Anyswap and the MPC Router Model

The MPC router model tried to avoid a single ordinary private key controlling bridge movements. Instead, an MPC node network used threshold-style signing so a route could be authorized when enough participants cooperated. In practice, TSS, or threshold signature, can make signing more distributed while still producing a normal-looking transaction on-chain.

That design does not remove key management risk; it changes where the risk sits. Operators, recovery procedures, software updates, signer membership, and emergency controls still matter. A revival entry at the Anyswap approach, which means its MPC or signer description should be treated as core infrastructure detail, not marketing background. The important question is who can move funds when conditions are normal and who can move them during stress.

The original Anyswap became Multichain in 2021. In 2023, the team said it lost access to MPC node keys after CEO Zhaojun's reported arrest, then a major drain and shutdown followed. That is the failure mode every router design must answer.