Polkdot: Interacción y operabilidad entre blockchains

Danilo Antonio Tovar Arias
Ingeniería de Sistemas
Universidad de Antioquia
Medellín, Antioquia
danilo.tovar@udea.edu.co

***Resumen*—En este artículo ...**
***Palabras clave*—blockchain, polkadot, tecnología**

I. Introducción

En las últimas décadas, se ha experimentado un progreso acelerado en las tecnologías de la información. Desde la creación de dispositivos de comunicación global, como la televisión satelital, hasta sistemas integrados de información y comunicación, como los teléfonos inteligentes, la sociedad ha cambiado sus hábitos y métodos de gobernanza sobre la información y cómo ésta se distribuye alrededor del mundo.

Asimismo, en los últimos años han surgido una serie de tecnologías innovadoras que prometen revolucionar la forma en que vivimos una vez más, especialmente en los métodos de control de activos y la gestión de trazabilidad de acciones en internet. Una de estas tecnologías que ha avanzado lo suficiente como para generar interés en diferentes sectores globales es la *blockchain*, generalmente definida como una base de datos descentralizada. Sin embargo, representa un cambio significativo en la forma en que están construidos los sistemas actuales en la web, debido a sus diversas derivaciones y casos de uso para problemas relacionados con la seguridad, persistencia y privacidad de la información.

Aunque la *blockchain* es una tecnología con muchas oportunidades todavía siguen existiendo problemas que la limitan, por lo que se explorará, describirá y probará una *blockchain* emergente que propone solucionar problemas de interoperabilidad y comunicación efectiva entre *blockchains* ya existentes, llamada *Polkadot*. Y para entender mejor la relevancia de la *blockchain* y la necesidad de un sistema de interacción entre diferentes sistemas basados en esta tecnología, primero es fundamental comprender algunos conceptos básicos sobre ella.

II. Blockchains

La *blockchain* nace a partir de la motivación por crear un sistema de intercambio o transferencia de confianza entre usuarios anónimos sin la necesidad de un intermediario, y consiste en una base de datos con las transacciones que realizan los miembros de una comunidad descentralizada sobre sus activos, organizados en una lista de bloques encadenados secuencialmente [1]. En la primera *blockchain Bitcoin*, esto se logra a partir del uso de ciertos elementos:

- Transacciones, es decir, acciones de intercambio o modificación sobre los activos y su posesión, como realizar un pago o alterar el precio de un producto en un mercado.
- *Merkle Tree*, correspondiente a un proceso de combinación de pares de valores y su encriptación mediante un método como SHA-256.
- *Merkle root*, el valor final obtenido del *Merkle Tree*
- *Hash*, entendido como el resultado o acción de encriptar mencionada anteriormente.
- Prueba de trabajo, mejor conocido como *Proof of work*, corresponde a un proceso de consolidación del bloque sobre la cadena existente a través del uso de esfuerzo computacional para cumplir una condición.
- *Nounce*, número que cumple con la condición necesaria de la prueba de trabajo.
- Número único de bloque, también conocido como *block hash*, corresponde a la identificación de cada bloque en la cadena, y es generado a partir realizar un *hash* sobre la combinación del número del bloque anterior, el *Merkle root* del bloque actual y el *nounce* con el que se resolvió la prueba de trabajo.
- Nodos, servidores o computadores donde se realiza la interacción con la *blockchain*.

La primera *blockchain* lanzada en 2009, *Bitcoin*, utiliza los componentes anteriores además de un conjunto de reglas de validación de transacciones, protocolos de comunicación entre los diferentes nodos de la red, protocolos de consenso sobre el estado de la cadena y un sistema de recompensas basadas en participación, para cumplir con el objetivo de mantener un intercambio de activos seguro, anónimo, confiable y prácticamente irreversibles entre diferentes usuarios.

Con la creación de *Bitcoin*, comienza la revolución de la tecnología *blockchain* que se conoce en la actualidad como Web3, pues ”se inició una primera ola de descentralización en campos tan importantes como son los pagos, las transferencias internacionales y las remesas” [2]. A medida que ha ido avanzando esta tecnología también se han desarrollado nuevos usos y mejoras sobre la idea inicial propuesta por *Bitcoin*, por ejemplo, el intercambio de los activos de una red por un valor equivalente en otra red, la creación de redes *blockchain* privadas para uso empresarial, la capacidad de crear contratos inteligentes que realizan tareas específicas, o

aplicaciones sobre la red donde las interacciones con la misma sean almacenadas sobre una *blockchain* conocidas como *dApps* (*decentralized Applications*, en inglés), entre muchos otros.

