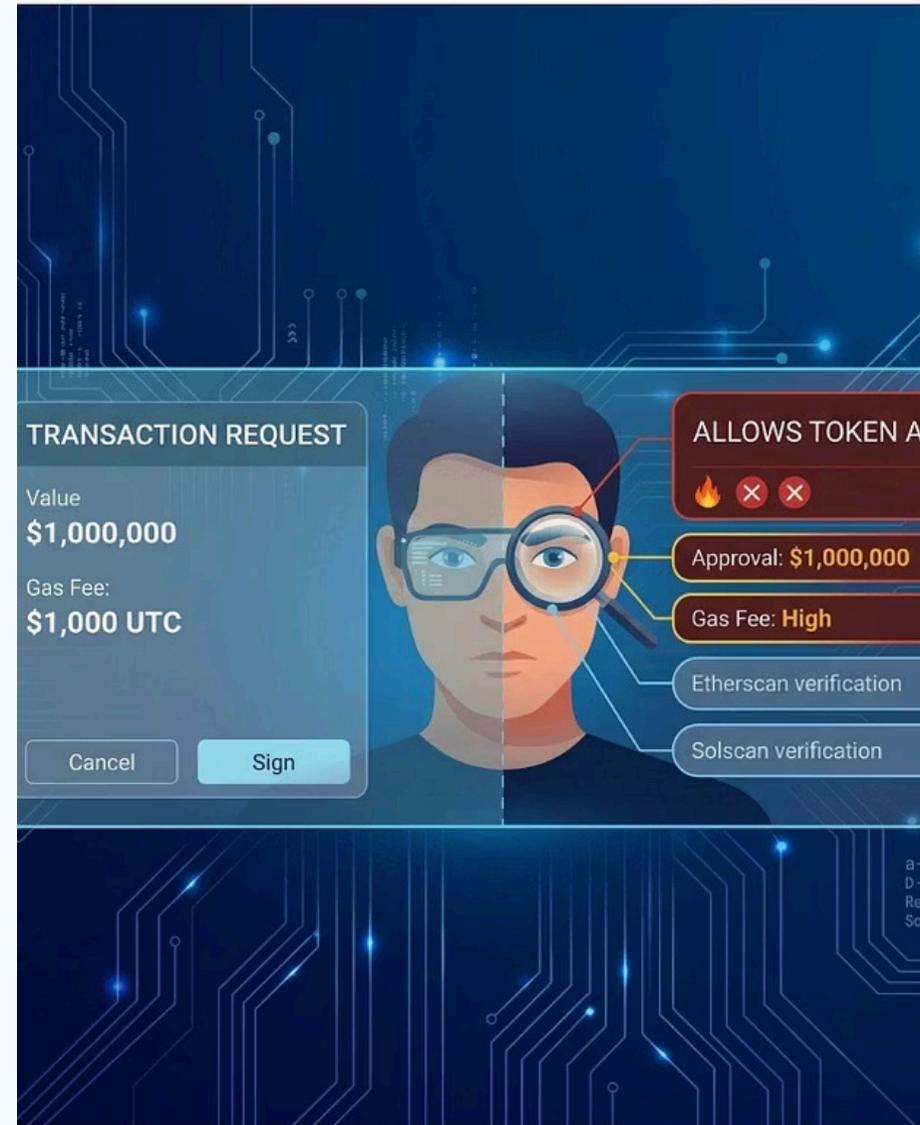# KERBERUS

How to Read a Crypto Transaction Before You Sign It

The most dangerous moment in crypto isn't after a transaction — it's the second before you click **Approve.**

Read full article at **Kerberus.com/Learn**

BEGINNER GUIDE   WEB3 SECURITY

$200M+ Lost – Not From Hacks, But From Signatures

Approval-based exploits caused over **$200 million in losses** in 2024–2025 alone, according to CertiK.

The transactions were technically valid. The wallets worked as designed. Users just didn't know what they were signing.

> 🗒 **Wallet drainers** don't crack passwords — they get you to sign something you didn't read.

What Is a Crypto Transaction?

