Tipos de *blockchain*

Blockchain y computación cuántica

CONTENIDO

Objetivos

- Entender las características comunes a los *blockchain* públicos y privados.
- Aprender las características propias de los *blockchain* públicos.
- Conocer las principales soluciones *blockchain* privadas o permisionadas.
- Introducir el concepto de consorcios y sus implicaciones.

Introducción

El origen de *bitcoin* se basa en la determinación de una o varias personas en generar un **sistema de pagos digitales** que no dependiera de entidades financieras y que fuera **accesible** para todo el mundo. *Bitcoin* se concibe como un sistema de **código abierto** que **mantiene la propia comunidad de usuarios**. Este es el origen de *blockchain* y el concepto que se aplica en las soluciones *blockchain* **denominadas públicas**.

La tecnología evoluciona y aparecen soluciones *blockchain* que atienden a la necesidad de disponer de **entornos seguros para compartir información** entre un conjunto de **participantes conocidos**, pero que no confían entre sí. Este tipo de soluciones son las **denominadas privadas o permisionadas**, donde la tecnología *blockchain* se adapta para generar un entorno controlado de intercambio de información.

Los dos tipos de *blockchain*, **públicos y privados**, comparten una serie de características [1]:

- Funcionan sobre una **red de nodos** con comunicación *peer-to-peer*.
- Se basa en un número de nodos que **validan la cadena y mantienen una copia** de esta.
- La información que se almacena en la **cadena de bloques es inmutable**, salvo consenso de la comunidad o de los participantes de la red.
- Tanto los *blockchain* públicos, como los privados o permisionados disponen de una gran variedad de soluciones *blockchain*, que permiten ofrecer servicios a empresas y personas basados en las principales características de *blockchain*.

Públicos

Los *blockchain* públicos son aquellos que **no requieren de un proceso de identificación para poder operar en la red** *blockchain*. La participación en la red es libre y no está controlada por ningún organismo. Esto permite ofrecer cierto nivel de **anonimato** a los participantes, consiguiendo que todos sean tratados por igual según las reglas establecidas por el *blockchain*.

Este tipo de *blockchain* presenta las siguientes características:

- Cuentan con una **criptomoneda**.
- La participación como usuario no está controlada, **cualquier persona puede crear una cuenta y operar**.
- Las operaciones sobre el *blockchain* requieren del **pago de los costes de ejecución de la transacción**.
- La participación como nodo es libre, no existen restricciones.
- La **participación como minero o nodo validador es libre**, pero en algunos *blockchain* requieren del cumplimiento de ciertos requisitos. Como el caso de *NEO* [2] que exige la identificación de los nodos para participar en el proceso de validación.
- La comunidad de nodos y de desarrolladores tienen un gran peso en la evolución del *blockchain*.
- Los mineros o validadores reciben una **recompensa por cada bloque generado**.
- La elección de los bloques ganadores se gestiona **mediante algoritmos de consenso**.
- La información de la cadena de bloques es pública y no se elimina.

Listado de los principales *blockchain* públicos

- ***Bitcoin:*** es la primera solución de pagos descentralizada que corre sobre una red distribuida.
- ***Ethereum:*** es el primer *blockchain* que incorpora *smart contracts* y que permite ejecutar reglas de negocio dentro de *blockchain*.
- ***NEM [2]:*** utiliza un algoritmo de consenso que premia la participación en la red, propiciando que los nodos validadores realicen una actividad constante en la red.
- ***EOS:*** este *blockchain* utiliza DPOS como algoritmo de consenso y elimina la necesidad de pagar por transacción, estableciendo un pago por mantenimiento de la red.

- ***NEO [2]:*** cuenta con un oráculo integrado para facilitar la comunicación de los *smart contracts* con el exterior. Dispone de un sistema de identidad auto-soberana personalizable y de un sistema de votación. El algoritmo de consenso es dBFT que proporciona escalabilidad y un alto número de transacciones por segundo.

