Bridges

Article Type: Description (see below for more detail)

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

***Resumen*—**

# INTRODUCCIÓN

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.

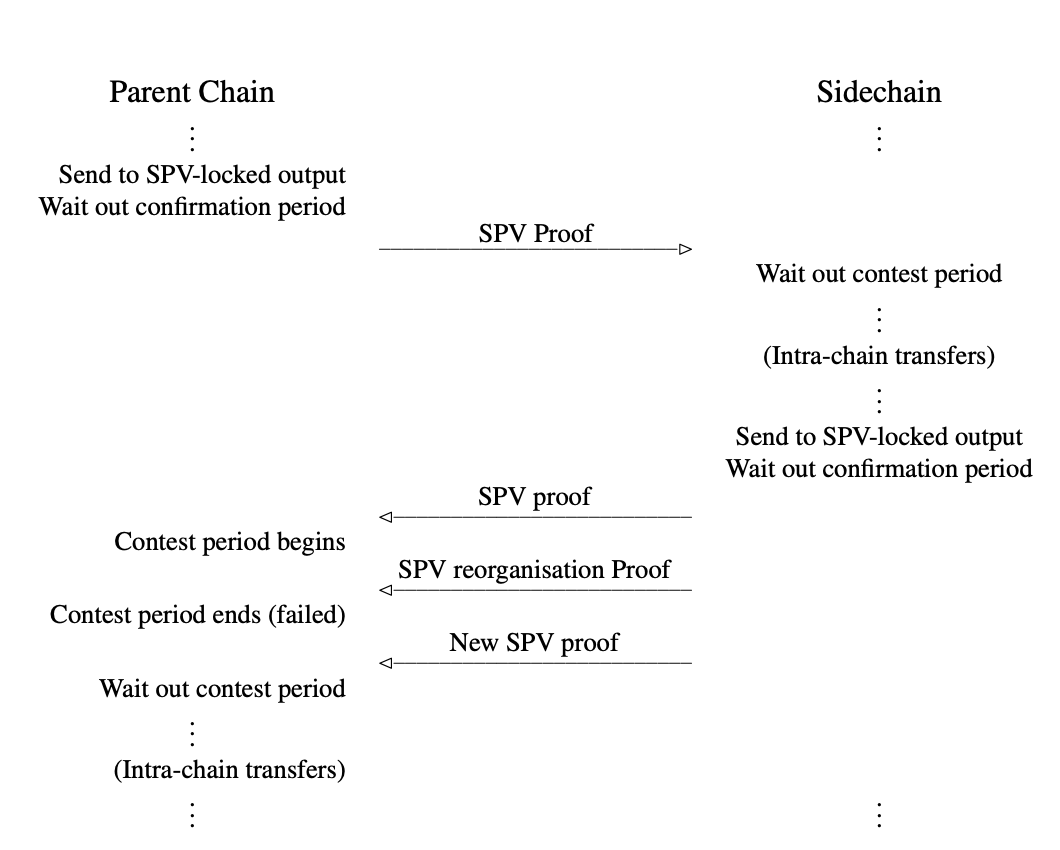
A partir de esta publicación comienza una revolución en el ámbito de las criptomonedas y la tecnología blockchain, llevando a que se diera la aparición de varios protocolos y arquitecturas aplicando esta estructura de datos. El rápido desarrollo de este modelo y el hecho de que no hubiera un estándar 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, Blockchain Bridges y soluciones basadas en Smart Contracts. 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, bridges más usados hoy en día en el mercado y cuáles son los mejores basados en diferentes características.

# MARCO TEóRICO

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. Dentro de las diferentes soluciones, a continuación serán explicadas someramente:  
  
 **Sidechains**: En el año 2009, un grupo de personas publicó un artículo “Enabling Blockchain Innovations with Pegged Sidechains” [4], 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, esto 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.  
  


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.

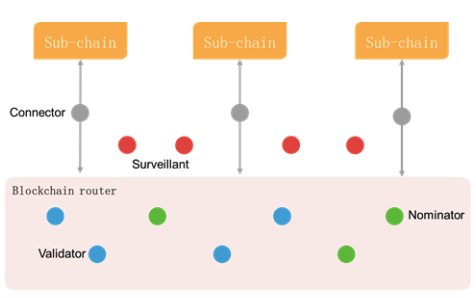
El router es usado para enlazar las subcadenas en la red de cadenas. Para comunicarse con otras subcadenas, una subcadena primero debe establecer conexión con el router blockchain siguiendo el protocolo de comunicación entre cadenas.

