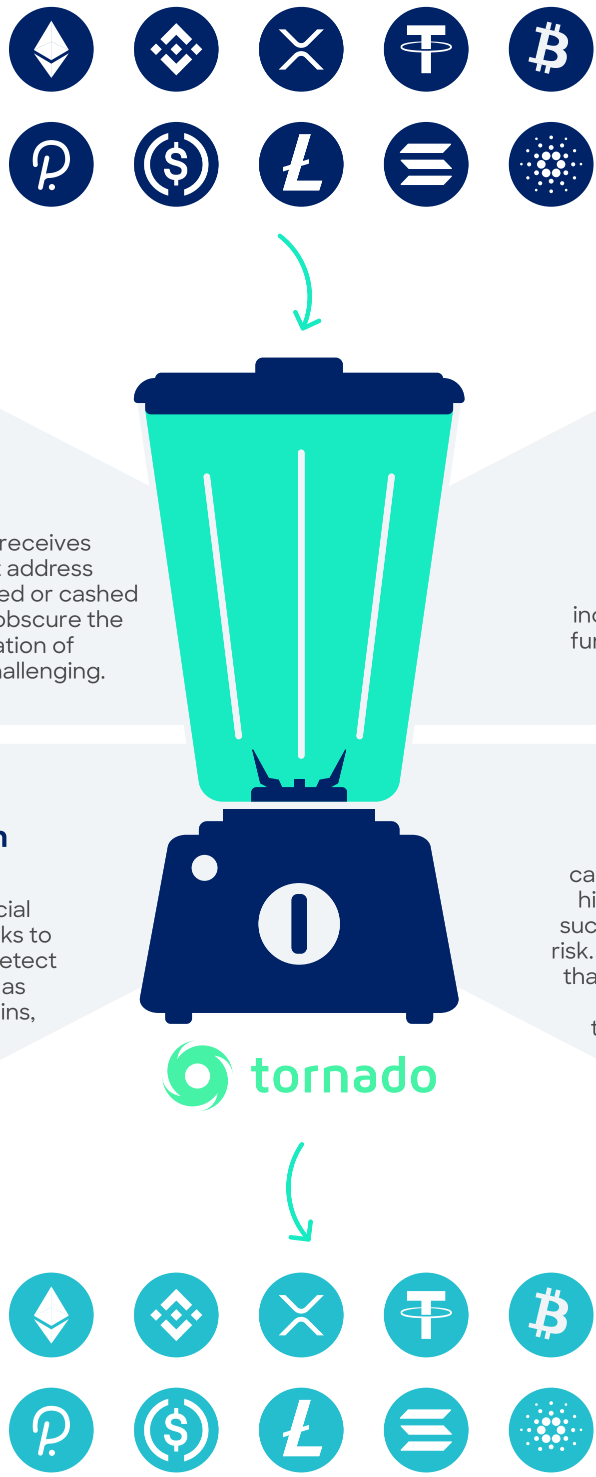
ACAMS

Tornado.Cash Sanctioned by the Office of Foreign Assets Control (OFAC)

Tornado.Cash has been sanctioned for laundering more than US$7 billion worth of virtual currency including over US$455 million stolen by the Lazarus Group, a North Korean hacking group. Tornado.Cash had previously announced its intention to use a blockchain tracing tool to track sanctioned wallets to comply with OFAC requirements.



1

The main purpose of a mixer is to protect user anonymity and privacy.

After the mixing process, the user receives tainted funds into a different wallet address from which funds can be transferred or cashed out. Decentralized mixer services obscure the link between the origin and destination of funds, making tracing proceeds challenging.

2

As traditional banks have strengthened cyber defenses, decentralized cryptoasset protocols have become a target for state actors

including North Korea to launder illicit funds in a similar way to cash through various bank accounts.

3

Cryptoasset exchanges must avoid process driven KYC at onboarding

to avoid missing clues as to beneficial ownership, source of funds, and links to high-risk jurisdictions. A failure to detect unusual transactional activity such as repeated use of mixers, privacy coins, or the use of opaque blockchains may prove attractive to criminals.

4

Flawed risk assessments

can also fail to take into consideration higher risk money laundering factors such as delivery channels and product risk. Financial institutions should ensure that sanctions evasion techniques are built into training programs to ensure suspicious activity can be identified and reported.