Blockchain Focus

Cross-chain Bridge Exploits: There Are More Risks Than You Know

Presto Research

June 3rd, 2024

Jaehyun Ha I Research Analyst
jaehyunha@prestolabs.io

Summary

- A cross-chain bridge is a technology that allows assets and data to be transferred between different blockchain networks, enabling interoperability among them. It usually works by locking assets on the source blockchain and minting equivalent tokens on the destination blockchain, or by using liquidity pools to facilitate immediate exchanges.
- However, because a cross-chain bridge comprises multiple components such as oracles and validators, it exposes several attack vectors to hackers. Numerous well-known bridge exploits through smart contract vulnerabilities (e.g., Wormhole, Qubit) and validator takeovers (e.g., Ronin) illustrate this risk.
- Even if there are no vulnerabilities in the bridge protocol, users can still have their funds stolen through Border Gateway Protocol (BGP) hijacking (i.e., exploiting the underlying network layer) if the bridge service's network provider lacks proper authority over the IP address ranges.

Figure 1: Cross-chain bridge has multiple point of failures Source: DALL•E, Presto Research

Introduction

Cross-chain bridge exploits are widely recognized as major risks in DeFi ecosystems. High-profile incidents in recent years, such as the Wormhole, Qubit, and Ronin exploits, each resulting in losses of hundreds of millions of dollars, have underscored the vulnerabilities of bridges. Smaller recent incidents such as the $4.3M compromise of Alex Lab in May 2024, add to the ongoing concerns. Such exploits occur very frequently, and account for more than half of all DeFi hacks. Why do these cross-chain bridge exploits persist?

In this article, we claim that it is inherently dangerous to use cross-chain bridges due to their multiple points of failure. Exploiting just one of these points can drain the funds locked in the bridge, presenting a significant risk. We will explore the different types of cross-chain bridges and discuss the various risks associated with them. While we will cover well-known risks such as smart contract vulnerabilities and private key compromises of validators, we will also highlight a less frequently discussed network layer attack, BGP hijacking, which, although unrelated to bridge implementation, can also result in stolen funds.

What is a Cross-chain Bridge?

A cross-chain bridge is a technology that facilitates the transfer of assets and data between different blockchain networks, enabling interoperability among them. As it stands, assets on-chain are not usable across different blockchains (i.e., “USDT” on Solana is not the same “USDT” on Ethereum). This functionality allows users to leverage the unique features and benefits of multiple blockchains without being confined to a single one. For instance, a user can transfer their Ethereum-based assets to the Solana blockchain to take advantage of Solana's higher transaction speeds and lower fees. Cross-chain bridges achieve this by depositing the original assets on the source blockchain and issuing the equivalent tokens on the destination blockchain, ensuring that the total supply of assets remains constant across chains.

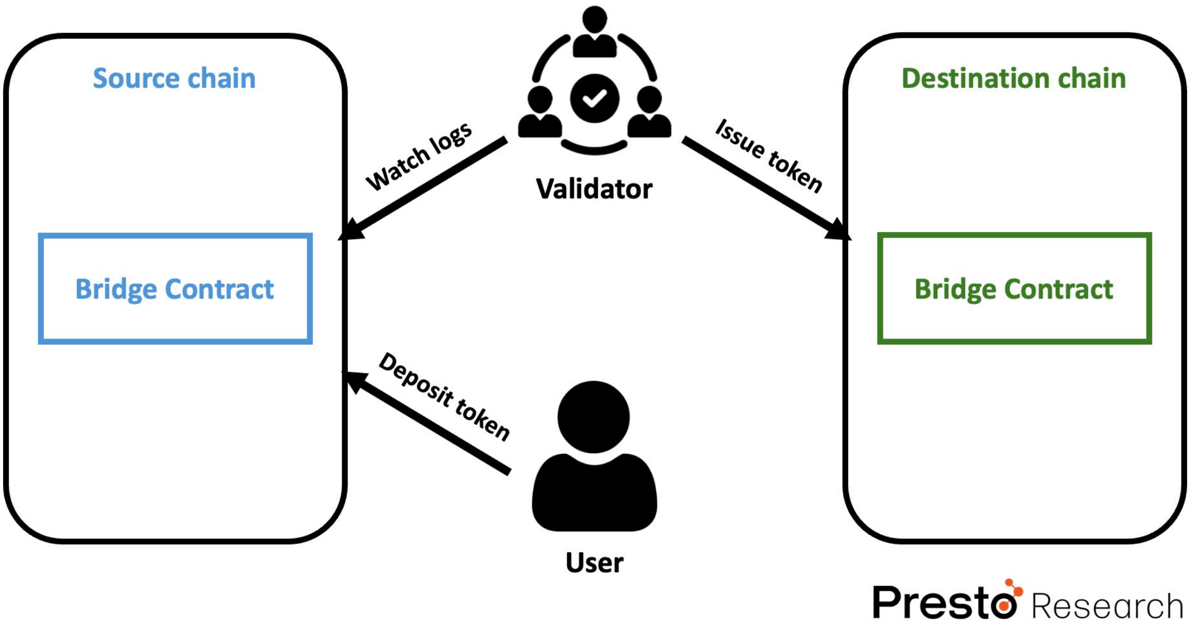
One prominent cross-chain bridge service is Wormhole, which connects various blockchains like Ethereum, Solana, and Binance Smart Chain, allowing seamless asset transfers among them. Another example is the Ronin Bridge, which was developed to facilitate transactions between the Ethereum blockchain and the Ronin sidechain, primarily used for the popular game Axie Infinity. Additionally, the Avalanche Bridge enables users to transfer assets between Ethereum and Avalanche, supporting the latter's rapidly growing DeFi ecosystem. These services play a crucial role in enhancing the functionality and interoperability of blockchain networks, driving innovation and user adoption in the DeFi space.

