

5

Week 5 of 6

Risk & security

Task

Write a post-mortem of one incident, then audit one real token on Orb.

Blog post

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

Today

1

Patterns, not
stories

2

Four root
causes

3

Risk with no
attacker

4

How analysts
judge a
protocol



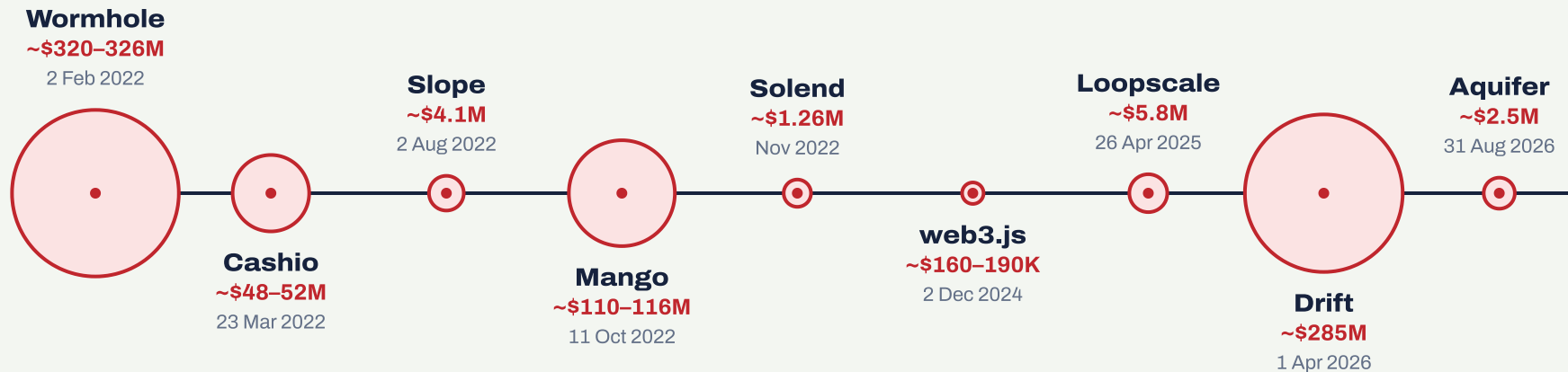
Post-mortem +
token audit



Patterns, not stories

Nine incidents. Four root causes.

Solana incidents, 2022 to 2026



Circle area tracks the reported loss. Figures from the course handbook, 11 Oct 2026.

Sort them by what went wrong

1. Unchecked accounts

Is this the real account?

Wormhole

\$320M+

Cashio

\$48M+

2. Oracle and pricing

Can someone push this price?

Mango

\$110M+

Solend

\$1.3M

Loopscale

\$5.8M

3. Keys, signers, ops

Who can sign, and what are they signing?

Slope

\$4.1M

Drift

\$285M

Aquifer

\$2.5M

4. Supply chain

Do I trust every package I install?

