

Week 5 · Risk and security

The idea in one line

Most DeFi losses fall into four patterns. Learn the patterns, then check for them before you trust anything.

The four buckets

1. Unchecked accounts: a program trusts an account it never checked (Wormhole, Cashio).
2. Oracles and pricing: a price that can be pushed lets fake value borrow real money (Mango, Loopscale).
3. Keys, signers and operations: whoever holds the key holds the money (Slope, Drift).
4. Supply chain: the code you didn't write (@solana/web3.js, Dec 2024).

Key terms

Term	Meaning
Mint authority	Can create more of a token
Freeze authority	Can freeze holders' token accounts
Permanent delegate	Can move or burn anyone's balance
Durable nonce	Lets a signed transaction stay valid until used
Timelock	A delay before admin changes take effect
TVL	Value deposited in a protocol

Three things to remember

1. On Solana, "is this the real account?" is the core security question.
2. Drift (1 Apr 2026, ~\$285M reported) had no code bug. Signers were tricked.
3. TVL can rise because prices rose or rewards were paid, not because people use the protocol.

Do and don't

- Check mint and freeze authority before buying any token.
- Simulate and read every transaction before signing.
- Mark every loss figure "reported" and give its date.

This week's task

Write a post-mortem of one incident: what happened, which bucket, who lost money, what would have prevented it.

Audit one real token on Orb: authorities and extensions.

Blog: "The risks of DeFi: lessons from Solana's failures."

Deck: /week-5/