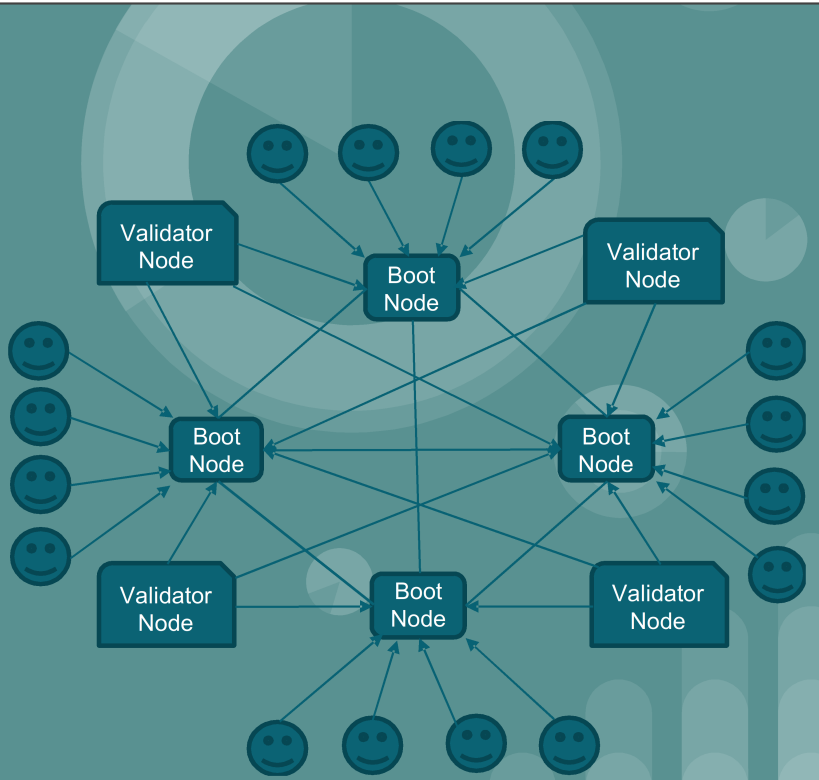
1. BOOT : Son los nodos que se encargan de mantener la topología de la red.

Todos los nodos tanto validadores como clientes se conectan a ellos y estos distribuyen la lista global de nodos conectados.

2. VALIDADOR : Son los nodos encargados de validar las transacciones.

No reciben conexiones de nadie y conectan automáticamente contra los nodos BOOT.

3. Nodo Cliente : *Son nodos que no requieren ninguna condición especial. En el arranque conectan con uno o más nodos BOOT y a partir de ese momento, ellos mismos pueden servir de distribuidores de red del resto de nodos.*



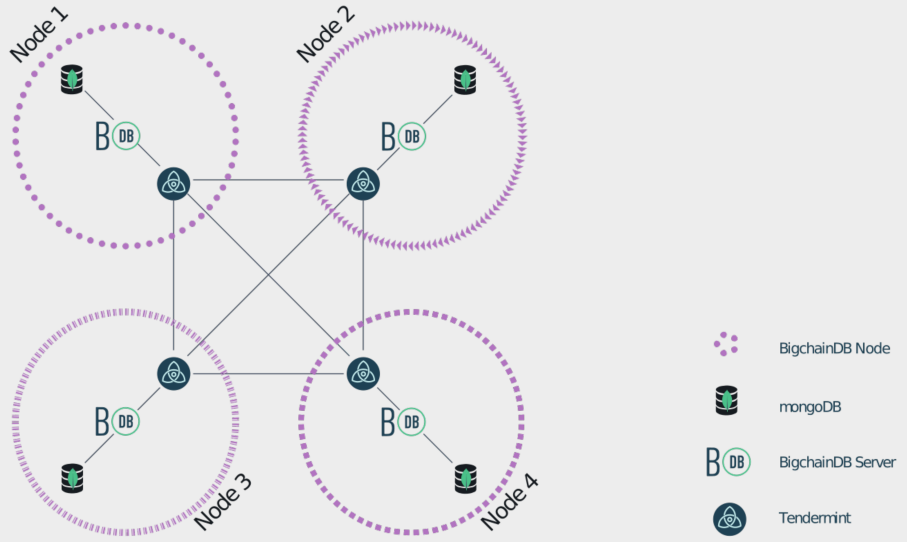
REQUISITOS COMUNES PARA CUALQUIER TIPO DE NODO

Los requisitos de hardware comunes a todos los nodos son:

- Maquina real o virtual.
- CPU : 1 core mínimo, recomendados 2.
- Memoria : 1GB mínimo, recomendados 4GB.
- Espacio en disco : mínimo 10GB, recomendado 100GB.