web3.js

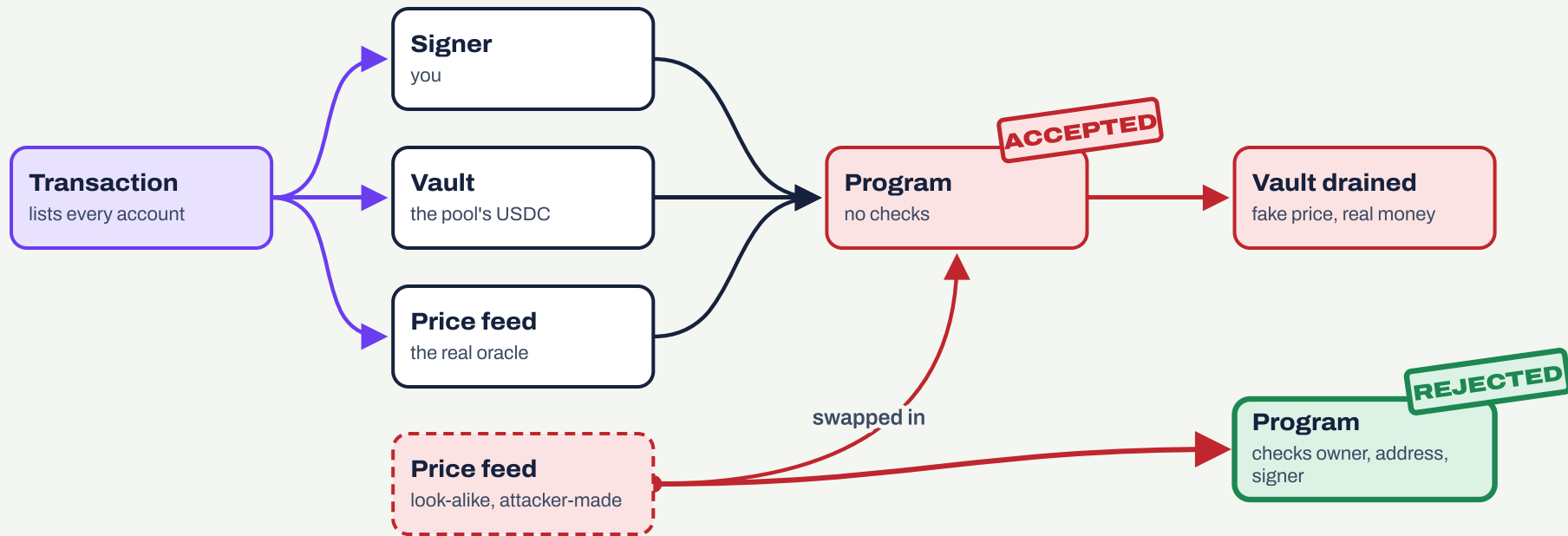
\$160K+

Biggest losses: two missing checks and one tricked council.

Bucket 1: unchecked accounts

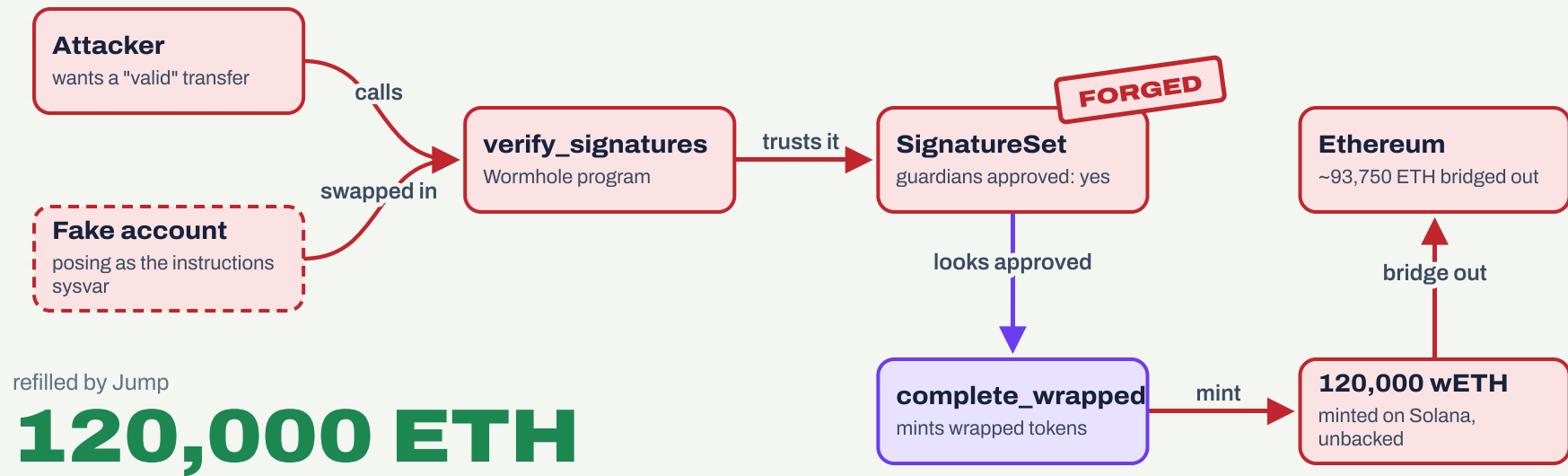
The bug that is special to Solana.