📄 **A Signed Instruction**

A permanent, unalterable record broadcast to the blockchain

🌐 **100% Public**

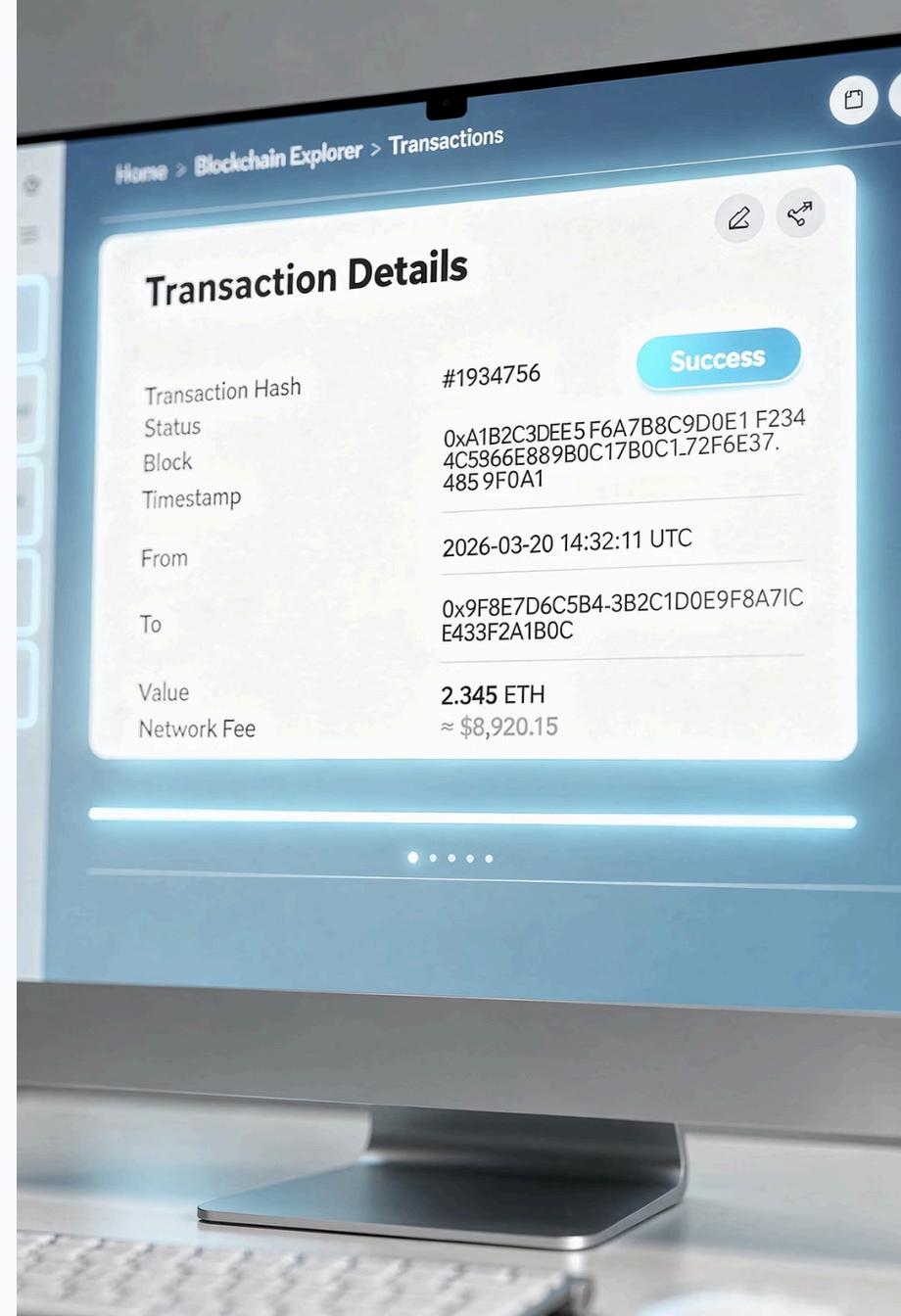Anyone can look up your transaction on a block explorer

⚠️ **Irreversible**

No undo button. The network executes exactly what you signed

Sends, swaps, mints, and approvals are all transactions. Once confirmed, they're permanent — whether you meant it or not.

Anatomy of a Transaction

Every transaction — on Ethereum, Solana, or any chain — shares the same core fields.

What Each Field Actually Means

1 **Transaction Hash (TXID)**

Unique tracking ID. Search this on Etherscan to pull up every detail.

2 **Status**

Success / Failed / Pending. Note: failed transactions still charge gas.

3 **From / To**

From = your wallet. **To** = recipient or smart contract address.