Requisitos software:

- Sistema operativo Ubuntu 18.04.
- BigchainDB versión v2.0.0b7.
- Tendermint versión v0.22.8.
- Base de datos MongoDB v3.6.3.
- Sincronización horaria NTP contra hora.roa.es



- BigchainDB versión v2.0.0b7.
- Tendermint versión v0.22.8.
- Base de datos MongoDB v3.6.3.
- ntp sincronización de hora
- ipfs sistema de ficheros distribuido

Fuente: www.bigchaindb.com

NODO BOOT: Anunciadores de nodos y configuración.

Aparte de los requisitos comunes, necesitará los siguientes:

- Conectividad continua a la red.
- Alimentación ininterrumpida.
- Dirección IP FIJA REAL (no traducida NAT de ninguna manera para evitar que el nodo reciba conexiones en la pública y anuncie su privada) (IPv4, IPv6 o ambas).
- Puertos abiertos en el firewall: 26656,26657 TCP
- Recomendado ssh solo por clave pública RSA y acceso root without-password o sudo .

Opcional :

- Demonio IPFS para intercambio de archivos.
- Software IPFS-CLUSTER .

NODO VALIDADOR: Validadores de las transacciones de la red.

Aparte de los requisitos comunes, necesitará los siguientes.

- Conectividad continua a la red.
- Alimentación ininterrumpida.
- Seguridad física controlada (CPD o similar).
- Dirección IP privada o protegida por firewall .

Su única conectividad será saliente (a los boot nodes), no se debe admitir ningún tipo de conexión entrante no previamente establecida.

- Recomendado ssh solo por clave pública RSA y acceso root without-password o sudo .
- Este nodo no ejecutará bajo ninguna circunstancia servicios adicionales como IPFS u otros, pueden admitirse servicios propios del sistema como NTP, pero en ningún caso servicios con posibilidad de acceso externo .

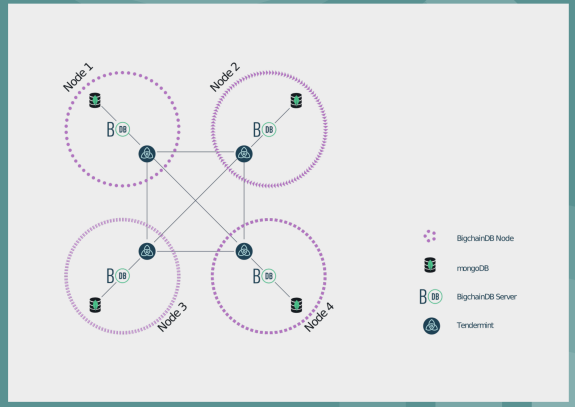
NODO CLIENTE:

Permite la lectura y escritura de la red.

Opcionalmente podrá instalarse:

- Demonio IPFS para intercambio de archivos.

- BigchainDB versión v2.0.0b7.
- Tendermint versión v0.22.8.
- Base de datos MongoDB v3.6.3.
- ntp sincronización de hora
- ipfs sistema de ficheros distribuido



Fuente: www.bigchaindb.com

SINCRONIZACIÓN HORARIA NTP

Los nodos BOOT y VALIDADORES, tomarán como fuente segura de tiempo fiable varios servidores de tiempo stratum 1 a través de comunicación con protocolo NTP

Los servidores hora.roa.es y minuto.roa.es que pertenecen al Instituto y Observatorio de la Armada (ROA) , el que, según lo dispuesto en el R.D. 1308/1992 de 23 de octubre, está encargado del mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC-ROA), que constituye la base de la hora legal en todo el territorio nacional.

Este real decreto también establece la escala UTC(ROA) como base de la hora legal española, aspecto que posteriormente ha sido recogido por la Ley 32/2014, de 22 de diciembre, de Metrología.
Esta señal se recibe a través de Internet (IPv4).

CONSENSO BFT

La tolerancia a fallas bizantinas (BFT) es la resistencia de un sistema informático a los fallos, en particular la de los sistemas informáticos distribuidos: Fallos de componentes electrónicos causando información imperfecta o corrupta si un componente no está funcionando como debe.

