Lesson 05 — Token Economics

Study Notes

Cryptoeconomics — BSc Level

Joerg Osterrieder

2025

Contents

Learning Objectives

By the end of this lesson, students should be able to:

1. **Classify** tokens by type (utility, governance, security, stablecoin, LP token) and explain the legal implications of each.
2. **Compare** supply models (fixed, inflationary, deflationary, elastic, dual-token) and explain how each affects token value.
3. **Derive** the total Bitcoin supply from the halving schedule and explain the stock-to-flow model.
4. **Evaluate** token distribution mechanisms (fair launch, ICO/IDO, airdrops, vesting) and identify red flags in tokenomics design.
5. **Analyse** stablecoin architectures and explain the UST collapse using a bank-run model.
6. **Apply** the token velocity equation ($MV = PQ$) to assess sustainable token value accrual.

Token Classification

Coins vs. Tokens

Coins vs. Tokens

Coins (native cryptocurrencies) run on their own blockchain (Bitcoin, Ether). They pay transaction fees and incentivise network security.
Tokens are created via smart contracts on an existing chain (e.g., ERC-20 on Ethereum). They do not have their own consensus layer; they inherit security from the host chain.
Key distinction: Coins are protocol-level; tokens are application-level.

Utility Tokens

Provide access to a product or service. Value is tied to platform usage, not profit expectations. Examples: BAT (Basic Attention Token, pays for advertising), FIL (Filecoin, pays for decentralised storage), LINK (Chainlink, pays oracle nodes for data feeds).

Common Pitfall

Regulatory Risk: In the United States, utility tokens may still be classified as securities if they pass the **Howey Test**: (1) investment of money, (2) in a common enterprise, (3) with expectation of profits, (4) from the efforts of others. Many "utility" tokens have been found to satisfy all four prongs.

Governance Tokens

Grant voting rights over protocol parameters: fee structures, smart contract upgrades, treasury allocations, risk parameters. Examples:

- **UNI** (Uniswap): Vote on protocol fee tiers and grants.

- **AAVE**: Vote on collateral risk parameters and listings.
- **MKR** (MakerDAO): Vote on collateral types, stability fees, and debt ceiling.

Governance attack: A large token holder can acquire enough tokens to pass malicious proposals. On-chain governance creates plutocracy risk: one token, one vote favours wealthy holders.

Security Tokens

Represent ownership or investment contracts (equity, debt, revenue shares). Subject to securities regulation (SEC in US, FCA in UK, FINMA in Switzerland). Must comply with KYC/AML requirements. Examples: tokenised shares, real estate tokens, bond tokens.

Stablecoins

Tokens designed to maintain a peg to a reference asset (usually USD). Three main architectures: fiat-backed, crypto-collateralised, and algorithmic (Section 7).

LP Tokens

LP Tokens

When a user deposits tokens into a **liquidity pool** (e.g., ETH/USDC on Uniswap), they receive **LP tokens** representing their proportional share. LP tokens:

- Accrue trading fees automatically as the pool grows.
- Can be redeemed ("burned") at any time for the underlying assets.
- Are composable: can be staked in yield farms, used as loan collateral, or traded.

Risk: *Impermanent loss* — if the price ratio of the two pooled assets diverges significantly, LP holders end up with less value than simply holding both assets separately.

AMMs maintain the *constant product* invariant $x \cdot y = k$ where x, y are reserves and k is constant. Swapping Δx tokens in gives:

$$\Delta y = y - \frac{k}{x + \Delta x}$$

Supply Models

Model	**Mechanism**	**Effect**	**Example**
Fixed cap	Hard-coded max supply	Predictable scarcity	Bitcoin (21M)
Inflationary	Continuous new issuance	Dilutes holders; funds security	Ethereum PoS
Deflationary	Net burn > issuance	Supply contracts over time	ETH (EIP-1559 periods)
Elastic/rebase	Supply adjusts to target price	Per-token price stable; bag value moves	Ampleforth (AMPL)
Dual-token	Separate utility and value tokens	Isolates volatility from utility	Terra (LUNA/UST)

Key metrics:

- **Total supply**: All tokens ever minted (including locked/burned).
- **Circulating supply**: Tokens currently tradeable on markets.
- **Max supply**: Protocol's hard cap (may be ∞).

