Bridges: facilitando la comunicación entre Blockchains

Yenifer D. Osorio, *Univerdad de Antioquia, Medellín, Antioquia, Colombia*

Resumen—

En 2008, Satoshi Nakamoto publica su artículo donde presenta una nueva tecnología y sienta las bases del blockchain, una estructura de datos descentralizada e inmutable para registrar transacciones digitales. Esto impulsa una revolución en las criptomonedas y la tecnología blockchain, generando que comiencen a aparecer diferentes protocolos y arquitecturas que al no estar bajo un estándar, hace que la comunicación entre ellos sea compleja, lo que lleva a investigar propuestas para dar solución a este problema de comunicación entre blockchains (interoperabilidad). Una de estas propuestas son los bridges, y es en estos en los que este artículo se centrará, hablando de conceptos claves, de cómo funcionan, de los mecanismos de verificación que usa, de cómo se comunican, entre otros aspectos de los mismos.

INTRODUCCION

En el año 2008, Satoshi Nakamoto publica el artículo [1] "Bitcoin: A Peer-to-Peer Electronic Cash System". En este artículo, basado en trabajo previo en criptografía y sistemas distribuidos, sentó las bases de lo que hoy se conoce como blockchain. En este artículo, Satoshi Nakamoto propone una estructura de datos descentralizada que guarda de manera inmutable transacciones digitales.

A partir de esta publicación comienza una revolución en el ámbito de las criptomonedas y la tecnología blockchain, llevando a que se diera la aparición de varios protocolos y arquitecturas aplicando esta estructura de datos. El rápido desarrollo de este modelo y el hecho de que no hubiera un estándar en los protocolos y en la estructura de los blockchain, ha ocasionado que cada uno sea un universo diferente y que la comunicación entre estos universos sea muy compleja. Este problema de comunicación ha llevado a que se hagan diferentes investigaciones respecto a cómo se puede romper esta barrera y es aquí donde aparece el termino interoperabilidad, que en términos de tecnología se refiere a la capacidad que tienen diferentes sistemas o plataformas de intercambiar datos, operar de manera conjunta y utilizar recursos de manera transparente y eficiente.

Este nuevo enfoque de estudio llevó a que se hicieran diferentes tipos de propuestas para solucionar el problema de la interoperabilidad entre blockchains. Dentro de estas propuestas surgieron soluciones como Sidechains, Blockchain Routers y Blockchain Bridges. Los Sidechains se describen como un enfoque que utiliza una conexión bidireccional para la comunicación; los Blockchain Routers tienen algunos nodos que actúan como enrutadores para transmitir solicitudes entre blockchains; y los Blockchain bridges actúan como pasarelas entre diferentes bloques. [2]

En este artículos se hará énfasis en los Blockchain Bridges. El sitio de Etherium.org da una definición para los bridges: [3] "se refieren a mecanismos que permiten la interoperabilidad y la comunicación entre diferentes blockchains o entre blockchains y sistemas externos. Estos Bridges desempeñan un papel crucial a la hora de facilitar el intercambio de activos, datos y

servicios a través de múltiples libros de contabilidad de blockchain".

Durante este artículo se ampliarán temas como los tipos de Bridges que actualmente se encuentran, conceptos claves para entender el funcionamiento de los mismos, la forma en que funcionan, las diferencias que tiene respecto a las otras soluciones y bridges más usados hoy en día en el mercado.

MARCO TEORICO

Tras la aparición de la interoperabilidad como uno de los principales problemas en blockchain, aparecen diversas tecnologías que buscaban darle una solución a dicho problema. A continuación serán explicadas algunas de estas someramente:

Sidechains: En el año 2009, un grupo de personas publicó un artículo "Enabling Blockchain Innovations with Pegged Sidechains" [5], donde propone una nueva tecnología, los Sidechains o cadenas laterales vinculadas. Esta nueva tecnología permite transferir bitcoins y otros activos contables entre múltiples cadenas de bloques. Esto brinda a los usuarios acceso a sistemas de criptomonedas nuevos utilizando los activos que ya poseen. Al reutilizar el Bitcoin, estos sistemas pueden interoperar entre sí y con Bitcoin, evitando la escasez de liquidez y las fluctuaciones del mercado asociadas con las nuevas monedas. Debido a que las cadenas laterales son sistemas separados, la innovación técnica y económica no se ve obstaculizada.