What Types of Cross-chain Bridges Exist?

There are various criteria for classifying the cross-chain bridges. They can be categorized based on the method of asset transfer, security features, or the way transactions are validated. Among these, here we introduce the two most widely used methods for asset transfers, which is lock-and-mint method and the liquidity pool method.

Figure 2: Cross-chain bridge explained

Source: Presto Research



Lock-and-Mint

The lock-and-mint cross-chain bridge works (Figure 2) by locking assets on the source chain and minting equivalent tokens on the destination chain. When a user initiates a transfer, their assets are locked in a smart contract on the source chain. This lock action is verified by the bridge's validators or guardians, who then authorize the minting of corresponding wrapped or pegged version of the tokens on the target chain. For instance, if you lock 10 ETH on Ethereum, the bridge mints 10 wrapped ETH (wETH) on another chain like Solana. The original assets remain locked until the user decides to reverse the process, where the wrapped tokens are burned on the destination chain, and the original assets are unlocked and returned on the source chain. This method ensures a 1:1 backing of the wrapped tokens, maintaining their value parity with the original assets.

Liquidity Pool

The liquidity pool type of cross-chain bridge operates differently by relying on pools of assets provided by liquidity providers on both the source and destination blockchains. When a user wants to transfer assets from one blockchain to another, they deposit their assets into a liquidity pool on the source chain. Instead of minting new tokens, the bridge uses the liquidity pool on the destination chain to fulfill the equivalent amount of assets to the user. This method allows for immediate transfers without the need to lock and mint tokens, relying instead on the liquidity available in the pools to facilitate the exchange.

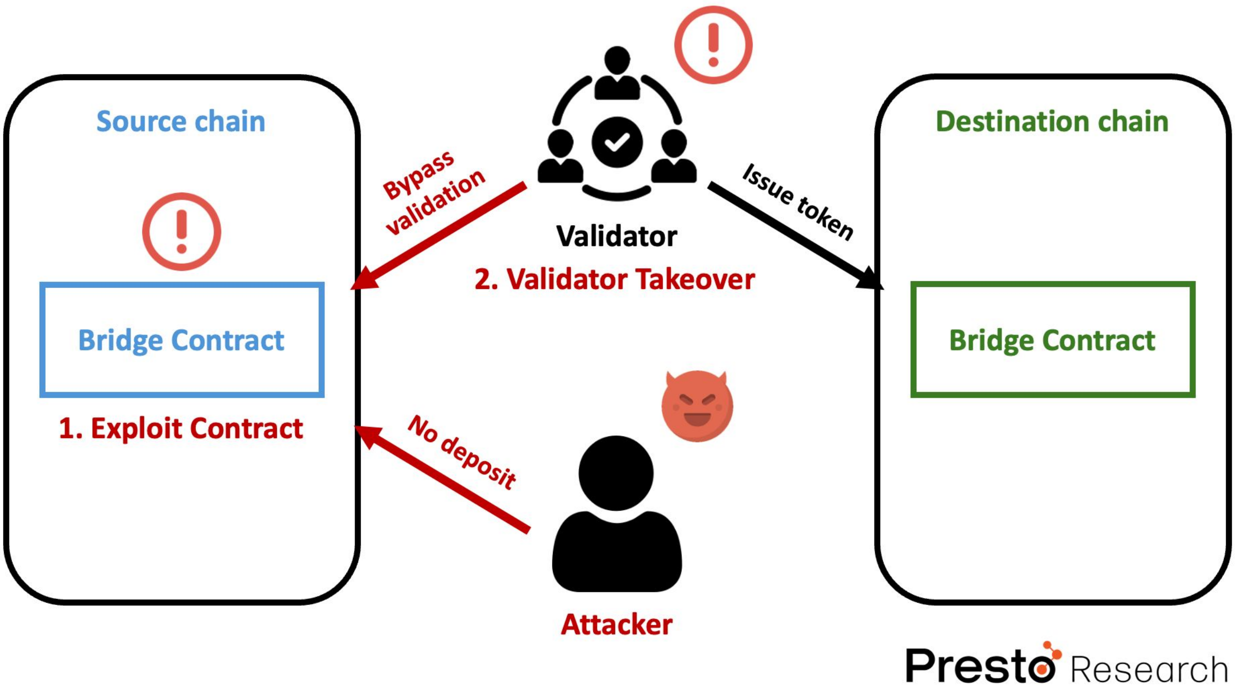
What Are the Risks of Cross-chain Bridges?

