

Tokenomics & Mechanism Design

Pre-Class Discovery Handout

Lesson 12 · Complete before class · 25–30 minutes

Activity 1: Token Supply Explorer

10 min

Visit **CoinGecko** (coingecko.com) and the individual project sites to research how token supply is designed and managed. Answer:

1. Compare the supply models of **Bitcoin (BTC)**, **Ethereum (ETH)**, and **Dogecoin (DOGE)**. What is each token's max supply, circulating supply, and current inflation rate? Where do these numbers come from?
2. What is **token burning**? Find 3 protocols that burn tokens (e.g., ETH post-EIP-1559, BNB, SHIB) and explain *why* each burns tokens and what effect it is intended to have on price.
3. Explain Bitcoin's **halving schedule**. When is the next halving? How does the block reward change, and how does this affect the stock-to-flow ratio and supply economics over time?
4. What is **token velocity**? Why might high velocity — tokens changing hands rapidly — be a problem for long-term token value? Which design mechanisms can reduce velocity?

Token	Max Supply	Circulating Supply	Inflation Rate	Burn Mechanism
BTC	_____	_____	_____	_____
ETH	_____	_____	_____	_____
DOGE	_____	_____	_____	_____

Activity 2: Bonding Curve Exploration

10 min

Research automated market makers and bonding curves — the mathematical pricing mechanisms that power decentralised exchanges. Answer:

1. What is a **bonding curve**? Explain in your own words how the token price changes as tokens are bought and as tokens are sold. Sketch the shape of a linear and an exponential bonding curve.
2. Look up **Uniswap's constant product formula** $x \times y = k$. Suppose a pool holds 100 ETH and 200,000 USDC. Using the formula, what is the effective price for buying **1 ETH**? What about buying **10 ETH**? Show your working.
3. What is **slippage**? Why does it occur in AMMs? How does increasing pool depth (total liquidity) affect the slippage a trader experiences?
4. Compare three AMM designs: **Uniswap v2** ($x \cdot y = k$), **Uniswap v3** (concentrated liquidity), and **Curve** (StableSwap invariant). What is each design optimised for, and what trade-offs does each make?

AMM Type	Formula	Best For	Slippage Profile
Uniswap v2	_____	_____	_____
Uniswap v3	_____	_____	_____
Curve StableSwap	_____	_____	_____

Activity 3: Incentive Design Analysis

5 min

Explore how game theory and mechanism design shape token holder behaviour in real protocols. Answer:

1. What is **staking**? Compare the staking rewards for **ETH 2.0**, **Solana (SOL)**, and **Cosmos (ATOM)**. What are the approximate annual yields, lock-up periods, and slashing risks for each?
2. What is **vote-escrowed (ve) tokenomics**? Look up **Curve's veCRV** model. Why would a rational token holder lock their CRV tokens for up to 4 years? What rewards does the lock-up unlock?
3. What is the **tragedy of the commons** in the context of on-chain governance? Find one real example of a **governance attack** on a DeFi protocol (e.g., Beanstalk, Compound) and describe how it was executed.
4. What happened with the **LUNA/UST death spiral** in May 2022? Which specific incentive mechanism was exploited, and why did the reflexive mint/burn relationship between LUNA and UST fail catastrophically?

Activity 4: Token Design Case Studies

5 min

Investigate real governance and utility token designs to understand how tokenomics choices reflect project values and economic goals. Answer:

1. Compare **UNI** (Uniswap), **MKR** (MakerDAO), and **CRV** (Curve) governance tokens. What utility does each provide *beyond* voting? Does holding each token entitle you to protocol revenue, and if so, how?
2. Look up the token vesting schedules for any 2 recent token launches (IDO/TGE in 2023–2024). What is the cliff period? What percentage of total supply goes to the team, investors, and community/ecosystem respectively?
3. What is a **fair launch**? Compare the launch mechanics of Bitcoin (no premine, no ICO) with a typical modern ICO or IDO launch. Which model distributes tokens more equitably, and what are the trade-offs?
4. List **3 common tokenomics red flags** that might indicate a project is poorly designed, extractive, or a potential scam. For each, explain why it is a warning sign.

Token	Type	Key Utility	Supply Model	Vesting Schedule	Market Cap
UNI	_____	_____	_____	_____	_____
MKR	_____	_____	_____	_____	_____
CRV	_____	_____	_____	_____	_____

Key Terms

Term	Definition
Tokenomics	The study of the economic design of a token system: supply schedule, distribution, incentive mechanisms, and how these factors influence token value and protocol behaviour over time.
Bonding Curve	A mathematical function that defines the price of a token as a function of its supply. Buying tokens moves up the curve (higher price); selling moves down. Used in automated token issuance and AMMs.
Token Velocity	The rate at which a token changes hands over a given period. High velocity implies tokens are not held as a store of value, which can suppress price even when transaction volume is high.
Halving	A pre-programmed reduction (typically by 50%) in the block reward paid to miners. Bitcoin halves approximately every 210,000 blocks (≈ 4 years), enforcing its 21 million coin cap via exponentially declining issuance.
Token Burn	The permanent removal of tokens from circulation by sending them to an unspendable address. Burns reduce supply and, if demand holds, apply upward price pressure. EIP-1559 introduced base-fee burning for ETH.
Staking	Locking tokens in a protocol to participate in consensus (Proof-of-Stake) or to earn yield. Stakers typically earn inflationary rewards and may face slashing penalties for misbehaviour.
Vote-Escrow (ve)	A tokenomics model (pioneered by Curve's veCRV) where users lock governance tokens for a fixed period to receive boosted voting power and fee sharing. Longer locks yield proportionally greater influence.
Nash Equilibrium	A game-theoretic state where no participant can improve their outcome by unilaterally changing their strategy, given the strategies of all others. Mechanism designers aim to make honest behaviour the Nash equilibrium.
Mechanism Design	The "inverse" of game theory: engineering rules and incentive structures so that rational, self-interested participants produce a collectively desirable outcome (e.g., truthful auctions, fair token distributions).
Vesting Schedule	A time-based release plan for tokens allocated to founders, investors, or employees. Prevents immediate sell pressure by releasing tokens gradually after an initial cliff period.
Cliff Period	The initial lock-up duration in a vesting schedule during which no tokens are released. After the cliff, tokens begin to vest (often linearly). Common cliffs are 6–12 months for team allocations.
Token-Curated Registry (TCR)	A mechanism where token holders stake tokens to vote on which entries belong in a curated list. Correct curators earn rewards; incorrect ones are penalised, aligning incentives with list quality.
Fair Launch	A token distribution where no tokens are pre-mined or pre-allocated to insiders; all participants gain access simultaneously and on equal terms. Bitcoin is the canonical example.
Impermanent Loss	The temporary loss in dollar value experienced by AMM liquidity providers when the price ratio of pooled assets changes relative to simply holding them. Loss is "impermanent" because it reverses if prices return to the original ratio.

Prepared by Prof. Dr. Joerg Osterrieder • Tokenomics & Mechanism Design — Lesson 12 • Pre-Class Discovery Handout