La base técnica de los Sidechains es el two-way peg. Este, es un mecanismo que permite la transferencia bidireccional de activos entre una cadena principal (mainchain) y una cadena lateral (sidechain) de manera segura y confiable. En un sistema de two-way peg, los activos se pueden mover desde la cadena principal a la cadena lateral y viceversa. Esto se logra generalmente a través de un proceso de bloqueo y liberación de activos en ambas cadenas.

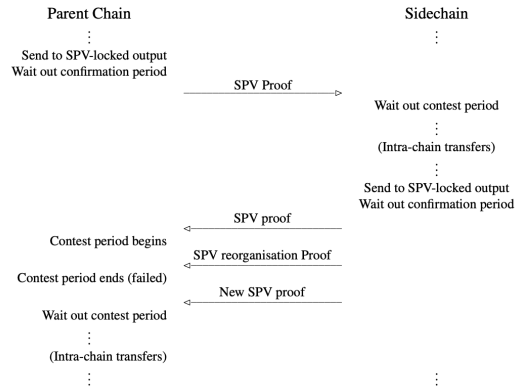

Figura 1: Flujo de los sidechains [5]

Para la verificación de la validez de las transacciones en la cadena principal (mainchain) sin necesidad de descargar y verificar toda la cadena de bloques, se usa SPV (Simplified Payment Verification). El SPV es un DMMS (Decentralized Mutable Merkle Sum Tree), es decir, un mecanismo de consenso y seguridad de blockchains. Una prueba SPV está compuesta por: una lista de encabezados de bloque que demuestran la prueba de trabajo, y una prueba criptográfica de que se creó una salida en uno de los bloques de la lista. Esta prueba puede ser invalidada por otra prueba que demuestre la existencia de una cadena con más trabajo que no incluya el bloque que creó la salida.

Blockchain routers o enrutadores de blockchain: el concepto de routers para blockchain lo introdujo por primera vez Hui Wang, Yuanyuan Cen y Xuefeng Li en su artículo "Blockchain Router: A Cross-Chain Communication Protocol" [6]. En este articulo ellos plantean un diseño para este concepto que se deriva de la arquitectura de enrutamiento de internet, en la cual, una red de enrutamiento básica consta de routers y dispositivos terminales. En términos de blockchain, los sistemas blockchain como Etherium y Bitcoin, serían las terminales de la red, a lo que se le llama subcadena y esta subcadena puede recibir mensajes de un router de cadena, o enviar mensajes a otra subcadena a través del router de cadena, pero no pueden comunicarse directamente entre sí.

El router es usado para enlazar las subcadenas en la red de cadenas. Para comunicarse con otras subcadenas, una subcadena primero debe establecer conexión con

el router blockchain siguiendo el protocolo de comunicación entre cadenas.

En la arquitectura de esta propuesta hay cuatro participantes:

1. **Validadores:** Verifican, concatenan y envían bloques a la ubicación correcta.
2. **Nominadores:** son recompensados por contribuir con sus propios fondos a los validadores.
3. **Supervisores:** monitorean el comportamiento del enrutador blockchain.
4. **Conectores:** son responsables de enviar la información de la subcadena al enrutador blockchain y viceversa.

En la siguiente imagen, se puede ver la arquitectura mencionada previamente con cada uno de los participantes de la misma:

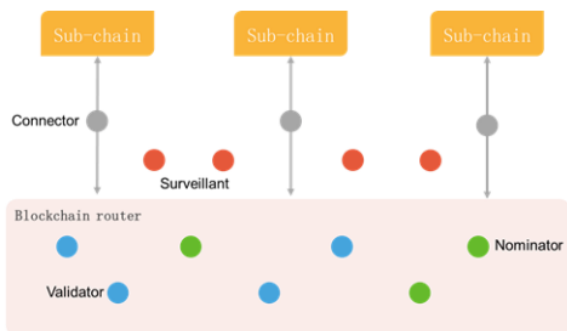

Figura 2: Diagrama que muestra funcionamiento de los Blockchain Routers [6]

Ahora, se procederá a hablar sobre el tema principal de este articulo: los bridges.