En la arquitectura de esta propuesta hay cuatro participantes:

1. Validadores: Verifican, concatenan y envían bloques a la ubicación correcta.

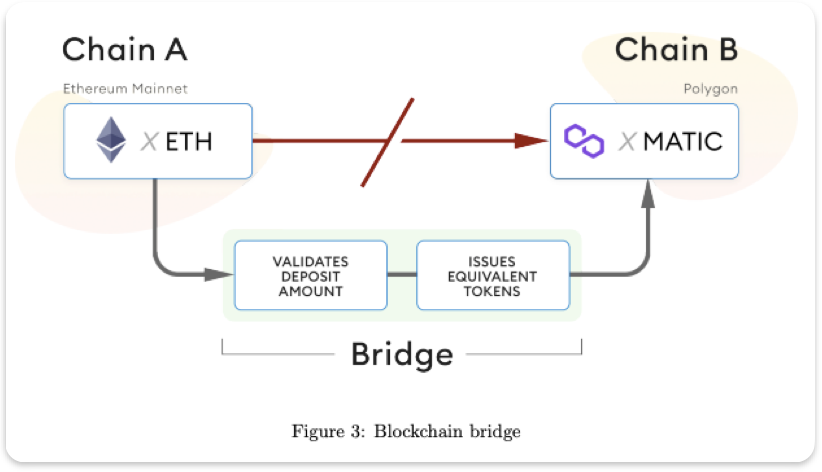
2. Nominadores: son recompensados por contribuir con sus propios fondos a los validadores.

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:



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 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 leyer 1 y la leyer 2.



Se puede hacer una categorización de puentes basado en tres estándares: mecanismos de confianza, 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.

1. 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 leyer 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 leyer 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.

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

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

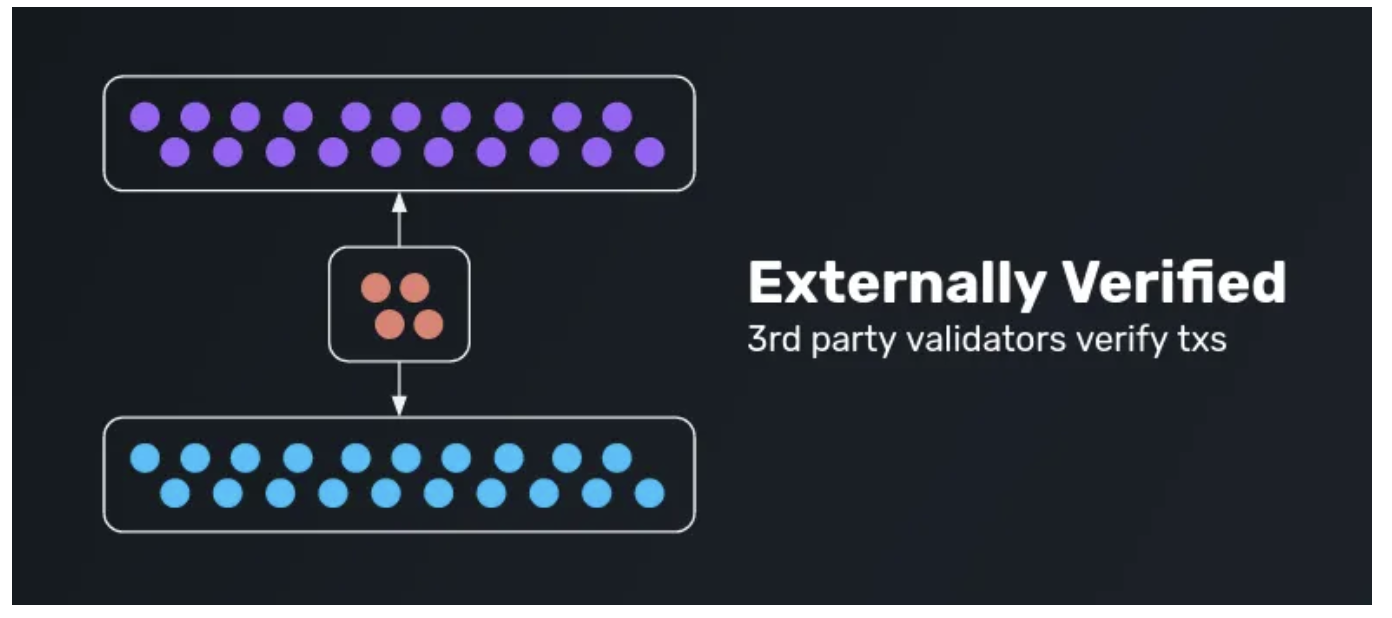
**Puentes específicos de cadena**: estos puentes suelen ser desarrollados por blockchains principales.