Restricciones y problemas

- Debido a que la información de la cadena no se elimina, en el caso de querer utilizar *smart contracts* **no se recomienda el uso de datos personales** por la ley de protección de datos.
- Debido al carácter permanente de la información, es **difícil cumplir con aspectos regulatorios** como el derecho al olvido o las leyes de protección de datos.
- En la mayoría de los casos, el coste de las operaciones está ligado a la cotización de la criptomoneda.

Privados

Los *blockchain* llamados **privados o permisionados requieren que los participantes se registren o identifiquen para poder operar en la red** *blockchain*. Este tipo de redes suele estar controladas por una o varias empresas u organizaciones que establecen ciertos criterios para la aceptación de los usuarios y miembros de la red.

Estas soluciones *blockchain* están pensadas principalmente para su **uso en organizaciones o empresas que necesiten disponer de ciertos niveles de seguridad, privacidad** y de rendimiento que permiten cumplir con los requisitos legales o regulatorios de cada negocio.

La gestión de la información se adapta al mundo empresarial y es posible **controlar el acceso a la información e incluso establecer comunicaciones privadas entre un subconjunto de los participantes**. En un entorno de *blockchain* privado existen muchos menos nodos y estos no suelen tener acceso a toda la información de la solución *blockchain*. Al contrario de lo que sucede en una *blockchain* público los miembros solo acceden a la información que les atañe según las políticas establecidas en la red *blockchain* privada.

Cada propuesta *blockchain* cuenta con unas características específicas y es conveniente conocer las principales soluciones *blockchain* privadas o permisionadas junto con sus características principales:

- ***Hyperledger fabric* [4]:** es el *blockchain* más utilizado en el entorno corporativo por su flexibilidad para adaptarse a las necesidades de una gran variedad de sectores. Este *blockchain* es un desarrollo de IBM que se incorpora a la organización *hyperledger* como un proyecto de código abierto en 2016.

  Hyperledger es una organización **gestionada por la** *Linux Fundation* que promueve un conjunto de proyectos, librerías y herramientas dentro del ámbito de las soluciones DLT.

  Fabric es uno de los proyectos más antiguos de *hyperledger* y cuenta con la **madurez** suficiente para ser utilizado en **entornos de producción**.

  Las principales características de *hyperledger fabric* son:

  - Cuenta con una arquitectura permisionada.
  - Dispone de alta modularidad.
  - Permite acoplar otros mecanismos de consenso.
  - Cuenta con un modelo de *smart contracts* **flexible** que se puede desarrollar en distintos lenguajes.
  - La confirmación final ofrece una **latencia muy baja**. Esto se debe a que las transacciones tienen dos fases, una simulación de la ejecución y la fase de consolidación donde se aplican los cambios definidos en la simulación si las validaciones son correctas.
  - Proporciona distintos mecanismos para la **gestión de datos privados**. Dispone de una **arquitectura multicanal** que permite crear distintas cadenas con distintos permisos de acceso. Por otro lado, permite gestionar datos de forma privada en las transacciones.
  - Está pensado para una operativa continua, **permitiendo la actualización** de manera gradual y la operativa con distintas versiones.
  - Los *smart contracts* **disponen de versiones** que permiten la evolución de la funcionalidad incorporada en los contratos inteligentes.
  - **Los datos** asociados a los *smart contracts* se **almacenan en bases de datos** que permiten consultas sobre los datos.

  La comunidad de *hyperledger fabric* es muy grande y la evolución que ha tenido este *blockchain* en los últimos años le ha situado como la principal referencia en entornos corporativos, contando con una gran variedad de casos de uso desarrollados con esta tecnología.

- ***Quorum* [5]:** inicialmente fue un proyecto desarrollado por J. P. Morgan tomando como **base** la solución de *ethereum* que se modificó para poder ofrecer **transacciones privadas entre miembros de la red**.

  Actualmente quorum es gestionado por *ConsenSys* siendo un proyecto que cuenta con dos soluciones:

  - ***Hyperledger besu stack:*** utiliza *besu* como *blockchain* y cuenta con un módulo para la gestión de transacciones privadas llamado *orion*.
  - ***GoQuorum stack:*** basado en *ethereum* cuenta con distintos módulos para la gestión de transacciones privadas llamado *tessera*.