Bridges: son otra solución propuesta al problema de interoperabilidad que tienen las blockchain. Los puentes en el mundo fisico permiten la comunicación entre dos lugares, en el caso de las blockchain, los puentes permiten la transferencia fluida bidireccional de activos y datos entre diferentes redes blockchain y entre la layer 1 y la layer 2.

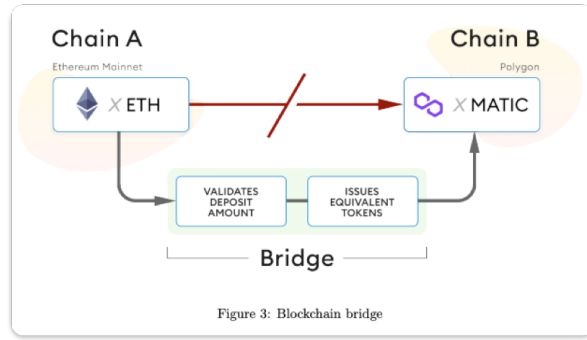

Figura 3: Diagrama que ilustra funcionamiento de un bridge [3]

Se puede hacer una categorización de puentes basado en tres estándares: mecanismos de confianza [4], conexiones de capa y funcionalidades.

1. Dentro del grupo de mecanismos de confianza, pueden ir:

Puentes centralizados: en blockchain se refieren a sistemas donde una organización de confianza controla toda la infraestructura del puente. Este enfoque facilita la transferencia de activos y datos entre diferentes cadenas de bloques. Los puentes centralizados al ser dependientes de una sola entidad pone un punto central de fallo, es decir, si el operador de puente falla o es comprometido, todo el puente podría ser interrumpido.

Puentes algo centralizados: Encuentran un equilibrio entre centralización y descentralización. Estos puentes distribuyen la responsabilidad entre varias entidades de confianza, formando un consorcio o un modelo federado. Esta repartición de la responsabilidad, hace que el riesgo de un único punto de falla reduzca.

Puentes descentralizados: tienen como objetivo eliminar la dependencia de cualquier entidad de confianza o consorcio. Operan a través de contratos inteligentes, permitiendo que se ejecuten transacciones de manera automatizada y verifiquen los datos en diferentes blockchains. Los puentes descentralizados enfrentan inconvenientes con la escalabilidad y la eficiencia debido al mayor gasto computacional requerido para el consenso y la validación en múltiples cadenas.

Puentes no confiables: este sistema opera entre blockchains que no comparten mecanismos de consenso o modelo de confianza común. Estos puentes usan técnicas criptográficas para verificar y validar

transacciones entre las cadenas conectadas. Los puentes no confiables pueden ser más complejos de implementar y pueden requerir protocolos criptográficos sofisticados.

2. Para el grupo de conexiones de capa, están los puentes que conectan no a nivel de blockchain, sino, a nivel de capa.

En blockchain, la capa 1 o layer 1, se refiere al protocolo base de una blockchain. Es la capa fundamental y comprende el protocolo de consenso, la validación de transacciones y la emisión de nuevos bloques. Por otro lado, la capa 2 o layer 2, se refiere a soluciones resultantes del trilema de las blockchain, el cual habla de los tres desafíos que tienen las blockchain en términos de descentralización, seguridad y escalabilidad, ya que mejorar unos de estos implica sacrificios en las otras dos.

Al haber estas capas, también se hace necesario establecer la conexión entre estas, es por esto que los puentes también se clasifican en dos categorías más: puestes L1 - L1 y puentes L1 - L2.

Puentes L1-L1: conectan diferentes blockchains que operan en la misma capa base o protocolo base.

Puentes L1-L2: establecen una conexión entre L1 y varias blockchains L2, mientras que las blockchains L2 también están interconectadas entre sí.