En una falla bizantina un componente como un servidor puede aparecer de manera inconsistente, fallando y funcionando a la vez para sistemas de detección, presentando diferentes síntomas a diferentes observadores. Es difícil para los otros componentes declarar qué falló y bloquearlo fuera de la red, ya que primero necesitan llegar a un consenso sobre qué componente no está funcionando correctamente.

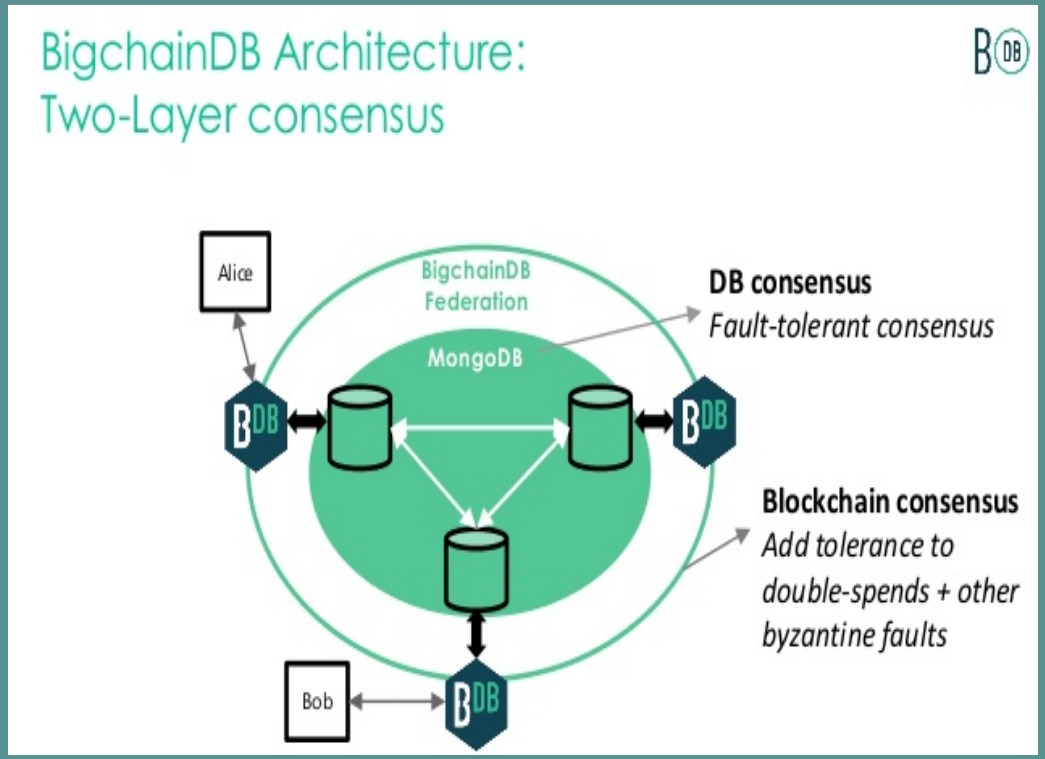
El término se deriva del problema de los generales bizantinos, en el que los actores deben acordar una estrategia común para evitar un error catastrófico, pero teniendo en cuenta que algunos de los actores no son de fiar.

CONSENSO BFT (cont.)

En una red blockchain , este consenso lo aportan los nodos VALIDADORES : Cada transacción es votada antes de incluirla en un bloque y solo es incluida si la mayoría absoluta, la mitad más uno, así lo decide. Es por esto que los nodos validadores no deberán ser demasiados.

Inicialmente en el génesis de la red se definieron cuatro nodos validadores y el comité de red, decidirá en cada momento que nuevos validadores deben ser incluidos. El número no deberá ser elevado para agilizar las votaciones en las transacciones.

La idoneidad de un nuevo nodo vendrá dada por su ancho de banda, potencia de cálculo, situación física y espacio en disco.



Fuente: www.bigchaindb.com

Tipos de diversidad de nodos

Deben tomarse medidas para dificultar que cualquier actor o evento controle o dañe "lo suficiente" a los nodos.

Hay muchos tipos de diversidad que se deben considerar y puede ser bastante difícil tener diversidad de todo tipo.