Ambas soluciones cuentan con un sistema de gestión de claves privadas que permite separar la creación de transacciones y la validación de estas.

Principales características de *quorum*:

- El **protocolo de capas** permite a las empresas trabajar sobre **redes públicas o privadas de** *ethereum*, ajustándose a los requisitos regulatorios y de seguridad.
- Dispone de **distintos mecanismos de consenso** para las dos soluciones disponibles.
- Proporciona la conectividad necesaria para **monitorizar** el desempeño de la red y gestionar los eventos para disponer de un entorno de alta disponibilidad.
- Permite que se puedan utilizar otros módulos o productos.
- Ofrece distintos servicios de **soporte para empresas**.

- ***Alastria [6]:*** es una **asociación** sin ánimo de lucro que fomenta la economía digital mediante la **promoción de tecnología descentralizadas como** *blockchain*. Alastria realiza una gran labor de divulgación de la tecnología *blockchain* y cuenta con el apoyo de grandes empresas española.

  Alastria se denomina como una red pública-permisionada compatible con la regulación.

  Las principales características de *alastria* son:

  - *Alastria* dispone de 3 redes que funcionan con distintas soluciones *blockchain*:
    - » *Quorum*
    - » *Hyperledger besu*
    - » *Hyperledger fabric*
  - No tiene criptomoneda embebida.
  - Ofrece un gran rendimiento **(>1000 tps)** y escalabilidad.
  - Ofrece validez legal al incorporar ID alastria (identidad digital).
  - Las transacciones no tienen coste.
  - Se requiere una **cuota de miembro**.
  - Es compatible con la red de *ethereum*.

  Una de las aportaciones más importantes de esta organización es la propuesta de identidad digital, que permite a los ciudadanos gestionar su información personal, sus títulos académicos, informes de solvencia y en general cualquier información relativa a la persona que sea generada por un tercero.

- ***Ripple [7]:*** es una red *blockchain* para realizar pagos donde participan bancos y empresas que permite operar con 40 monedas.

  Es una solución que permite realizar pagos globales más rápido y a un menor coste que los modelos tradicionales de cambio de divisa.

  Las principales características son:

  - Los pagos se **consolidan en 4 segundos** y gestiona 1500 transacciones por segundo.
  - Este *blockchain* permisionado **dispone de una criptomoneda**, siendo una característica muy particular de este *blockchain*.

- *Ripple* es un *blockchain* permisionado pensado para las empresas que requieran realizar pagos globales, siendo una solución *blockchain* muy particular especialmente dentro del conjunto de *blockchain* permisionados.

- ***Corda [8]:*** esta solución *blockchain* de **código abierto está gestionado por R3** que es una empresa de desarrollo *software* que colabora con más de 350 instituciones.

  Inicialmente se planteó una solución para el entorno financiero que permitía establecer flujos de intercambio de información sobre *smart contracts*. Más tarde se flexibilizó la solución para dar soluciones al mundo empresarial más allá del entorno financiero, permitiendo que los *smart contracts* puedan implementar procesos de negocio.

  Las principales características son:

  - Las **transacciones son privadas** y solo llegan a los participantes o interesados en las transacciones.
  - Las transacciones se componen de unos valores de entrada y unos valores de salida. La gestión de una **transacción** tiene una primera fase de propuesta que ha de ser **firmadas digitalmente por los participantes** y una segunda fase de consolidación donde interviene la lógica definida en los *smart contracts*.
  - El modelo de Corda funciona mediante **transacciones que funcionan como propuestas de cambio de estado** en la cadena de bloques, donde un participante propone un cambio de estado indicando unos estados actuales o entradas y generando unas salidas o estado finales. Estos cambios han de ser aceptados por el resto de participantes, por último, el *smart contract* valida los estados finales para incluir la transacción en la cadena si las validaciones son correctas.

Análisis de los tipos de blockchain

Cada tipo de *blockchain* proporciona una serie de características *(tabla 1)*, es importante entender cada una de las características asociadas a los tipos de *blockchain* para poder plantear las soluciones *blockchain* que mejor se ajustan a las necesidades de los negocios o de los usuarios [9].