Sin embargo, a pesar de los avances realizados en el desarrollo tecnológico con *blockchain*, existen problemas o limitaciones intrínsecas a esta tecnología expresados en [3] como:

- **Comunicación:** Entre diferentes redes es complicado hacer transferencia de información sobre transacciones realizadas sin intermediarios, debido a que la estructura de la información en cada *blockchain* es diferente y está generalmente ligada con el otros elementos dentro de la misma cadena.
- **Escalabilidad:** No se ha observado la aplicabilidad de la tecnología a gran escala ya que el promedio de transacciones por segundo (tps) de las *blockchains* es bajo dado los sistemas de validación, consolidación y consenso de los bloques, por ejemplo, *Bitcoin* posee una velocidad de aproximadamente 7 tps y *Ethereum* posee aprox. 25 tps, mientras que sistemas centralizados como Visa posee una velocidad de aprox. 1736 tps. Así mismo, debido a la necesidad de procesamiento de una gran cantidad de transacciones se producen comisiones y recargos excesivos sobre las transacciones que se realizan.
- **Seguridad:** Debido a que la seguridad de los bloques está asociada con la frecuencia y velocidad de creación de nuevos bloques, muchas redes nuevas son hackeadas por no tener una comunidad activa antes de su creación.
- **Personalización:** La creación de funcionalidades específicas para satisfacer las necesidades de las aplicaciones construidas en *blockchains* es complicada debido a que las cadenas poseen funcionalidades limitadas a su enfoque, lo que genera la posibilidad de necesitar empezar de cero con la creación de una *blockchain* con las capacidades requeridas.
- **Gobernanza:** El futuro de las redes *blockchain* están generalmente limitado por la falta de un sistema de gobernanza sobre la cadena, produciendo que las decisiones sean tomadas por un grupo central de usuarios o en ad hoc, ó incluso que no exista un toma de decisiones.
- **Actualización:** Las mejoras que se realizan sobre una red *blockchain* pueden causar divisiones en la comunidad o la cadena debido a que se generan bloques diferentes entre los usuarios que hacen uso de la versión anterior y la versión actualizada de la cadena, por lo que las aplicaciones deben de actualizarse con antelación para acomodarse a los cambios y evitar problemas cuando se actualiza la *blockchain*.

Este conjunto de dificultades son afrontadas por diferentes *blockchains* a través de cambios a la estructura o a los protocolos con los que funcionan; pero existe una alternativa que permitiría a los desarrolladores concentrarse en las aplicaciones que quieren realizar mientras que internamente estos problemas son resueltos de manera automática, correspondiente a *Polkadot*.

III. Polkadot

A. Visión

Polkadot corresponde a una *blockchain* de capa-0, es decir, una infraestructura diseñada para soportar y facilitar procesos de interacción y operación entre diferentes *blockchain* capa-1 como Bitcoin o Ethereum. Inicialmente en [4] Wood expresa que la estrategia que adopta Polkadot para crear una plataforma que permita la escalabilidad de sistemas de computo descentralizados consiste en desacoplar la arquitectura de consenso y el mecanismo de transición de estados, y el protocolo a utilizar para cumplir con este propósito mantiene el mismo nombre. Así mismo, Wood expresa que la propuesta inicial es experimental y funciona como un punto de partida para el desarrollo de mejoras y cambios a partir de las opiniones, criticas e ideas que surjan desde la comunidad al ser un proyecto abierto, es decir, *Polkadot* esta diseñado para ser un banco de pruebas de desarrollo, implementación e interacción de *blockchains* totalmente extensibles y escalables.

B. Polkadot protocol y soluciones

Siguiendo con lo expuesto en [4] *Polkadot* es una multicadena heterogénea escalable, es decir, a diferencia de implementaciones anteriores de *blockchain* que se han centrado en proporcionar una única cadena con diversos grados de generalidad para la realización de aplicaciones, *Polkadot* en sí está diseñado para no proporcionar ninguna funcionalidad inherente a la aplicación. En su defecto, *Polkadot* proporciona la "cadena de retransmisión" (*Relay chain*, en inglés) sobre la cual se pueden alojar una gran cantidad de estructuras de datos dinámicas validables y globalmente coherentes. A estas estructuras de datos las llamamos cadenas "paralelizadas" o *parachains*, aunque no existe una necesidad específica de que sean de naturaleza *blockchain*.

Estos componentes corresponden a la base fundamental sobre la que funciona *Polkadot*, y permiten dar solución a los problemas de *blockchain* expuestos anteriormente cuando se combinan con algunos aspectos más técnicos que se explicarán en la siguiente sección, permitiendo según [3] las siguientes posibilidades:

- Conectar diferentes redes: A través de *blockchains* integradas al sistema de *Polkadot* por medio del método *sharding* correspondiente a una separación de datos únicos entre diferentes nodos; adicionalmente el uso de *bridges* permiten la comunicación con redes tradiconales como *Bitcoin*.
- Habilita la posibilidad de creación de redes personalizadas: *Blockchains* en *Polkadot* son construidas para cumplir con propósitos específicos, donde se puede escoger las áreas en las que se desempeñará y modificarlas para cumplir con las necesidades de las aplicaciones.
- Maneja tráfico pesado a escala: La capacidad teórica máxima de transacciones por segundo de la red es mayor a 166.000 tps, con estudios más recientes presentando a posibilidad de superar las 500.000 tps, mientras que Visa posee una capacidad máxima de 65.000 tps.