Bridge Exploits: Your Assets are no Longer Backed Up

The biggest risk for cross-chain bridges, of course, is being exploited by hackers for various reasons such as smart contract vulnerabilities or the private key compromise of validators. These exploits due to hacking can occur in any type of bridge, but are especially frequent in lock-and-mint bridges.

Figure 3: Bridge exploits explained

Source: Presto Research



While the specifics of each attack may vary, they generally follow the same pattern: issuing tokens on the destination chain and withdrawing them without making a legitimate deposit on the source chain.

False Deposit: Exploiting Bridge Contracts

The first type of attack is the **false deposit**. In this case, the attacker exploits a logical flaw in the bridge contract to trigger the issuance of tokens on the destination chain without actually depositing valid tokens. A representative example is Qubit Finance’s Ethereum-BSC bridge exploit that occurred in January 2022. At that time, Qubit’s bridge contract was using custom code instead of OpenZeppelin’s SafeERC20 library, which is the recommended standards for secure bridge transfers. The attacker discovered that by inputting the null address (0x000…0000) as the token contract address in the deposit() function of this custom code, they could bypass all the validation process and mint tokens on the destination chain without depositing any valid tokens on the source chain.

Consequently, the attacker minted approximately $185M worth of qXETH on the BSC chain (with depositing 0 ETH) and exchanged it for other cryptocurrencies, resulting in a total loss amounting to around $80M.

Taking Over Validators: Exploiting the Centralized Validation Process

Another type is **taking over the validators**. As of May 2024, most cross-chain bridges still validate cross-chain transactions through external validators and federations. In this case, the attacker can compromise the majority of the small-size validator committee by stealing their private keys. A prominent example is the Ronin bridge exploit that occurred in March 2022. At that time, Ronin, the gaming-optimized chain, was using a Proof-of-Authority (PoA) consensus model that sacrificed some decentralization and security in favor of speedy transaction processing and reduced transaction fees for users. This meant that the security of the entire Ronin network relied on nine validators. If an attacker could compromise the private keys of a majority, specifically five out of the nine validators, they could validate any malicious transactions. An attacker exploited this vulnerability by creating and approving a transaction that transferred 173,600 ETH and 25.5M USDC to their own address, despite not holding any wETH on the Ronin chain. This resulted in approximately $625M in losses with just two transactions.

Stay In Your Chain

These major incidents related to cross-chain bridge exploits are well-known, and readers might think, "Sure, if a bridge gets hacked, the funds locked in it will obviously be stolen. What is your point?" The critical point to recognize is that assets deposited into a cross-chain bridge are no longer protected by the robust self-regulating consensus mechanisms of each blockchain or high Total Value Locked (TVL).

Even if the Ethereum or Solana network were to suffer a 51% attack, your funds would not be stolen. A 51% attacker can only revert the blockchain or censor specific transactions; they cannot steal your assets by compromising your private key.

Even if they were to revert all transactions that sent assets to you, your assets would remain safe. Honest nodes would not follow the malicious chain, and in the event of a significant revert, the community would likely intervene, potentially forking the chain as seen with Ethereum Classic. Moreover, in a Gasper-based PoS chain, reverting finalized blocks is nearly impossible.