3. En el grupo de puentes según sus funcionalidades, están:

Puentes específicos de activos: solo permiten la transferencia de un activo específico.

Puentes específicos de cadena: estos puentes suelen ser desarrollados por blockchains principales.

Puentes específicos de aplicación: tienen funcionalidad limitada y están diseñados para manejar solo aplicaciones específicas, especialmente intercambios de activos.

Puentes generalizados: permiten la transferencia de varios tipos de información, como activos, llamadas de contrato, pruebas y estados. No están restringidos a blockchains o aplicaciones particulares, y en su lugar pueden facilitar la comunicación entre una diversa variedad de redes desconectadas.

Para llevar a cabo un consenso y transmitir mensajes según sea necesario entre las diferentes blockchain o entre las capas de las mismas, los puentes usan diferentes protocolos. [7] Los mecanismos de verificación que usan los protocolos en los puentes, pueden ser clasificados en cuatro categorías: verificación externa, verificación optimista, verificación local y verificación nativa.

Verificación externa (EV): Se basa en validadores externos, quienes verifican la validez de transacciones entre las blockchain. Los puentes que operan con este tipo de verificación, asumen que la mayoría de validadores son honestos y normalmente usan mecanismos de firma múltiple, en el que se establece un umbral para el número de validaciones requeridas para firmar una transacción y cada validador tiene una clave privada completa; o computación multipartita (MPC), el cual requiere que los validadores generen conjuntamente una clave privada. Este mecanismo es sencillo de implementar y muy usado, pero está expuesto a riesgos considerables si los validadores externos no son de confianza o son hackeados. Protocolos como Cross-Chain Interoperability Protocol (CCIP) y Omnichain interoperability protocol (LayerZero), utilizan este tipo de comunicación.

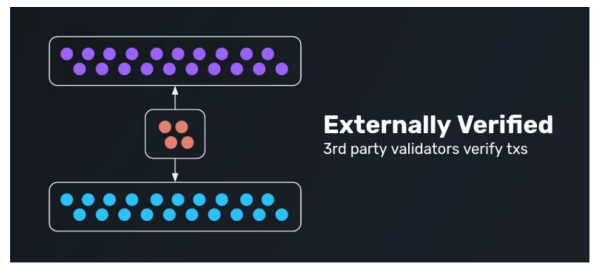

Figura 4: Diagrama que ilustra funcionamiento de la verificación externa [8]

Verificación optimista (OV): opera bajo el supuesto de que una transacción es válida en el momento que llega por primera vez al puente, no verifica su validez de inmediato, sino que entra en una “espera optimista”. Durante este periodo optimista, se permite que la transacción se complete y se ejecute en la blockchain de destino. Sin embargo, se establece un período de

tiempo durante el cual cualquier parte interesada puede presentar un "desafío" si sospecha que la transacción es fraudulenta o inválida, aquí se lleva a cabo una investigación para determinar la validez de la transacción. Si se encuentra que la transacción es válida, se mantiene y se completa como de costumbre. En caso contrario, se revierte y se penaliza a los actores malintencionados. Los puentes bajo esta categorización a menudo tienen una latencia más larga debido al período de desafío. Además, dichos puentes requieren al menos un observador honesto para verificar las actualizaciones y detectar actividad fraudulenta. Un protocolo que usa este mecanismo de verificación es el Optimistic Interchain Communication Protocol (Optics).

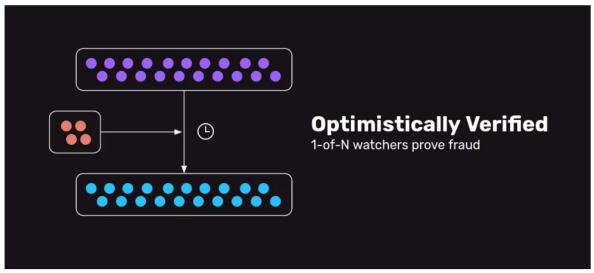

Figura 8: Diagrama que ilustra funcionamiento de la verificación optimista [8]

Verificación local: requiere únicamente que las partes involucradas en una transacción la verifiquen, convirtiéndolo en un mecanismo de verificación entre dos partes donde cada parte verifica únicamente a su contraparte. Un ejemplo de protocolo que use este mecanismo de verificación es Connext's NXTP

