

Lesson 20: Tokens – ERC-20 and NFTs

Module 2: Blockchain Fundamentals

Digital Finance

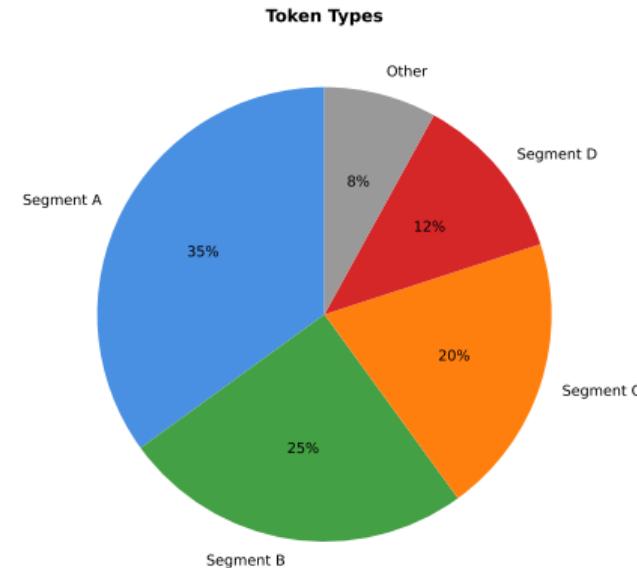
What is a Token?

Definition:

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

Types:

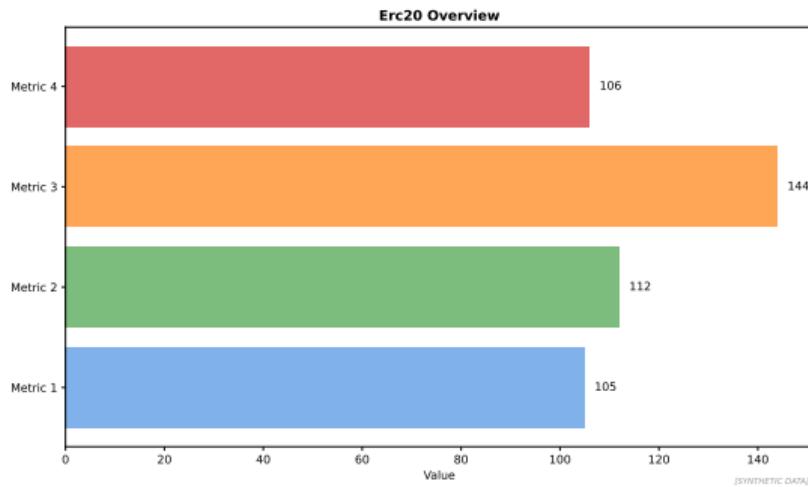
- **Fungible:** Interchangeable (e.g., USDC, UNI)
- **Non-Fungible:** Unique (e.g., NFTs, real estate)
- **Semi-Fungible:** Hybrid (e.g., gaming items)



[SYNTHETIC DATA]

Clear definitions are essential for understanding complex technical concepts.

ERC-20: Fungible Token Standard



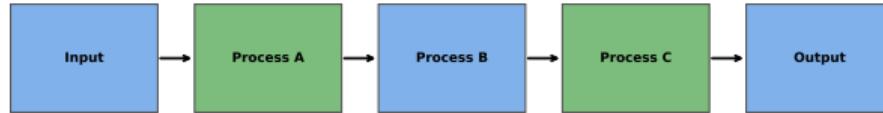
Standard Functions:

- `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

Erc20 Code Structure

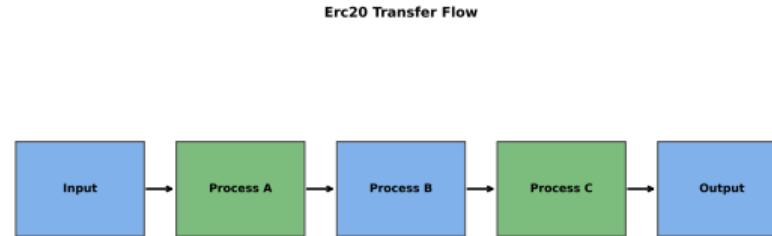


[SYNTHETIC DATA]

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.



(SYNTHETIC DATA)

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.