The caller hands you every account



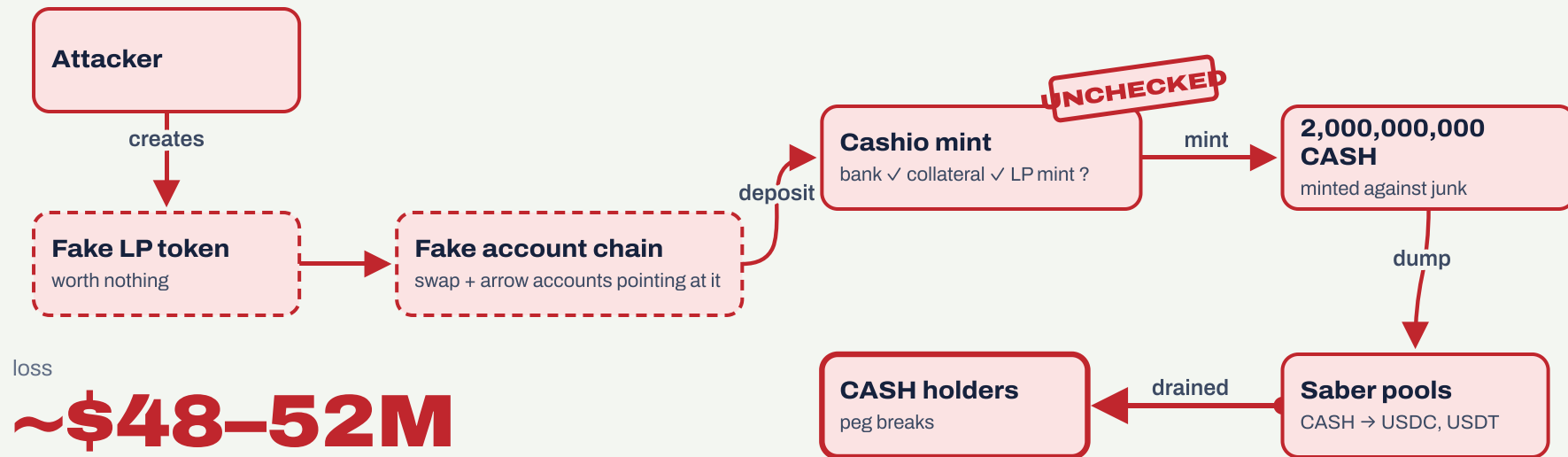
4/4 The fix: check owner, address and signer before reading a single byte.

Wormhole - 2 Feb 2022



6/6 Jump Crypto puts 120,000 ETH back. Users are made whole. The bug was one missing check.

Cashio · 23 Mar 2022



7/7 CASH loses its peg. Users absorb most of the ~\$48–52M loss.

Builders: the missing check, fixed

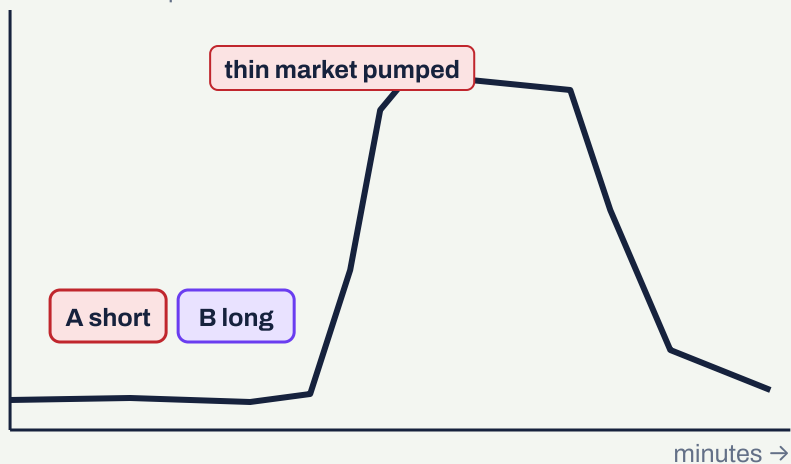
```
1 // Fix 2: the price feed must be the exact account, owned by the oracle program
2 #[derive(Accounts)]
3 pub struct Withdraw<'info> {
4     pub authority: Signer<'info>,
5     #[account(mut, has_one = authority)]
6     pub vault: Account<'info, Vault>,
7     /// CHECK: address and owner pinned below
8     #[account(address = SOL_USD_FEED, owner = ORACLE_PROGRAM_ID)]
9     pub price_feed: AccountInfo<'info>,
10 }
```