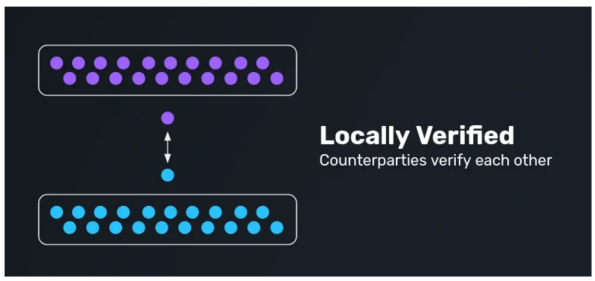

Figura 9: Diagrama que ilustra funcionamiento de la verificación local [8]

Verificación nativa: requiere que la blockchain de destino ejecute un cliente ligero de la blockchain de origen para verificar los eventos y estados relacionados con una transacción. Los clientes ligeros almacenan la información mínima requerida (encabezados de los bloques), necesaria para verificar el estado de una blockchain en particular. Este enfoque es considerado altamente seguro, debido a que usa las mismas suposiciones de la blockchain. Sin embargo, tener clientes ligeros para todas las blockchain es costoso, porque requiere recursos adicionales. MAP Protocol es uno de los protocolos que usa este tipo de mecanismo de verificación.

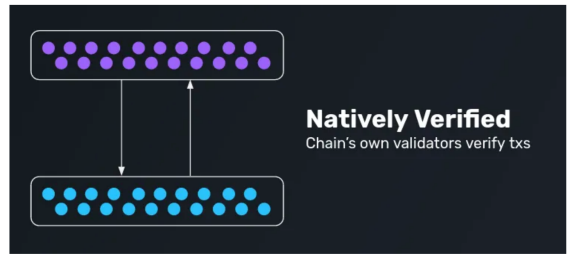

Figura 10: Diagrama que ilustra funcionamiento de la verificaciónnativa [8]

Los puentes también tienen dos formas de entablar comunicación entre dos blockchains o layers. Estas dos formas de comunicación son: Lock-and-Mint; Burn-and-Release; y Liquidity-Pool-Based.

Para el entendimiento de los flujos presentados a continuación es necesario tener el significado de lo siguiente:

- **AS (Account Source)**: cuenta del usuario en la cadena de origen.
- **CS (Source Chain)**: cadena de origen.
- **CD (Destination Chain)**: cadena de destino.
- **AD (Account Destination)**: La cuenta del usuario en la cadena de destino.
- **BD (Bridge Destination)**: puente usado para llevar a cabo la transferencia.
- **TLock**: La transacción que bloquea los tokens en la cadena de origen.
- **TMint**: La transacción que emite los tokens en la cadena de destino.
- **TBurn**: La transacción que quema los tokens en la cadena de destino.
- **TRelease**: La transacción que libera los tokens bloqueados en la cadena de origen.

El modelo lock-and-mint; burn-and-release, consta de dos fases principales: "bloqueo y emisión" para transferir tokens de una cadena de bloques a otra, y "quema y liberación" para devolver los tokens a la

cadena original. Este modelo sigue el siguiente flujo en el caso específico de transferencia y retiro de tokens entre cadenas:

Fase 1: Bloqueo y Emisión

1. Ejecución de la transacción de bloqueo (TLock):
    - El usuario (AS) que desea transferir tokens desde la cadena de origen (CS) a la cadena de destino (CD) envía una transacción (TLock) a la cuenta del puente en CS.
    - Esta acción bloquea los tokens en la cadena de origen.
    - Se emite un evento de depósito para que el servidor lo registre y lo verifique.
2. Envío de la transacción de emisión (TMint):
    - El servidor verifica que la información del evento de depósito es correcta.
    - Si todo es correcto, se crea y se firma una transacción (TMint) por parte de los validadores y se envía a la cadena de destino (CD).
3. Ejecución de la transacción de emisión (TMint):
    - La transacción TMint es enviada desde el puente en la cadena de destino.
    - Durante la ejecución, se verifican las firmas de los validadores.
    - Si se verifican correctamente, se emiten nuevos tokens en la cadena de destino (TD), que son versiones envueltas de los tokens originales (TS).
    - Estos nuevos tokens se transfieren a la cuenta del usuario (AD) en la cadena de destino.

