

# ERC-20: Standard pro zaměnitelné tokeny

**ERC-20** je technický standard používaný pro všechny chytré smlouvy na blockchainu Ethereum, které implementují zaměnitelné (fungible) tokeny. „Zaměnitelný“ znamená, že každý žeton má stejnou hodnotu jako jakýkoli jiný žeton stejného typu (podobně jako jedna stakoruna je stejná jako jiná stakoruna).

## 1. Proč standard vznikl?

Před vznikem ERC-20 (v roce 2015) měl každý token v síti Ethereum svou vlastní unikátní strukturu kódu. To znamenalo, že:

- Burzy musely psát vlastní kód pro každý nový token, který chtěly zalistovat.
- Peněženky měly problém s univerzálním zobrazováním zůstatků.
- [Decentralizované aplikace \(dApps\)](#) nemohly snadno interagovat s různými tokeny.

ERC-20 vytvořil jednotné rozhraní, díky kterému může jakákoli aplikace automaticky spolupracovat s jakýmkoli ERC-20 tokenem.

—

## 2. Povinné funkce a události

Aby byl kontrakt považován za ERC-20, musí implementovat následujících 6 funkcí a 2 události:

### Funkce (Metody)

- **totalSupply():** Vrací celkové množství tokenů v oběhu.
- **balanceOf(address owner):** Vrací počet tokenů, které drží konkrétní adresa.
- **transfer(address to, uint value):** Umožňuje odeslat tokeny z adresy volajícího na jinou adresu.
- **approve(address spender, uint value):** Dává povolení jiné adrese (např. chytré smlouvě burzy) vybrat z vašeho účtu určitý počet tokenů.
- **allowance(address owner, address spender):** Vrací množství tokenů, které majitel povolil utratit třetí straně.
- **transferFrom(address from, address to, uint value):** Umožňuje autorizované třetí straně převést tokeny mezi dvěma adresami (využívá se u automatizovaných plateb).

### Události (Events)

- **Transfer:** Vyvolá se při každém převodu tokenů.
- **Approval:** Vyvolá se při každém schválení limitu pro výběr.

—

## 3. Volitelné vlastnosti

Většina tokenů obsahuje také tři doplňkové informace, které zlepšují čitelnost pro lidi:

- **Name:** Například „Basic Attention Token“.
- **Symbol:** Například „BAT“.
- **Decimals:** Určuje, na kolik desetinných míst lze token dělit (standardem je 18, podobně jako u Etheru).

—

## 4. Bezpečnost a rizika

Standard ERC-20 má jednu známou slabinu, která vedla ke vzniku alternativních standardů (např. ERC-223):

- **Ztráta tokenů:** Pokud omylem pošlete ERC-20 tokeny přímo na adresu chytré smlouvy, která s nimi neumí pracovat, tokeny se navždy „zaseknou“ v kódu a nelze je získat zpět.
- **Schvalování (Approve):** Uživatelé často schvalují aplikacím „neomezený přístup“ (Infinite Allowance) ke svým tokenům. Pokud je taková aplikace později hacknuta, útočník může vybrat všechny prostředky uživatele.

—

## 5. Příklady ERC-20 tokenů

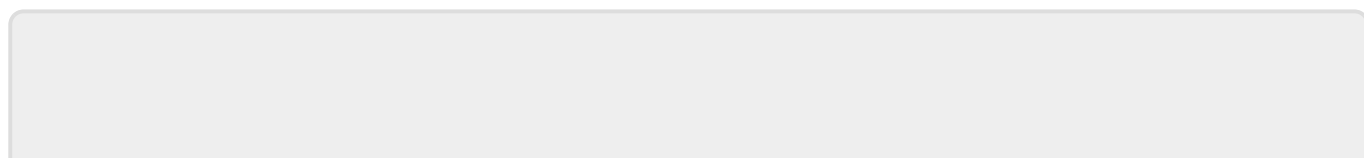
Dnes na tomto standardu běží tisíce projektů, včetně těch nejvýznamnějších:

- **Stablecoiny:** USDT (Tether), USDC (Circle), DAI.
- **Utility tokeny:** LINK (Chainlink), UNI (Uniswap), AAVE.
- **Wrapped Assets:** WBTC (Wrapped Bitcoin – Bitcoin převedený do sítě Ethereum).

*Související články:*

- [Ethereum: Platforma pro tokeny](#)
- [Solidity: Jak naprogramovat vlastní token](#)
- [DEX: Kde se obchodují ERC-20 tokeny](#)

*Tagy: it ethereum tokens erc-20 smart-contracts crypto standards*



From:

<https://serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:

<https://serviceit.cz/doku.php?id=it:sw:tokens>

Last update: **2026/01/02 20:14**