Bucket 2: oracles and pricing

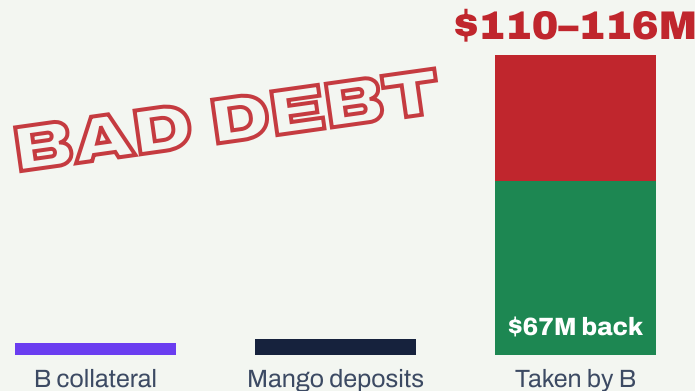
If a price can be pushed, collateral can be faked.

Mango Markets · 11 Oct 2022

MNGO oracle price



Mango, in dollars



7/7 A DAO vote lets \$67M come back as a "bounty". The attacker keeps the rest.

Is code law?

Oct 2022

Attacker says it was "a highly profitable trading strategy"

Apr 2024

Avraham Eisenberg convicted of fraud and manipulation

23 May 2025

Judge throws out all criminal convictions

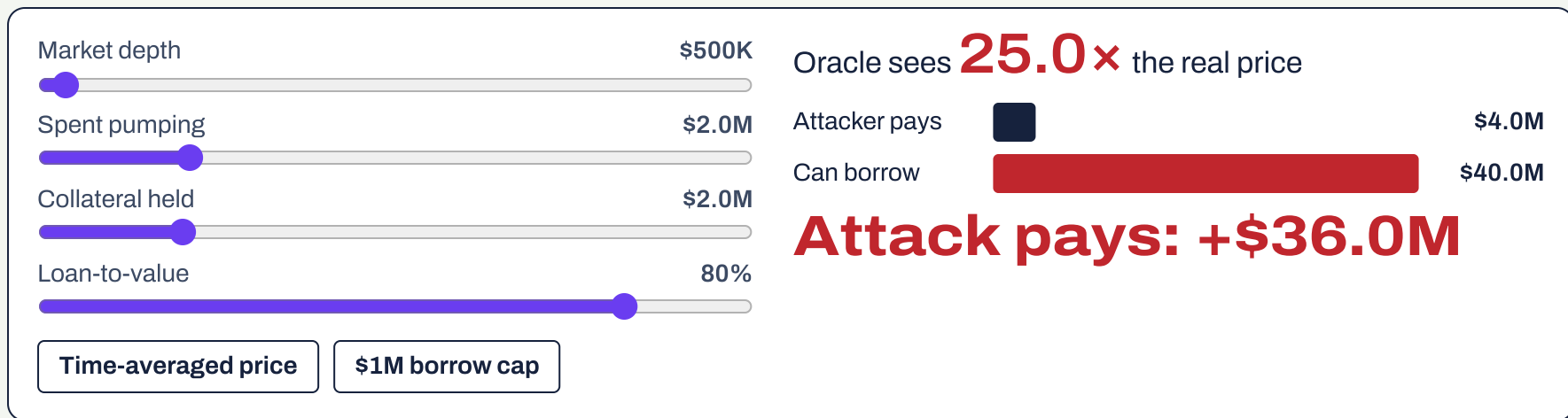
After

SEC and CFTC civil cases continue

Debate: if a program lets you do it, is it allowed?

Does an oracle attack pay?

Solend (Nov 2022, ~\$1.26M) and Loopscale (Apr 2025, ~\$5.8M) were this pattern at smaller scale.