4 **Value**

Raw ETH sent. Zero doesn't mean nothing happened.

5 **Input Data**

The actual instructions to the contract. Most beginners ignore this. Scammers count on it.

Simple Transfer vs. Smart Contract

✅ Simple Transfer

Send ETH from wallet to wallet. You see the address and amount. What you see is what you get.

⚠️ Smart Contract Call

Swap, mint, or approve. Value may show **0 ETH** — but the contract can move all your tokens.

🗒 **The trap:** A 0 ETH transaction with input data is calling a function on a contract. That function might be draining your wallet. The "zero" just means no raw ETH moved — not that nothing happened.

Check the **Input Data** and **Token Transfers** tabs on Etherscan to see what actually moved.

What Is Your Wallet Really Asking?

Every wallet popup is one of three things. Knowing which one can save everything.
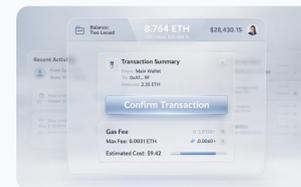
3 Types of Wallet Prompts

Sign a Message

Off-chain. No gas. Usually for login. **Low risk** — unless it contains token amounts or contract addresses.

Approve Token Spend

Grants a contract the right to spend your tokens. Unlimited approvals = **permanent risk** until revoked.

Sign a Transaction

On-chain, irreversible, costs gas. Dangerous when your wallet shows a hash instead of plain language — that's **blind signing.**

The Unlimited Approval Trap

When a DeFi protocol asks to spend an **"unlimited"** amount of your tokens, it can move every single one — forever — until you manually revoke it.

setApprovalForAll

Grants access to every NFT in a collection. One exploit = entire collection gone.

Blind Signing

Wallet shows a hash, not plain language. You're signing a contract you cannot read.

Before You Click Approve
🚩 Red Flags Checklist

→ **Unlimited approval from an unfamiliar contract**

Verify the contract address independently before approving anything.

→ **0 ETH value + complex input data**

Zero value does not mean harmless. Check what function is being called.

→ **setApprovalForAll request**

Very few legitimate operations need access to your entire NFT collection.

→ **Wallet shows a hash, not readable text**

If your wallet can't decode it, don't sign it without a second tool to translate.

→ **Urgency pressure ("Sign now or miss out")**

Scammers manufacture urgency. Legitimate opportunities don't vanish in 60 seconds.

→ **Contract address doesn't match the site**

If the address in your wallet doesn't match the protocol's verified address — close the tab.