Consorcios

Los *blockchain* privados suelen agrupar distintas empresas u organizaciones en un consorcio para acordar el mecanismo que permitirá gobernar el proyecto *blockchain*. En muchas ocasiones se formaliza un consorcio donde los participantes han de acordar el roll de cada participante y deben abordar las siguientes cuestiones:

- ¿Quién se hace cargo del coste del desarrollo y la parte operativa de la red?
- ¿Dónde se van a instalar los nodos?
- ¿Cuándo y de qué manera se unen los participantes a la red?
- ¿Cuáles son las reglas de confidencialidad en la red?
- ¿Quién es responsable de fallos? Por ejemplo, en el caso de un *smart contract* compartido.

También es necesario evaluar los intereses de los potenciales participantes para elaborar un modelo empresarial viable.

- **Beneficio mutual -> coste compartido**
  - **Ejemplo:** red donde se comparte información de referencia

Públicos	Privados
• Cualquier persona puede participar • La información incluida en la cadena es inmutable • Los ataques requieren de un gran poder computacional o de un gran coste económico • Disponen de una criptomoneda que permite realizar transferencias de valor en la red y costear la ejecución de las operaciones en la red.	• El acceso está controlado, solo los participantes con permiso pueden participar. • Suelen ofrecer un procesamiento de transacciones bastante elevado • Están pensados para ofrecer una gran escalabilidad de las soluciones • Permite cumplir con los requisitos o estándares que se aplican en los entornos corporativos. • El consenso de los bloques se logra con menos nodos y utilizando otros algoritmos de consenso

Tabla 1. Comparativa entre *blockchain* públicos y privados.

- **Beneficio asimétrico -> Plantear un pago proporcional**
  - **Ejemplo:** pago por acceso a KYC

Los *blockchain* privados o permisionados, no suelen disponer de una criptomoneda, por lo que la cuantificación del uso de la red y de los recursos ha de plantearse utilizando otros criterios.

Resumen

La evolución de blockchain hacia el mundo empresarial ha supuesto la aparición de soluciones blockchain permisionadas con grandes capacidades enfocadas a cubrir las necesidades empresariales.

Blockchain se abre a nuevos desafíos como gestionar datos sensibles y controlar el acceso de la información que se guarda en *blockchain*. Estas nuevas características se suman a las que comparten los *blockchain* públicos y privados, que mediante una red de nodos distribuida y la comunicación *peer-to-peer* son capaces de proporcionar un sistema de validación de la información, soportado por los nodos que mantienen réplicas de la cadena de bloques.

Existen muchas soluciones privadas o permisionadas que permiten a las empresas plantear nuevos modelos de colaboración, pero estos nuevos modelos basados en *blockchain* requieren también de una buena definición de gobierno de la red y de la elaboración de un modelo de negocio que permita la adopción de nuevos casos de uso.

Bibliografía

[1] L. Shiff. *Public vs private blockchains: what's the difference?* 2018 [En línea]. Disponible: https://www.bmc.com/blogs/public-vs-private-Blockchain/

[2] C. Comben. *Explicación de la tolerancia a errores bizantina delegada (dBft)*. 2019 [En línea]. Disponible: https://coinrivet.com/es/delegated-byzantine-fault-tolerance-dbft-explained/

[3] NEM. *Nemplatform.com* 2020 [En línea]. Disponible: https://nemplatform.com/#advantages

[4] Hyperledger. *Hyperledger fabric*. 2020 [En línea]. Disponible: https://www.hyperledger.org/use/fabric

[5] Consensys.net. *Quorum*. 2020 [En línea]. Disponible: https://consensys.net/quorum/

[6] Alastria.io. *Alastria* 2020 [En línea]. Disponible: https://alastria.io/

[7] Ripple.com. *Ripple*. 2020 [En línea]. Disponible: https://ripple.com/

[8] Corda.net. *Corda*. 2020 [En línea]. Disponible: https://www.corda.net/

[9] D. Massessi. *Public vs private blockchain in a nutshell*. 2018 [En línea]. Disponible: https://medium.com/coinmonks/public-vs-private-Blockchain-in-a-nutshell-c9fe284fa39f