

TRACING FUNDS ACROSS CHAINS: THE USE OF BRIDGES AND THE FINANCIAL CRIME PERSPECTIVE

1. Blockchain Bridges: Definition and Operating Mechanism

With the development of the crypto asset ecosystem, numerous blockchain networks with different technical infrastructures and protocols have emerged. However, due to their underlying structures, these networks cannot communicate directly with each other, and assets held on one blockchain cannot be natively used on another blockchain. Blockchain bridges are protocols that establish connections between different blockchain networks, enabling the transfer of crypto assets and data across chains. Through these bridges, users can access different blockchain ecosystems without having to convert their assets through a centralized exchange. Although the operating mechanism of bridges varies depending on the model used, one common method involves locking an asset on the source chain and creating an equivalent token representing that asset on the destination chain (*lock & mint*). When the transaction is reversed, the token created on the destination chain is burned, and the original asset locked on the source chain is released (*unlock*).



2. Blockchain Bridge Models and Key Platforms

Blockchain bridges can be categorized into different models based on their operating mechanisms and trust structures. The most fundamental distinction is between custodial and non-custodial bridges. In custodial bridges, users rely on a centralized operator to securely manage assets during the transfer process, whereas in non-custodial bridges, the process is primarily executed through smart contracts and protocol rules. In addition, while certain bridges operate based on a model where assets are locked on the source chain and corresponding “wrapped” tokens representing those assets are created on the destination chain, others utilize mechanisms such as burn & mint, liquidity pools, or intent-based models. Each of these models presents different advantages and risks in terms of speed, cost, user experience, liquidity, and security.

Among the prominent platforms, Wormhole is positioned as a multi-chain infrastructure that enables the transfer of tokens, data, and applications across different blockchain networks. Polygon Portal is one of the official bridge interfaces that facilitates asset transfers between Ethereum and the Polygon PoS network. Avalanche Bridge provides bridging infrastructure for transferring assets from Bitcoin and Ethereum to the Avalanche network. Unlike traditional bridging models, THORChain operates as a cross-chain liquidity protocol that enables the decentralized exchange of native assets across different blockchains.



3. The Role of Blockchain Bridges from a Financial Crime Perspective

Although blockchain bridges serve as important infrastructures that enable asset transfers across different networks and enhance interoperability within the crypto ecosystem, their ability to facilitate cross-chain movement has also made them a critical area of analysis in financial crime investigations. Traditional blockchain analysis generally examines fund flows by tracing transaction histories within a specific network; however, the use of bridges allows crypto assets to be transferred across different blockchain networks, requiring fund movements to be analyzed across multiple chains. Therefore, bridge transactions play an important role in investigations involving the tracing of crypto asset movements, particularly in cases related to cyberattacks, fraud, and money laundering activities.

Criminal actors may leverage cross-chain transfers in money laundering processes aimed at concealing the source, movement, or ultimate destination of crypto assets obtained through illicit activities. In this context, multi-stage transaction patterns may involve transferring funds across different blockchain networks (*chain hopping*), converting them into different crypto assets, and using bridge transactions in combination with decentralized exchanges, mixing services (*mixers*), or other methods. Since these techniques require establishing connections between different networks, they may increase the complexity of blockchain analysis processes.

4. Notable Cases in Crypto Asset Investigations

One of the notable examples of the use of cross-chain bridges in money laundering processes is RenBridge. According to an analysis published by Elliptic, since 2020, RenBridge has been used to transfer at least USD 540 million worth of crypto assets originating from various criminal activities, including theft, fraud, and ransomware, across different blockchains. For example, in August 2021, following the attack against the Japanese crypto asset platform Liquid, which was linked to North Korean actors, USD 33.8 million out of approximately USD 97 million worth of stolen assets was transferred through RenBridge. Similarly, following the Nomad Bridge attack in August 2022, it was identified that approximately USD 2.4 million worth of stolen assets were transferred across different chains through RenBridge within a short period of time. In these incidents, RenBridge was not the target of the attacks; rather, it emerged as one of the cross-chain infrastructures used to move the obtained assets across different blockchain networks.

In February 2025, Bybit, one of the world's largest crypto asset platforms, was targeted in a cyberattack resulting in the theft of approximately USD 1.5 billion worth of Ethereum-based crypto assets. According to an analysis conducted by TRM Labs, following the attack attributed to North Korean-linked actors, numerous intermediary wallets, decentralized exchanges (*DEXs*), and cross-chain bridges were used in the process of moving the stolen funds. It was identified that the attackers attempted to complicate the flow of funds by converting the assets into different cryptocurrencies and transferring them across different blockchain networks. In this incident, cross-chain bridges were used as part of a multi-stage fund movement process involving the rapid transfer of stolen assets across different networks and the laundering of criminal proceeds.