However, the situation is different if your assets are locked in a cross-chain bridge. The security of your assets depends solely on the bridge contract and the external validator committee. If a bridge exploit occurs, your assets can be immediately stolen. For instance, if you lock 100 ETH on the Ethereum side of an Ethereum-Solana bridge and mint 100 wETH on the Solana side, the value of 100 wETH is backed by the guarantee that you can convert it back to 100 ETH through the bridge. But if an exploit causes the 100 ETH locked on the Ethereum side to be stolen (i.e., sent to the attacker's address), the 100 wETH on Solana becomes worthless as it is no longer backed by anything. Since those asset withdrawal transactions by attackers are regarded as legitimate transactions on both blockchain networks, there is no way to revert them.

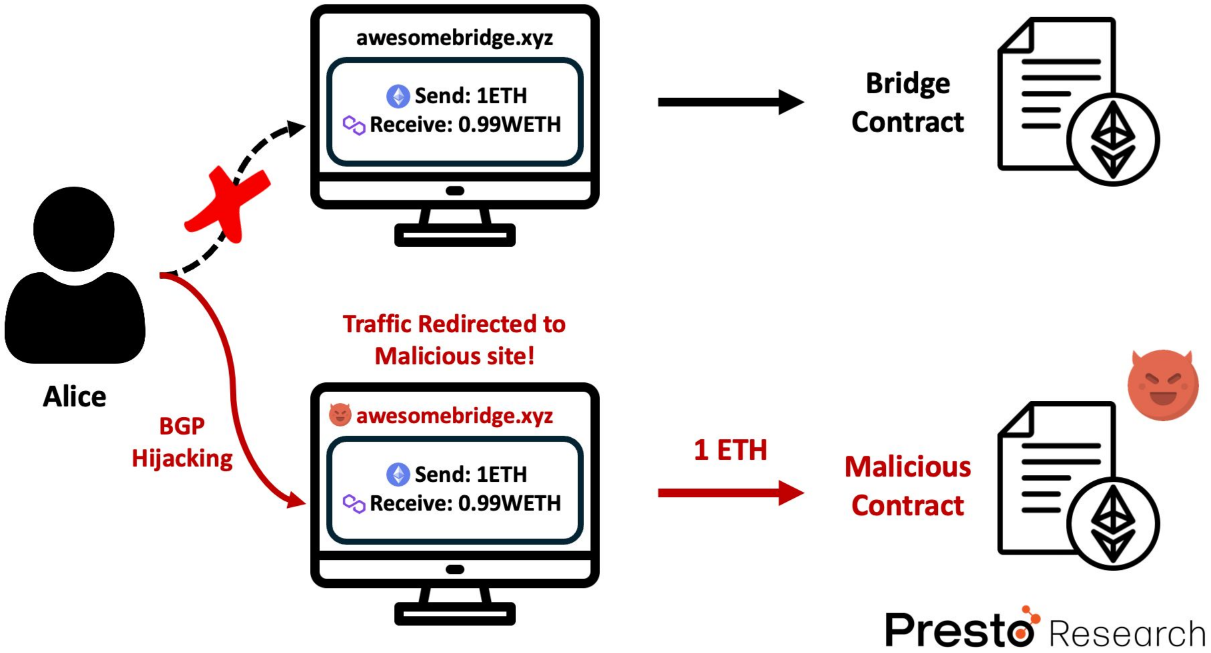
The same goes for Total Value Locked (TVL); generally, a higher TVL in a blockchain is considered indicative of stronger security assurances. However, an increase in TVL in a cross-chain bridge does not enhance its security; it merely makes it a more attractive target for hackers.

BGP Hijacking: Network Security is Often Neglected

In the bridge exploits described above, the responsibility often lies with the bridge services due to factors such as smart contract bugs, poor private key management, or vulnerable cross-chain protocols. However, even when these issues are thoroughly addressed, funds can still be stolen through **BGP (Border Gateway Protocol) hijacking.**

Figure 4: BGP hijacking attack against bridges

Source: Presto Research



BGP hijacking attacks on bridges differ significantly from the previously discussed types of attacks. This method does not exploit vulnerabilities within the bridge implementation itself and does not drain assets already locked in the contract or held in the liquidity pool managed by the bridge. Instead, BGP hijacking targets the routing protocol at the network layer underlying the bridge service (i.e., the application layer). When a user attempts to deposit assets via the bridge's landing page (front-end), the attacker redirects this traffic to a phishing site that looks identical to the legitimate one. Consequently, the assets are sent to a malicious smart contract controlled by the attacker instead of the bridge's genuine smart contract, resulting in the theft of funds intended for transfer.