1. Diversidad jurisdiccional.
   Los nodos deben ser controlados por entidades dentro de múltiples jurisdicciones legales, de modo que se hace difícil usar medios legales para obligar a suficientes de ellos a hacer algo.
2. Diversidad geográfica.
   Los servidores deben estar ubicados físicamente en varias ubicaciones geográficas, de modo que se vuelve difícil para un desastre natural (como una inundación o un terremoto) dañar lo suficiente como para causar problemas
3. Diversidad del Hosting.
   Los servidores deben estar alojados por varios proveedores de alojamiento (por ejemplo, servicios web de Amazon, Microsoft Azure, Digital Ocean, Rackspace), por lo que resulta difícil para un proveedor de alojamiento influir o en Go, etc.), de modo que un consorcio también podría tener una diversidad de Implementaciones de servidor.

Tipos de diversidad de nodos (cont.)

Deben tomarse medidas para dificultar que cualquier actor o evento controle o dañe "lo suficiente" a los nodos.

4. La diversidad en general.

En general, la diversidad de miembros (de todo tipo) confiere muchas ventajas a un consorcio.

Nota: si todos los nodos ejecutan el mismo código, es decir, la misma implementación de BigchainDB, entonces si hay un error en ese código podría ser utilizado para comprometer todos los nodos. Idealmente, habría varias implementaciones diferentes y bien mantenidas del servidor BigchainDB (por ejemplo, uno en Python, uno en Go, etc.), de modo que un consorcio también podría tener una diversidad de implementaciones de servidor.
Se pueden hacer observaciones similares sobre el sistema operativo.

¿Por qué BigchainDB es inmutable?

El término "inmutable" significa "invariable en el tiempo o que no se puede cambiar". La comunidad de blockchain a menudo describe las cadenas de bloques como "inmutables", significa que los datos de blockchain son invariables o permanentes, lo cual podría resultar absurdo. El dato puede cambiar.

Es cierto que los datos de la cadena de bloques son más difíciles de cambiar (o eliminar) de lo habitual. Es más que "resistente a las manipulaciones" (lo que implica un intento), los datos de la cadena de bloques también resisten los cambios aleatorios que pueden ocurrir sin ningún tipo de intención, como la corrupción de datos en un disco duro.

Por lo tanto, en el contexto de las cadenas de bloques, interpretamos la palabra "inmutable" como un significado prácticamente inmutable, para todos los propósitos.

¿Por qué BigchainDB es inmutable? (cont.)

Los datos de blockchain pueden hacerse inmutables de varias maneras:

1.No existe API para cambiar o eliminar datos. El software de BigchainDB por lo general no expone ningún API para cambiar o eliminar los datos almacenados en el blockchain. BigchainDB no tiene tales APIs. Esto no evita que se produzcan cambios de otra manera; es solo una línea de defensa.

2. Replicación. Todos los datos se replican (copian) en varios lugares diferentes. Cuanto mayor sea el factor de replicación, más difícil será cambiar o eliminar todas las réplicas.

3. perros guardianes internos. Todos los nodos supervisan todos los cambios y, si se produce algún cambio no permitido, se puede realizar una acción apropiada.

4. perros guardianes externos. Un consorcio puede optar por confiar en terceros para monitorear y auditar sus datos, buscando irregularidades. Para un consorcio con datos legibles públicamente, el público puede actuar como un auditor.

¿Por qué BigchainDB es inmutable? (cont.)

5. Incentivos económicos. Algunos sistemas de cadena de bloques hacen que sea muy costoso cambiar los datos almacenados. Los ejemplos incluyen sistemas de prueba de trabajo y prueba de juego. BigchainDB no usa incentivos explícitos.

6. Los datos se pueden almacenar utilizando técnicas sofisticadas, como códigos de corrección de errores.

7. Las firmas criptográficas se utilizan a menudo como una forma de verificar si los mensajes (por ejemplo, las transacciones) se han manipulado en ruta, y como una forma para verificar quién firmó los mensajes. En BigchainDB, cada transacción debe estar firmada por una o más partes.

