---

title: How to identify scam tokens description: Understanding scam tokens, how they make themselves look legitimate, and how to avoid them. lang: en

---

How to identify scam tokens {#identify-scam-tokens}

One of the most common uses for Ethereum is for a group to create a tradable token, in a sense their own currency. These tokens typically follow a standard, ERC-20. However, anywhere there are legitimate use cases that bring value, there are also criminals who try to steal that value for themselves.

There are two ways in which they are likely to deceive you:

- **Selling you a scam token**, which may look like the legitimate token you want to purchase, but are issued by the scammers and worth nothing.
- **Tricking you into signing bad transactions**, usually by directing you into their own user interface. They might try to get you into giving their contracts an allowance on your ERC-20 tokens, exposing sensitive information that gives them access to your assets, etc. These user interfaces might be near-perfect clones of honest sites, but with hidden tricks.

To illustrate what scam tokens are, and how to identify them, we are going to look at an example of one: wARB. This token attempts to look like the legitimate ARB token.

Arbitrum is an organization that develops and manages optimistic rollups. Initially, Arbitrum was organized as a for-profit company, but then took steps to decentralize. As part of that process, they issued a tradeable governance token.

There is a convention in Ethereum that when an asset is not ERC-20 compliant we create a "wrapped" version of it with the name starting with "w". So, for example, we have wBTC for bitcoin and wETH for ether.

It does not make sense to create a wrapped version of an ERC-20 token that is already on Ethereum, but scammers rely on the appearance of legitimacy rather than the underlying reality.

How do scam tokens work? {#how-do-scam-tokens-work}

The whole point of Ethereum is decentralization. This means that there is no central authority that can confiscate your assets or prevent you from deploying a smart contract. But it also means that scammers can deploy any smart contract they wish.

Smart contracts are the programs that run on top of the Ethereum blockchain. Every ERC-20 token, for example, is implemented as a smart contract.

Specifically, Arbitrum deployed a contract that uses the symbol ARB. But that doesn't stop other people from also deploying a contract that uses the exact same symbol, or a similar one. Whoever writes the contract gets to set what the contract will do.

Appearing legitimate {#appearing-legitimate}

There are several tricks that scam token creators do to appear legitimate.

- **Legitimate name and symbol**. As mentioned before, ERC-20 contracts can have the same symbol and name as other ERC-20 contracts. You cannot count on those fields for security.

- **Legitimate owners**. Scam tokens often airdrop significant balances to addresses that can be expected to be legitimate holders of the real token.

For example, let's look at wARB again. About 16% of the tokens are held by an address whose public tag is Arbitrum Foundation: Deployer. This is *not* a fake address, it really is the address that deployed the real ARB contract on Ethereum mainnet.

Because the ERC-20 balance of an address is part of the ERC-20 contract's storage, it can be specified by the contract to

be whatever the contract developer wishes. It is also possible for a contract to forbid transfers so the legitimate users won't be able to get rid of those scam tokens.

- **Legitimate transfers**. *Legitimate owners wouldn't pay to transfer a scam token to others, so if there are transfers it must be legitimate, right?* **Wrong**. `Transfer` events are produced by the ERC-20 contract. A scammer can easily write the contract in such a way it will produce those actions.

Scammy websites {#websites}

Scammers can also produce very convincing websites, sometimes even precise clones of authentic sites with identical UIs, but with subtle tricks. Examples might be external links that seem legitimate actually sending the user to an external scam site, or incorrect instructions that guide the user to exposing their keys or sending funds to an attacker's address.

The best practice for avoiding this is to carefully check the URL for the sites you visit, and save addresses for known authentic sites in your bookmarks. Then, you can access the real site through your bookmarks without accidentally making spelling errors or relying on external links.

How can you protect yourself? {#protect-yourself}

1. **Check the contract address**. Legitimate tokens come from legitimate organizations, and you can see the contract addresses on the organization's website. For example, for `ARB` you can see the legitimate addresses here.
2. **Real tokens have liquidity**. Another option is to look at liquidity pool size on Uniswap, one of the most common token swapping protocols. This protocol works using liquidity pools, into which investors deposit their tokens in hope of a return from trading fees.

Scam tokens typically have tiny liquidity pools, if any, because the scammers don't want to risk real assets. For example, the `ARB`/`ETH` Uniswap pool holds about a million dollars (see here for the up to date value) and buying or selling a small amount is not going to change the price:

But when you try to buy the scam token `wARB`, even a tiny purchase would change the price by over 90%:

This is another piece of evidence that shows us `wARB` is not likely to be a legitimate token.

1. **Look in Etherscan**. A lot of scam tokens have already been identified and reported by the community. Such tokens are marked in Etherscan. While Etherscan is not an authoritative source of truth (it is the nature of decentralized networks that there can't be an authoritative source for legitimacy), tokens that are identified by Etherscan as scams are likely to be scams.

Conclusion {#conclusion}

As long as there is value in the world, there are going to be scammers who attempt to steal it for themselves, and in a decentralized world there is nobody to protect you except for yourself. Hopefully, you remember these points to help tell the legitimate tokens from the scams:

- Scam tokens impersonate legitimate tokens, they can use the same name, symbol, etc.
- Scam tokens *cannot* use the same contract address.
- The best source for the address of the legitimate token is the organization whose token it is.
- Failing that, you can use popular, trusted applications such as Uniswap and Etherscan.