Bitcoin's Monetary Policy

Halving Schedule

Every **210,000 blocks** (approximately 4 years), the block reward halves:

Halving	**Block Height**	**Approx. Date**	**Block Reward (BTC)**
Genesis	0	Jan 2009	50.000
1st	210,000	Nov 2012	25.000
2nd	420,000	Jul 2016	12.500
3rd	630,000	May 2020	6.250
4th	840,000	Apr 2024	3.125
5th	1,050,000	$\approx$ 2028	1.5625
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\approx$32nd	6,720,000	$\approx$ 2140	$< 10^{-8}$ (effectively 0)

Total supply derivation (geometric series):

$$S = \sum_{k=0}^{\infty} 210{,}000 \times \frac{50}{2^k} = 210{,}000 \times 50 \times \sum_{k=0}^{\infty} \frac{1}{2^k} = 10{,}500{,}000 \times 2 = 21{,}000{,}000 \text{ BTC}.$$

Diminishing issuance: The annual inflation rate falls with each halving. After the 4th halving (2024) it is $\approx 0.85\%$/year.

Stock-to-Flow Model

The **stock-to-flow ratio** (S/F) measures scarcity as the ratio of existing supply (stock) to annual production (flow):

$$S/F = \frac{\text{Current supply}}{\text{Annual new issuance}}$$

Bitcoin's S/F approximately doubles with each halving, making it progressively more "gold-like" in scarcity. Gold has $S/F \approx 60$; Bitcoin surpassed that after the 3rd halving. The model predicts price as a power function of S/F, though this relationship is contested and should not be used for investment decisions.

Common Pitfall

Model Limitation: The stock-to-flow model assumes demand is constant and that supply scarcity mechanically determines price. It ignores demand shocks, regulatory changes, and the transition from miner revenue to fee revenue. Multiple empirical studies find the model loses predictive power post-2021.

Token Distribution

Fair Launch

No pre-mine, no pre-sale. All tokens earned through participation from day one. Most decentralised approach; provides no development funding. Examples: Bitcoin (Satoshi mined alongside everyone), Dogecoin, Monero.

ICO / IDO

Initial Coin Offering (ICO): Projects sell tokens to the public before product launch. The 2017–2018 boom raised ~$10B+ but was plagued by fraud, failed deliverables, and immediate sell pressure after listing. Regulatory crackdowns followed in most jurisdictions.

Initial DEX Offering (IDO): Token sold directly through a DEX liquidity pool at launch. Reduces gatekeepers but retains sell pressure risk. **Initial Exchange Offering (IEO)**: Sold via a centralised exchange acting as curator; provides some due diligence.

Common allocation categories:

- Team/Founders: 15–25% (must have vesting)
- Investors (seed, private, public): 10–20%
- Treasury/Foundation: 10–20% (grants, future development)
- Community/Ecosystem: 40–60% (mining, staking, airdrops)

Airdrops

Free token distribution to eligible wallet addresses. Purposes: (1) reward early users, (2) bootstrap decentralisation of governance, (3) attract attention/liquidity. Famous examples:

- **Uniswap (UNI, 2020)**: 400 UNI to each historical user of the DEX. Worth ≈\$1,200 at launch, later over \$10,000.
- **ENS (2021)**: Distributed based on domain registration date and duration.
- **Optimism (OP, 2022)**: Multi-criteria formula including L1 gas usage, Gitcoin donations, and early OP mainnet activity.

Vesting and Unlocks

Cliff Period and Linear Vesting

Vesting Schedule

A **vesting schedule** controls when locked tokens become transferable.

- **Cliff**: A period during which *no* tokens unlock. If the team member leaves before the cliff, they receive nothing.
- **Linear vesting**: After the cliff, tokens unlock at a constant rate (monthly or quarterly) until the schedule completes.

Typical structure for team/investors: 1-year cliff + 3-year monthly linear vesting = 4 years total.

Example: Vesting Calculation

A project allocates 100,000 tokens to an early investor with a 1-year cliff and 3-year linear vesting (monthly, 36 installments after cliff).
Month 12: Cliff expires. Tokens unlocked = 0 (cliff, no TGE unlock assumed).
Month 13 onwards: $\frac{100{,}000}{36} \approx 2{,}778$ tokens unlock per month.
Month 48: All 100,000 tokens fully vested.

$$\text{Unlocked at month } t = \begin{cases} 0 & t < 12 \\ \frac{100{,}000}{36}(t-12) & 12 \le t \le 48 \end{cases}$$

Smart Contract Enforcement

Modern vesting is enforced on-chain: tokens are locked in a smart contract that releases them automatically per the schedule, removing the need to trust the project team. Key parameters stored in the contract: beneficiary address, start timestamp, cliff duration, total duration, total amount.