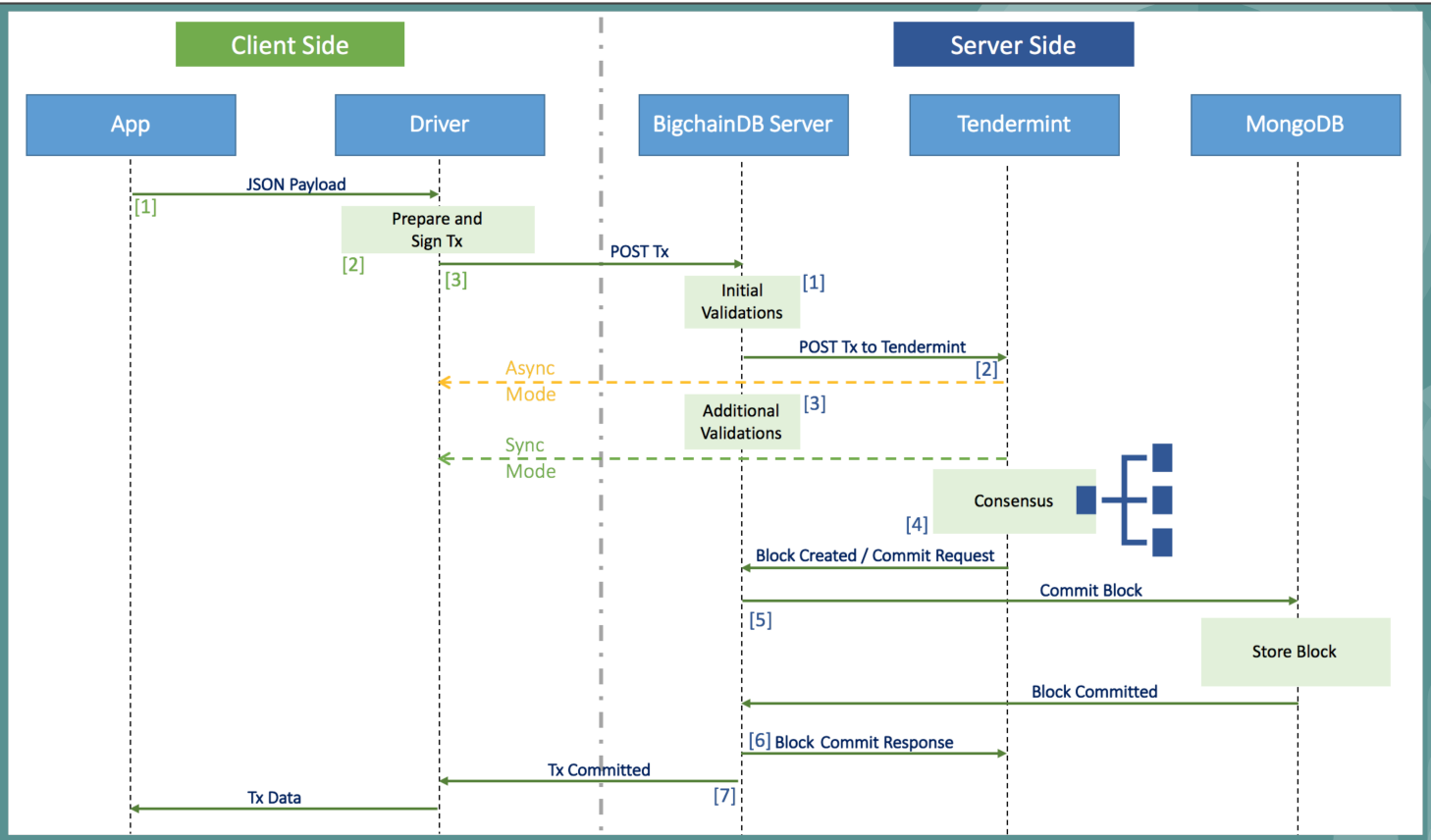
8.Las copias de seguridad completas o parciales se pueden registrar de vez en cuando, posiblemente en el almacenamiento secundario o de backup, otras cadenas de bloques, impresiones, etc.

9.Políticas de seguridad. Los propietarios de los nodos pueden adoptar y hacer cumplir fuertes políticas de seguridad.

10.Diversidad de nodos. La diversidad hace que ninguna cosa (por ejemplo, un desastre natural o un error del sistema operativo) pueda comprometer lo suficiente de los nodos.

Características principales

	Blockchain típico	BD Distribuida típica	BigchainDB
Descentralización	X		X
BFT Tolerancia Fallas Bizantinas	X		X
Inmutabilidad	X		X
Control de Activos por el propietario	X		X
Alto Rendimiento nº de Transacciones		X	X
Baja Latencia		X	X
Indexado y Consulta de Datos estructurados		X	X



Fuente: www.bigchaindb.com