Fase 2: Quema y Liberación

1. Ejecución de la transacción de quema (TBurn):
    - Cuando el usuario (AS) desea devolver los tokens a la cadena de origen, envía una transacción (TBurn) desde su cuenta (AD) en la cadena de destino (CD) para quemar los tokens envueltos (TD).
    - Los tokens se envían a la cuenta del puente o a la dirección cero, eliminándolos efectivamente de circulación.
    - Se emite un evento de quema para que el servidor lo monitoree.
2. Verificación y envío de la transacción de liberación (TRelease):
    - El servidor verifica el evento de quema, es decir, de eliminación de los tokens.
    - Si la verificación es correcta, se crea una transacción de liberación (TRelease) que es firmada por los validadores y enviada a la cadena de origen (CS).
3. Ejecución de la transacción de liberación (TRelease):
    - La transacción TRelease es ejecutada en la cadena de origen.
    - Los tokens bloqueados inicialmente son liberados y transferidos de vuelta a la cuenta del usuario (AS) en la cadena de origen.

La otra forma de lograr la comunicación entre blockchains, es a través del modelo Liquidity-Pool-Based. Para dejar explicito el flujo que sigue este modelo, se usará el mismo caso específico anterior: transferencia y retiro de tokens entre cadenas.
En el caso de transferencia, el usuario AS quiere enviar dinero desde una cadena a su propia cuenta SD en otra cadena, esta transacción por medio de esto modelo sigue el siguiente flujo:

1. **Ejecución de la transacción:**
    - El puentes crea el fondo de liquidez que solo contienen el token TS. El fondo de liquidez de los puentes solo tienen un tipo de token para evitar pérdidas transitorias para los proveedores de liquidez.
    - Los proveedores de liquidez, agregan liquidez al fondo agregando tokens TS.

- La transacción TSrc de AS a CS es ejecutada realizando una transferencia de token y emitiendo el evento de depósito para que el servidor lo escuche y lo registre.

2. **Envío de la transacción Dest:**
   - El servidor verifica que la información del evento de depósito es correcta.
   - Una vez verificado, se crea y firma la transacción Dest.
   - La transacción Dest se envía a la cadena de destino para continuar con la transferencia de los tokens.

3. **Ejecución de la transacción Dest:** Antes de este paso, los fondos de liquidez en la cadena de destino también deben estar preparados. En el fondo de la cadena destino, el fondo que solo contiene tokens TD es creado por el puente y los proveedores de liquidez agregan liquidez al fondo. Los tokens TS y TD representan los mismos tokens en diferentes blockchains. Mientras tanto, la transacción Dest enviada desde BD a CD realizará la verificación y luego transferirá los tokens TD desde el fondo de liquidez a AD.

RESULTADOS

A continuación se procederá a hablar un poco sobre algunos puentes existentes, con la intención de más adelante hacer una pequeña comparación enfocándose en algunos tipos de bridges que existen:

1. **Satellite by Axelar:** Según el sitio oficial de axelar, es una aplicación web construida sobre la Red Axelar. Proporciona una interfaz fácil de usar que permite a los usuarios transferir sus activos criptográficos de una cadena a otra. Satellite Funciona como un Puente descentralizado Además, utiliza contratos inteligentes para gestionar las transferencias de tokens entre cadenas. Sattellite utiliza DPoS(Delgated Proof of Steake), como mecanismo de consenso. Este puente permite transacciones entre aproximadamente 19 blockchains.

2. **Voltaje Bridge:** es un protocolo de finanza descentralizado (Defi) construido por Fuse Network. Su objetivo es proporcionar una plataforma segura, transparente y fácil de usar, que se centra en minimizar costos de transacción y las tarifas de gas. Usa fondos de liquidez para permitir estas transacciones. Tiene una función puente de token nativo para permitir a los usuarios mover tokens entre Fuse, Ethereum y BNB.