Bucket 3: keys, signers, operations

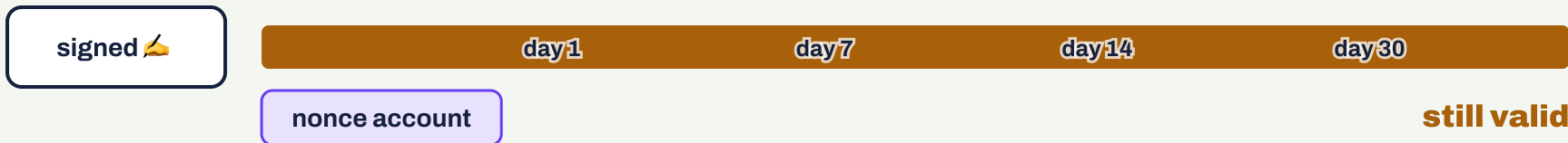
The code was fine. The people were the way in.

Why an old signature can still bite

Normal transaction

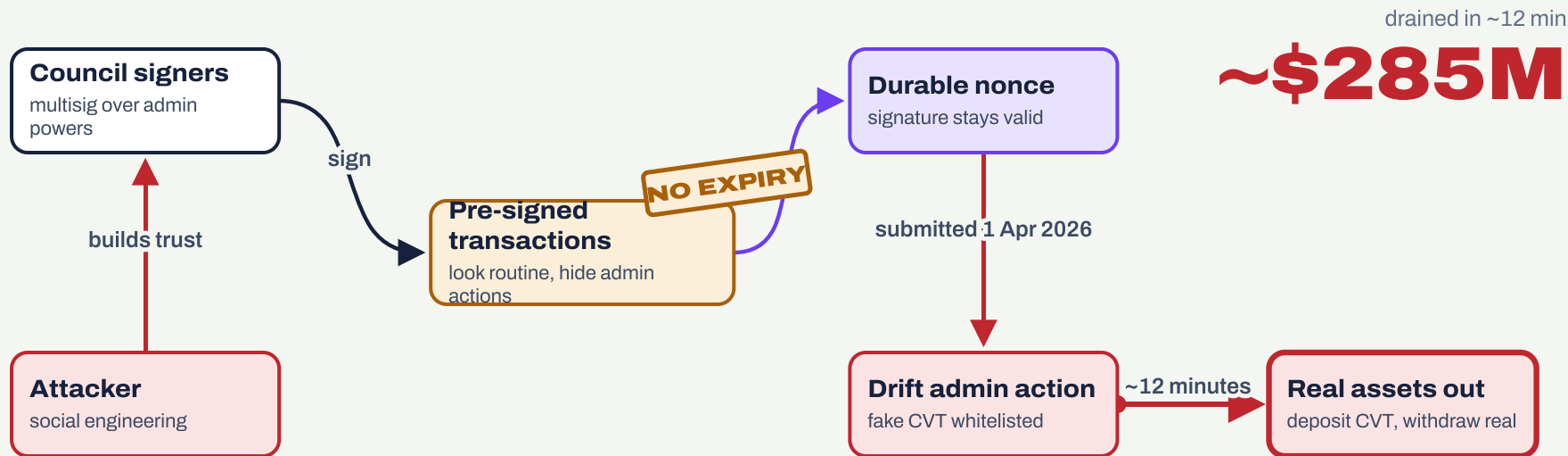


Durable nonce transaction



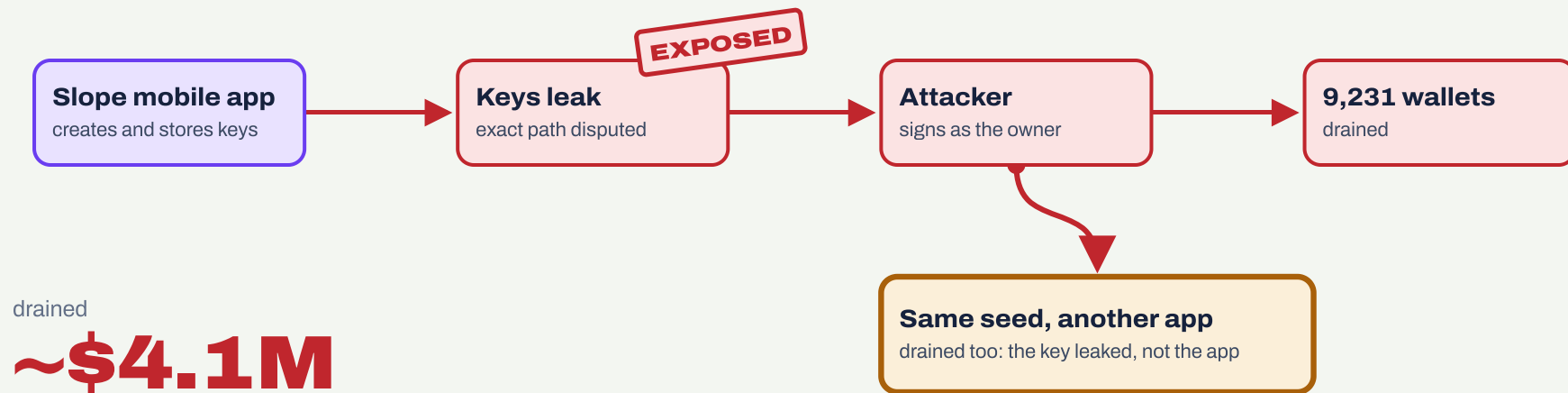
6/6 Useful for offline signing and slow multisigs. Dangerous when you do not know what you signed.