- Revoluciona la governanza en línea a través de un sistema abierto y dirigido por la comunidad: A través de un sistema de propuestas y votación similar a un sistema democrático donde la comunidad que hace uso de *Polkadot* puede participar.
- Seguridad lider en la industria: Permite a las *blockchain* integrarse al sistema de seguridad compartida de *Polkadot*, sin necesidad de desviarse del propósito para el que son creadas.
- Actualización propia de la red: *Polkadot* puede actualizarse sin dividir la comunidad o las *blockchains*, debido a su capacidad de realizar el proceso de manera interna sin la necesidad de acciones manuales por parte de sus usuarios.

C. Arquitectura

La arquitectura de *Polkadot* está formada por diferentes componentes especializados para cumplir con el objetivo de su creación, a partir de la información en [4]–[6] estos son:

1) ***Relay chain:*** Como se ha mencionado anteriormente, corresponde a la base principal de *Polkadot* y funciona como un centro de operaciones para las *parachains*, donde se coordina y asegura el correcto funcionamiento de la red.
2) ***Parachain***:
3) **Actores**:
   - *Validadores (Validators):*
   - *Nominadores (Nominators):*
   - *Pescadores (Fisherman):*
   - *Coladores (Collators):*
4) **XCM**:
5) ***Bridges***:
6) **Protocolos de consenso**:
   - **NPoS**:
   - **GRANDPA**:
   - **BABE**:

La mayoría de estos elementos se pueden ver representados en la Fig. 1. tal que [...]

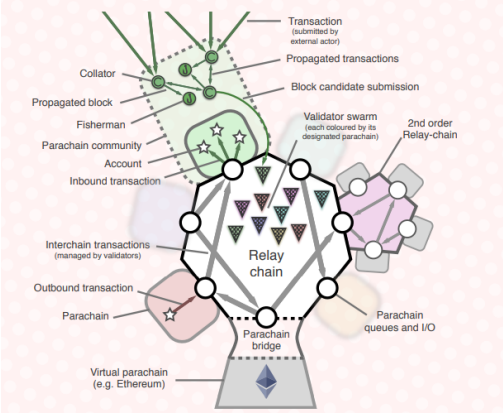

Fig. 1. Esquema resumido del sistema *Polkadot*

D. Información adicional

[Slot Auctions] [Polkadot-JS] [OpenGov] [Testnets]

IV. Implementación de un contrato inteligente en una Testnet de Polkadot

** Pendiente: https://www.linkedin.com/pulse/deploying-polkadot-smart-contracts-step-by-step-guide-burlakov-b8uoe

V. Conclusiones y trabajo futuro

[Conclusiones]

References

[1] F. J. Moreno-Arboleda, Rodríguez-Camacho, Johan S, y D. Giraldo-Muñoz, “Comparación de Dos Plataformas de Blockchain: Bitcoin y Hyperledger Fabric”, Ingeniería y competitividad, vol. 24, no. 1, p. -, 2022, doi: https://doi.org/10.25100/iyc.24i1.11027.

[2] A. Preukschat and C. Kuchkovsky, Blockchain : la revolución industrial de Internet. Barcelona Booket, 2019.

[3] Polkadot, “What is Polkadot? A Polkadot for Beginners Guide and Intro to Blockchain”, YouTube, May 21, 2020, https://www.youtube.com/watch?v=kw8eu2VadFA (accessed Oct. 18, 2024).

[4] G. Wood, ”Polkadot: Vision for a Heterogeneous Multi-Chain Framework”, Polkadot, 2016, https://polkadot.com/papers/Polkadot-whitepaper.pdf (accessed Oct. 18, 2024).

[5] H. Abbas, M. Caprolu, and R. Di Pietro, “Analysis of Polkadot: Architecture, Internals, and Contradictions”, IEEE Xplore, Aug. 01, 2022. https://ieeexplore.ieee.org/document/9881859 (accessed Oct. 24, 2024)

[6] “Architecture”, Polkadot, Oct. 3, 2024, https://wiki.polkadot.network/docs/learn-architecture (accessed Oct. 18, 2024).

[7] “Web3 and Polkadot”, Polkadot, Sep. 19, 2024, https://wiki.polkadot.network/docs/web3-and-polkadot (accessed Oct. 18, 2024).

[8] “Polkadot Developer Portal”, Polkadot, Oct. 3, 2024, https://wiki.polkadot.network/docs/learn-architecture (accessed Oct. 18, 2024).