Red Flags in Unlock Schedules

- No cliff or cliff < 6 months.
- Large TGE unlock ($> 20\%$ at launch) — immediate sell pressure.
- Short total vesting (< 2 years) for team tokens.
- Unlock cliffs coinciding with token exchange listings.
- FDV/market cap ratio $> 10\times$ at launch (huge future dilution).

Stablecoins Deep Dive

Fiat-Backed Stablecoins

Fiat-Backed Stablecoins (USDT, USDC)

The issuer holds fiat currency (or equivalent) in bank accounts. Each token is redeemable 1:1 for $1. Relies on *custodial trust*: users must trust the issuer to hold adequate reserves and not freeze accounts.
USDT (Tether): Largest by market cap. Has faced controversy over reserve composition (commercial paper, loans to affiliates). Regulated primarily in the British Virgin Islands.
USDC (Circle): Backed by USD and short-term US Treasuries. Monthly reserve attestations by Grant Thornton. Regulated in the US; complies with NYDFS.

Crypto-Collateralised Stablecoins

DAI (MakerDAO)

DAI is backed by *over-collateralised* crypto assets (ETH, WBTC, etc.) held in *Collateralised Debt Positions (CDPs)*. To mint 100 DAI a user deposits at least 150 USD worth of collateral (150% minimum collateralisation ratio). If collateral falls below the liquidation ratio ($\approx$150%), the position is automatically liquidated.
Stability mechanism: The protocol adjusts the *Stability Fee* (borrowing cost) via MKR governance to control DAI supply. Higher fees reduce minting; lower fees encourage minting.
Risk: If ETH price crashes rapidly, not all CDPs can be liquidated before falling below 100% collateralisation ("black swan" liquidations). This occurred in March 2020 ("Black Thursday").

Algorithmic Stablecoins: UST Collapse

Terra/UST — Case Study in Algorithmic Failure

Design: TerraUSD (UST) maintained its $1 peg through an algorithmic mint/burn mechanism with LUNA:

- To mint 1 UST, burn $1 worth of LUNA.

- To redeem 1 UST, burn 1 UST and receive $1 worth of LUNA.

This created a reflexive relationship: UST supply growth required LUNA price appreciation, and vice versa.

Anchor Protocol: Offered 20% APY on UST deposits, attracting $14B in UST. This yield was subsidised, not earned from real protocol revenue.

The Death Spiral (May 2022):

1. Large UST withdrawals from Anchor destabilised the peg.
2. Arbitrageurs redeemed UST for LUNA, massively increasing LUNA supply.
3. LUNA price collapsed under hyperinflation ($> 10^{12}$ LUNA minted).
4. More LUNA inflation → less confidence in redemption → UST below peg → more redemptions (bank run).
5. UST fell to $< \$0.01$; LUNA fell from ∼$80 to near zero.
6. ∼$40B in market value destroyed in < 1 week.

The collapse illustrates the **reflexivity problem** in algorithmic stablecoins: the "collateral" (LUNA) derives value from confidence in the stable asset (UST), creating a circular dependency with no fundamental floor.

Common Pitfall

Misconception: "High stablecoin yields are risk-free."

Correction: Yield must come from somewhere. Anchor's 20% APY was subsidised by the Terra foundation and was unsustainable. Any yield significantly above risk-free rates implies commensurate risk. Always ask: *where does the yield come from?*

Tokenomics Design Framework

A robust tokenomics design addresses three questions:

1. **Utility**: What is the token *required* for? Tokens used for gas, access, or collateral create organic demand. Tokens whose only utility is governance of a low-revenue protocol have weak fundamental demand.
2. **Value Capture**: How does value flow from protocol usage to token holders?
   - *Fee distribution*: Protocol fees distributed to stakers (e.g., GMX: 30% of fees to GMX stakers).
   - *Buyback and burn*: Revenue used to buy tokens from the market and destroy them, reducing supply (e.g., MKR, BNB).
   - *Required collateral*: Using the token as collateral locks supply off the market.

3. **Incentive Alignment**: Are user, developer, and investor incentives compatible in the long run?
    - Long vesting ensures team is invested in multi-year success.
    - Governance rights give large holders reason to maintain protocol health.
    - Emissions schedules that decline over time avoid permanent inflation.

Market Cap and Valuation

Key Metrics

$$\text{Market Cap} = \text{Price} \times \text{Circulating Supply}$$

$$\text{FDV} = \text{Price} \times \text{Max Supply}$$

where FDV is the **Fully Diluted Valuation** — the market cap if all tokens (including locked, unvested, and unminted future tokens) were in circulation today.