Drift Protocol - 1 Apr 2026



6/6 Deposit CVT, withdraw real assets: about \$285M in roughly 12 minutes.

Slope wallet · 2 Aug 2022



5/5 Moving the seed to another wallet did not help. The key itself was exposed.

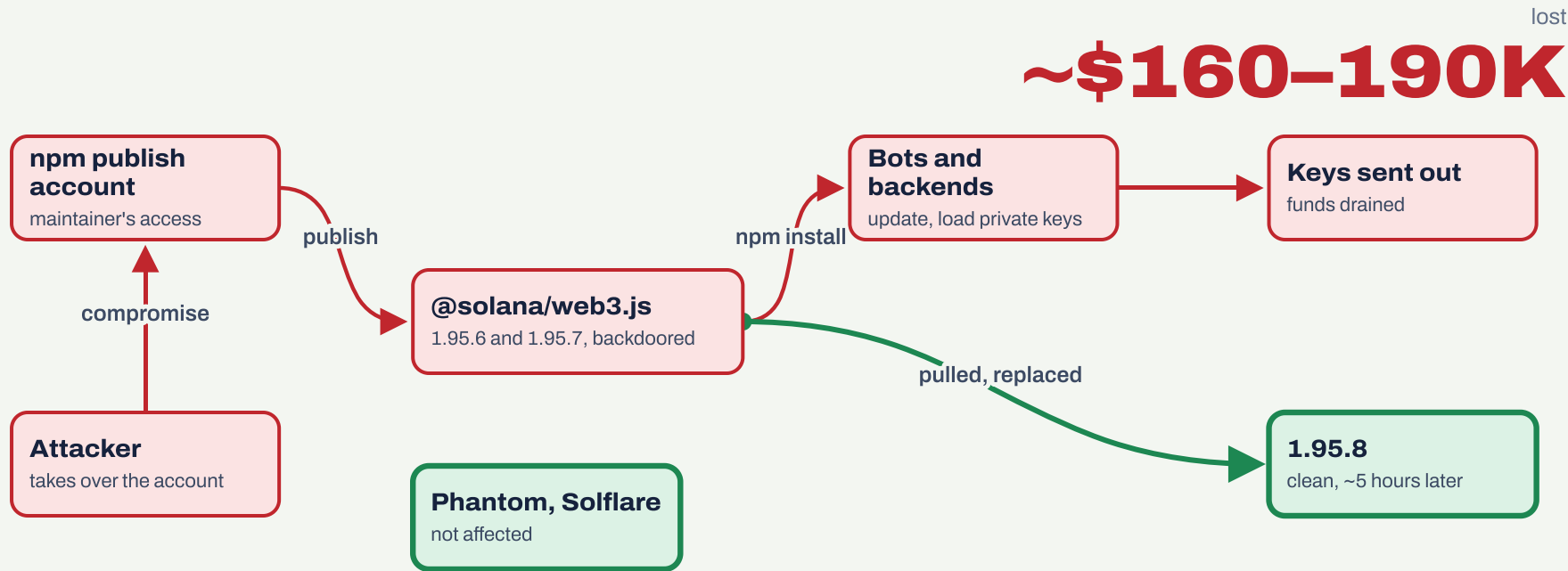
Aquifer · 31 Aug 2026 · ~\$2.5M

Cause not confirmed by the team. Reports point to compromised keys. Treat it as unproven.