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

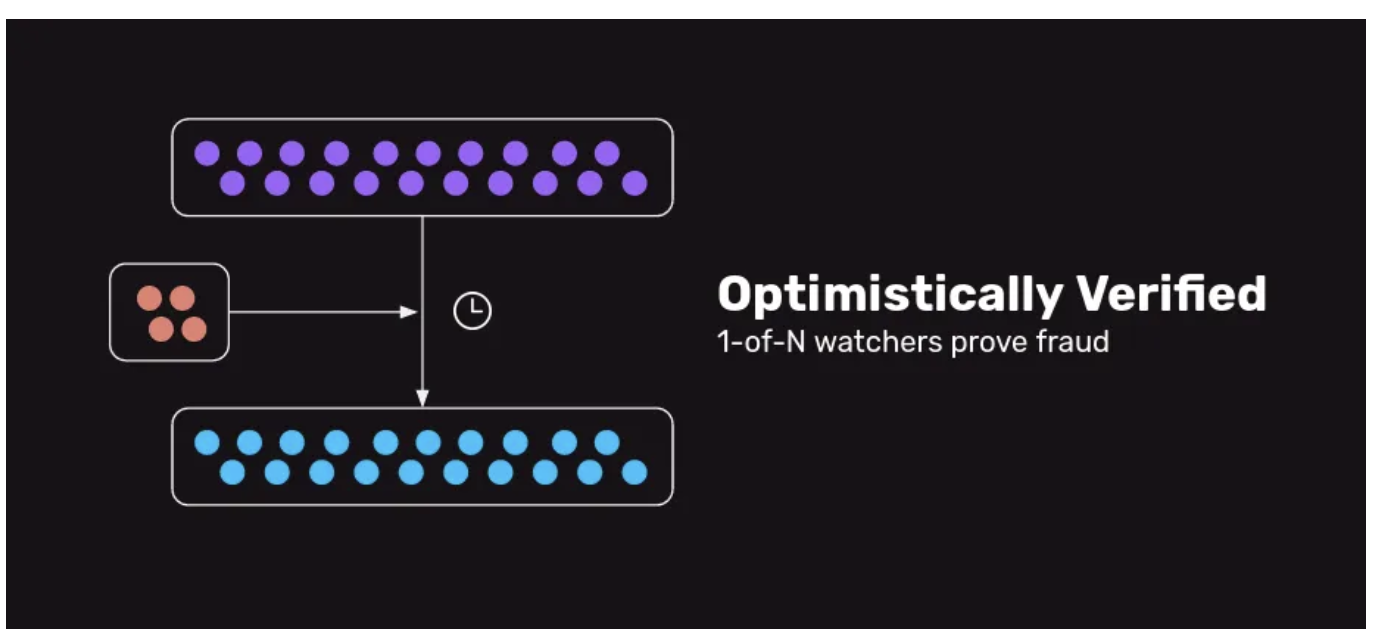
**Puentes generalizados:** permiten la transferencia de varios tipos de información, como activos, llamadas de contrato, pruebas y estados. No están restringidos a blockchains o aplicaciones particulares, y en su lugar pueden facilitar la comunicación entre una diversa variedad de redes desconectadas.

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. 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.

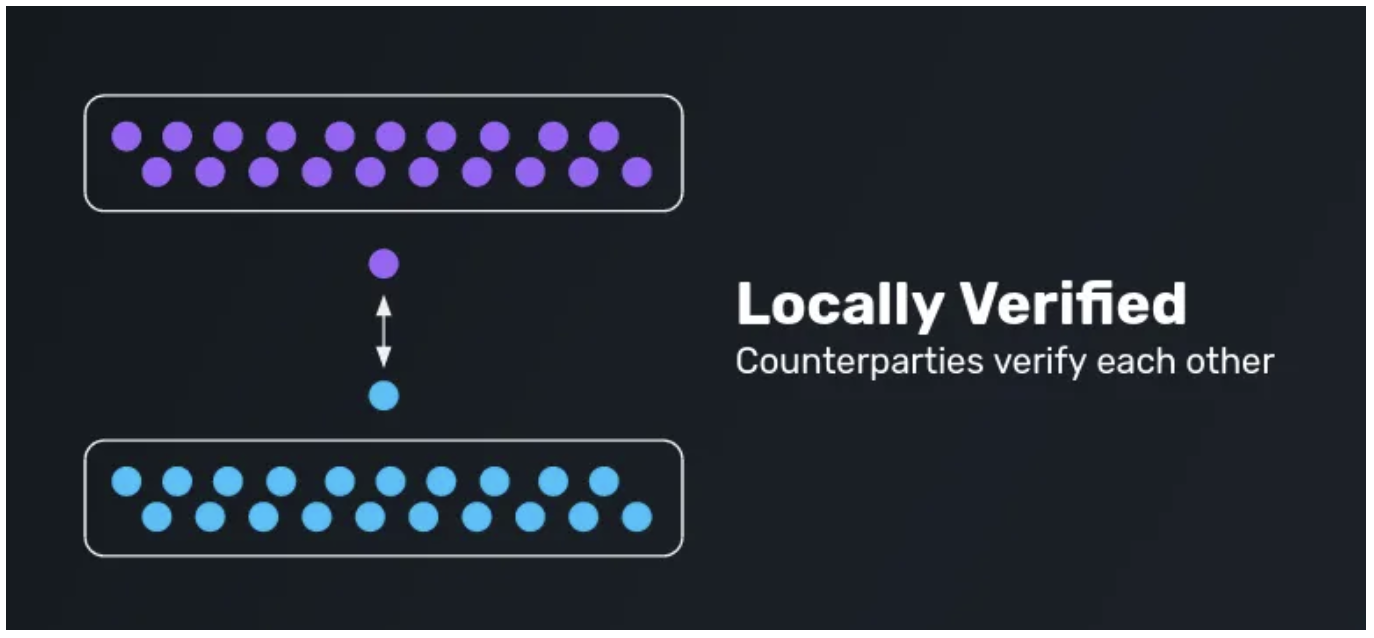
**Verificación externa (EV):** Se basa en validadores externos, quienes verifican la validez de transacciones entre las blockchain. Los puentes que operan con este tipo de verificación, asumen que la mayoría de validadores son honestos y normalmente usan mecanismos de firma múltiple, en el que se establece 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.



