Imagine standing at the edge of a vast canyon, your destination visible but unreachable due to the expanse separating you from it. In blockchains, these canyons represent the lack of interoperability between different blockchain networks.

Each blockchain operates in isolation, with its own set of rules, protocols, and assets. However, just as bridges span physical chasms, blockchain bridges offer a solution to connect these worlds, enabling a seamless flow of information and value.

In this guide you'll learn everything you need to know about multi-chain blockchain bridges

, and how they work.

What is a multichain blockchain bridge?

At their core, multichain or cross-chain blockchain bridges facilitate the transfer of assets and data across different blockchain platforms.

They act as facilitators for interoperability, allowing blockchains to communicate and interact more efficiently.

By allowing digital assets and information to traverse from one blockchain to another, bridges extend the utility and accessibility of decentralized applications (dApps) and assets beyond the confines of a single network.

How do cross-chain blockchain bridges work?

Blockchains are isolated by design, so there is no way they interact with the natural world or other blockchains. So, how can a bridge transfer data and assets from one blockchain to another?

Blockchain bridges employ various mechanisms to achieve interoperability

. One common approach involves locking assets on one blockchain and minting equivalent assets on another.

This process often managed through smart contracts, ensures that the original assets are securely held while their counterparts circulate within another ecosystem.

How blockchain bridges work: step-by-step

To understand how a blockchain bridge actually works, let’s see an example in which we are going to explore the process step by step.

Initial Setup:

- Blockchain "A"

: The original blockchain where the assets currently reside.

- Blockchain "B"

: The target blockchain to which you want to transfer your assets.

- Assets

: These are the tokens or cryptocurrencies you wish to move to Blockchain "B."

- Smart Contract on Blockchain "A"

: A pre-deployed contract that initiates the bridge process.

- Smart Contract on Blockchain "B"

: A counterpart contract that receives signals from Blockchain "A" to mint equivalent assets.

Step 1: Initiating the Transfer between blockchains

- User Action

: As the asset holder on Blockchain "A," you decide to transfer your assets to Blockchain "B." You interact with the bridge's interface (or dApp), specifying the number of assets you wish to transfer and the destination address on Blockchain "B."

- Send the assets to Smart contract on Blockchain "A"

: This will send the assets you want to transfer on blockchain in “A,” using a function like transferFrom, to the smart contract deployed on Blockchain "A."

Step 2: Locking Assets on Blockchain "A"

- Execute Function "X" on Blockchain "A":

The Smart contract executes a function, let’s call it lockAssets, on the smart contract deployed on Blockchain "A".

- Locking Mechanism

: Upon executing the lockAssets function, the smart contract securely locks the specified amount of your assets. This means the contract now holds the assets and is temporarily removed from circulation on Blockchain "A," ensuring they cannot be spent elsewhere.

Step 3: Verifying and Signaling through the Blockchain bridge

- Verification and Signal

: The smart contract on Blockchain "A" then records the transaction details and sends a signal (or a cryptographic proof) to the smart contract on Blockchain "B." This signal acts as a verified notification that assets have been locked on Blockchain "A" and are ready to be minted on Blockchain "B."

Step 4: Minting Assets on Blockchain "B"

- Minting Function on Blockchain "B"

: The smart contract on Blockchain "B," upon receiving the signal from Blockchain "A," executes its own function. Let's call it mintAssets. This function mints an equivalent amount of the assets or a wrapped version of them on Blockchain "B," which is initially allocated to the destination address you specified.

- Completion

: The minted assets on Blockchain "B" are now under your control, ready to be used or traded within the ecosystem of Blockchain "B."

Categories of Blockchain multichain bridges

One crucial question is, who manages the signal from Blockchain “A” to know that new tokens must be minted on token “B”?

This largely depends on the type of blockchain crosschain bridge we are interacting with and thus creates a wide spectrum of crosschain bridges with the following categorization:

Trusted Blockchain Bridges

:

Rely on a centralized authority to manage the transfer of assets. While they offer ease of use and quick transactions, they pose risks associated with centralization.[

Binance Bridge](https://www.bnbchain.org/en/bnb-chain-bridges) is an example of a trusted bridge that allows users to

convert their assets between blockchains supported by the Binance ecosystem. Users send their cryptocurrency to a specified address managed by Binance, which then credits the equivalent asset on the target blockchain to the user's account, either on the Binance platform or directly to a specified wallet address.

Trustless Blockchain Bridges

:

Operate decentralized using smart contracts, removing the need for a central authority and offering a more secure and transparent solution.

Wrapped Bitcoin (WBTC) is an example of a trustless bridge mechanism that brings Bitcoin's liquidity to Ethereum's ecosystem. It operates through a decentralized autonomous organization (DAO) comprising several DeFi projects without a single central authority overseeing the process.