→ **You arrived via a DM, reply on X, or unsolicited link**

Assume it's malicious until proven otherwise. Most drainer attacks start with social engineering.
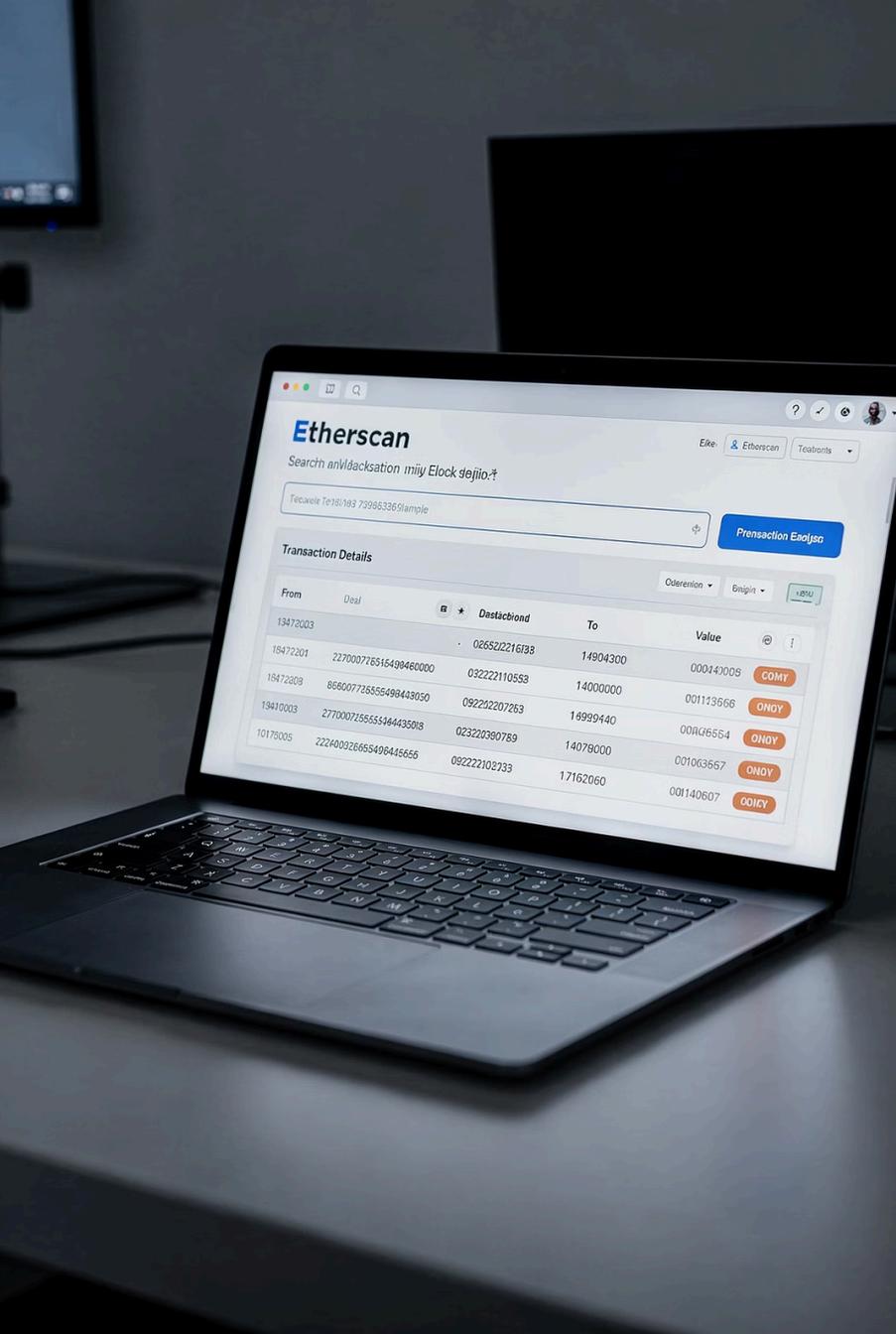
Chapter 3

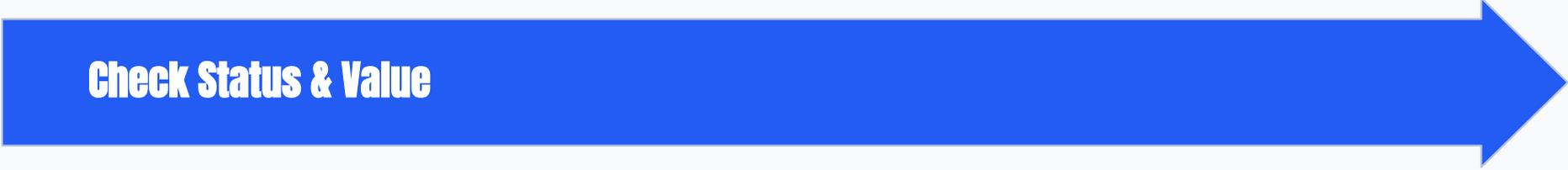# How to Verify Any Transaction Yourself
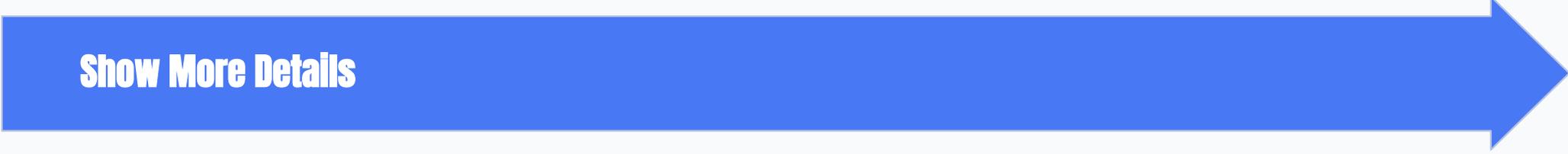
Etherscan Walkthrough

Copy TXID

Paste in Etherscan

Check Status & Value

Show More Details

Takes under 2 minutes. Works for Ethereum and all EVM-compatible chains (BscScan, Arbiscan, and others work identically).

