Canonical Asset Maximalism

Canonical assets are the only secure way to represent value across chains. Intent bridges like Across Bridge enable interoperability with canonical assets at faster speeds and lower fees than 3rd party messaging bridges without the security tradeoffs.

Understanding Canonical Assets

Canonical assets refer to the original or "native" form of a token on its home blockchain. In the context of interoperability, tokens can either be "canonical" or "representative." The distinction generally comes down to the trust assumptions in securing assets on secondary chains.

How Assets Move between Chains

Regardless of chain, interoperability protocol or technology, there is only a singular way to "move" a token from its native chain to a secondary chain (and it's not really moving at all): 1. 1. 2. locking (or burning) the token on its native chain (the origin) 3. 2. 4. sending a message from the origin chain to the destination chain after the locking (or burning) is complete 5. 3. 6. minting a new token on the destination chain The critical component in the above flow is step #2, and specifically the verification process ensuring the message is not faulty. The verification method used is precisely what distinguishes "canonical" vs. "representative" assets. At the highest level there are two verification methods: 1. 1. 2. Via the canonical bridge: 3. Canonical bridge contracts, which already underpin the security of the chain, connecting the chain to mainnet Ethereum in the most trust minimized way, is responsible for verifying messages to mint tokens. These are considered "canonical" tokens given they do not increase trust assumptions vs. simply using the chain. 4. 2. 5. Via a 3rd party message bridge: 6. A 3rd party bridge, which can have any number of trust models, is responsible for verifying messages to mint tokens. These are considered "representative" tokens given they 7. do 8. increase trust assumptions, as users now have to trust a 3rd party to never allow a faulty message (and if they do, it could result in an infinite mint and unbacked token on the secondary chain).

Canonical Asset Maximalism

In a trust minimized world, only canonical bridges, and only canonical assets would be used. But the current speed of canonical bridges (1 hour to 7 days) makes them an untenable solution for many applications. 3rd party message bridges can be much faster, but they come with security tradeoffs inherent in minting representative assets. Across' intent-based bridge introduces a new architecture in interoperability that doesn't suffer from the security hurdles of 3rd party message bridges, and is empirically faster and cheaper than canonical bridges. Across achieves this by inserting a 3rd party relayer to quickly fulfill users' bridging requests using their own inventory of canonical assets, and a settlement layer that sits on top of canonical bridges to slowly verify and repay relayers. In other words, Across' intent-bridge decouples the urgent need of fast-filling users from the eventual need of verification. Users and developers don't need to make the trust vs. convenience trade-off in canonical vs. representative assets: intent systems like Across offer the best of both worlds. Diagrams inspired by the insightful work from the Connext Network team. Concepts -Previous Intent Lifecycle in Across Next- Integration Guides Across Bridge Integration Last modified19d ago On this page Understanding Canonical Assets How Assets Move between Chains Canonical Asset Maximalism