TL;DR

Usually in sharded or multi-chain architectures, a compromise of a single shard leads to a catastrophic event of the entire system.

In a world, where there are potentially millions of chains, a different approach is needed.

An architecture is described where a compromise of a single chain does not lead to a global compromise.

Description.

It is clear that the crypto world is becoming multi-chain and multi-project.

It is important that the compromise of a single chain or a single project does not lead to a global catastrophe.

Many sharded chains including earlier proposals for ETH2 had a property that a compromise of a single shard led to a global compromise.

If you compromised a single shard you could print an infinite amount of a particular token and move it to other shards.

When the number of shards/chains increases the complexity of a system grows and a compromise of a single chain becomes is almost inevitable.

Therefore, the system needs to survive if a particular chain or shard is compromised.

It turns out that the simplest way to do this is to follow the steps described below:

1. Each ERC or NFT token X

is assigned OwnerChain

1. Only OwnerChain can mint the token X

.

1. OwnerChain keeps track of token X

balances on any other chain.

1. Only token transfers between OwnerChain and other chains are allowed. Cross chain transfers are prohibited.

For example, if token X

needs to be transferred from chain Y

to chain Z

, it first goes from Y

to OwnerChain

and then from OwnerChain

to Z

.

This is done because OwnerChain

needs to update token balances for chains X

and Y

.

It is clear from described above, that compromise of, say, chain Y

does not lead to a global compromise of token X

. The damage is limited to the balance of X

on Y

.

Once the architecture described above is established, the blockchain world separates into three types of chains:

- DappChains : these are chains where dapps run. Each DappChain will typically own a single token
- DefiChains: these are chains where defi applications, such as DEXes run. Typically users will transfer tokens from DAppChains to DefiChains to exchange them for stablecoins such as USDC.
- finally, ConnectorChains can be used by external centralized entities to hold tokens. For instance, to exchange USDC into fiat you would transfer it to Binance ConnectorChain