Lesson 20: Tokens – ERC-20 and NFTs

Module 2: Blockchain Fundamentals

Digital Finance

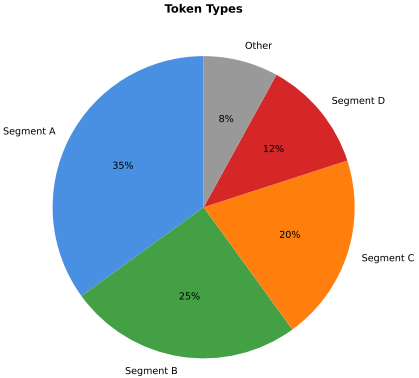
What is a Token?

Definition:

- Digital asset on blockchain
- Smart contract manages ownership
- Not native currency (e.g., not ETH)
- Programmable properties

Types:

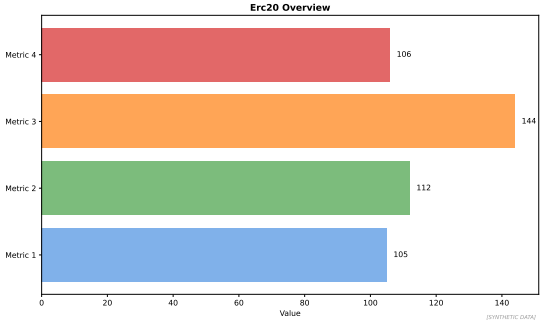
- **Fungible:** Interchangeable (e.g., USDC, UNI)
- **Non-Fungible:** Unique (e.g., NFTs, real estate)
- **Semi-Fungible:** Hybrid (e.g., gaming items)



[SYNTHETIC DATA]

Clear definitions are essential for understanding complex technical concepts.

ERC-20: Fungible Token Standard

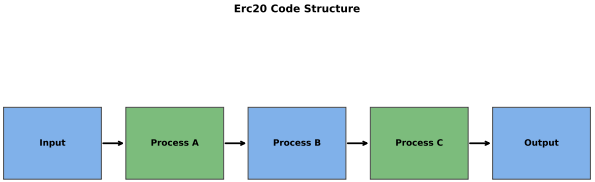


Standard Functions:

- `totalSupply()`: Returns total token supply
- `balanceOf(address)`: Returns balance of account
- `transfer(to, amount)`: Send tokens
- `approve(spender, amount)`: Allow third party to spend
- `transferFrom(from, to, amount)`: Third-party transfer (after approval)

Tokens represent digital assets and enable new business models on blockchain.

ERC-20 Implementation Example



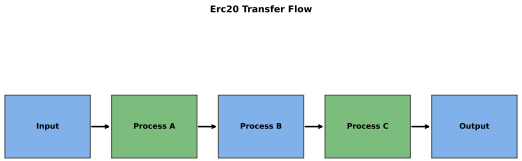
[SYNTHETIC DATA]

Key Components:

- **State Variables:** `balances`, `allowances`, `totalSupply`
- **Events:** `Transfer(from, to, amount)`, `Approval(owner, spender, amount)`
- **Metadata:** Name, symbol, decimals (usually 18)

Case studies provide concrete evidence of technology impact and adoption patterns.

ERC-20 Transfer Flow



Direct Transfer:

1. User calls `transfer(recipient, 100)`
2. Contract checks balance
3. Updates `balances[sender] -= 100`, `balances[recipient] += 100`
4. Emits `Transfer` event

Understanding the process flow is key to identifying optimization opportunities.

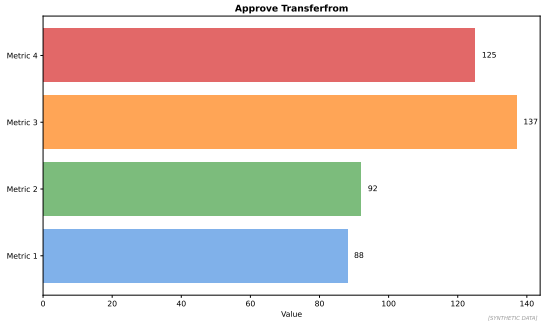
Approval and TransferFrom Pattern

Use Case:

- Allow smart contract to spend your tokens
- Required for DeFi (DEXs, lending)
- Two-step process

Steps:

1. User approves DEX: `approve(DEX, 1000)`
2. DEX calls: `transferFrom(user, pool, 500)`
3. Check allowance, transfer tokens



Security Note: Approve 0 before changing allowance to prevent race conditions

Source: Protocol documentation and distributed systems research

Should be updated to 2025 data

Token	Symbol	Market Cap	Use Case
$186-199B (Dec 2025)[1]	LINK	$8B+	Oracle network payments
$77B (Dec 2025)[2]			
$3.88B (Dec 2025)[3]			
Chainlink			
Wrapped Bitcoin	WBTC	$10B+	Bitcoin on Ethereum

Total ERC-20 Tokens: >500,000 deployed on Ethereum

Tokens represent digital assets and enable new business models on blockchain. [Source: Nilson Report, World Bank 2024]

Token Utility: Why Create Tokens?

Governance:

- DAO voting rights (e.g., UNI, COMP)
- Protocol parameter changes
- Treasury allocation

Incentives:

- Liquidity mining rewards
- Early adopter benefits
- Network effects

Access:

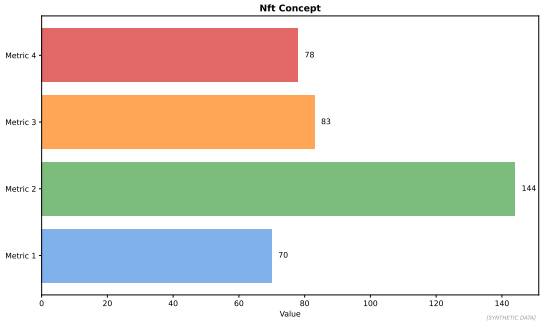
- Platform access (e.g., Filecoin storage)
- Fee discounts (e.g., BNB on Binance)
- Staking for rewards

Speculation:

- Investment asset
- Price appreciation
- Trading on exchanges

Tokens represent digital assets and enable new business models on blockchain.

NFTs: Non-Fungible Tokens



Key Properties:

- **Unique:** Each token has distinct identifier (tokenId)
- **Indivisible:** Cannot split (unlike ERC-20)
- **Provably Scarce:** Limited supply enforced by contract
- **Metadata:** Points to off-chain data (image, video, properties)

Tokens represent digital assets and enable new business models on blockchain.

ERC-721: NFT Standard

Required Functions:

- `balanceOf(owner)`: Number of NFTs owned
- `ownerOf(tokenId)`: Who owns specific token
- `transferFrom(from, to, tokenId)`: Transfer NFT
- `approve(to, tokenId)`: Approve transfer
- `safeTransferFrom(...)`: Safe transfer (checks recipient can receive)

Optional Metadata Extension:

- `tokenURI(tokenId)`: Returns URL to metadata JSON
- Metadata typically stored on IPFS or centralized server

Example: CryptoPunks, Bored Ape Yacht Club, Azuki

Source: Protocol documentation and distributed systems research

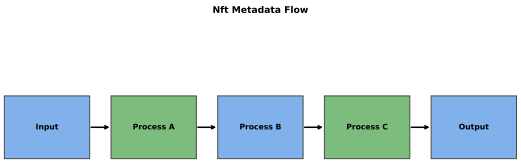
NFT Metadata Structure

On-Chain (Contract):

- Token ID
- Owner address
- Approval state
- Pointer to metadata URI

Off-Chain (IPFS/Server):

- Name, description
- Image/video URL
- Attributes (rarity traits)
- Properties



Centralization Risk: If server hosting image goes down, NFT becomes broken link

Quality data is the foundation for effective machine learning models.