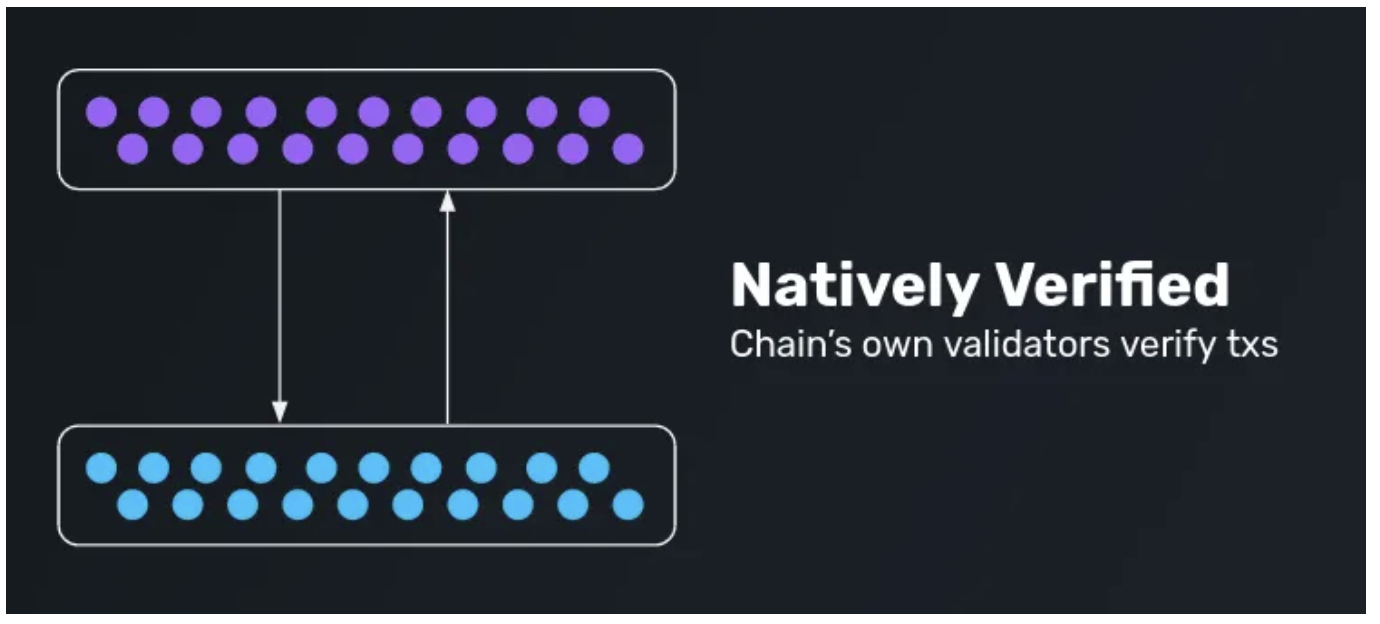
**Verificación optimista (OV):** opera bajo el supuesto de que una transacción es válida en el momento que llega por primera vez al puente, no verifica su validez de inmediato, sino que entra en una “espera optimista”. Durante este periodo optimista, se permite que la transacción se complete y se ejecute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



**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



**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.



Los puentes también tienen dos formas de entablar comunicación entre dos blockchains o leyers. Estas dos formas de comunicación son: Lock-and-Mint, modelo basado en quemar y liberar; y liquidity-pool-based, modelo basado en el fondo común de liquidez.

# CONCLUSIONes

The manuscript should include future directions of the research. Authors are strongly encouraged not to reference multiple figures or tables in the conclusion; these should be referenced in the body of the paper.

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&amp;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>

**Yenifer D. Osorio** Información de la autora