Bucket 4: supply chain

The code you did not write.

@solana/web3.js · 2 Dec 2024



6/6 About five hours later the bad versions are gone. Wallet apps were not hit.

Risk with no attacker

Most money in DeFi is lost without anyone hacking anything.

Place the risks yourself

	Likelihood			
Smart-contract bug				
Oracle manipulation	High			
Key or signer compromise				
Bridge failure				
Stablecoin depeg				
Liquidation in a crash	Medium			
Impermanent loss				
Withdrawal crunch				
Governance attack	Low			
Supply-chain compromise				
Rug pull or insider				
Regulatory change				
		Low	Medium	High
			Impact	

Show one analyst's view

Clear

Oracle manipulation

Cause

A price feed follows a market someone can push.

Example

Mango, Loopscale

Mitigation

Time-averaged prices, borrow caps on thin assets.

Read the token page first

Token page what the explorer shows

Issuer	Unknown team
Mint authority	7xKp...f3Qa
Freeze authority	7xKp...f3Qa
Permanent delegate	None
Transfer hook	None
Transfer fee	0%
Top 10 holders	62%

Walk away

Mint authority active

Someone can print more and dilute you to zero.

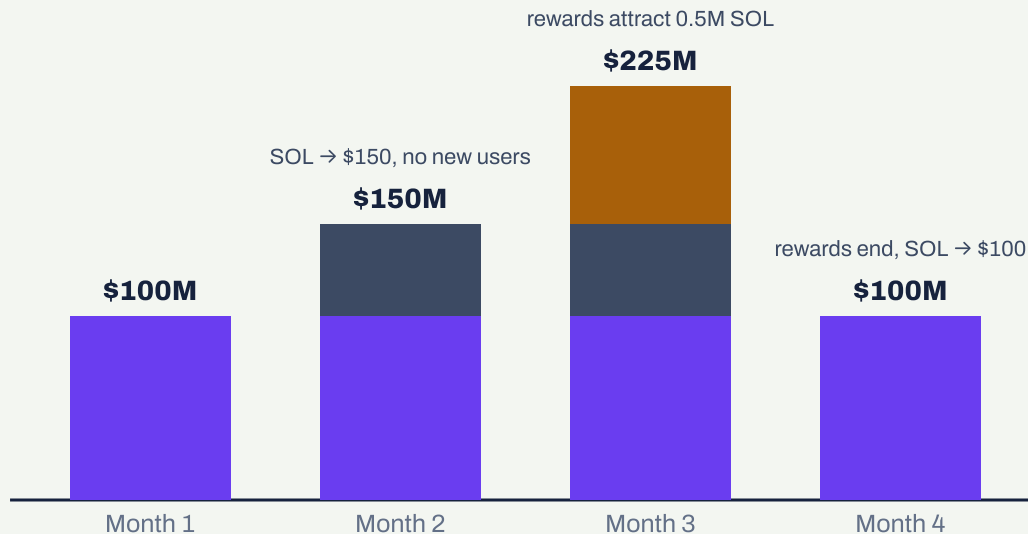
Freeze authority active

Your token account can be frozen: you could buy but never sell.

Top 10 wallets hold 62%

A few wallets can crash the price by selling.

TVL is a number, not a verdict



Back to \$100M: the growth was never users.

- Real deposits
- Price went up, not usage
- Rented by rewards

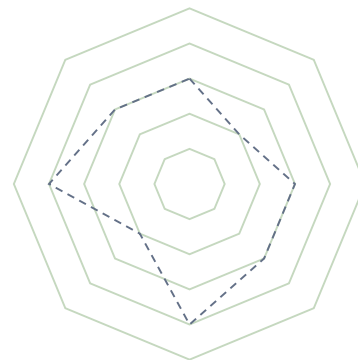
Double counting

SOL worth \$100M → staked: \$100M →
lent: \$100M

Some dashboards add both: **\$200M** of "TVL" from **\$100M** of SOL.