3. **Rainbow Bridge:** es un protocolo sin confianza y sin permiso para conectar cadenas de bloques. Este es un tipo de puente que permite transacciones entre layers 1. Su mecanismo de verificación es nativo y su forma de realizar las transacciones es Lock-and-Mint. El uso principal de Rainbow Bridge es la transferencia de tokens ERC-20 entre Ethereum, Aurora y Near.

Los anteriores bridges son solo algunas de las soluciones para la interoperabilidad que hay en el mercado. Todos estos tienen una característica en común y es que son puentes Trustless, es decir, sin confianza y que usan los contratos inteligentes para comunicarse.

Basándose en el marco teórico presentado anteriormente, y en la tabla IV expuestas en el articulo “SoK: Security of Cross-chain Bridges: Attack Surfaces, Defenses, and Open Problems” [7], se construyó la siguiente tabla que muestra las características centralizadas de los tres puentes anteriores:

Bridge	Verificación	Modelo de comunicación	Mecanismo de confianza
Rainbow Bridge	Nativo	Lock and Mint	Trustless
Satellite by Axelar	Nativo	Lock and Mint	Trustless
Voltage Bridge	Local	Liquidity-Pool-Based	Trustless

Tabla 1: Expone las características de los puentes basándose en el marco teórico

CONCLUSIONES

- Hay una gran variedad de puentes, cada uno con una casos de uso, características, ventajas y desventajas. Entonces, cuál usar depende

explícitamente de lo que el usuario esté buscando.

- Hay soluciones de bridges que se pueden usar entre blockhains específicos y otros que tienen mayor alcance, como por ejemplo el Satellite by Axelar que sirve para llevar a cabo transacciones para aproximadamente 19 blockchains.
- Los bridges no solo sirven para la transferencia de tokens entre blockchains, también permiten la transferencia de otro tipo de información.
- Con los bridges se reduce el problema de comunicación entre blockchains debido a las continuas actualizaciones de los bridges existentes y a la aparición de nuevos. Además de las investigaciones para cada día volverlos más seguros

REFERENCIAS

[1] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". Bitcoin - Open source P2P money. Accedido el 3 de mayo de 2024. [En línea]. Disponible: https://bitcoin.org/bitcoin.pdf

[2] S. Kotey *et al.* "Blockchain interoperability: the state of heterogenousblockchain-to-blockchain communication". https://ietresearch.onlinelibrary.wiley.com/doi/epdf/10.1049/cmu2.12594.

[3] "Introduction to blockchain bridges | ethereum.org". ethereum.org. Accedido el 27 de abril de 2024. [En línea]. Disponible: https://ethereum.org/en/bridges/

[4] P. Cuesta. "Analysis of bridge-solutions for public blockchains". Pàgina inicial de UPCommons. Accedido el 27 de abril de 2024. [En línea]. Disponible: https://upcommons.upc.edu/bitstream/handle/2117/403247/TFM_Pau_Cuesta_Arcos.pdf?sequence=3&isAllowed=y

[5] A. Back *et al.* "Enabling Blockchain Innovations with Pegged Sidechains". Blockstream: Bitcoin and digital asset infrastructure. Accedido el 3 de mayo de 2024. [En línea]. Disponible: https://blockstream.com/sidechains.pdf

[6] Wang, H., Cen, Y., & Li, X. (2017, marzo). *Blockchain router | proceedings of the 6th international conference on informatics, environment, energy and applications.* ACM Other conferences. https://dl.acm.org/doi/10.1145/3070617.3070634

[7] Zhang, M., Zhang, X., Barbee, J., Zhang, Y., & Lin, Z. (2023, diciembre). *SoK: Security of Cross-chain Bridges: Attack Surfaces, Defenses, and Open Problems.* arXiv.org e-Print archive. https://arxiv.org/pdf/2312.12573#page=18&zoom=100,65,840

[8] Bhuptani, A. (2021, octubre). *The Interoperability Trilemma.* Medium. https://medium.com/connext/optimistic-bridges-fb800dc7b0e0