Etherscan Pro Tips

✅ Verified Contract

Contract name appears next to the To address. Legitimate projects almost always verify.

⚠️ Unverified Contract

No name shown — just an address. Worth noting before approving anything.

🔍 Input Data Decoded

Etherscan often translates function calls into plain text. Look for the decoded tab.

Other Explorers

Solscan – Solana

Acquired by Etherscan in 2024. Check all instructions in a transaction — Solana can bundle multiple actions in one.

Blockchain.com – Bitcoin

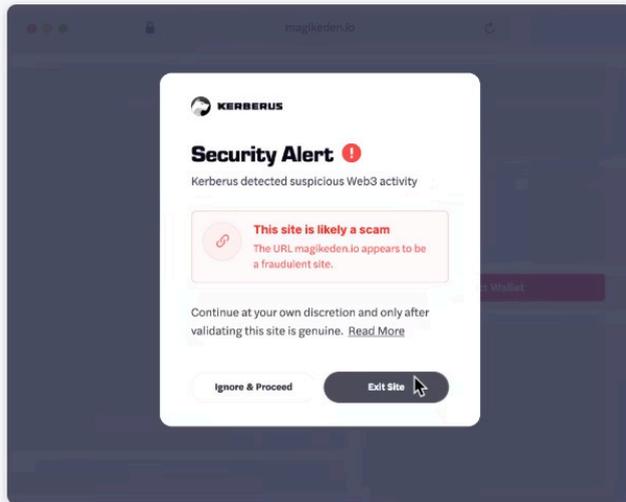Simple and reliable for BTC transaction lookups.

Stop Signing Blind – Automatically

Manual verification is powerful. But no one can cross-reference every contract under pressure. That's what **Kerberus Sentinel3** is for.
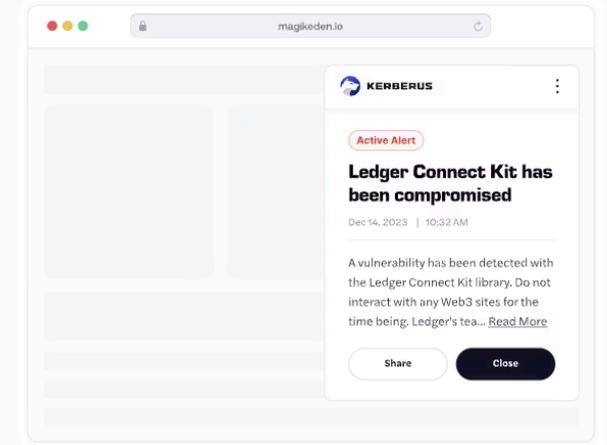
How Kerberus Sentinel3 Protects You

Real-Time Translation Layer

Sentinel3 sits between you and your wallet. Before you sign anything, it scans the site and the transaction — and flags threats in plain language.

99.9% Detection Rate

Across 1,000+ EVM chains and Solana

Up to $30K Coverage

On qualifying losses if something slips through

250,000+ Users

Zero losses on record

Quick Reference – FAQ

What is a TXID?

A unique receipt number for your transaction. Paste it into Etherscan to see every detail.

Why does my tx show 0 ETH?

You interacted with a smart contract. Check the **Token Transfers** tab to see what actually moved.

What does "pending" mean?

Not yet confirmed. High congestion or low gas fee. On Ethereum, resubmit with a higher fee using the same nonce.

How do I revoke an approval?

Use **Revoke.cash**. Connect your wallet, sort by recent, and revoke unused or unlimited approvals.

Read First. Sign Second. Always.

1 ### Every transaction is readable

Block explorers like Etherscan and Solscan are free and take 2 minutes to use.

2 ### Zero ETH = zero risk

Input data and token approvals are where the real danger hides.

3 ### Know your three prompt types

Message signing, token approval, and transaction signing each carry different risks.

4 ### Use tools that translate for you

Kerberus Sentinel3 catches what human eyes miss — in real time, before you approve.

Ready to Stop Signing Blind?

Join **250,000+ users** who have experienced zero losses with real-time transaction protection.

🛡️ Install Kerberus Extension

Free browser extension. Active in seconds. Covers 1,000+ chains.

🔍 Learn More

Explore wallet drainer threats, Web3 security guides, and wallet hygiene best practices.

Kerberus — Real-time Web3 security across 1,000+ chains. Zero losses. Up to $30,000 in coverage.