For those who are not familiar with computer networks, the term “BGP” might not be well known. Simply put, BGP is like the **GPS navigation system** for the internet, guiding data packets across different networks to their destination. Using BGP messages, each network can advertise the IP address ranges they can reach (e.g., "I own 76.76.0.0/16, and this is how to reach me") to adjacent networks. These neighbouring networks then propagate this information to their neighbours, collectively forming a comprehensive routing map of the internet. This map helps each router find the most efficient route for sending data.

To prevent malicious attackers from impersonating a network that holds a specific IP address range, some hosting services or infrastructure maintainers adopt security measures like RPKI (Resource Public Key Infrastructure) or IRR (Internet Routing Registry). While we won’t delve into the details of how each security measure works, suffice it to say that they provide certified authority to networks for announcing a specific IP address range. However, the problem is that not all internet providers for bridge services have fully implemented these security measures. Some providers lack authority over the IP ranges hosting the bridge service, allowing attackers to obtain authority over those IP ranges. This vulnerability allows for BGP hijacking, which involves tricking the internet's "GPS navigation" system. Consequently, attackers can falsely announce that they own the IP ranges of those bridge services and redirect traffic intended for the legitimate bridge service to their own malicious addresses.

The BGP hijacking attack targeting KLAYswap in February 2022 resulted in approximately $1.9 million in losses, while a similar attack against Celer cBridge in August 2022 caused around $235,000 in damages. These incidents highlight the significant impact of BGP hijacking, demonstrating the need for not only auditing bridge protocols but also preparing defenses against network-level attacks.

Conclusion

In this article, we have examined the widely known risks of cross-chain bridges, such as contract vulnerabilities and validator takeovers, as well as the relatively less known risk of BGP hijacking. While cross-chain bridges are a convenient technology that allows blockchain assets to be used quickly and easily across multiple chains, their multi-component composition creates multiple points of failure, necessitating careful attention when using them. Thus, users who wish to use bridges safely must meticulously check that the security measure of the bridges' on-chain smart contracts, protocol implementations and underlying network layer security are properly in place. If this seems too cumbersome, using the native tokens of a blockchain network solely within that chain is a prudent move to reduce the risk of losing assets.

About Presto

Presto is a Singapore-based algorithmic trading and financial services firm founded in 2014. Presto focuses on delivering exceptional value for clients through rigorous research-driven approach to investment and trade execution. With more than a 100 million trade executions in a day, Presto is a leading financial services firm in both digital assets and traditional finance markets.

Find out more at https://www.prestolabs.io.
Follow Presto for more content: X, LinkedIn

Authors

Jaehyun Ha, Research Analyst : X, LinkedIn

Required Disclosures

Any expression of opinion (which may be subject to change without notice) is personal to the author and the author makes no guarantee of any sort regarding accuracy or completeness of any information or analysis supplied. The views and opinions expressed herein are those of the author(s) and do not necessarily reflect the views of Presto Labs or its affiliates. This material by itself, is not and should not be construed as an offer or a solicitation to deal in any investment product or to enter into any legal relations. This material is for informational purposes only and is only intended for sophisticated investors, and is not intended to provide accounting, legal, or tax advice, or investment recommendations, or an official statement of Presto Labs or its affiliates. Presto Labs, its affiliates and its employees make no representation and assume no liability to the accuracy or completeness of the information provided. Presto Labs, its affiliates and its employees also do not warrant that such information and publications are accurate, up to date or applicable to the circumstances of any particular case. Certain statements in this document provide predictions and there is no guarantee that such predictions are currently accurate or will ultimately be realized. Prior results that are presented here are not guaranteed and prior results do not guarantee future performance. Recipients should consult their advisors before making any investment decision. Presto Labs or its affiliates may have financial interests in, or relationships with, some of the assets, entities and/or publications discussed or otherwise referenced in the materials. Certain links that may be provided in the materials are provided for convenience and do not imply Presto Labs' endorsement, or approval of any third-party websites or their content. Any use, review, retransmission, distribution, or reproduction of these materials, in whole or in part, is strictly prohibited in any form without the express written approval of Presto Labs. Presto Research and related logos are trademarks of Presto Labs, or its affiliates.