A due-diligence scorecard

Criterion	Weight	Score	Evidence
Security record Audits (who, when, scope), incidents, bug bounty size.	20%		None yet
Admin keys and governance Who can upgrade? Multisig size, timelock, who signs.	15%		None yet
Revenue quality Fees paid by users vs rewards paid in its own token.	15%		None yet
Oracles and dependencies Which price feeds, bridges, other protocols it relies on.	10%		None yet
Liquidity depth Can users exit at size without moving the price?	10%		None yet
Token distribution Team and investor share, unlock schedule, top holders.	10%		None yet
Transparency and docs Public code, clear docs, incident reports published.	10%		None yet
Team and maintenance Commits, releases, response to past issues.	10%		None yet



0/100

Not enough evidence to judge

-- claimed — backed by evidence

Researching risk responsibly

- **Disclose** if you hold the token you write about.
- **Separate** what you saw on-chain from what you think it means.
- **Date** every number. Say what you could not verify.
- **Teach, don't advise.** Research is not "you should buy this".

**A program trusts a price account the caller passed in, without checking who owns it.
Which bucket?**

A Oracle manipulation

B Unchecked accounts

C Supply chain

D Keys and signers

TVL rose 40% this month. What should you check first?

A Whether the token price rose

B Whether to buy the token

C The number of tweets

D Nothing, TVL is reliable

This week's task

Users

1. Pick **one incident** from today.
2. Write a post-mortem: what happened, **which bucket**, who lost money, what would have prevented it.
3. Open one real token on **Orb**. Who holds **mint** and **freeze** authority? Any Token-2022 extensions?

Builders

1. Write a tiny **Anchor program with a missing owner or signer check**.
2. Write the **exploit as a LiteSVM test**. It should pass (the attack works).
3. Add the check. The exploit test should now **fail**.

This is Wormhole and Cashio in 40 lines.

Blog post

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

Name the **bucket** for every incident you mention. Drift is the strongest story: **a people problem, not a code problem.**



Teacher prep

For the mentor. Skip in class.

You, before class

- Read **Chainalysis** or **TRM Labs** on the Drift hack. Then one write-up each for **Wormhole** and **Mango**.
- Know the **Mango legal ending**: convicted Apr 2024, convictions thrown out 23 May 2025, civil cases continuing.
- Builders' reference: the security sections of **Cyfrin Updraft's** free Solana course and **Blueshift's** challenges.
- Do the builders' task yourself: vulnerable program, LiteSVM exploit, fix.
- Open **USDC's mint on Orb** and one trending new token. Screenshot both for the red-flag demo.

The case library

Incident	Date	Loss	Root cause
Wormhole	2 Feb 2022	~\$320–326M	Fake sysvar account; forged guardian signatures
Cashio	23 Mar 2022	~\$48–52M	LP collateral mint never checked; 2B CASH minted
Mango Markets	11 Oct 2022	~\$110–116M	Thin-market oracle pump; \$67M returned
Solend	Nov 2022	~\$1.26M	Oracle attack on a thin asset
Loopscale	26 Apr 2025	~\$5.8M	RateX PT collateral mispriced; ~12% of TVL
Slope wallet	2 Aug 2022	~\$4.1M	Keys tied to the app leaked; 9,231 wallets
Drift	1 Apr 2026	~\$285M	Signers tricked into durable-nonce admin txs
Aquifer	31 Aug 2026	~\$2.5M	Cause unconfirmed; reports suggest compromised keys
@solana/web3.js	2 Dec 2024	~\$160–190K	npm account hijack; 1.95.6 and 1.95.7 backdoored

Verify before class

Drift and Aquifer are recent

Drift (Apr 2026) and Aquifer (Aug 2026) figures come from early reports. Re-read the latest post-mortems; attribution and totals can change.

Mango civil cases

The SEC and CFTC cases were continuing as of the handbook check. Look up their current status.

Token pages change

Mint and freeze authorities, extensions and holder shares change. Screenshot the tokens you demo on the day.