Federated multichain Bridges

Utilize a consortium of validators from both chains involved in the transfer process. They offer a balance between centralized and decentralized models.

The Liquid Network is a sidechain-based federated bridge; users lock their bitcoins into a multi-sig contract on the Bitcoin blockchain, and the equivalent amount of Liquid Bitcoin (LBTC) is minted on the Liquid sidechain. The federation of members validates transactions on the Liquid Network, providing a balance between centralization and decentralization.

Liquidity crosschain Bridges

Enable asset transfers using liquidity pools, facilitating instant swaps without locking and minting.

Synapse Protocol offers a liquidity bridge that facilitates cross-chain asset swaps using liquidity pools. Users deposit assets into a liquidity pool on one blockchain and withdraw an equivalent value of another asset from a pool on the target blockchain. The process relies on the liquidity available in the pools, enabling instant swaps.

Sidechain Blockchain Bridges

Connect a main blockchain with a sidechain, allowing for scalable and efficient transactions while maintaining security tethered to the main chain.

Polygon (previously Matic Network) provides a sidechain bridge that connects Ethereum to the Polygon sidechain. Users can lock their Ethereum assets in a smart contract, and the Polygon Bridge then facilitates the transfer of these assets to the Polygon network. A corresponding amount of assets is minted on Polygon, which users can use within the Polygon ecosystem. The process is secured by validators who oversee the bridge's operations.

Each type of bridge works with a third-party entity. This could be an oracle (centralized/or decentralized) or external validator for the bridging process.

These third parties then are responsible for listening to any event triggered on Smart Contract “A” and performing the subsequent minting of Smart Contract “B assets.” The way they perform this process is decided individually by each bridge, which involves a wide range of consensus mechanisms, validations, signatures, and additional rules.

The person bridging the assets must decide whether one bridge is better based on trust, reliability, and fees the bridge presents. Considering that none of the mentioned categories are free of potential security risks and vulnerabilities.

Navigating the risks of crosschain bridges

Blockchain bridges are not bulletproof, independent of whether a decentralized oracle or a centralized authority manages it. The complexity of bridging different blockchains together inevitably introduces risks, including smart contract vulnerabilities and the potential for security breaches.

The infamous bridge hacks of recent years highlight the importance of rigorous security measures and continuous

innovation in bridge technologies to safeguard against such vulnerabilities.

Here is a list of security considerations both users and bridges should take when selecting a solution:

1. Audit status

: This is obvious, but we cannot stop recommending that you verify if the bridge you want to use was properly audited in different scopes, both private and competitive audits.

1. Locking mechanism

: Technically, the user is sending the ownership of the tokens to the bridge contract, and bridges, most of the time, handle millions of dollars. They are one of the favorite targets for malicious actors. So, you must be sure the lock mechanism (the contract locking the assets on the base chain) is as solid as a rock.

1. Trusted or centralized bridges:

Here, asset transfers are overseen by a single entity or a consortium, which poses significant security and trust concerns. Centralization introduces a single point of failure, making the bridge susceptible to internal fraud, mismanagement, or external attacks targeting the central authority.

1. Federated bridges:

They rely on validators to approve transactions and secure the bridge. If a significant proportion of these validators are compromised or act maliciously, they could approve fraudulent transactions, leading to asset theft or loss. The security of federated bridges heavily depends on the trustworthiness and security practices of the validators.

1. Replay Attacks:

A valid data transmission is maliciously or fraudulently repeated or delayed in a replay attack. In the context of blockchain bridges, this could involve replaying transaction messages between chains to illicitly mint or unlock assets.

Blockchain Multichain Bridges for Innovation and Efficiency

The implications of blockchain bridges extend far beyond mere asset transfers. They are instrumental in enabling dApps to leverage the strengths of multiple blockchain platforms.

For instance, a dApp could utilize Ethereum's robust smart contract capabilities while taking advantage of the low transaction fees on another chain like Binance Smart Chain. This enhances the app's functionality and improves user experience by offering the best of multiple worlds.

Moreover, bridges can significantly lower transaction costs and speed by navigating assets through more efficient routes. This is particularly beneficial when transaction fees vary widely across networks.

Conclusion

Blockchain bridges represent a key technological advancement in the quest for blockchain interoperability. By enabling the free flow of assets and information across different networks, bridges pave the way for a more integrated, efficient, and innovative blockchain ecosystem.

Suppose you want to become a top-tier, best-paid auditor in the industry. In that case, you must understand and apply techniques like this one daily, and the best Blockchain Developers out there must also nail these techniques to build more robust, secure, and reliable protocols.

Want to level up your smart contract security skills

? Take our 20+ hours smart contract auditing course on Cyfrin Updraft, completely free!