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.

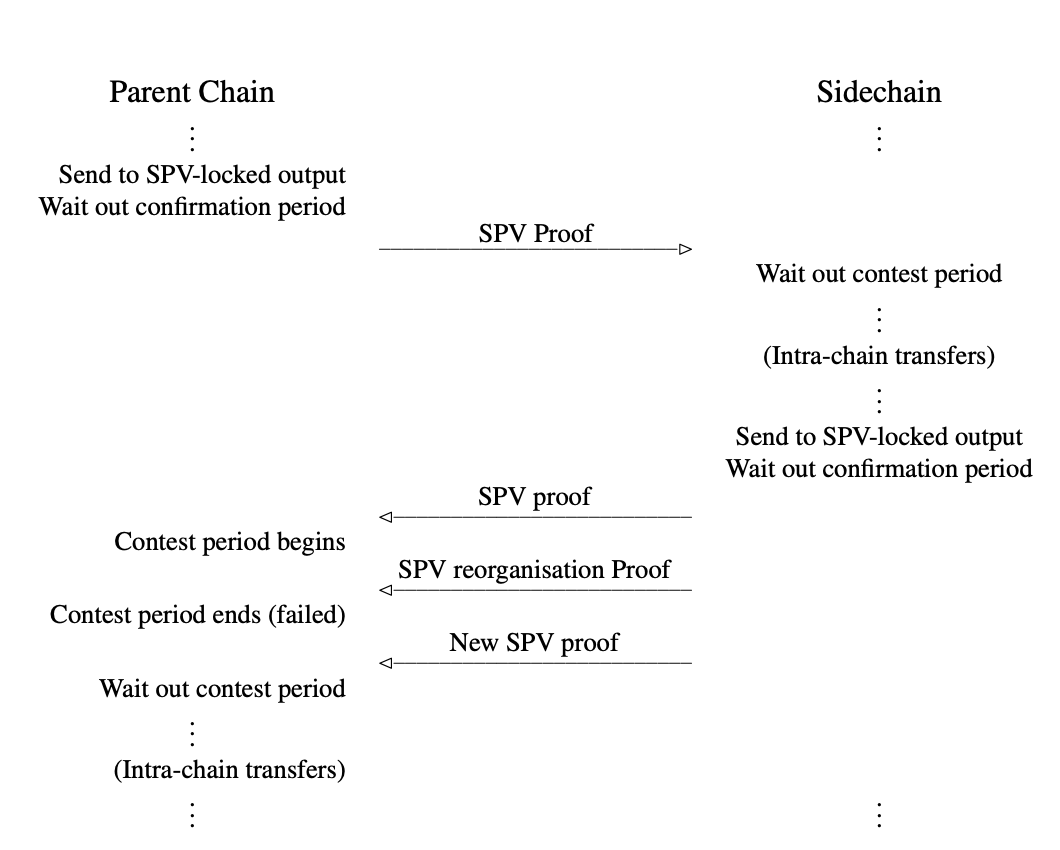
A partir de esta publicación comienza una revolución en el ámbito de las criptomonedas y la tecnología blockchain, llevando a que se diera la aparición de varios protocolos y arquitecturas aplicando esta estructura de datos. El rápido desarrollo de este modelo y el hecho de que no hubiera un estándar 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; los Blockchain bridges actúan como pasarelas entre diferentes bloques; y las soluciones basadas en contratos inteligentes utilizan contratos inteligentes para crear protocolos interoperables entre las diferentes cadenas de 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.

# 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>

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