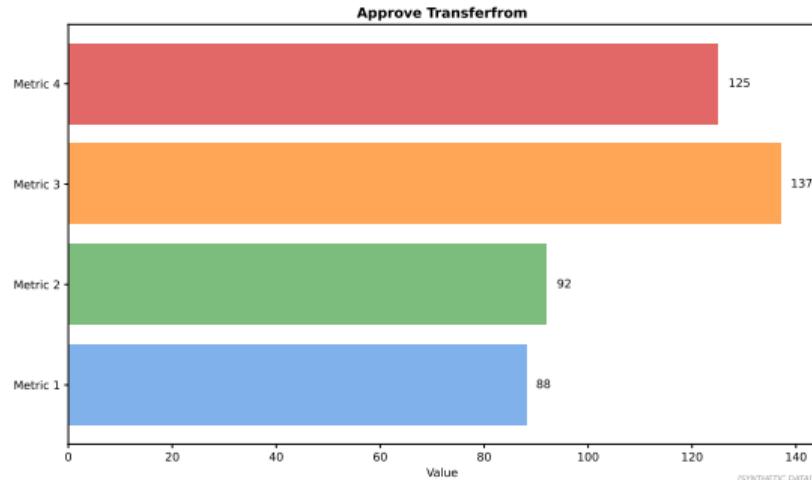
Approval and TransferFrom Pattern

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

Key concepts from this slide inform practical applications in finance.

Popular ERC-20 Tokens (2024)

| Token | Symbol | Market Cap | Use Case |
|-----------------|--------|------------|----------------------------|
| Tether | USDT | \$100B+ | Stablecoin (pegged to USD) |
| USD Coin | USDC | \$30B+ | Regulated stablecoin |
| Uniswap | UNI | \$5B+ | DEX governance token |
| Chainlink | LINK | \$8B+ | Oracle network payments |
| 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.

Token Utility: Why Create Tokens?

Governance:

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

Access:

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

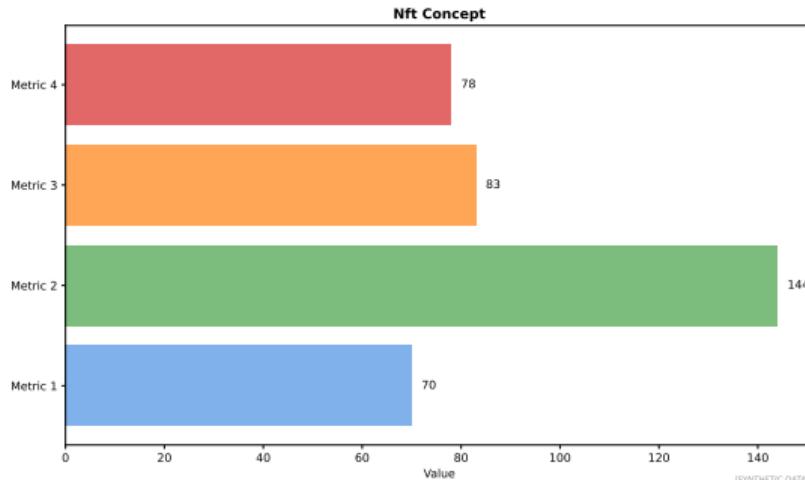
Incentives:

- Liquidity mining rewards
- Early adopter benefits
- Network effects

Speculation:

- Investment asset
- Price appreciation
- Trading on exchanges

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



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.

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

Key concepts from this slide inform practical applications in finance.

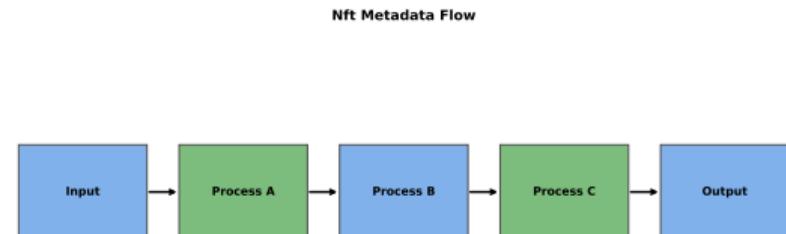
NFT Metadata Structure

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



(SYNTHETIC DATA)

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

Quality data is the foundation for effective machine learning models.

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:

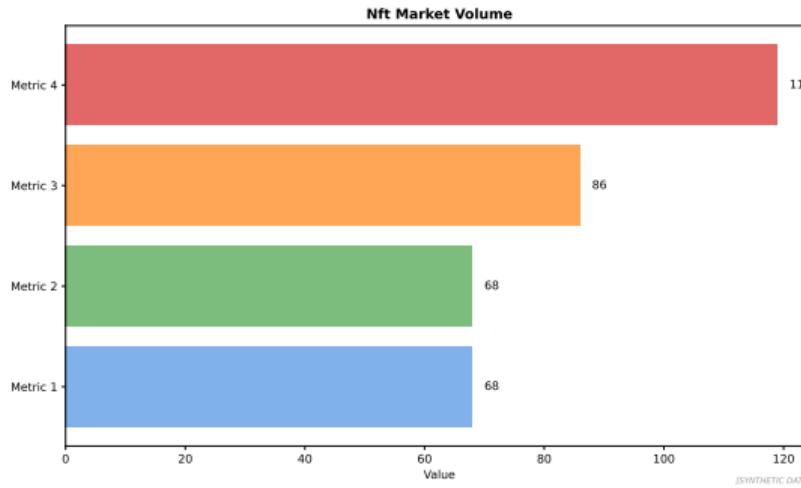
- Digital diplomas
- Membership badges
- Soulbound tokens (non-transferable)

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):

- Monthly volume: \$5B+ on OpenSea
- Bored Ape floor price: 150 ETH (\$600K)
- Celebrity endorsements, mainstream media

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

Key concepts from this slide inform practical applications in finance.