NFT Use Cases

Digital Art:

- Provable ownership
- Royalties on resales (via marketplaces)
- Scarcity enforcement

Gaming:

- In-game items (weapons, skins)
- Land ownership (Decentraland)
- Cross-game interoperability

Identity/Credentials:

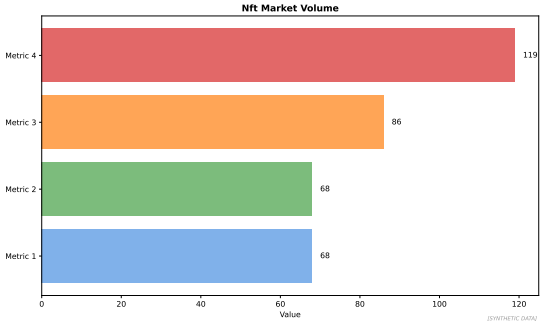
- Digital diplomas
- Membership badges
- Soulbound tokens (non-transferable)

Real-World Assets:

- Real estate deeds
- Luxury goods authentication
- Tickets/event access

Real-world applications demonstrate the practical value of blockchain technology.

NFT Mania: 2021 Boom and Bust



Peak (Aug 2021 – Jan 2022):

Weekly volume now ∼$115M (92∼7-10 ETH (∼$14K) as of Dec 2025[4]

- Celebrity endorsements, mainstream media

Crash (2022–2024): 90%+ decline in volume, floor prices collapsed

---

Source: NFT marketplace data; Digital art market analysis

[4] Source: `https://www.coingecko.com/en/nft/bored-ape-yacht-club`

Criticisms of NFTs

- **Ownership Confusion:** You own token, not copyright or image itself
- **Environmental (Pre-Merge):** High energy usage on PoW Ethereum
- **Speculation Bubble:** Most projects have no utility, pure speculation
- **Centralization:** Metadata often on centralized servers, not fully decentralized
- **Money Laundering:** Wash trading, inflated sale prices
- **IP Issues:** Plagiarism, unauthorized minting of others' art
- **Market Manipulation:** Pump-and-dump schemes, insider trading

Counterargument: Technology has legitimate use cases beyond JPEGs (credentials, gaming, ticketing)

Source: Protocol documentation and distributed systems research

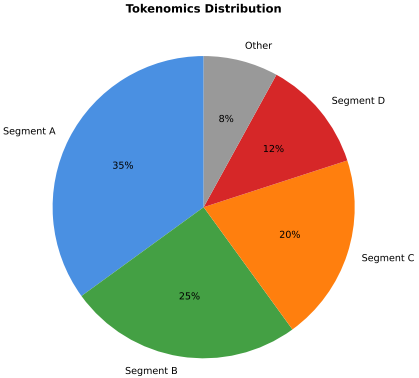
Tokenomics: Designing Token Economics

Supply Mechanics:

- **Fixed Supply:** Bitcoin (21M cap)
- **Inflationary:** Continuous issuance (older Ethereum)
- **Deflationary:** Burn mechanisms (EIP-1559)
- **Elastic:** Rebasing (Ampleforth)

Distribution:

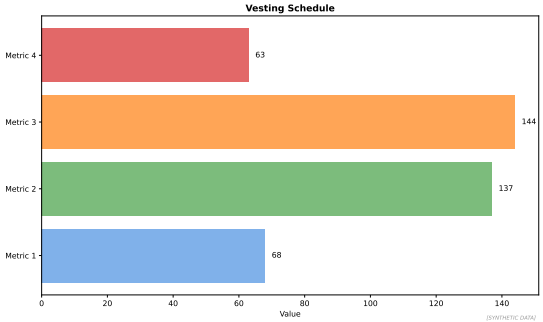
- Team allocation (with vesting)
- Investors/VCs (lockup periods)
- Community rewards (airdrops, mining)
- Treasury for governance



[SYNTHETIC DATA]

Tokens represent digital assets and enable new business models on blockchain. [Source: Blockchain.com, CoinMetrics 2024]

Vesting and Lock-Ups



Purpose: Prevent early investors/team from immediate sell-off (dump)

Typical Schedule:

- **Cliff:** 6–12 months (no tokens released)
- **Linear Vesting:** Monthly releases over 2–4 years
- **Example:** 1-year cliff, then 25% per year for 4 years

Source: Protocol documentation and distributed systems research

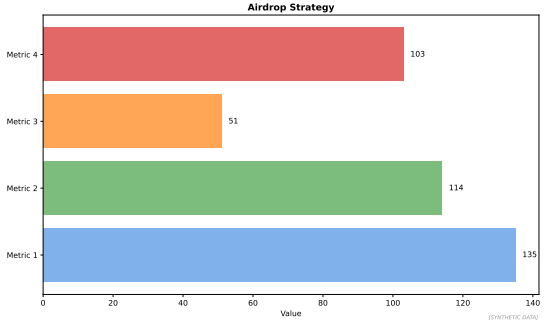
Airdrops: Free Token Distribution

Reasons:

- Reward early users
- Decentralize governance
- Marketing/awareness
- Avoid securities regulations (gift, not sale)

Famous Examples:

- Uniswap: 400 UNI to all users ($1200+)
- Ethereum Name Service: Retroactive airdrop
- Arbitrum: Governance token to users



Tokens represent digital assets and enable new business models on blockchain. [Source: Etherscan, DeFi Llama 2024]

Token Launch Models

Model	Mechanism	Pros/Cons
ICO (2017–18)	Public sale at fixed price	Simple, but many scams, regulatory issues
IEO (2019)	Sale on exchange (e.g., Binance Launchpad)	Vetted, but centralized
Fair Launch (2020)	No pre-sale, everyone equal	Community-driven, but vulnerable to bots
LBP (2021)	Liquidity Bootstrapping Pool (declining price)	Price discovery, less FOMO

Trend: Moving away from ICOs toward fairer, community-first models

Tokens represent digital assets and enable new business models on blockchain. [Source: Chainalysis, CoinGecko 2024]

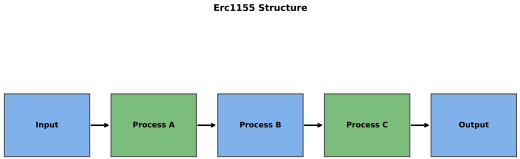
ERC-1155: Multi-Token Standard

Innovation:

- Single contract manages multiple token types
- Fungible, non-fungible, semi-fungible
- Batch operations (gas efficient)

Use Case: Gaming

- Gold (fungible)
- Sword #123 (non-fungible)
- Health potion (semi-fungible, limited)
- All in one contract



Tokens represent digital assets and enable new business models on blockchain. [Source: Chainalysis, CoinGecko 2024]

Token Security: Common Vulnerabilities

- **Reentrancy:** External calls before state updates (use checks-effects-interactions)
- **Integer Overflow/Underflow:** Fixed in Solidity 0.8+ (automatic checks)
- **Approval Race Condition:** Approve 0 before changing allowance
- **Unchecked Return Values:** ERC-20 transfer may silently fail
- **Front-Running:** Miners/bots see pending transactions, exploit
- **Centralization:** Owner has mint/burn/pause powers (rug pull risk)

Best Practice: Use OpenZeppelin audited contracts, multiple audits, time-locks on admin functions

---

Tokens represent digital assets and enable new business models on blockchain.

Tokens: Key Takeaways

- **ERC-20:** Fungible token standard, balances, transfer, approve/transferFrom
- **ERC-721 (NFTs):** Unique tokens, digital art/collectibles/gaming
- **NFT Metadata:** On-chain ownership, off-chain images (IPFS/centralized)
- **Tokenomics:** Supply, distribution, vesting, airdrops
- **ERC-1155:** Multi-token standard, efficient for gaming
- **Security:** Reentrancy, overflows, centralization risks

Next Lesson: DeFi Fundamentals – AMMs, liquidity pools, lending protocols

Swiss Token Regulation: FINMA Framework

FINMA Token Categories (2018):

- **Payment tokens**: Cryptocurrencies for payments
- **Utility tokens**: Access to digital services
- **Asset tokens**: Securities (equities, bonds)
- **Hybrid tokens**: Multiple functions

Regulatory Treatment:

- Payment: AML compliance required
- Utility: Usually unregulated
- Asset: Full securities regulation

Swiss DLT Act (Aug 2021):

- Introduced "ledger-based securities"
- Tokenized shares transferable on-chain
- No written documents required
- DLT trading facility license

Key Milestone:

- SIX Digital Exchange (SDX) licensed 2021
- World Bank CHF 200M digital bond (2024)

Switzerland was among the first countries to create comprehensive blockchain regulation. Source: FINMA ICO Guidelines (2018), Swiss DLT Act (2021)