- **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)

Key concepts from this slide inform practical applications in finance.

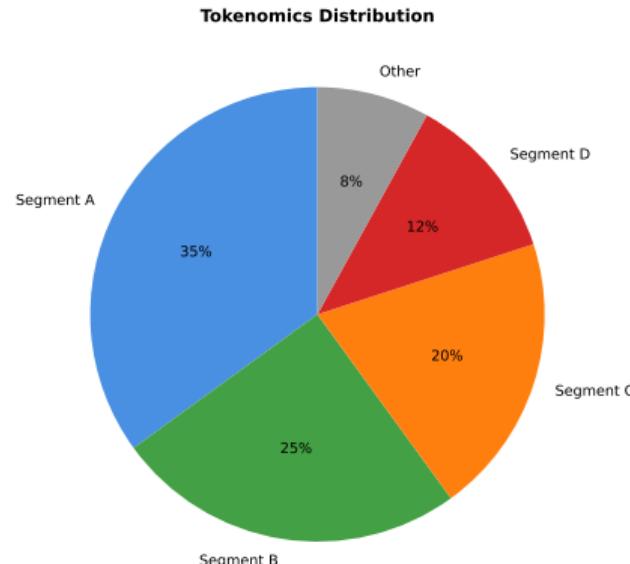
Tokenomics: Designing Token Economics

Supply Mechanics:

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

Distribution:

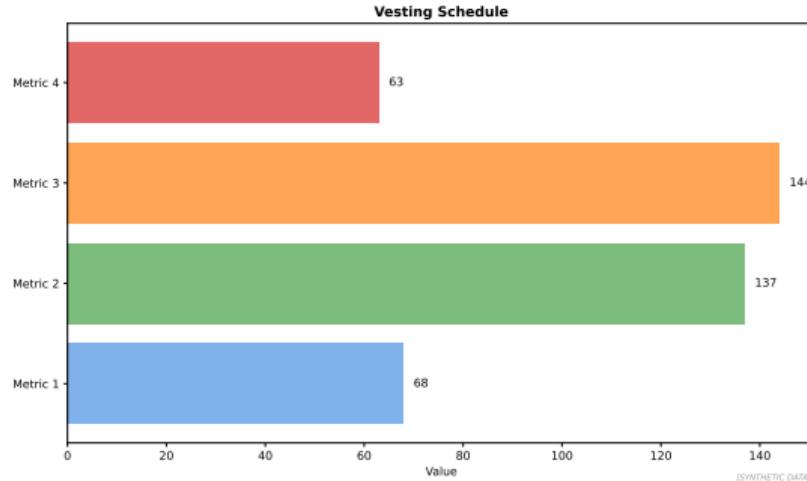
- Team allocation (with vesting)
- Investors/VCs (lockup periods)
- Community rewards (airdrops, mining)
- Treasury for governance



[SYNTHETIC DATA]

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

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

Key concepts from this slide inform practical applications in finance.

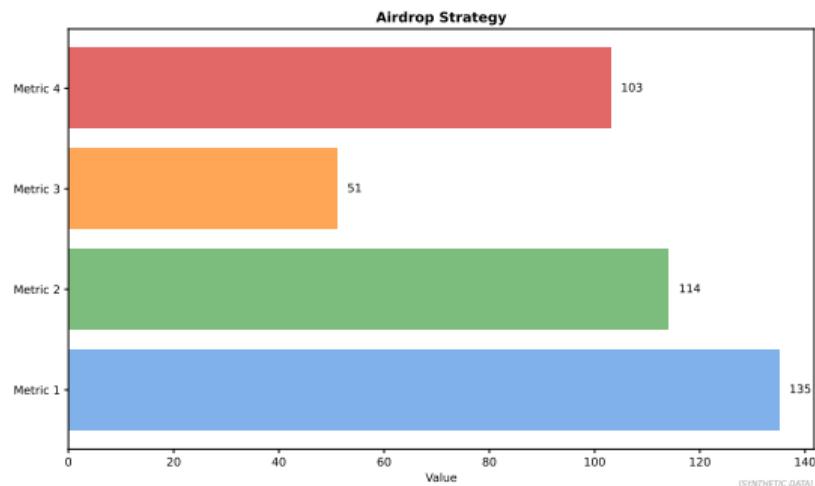
Airdrops: Free Token Distribution

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.

| 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.

ERC-1155: Multi-Token Standard

Innovation:

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

Erc1155 Structure



Use Case: Gaming

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

[SYNTHETIC DATA]

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

- **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.

- **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