FDV / Market Cap ratio: A ratio $\gg 1$ signals large future dilution. Example: if 10% of tokens circulate at launch and FDV is $1B, market cap is $100M but $900M worth of tokens will eventually enter circulation, creating significant sell pressure.

The Velocity Trap

From the **Equation of Exchange** ($MV = PQ$, due to Irving Fisher):

$$M \times V = P \times Q \implies P = \frac{M \times V}{Q}$$

where M is token supply, V is velocity (turnover rate), P is the price level in the token economy, and Q is the transaction volume.

Rearranging for token price:

$$\text{Token Price} = \frac{\text{Transaction Volume}}{V \times \text{Supply}}$$

High velocity problem: If users buy a token, use it immediately, and sell (e.g., a pure-utility payment token), V is high. For the same transaction volume and fixed supply, high V implies low per-token price. Protocols address this by creating *holding incentives*: staking, governance power, fee discounts, lock-up requirements.

P/F Ratio

By analogy with equity's P/E ratio, the **Price-to-Fees** (P/F) ratio compares market cap to annualised protocol fee revenue. Lower P/F suggests better fundamental value. Published by Token Terminal for major DeFi protocols.

Token Burns and Buybacks

EIP-1559 and Ethereum's Burn Mechanism

Pre-EIP-1559, all transaction fees went to miners. **EIP-1559** (August 2021) reformed the fee market:

- **Base fee**: Algorithmically determined, targets 50% block utilisation. The base fee is *burned* (sent to address `0x000...dead`).
- **Priority fee (tip)**: Set by the user; goes to validators.

When network activity is high, the base fee rises and the burn rate increases. If burned ETH exceeds new validator issuance, Ethereum becomes **net deflationary** ("ultrasound money"). As of early 2026, over 3.5 million ETH have been burned since EIP-1559 activation.

BNB Quarterly Burns

Binance burns BNB quarterly until 100 million BNB (50% of total supply) remains. Initially tied to Binance exchange profits; since 2021 uses an **auto-burn formula** based on BNB price and block count:

$$\text{Burn Amount} = \frac{k}{\text{BNB Price}} \times \text{Block Count}$$

This creates a predictable, non-discretionary supply reduction schedule.

Buyback and Burn vs. Dividend Distribution

Mechanism	Tax Treatment	Effect
Burn	No taxable event for holders	Increases per-token value
Dividend / fee share	Taxable income in most jurisdictions	Direct cash flow
Staking reward	Often taxable as income	Increases staked holder return

Practice Problems

Example: Problem 1 — Circulating Supply and FDV

Question: A DeFi project launches with:

- Max supply: 1,000,000 tokens
- Circulating supply at launch: 80,000 tokens
- Launch price: $5

Compute (a) market cap at launch, (b) FDV at launch, and (c) the FDV/Market Cap ratio. Interpret the result.

Solution:

$$\text{(a) Market Cap} = 80{,}000 \times \$5 = \$400{,}000$$
$$\text{(b) FDV} = 1{,}000{,}000 \times \$5 = \$5{,}000{,}000$$
$$\text{(c) FDV/MC} = \frac{\$5{,}000{,}000}{\$400{,}000} = 12.5$$

Interpretation: Only 8% of tokens are circulating. At current price, the remaining 92% of supply (920,000 tokens) represents $4.6M of future selling pressure. This is a significant dilution risk.

Example: Problem 2 — Real Staking Yield

Question: A PoS chain offers 12% nominal staking APY. Annual token inflation is 8%. (a) What is the real yield for stakers? (b) What is the annual percentage dilution for *non-stakers*?

Solution:

- (a) $r_{\text{real}} = 12\% - 8\% = \mathbf{4}\%$ real yield for stakers.
- (b) Non-stakers hold a fixed amount of tokens while total supply grows by 8%, so their fractional ownership decreases by $\frac{8}{100+8} \approx 7.4\%$ per year.

Staking is not "free money" — the 12% partially compensates for inflation that would otherwise dilute holders.

Example: Problem 3 — Vesting Schedule

Question: A founder receives 2,000,000 tokens with a 6-month cliff and 24-month linear monthly vesting after the cliff. (a) How many tokens are unlocked after 9 months? (b) After 30 months?

Solution:

- (a) At month 9: cliff is 6 months, so 3 months of vesting have passed. Monthly rate: $2{,}000{,}000/24 = 83{,}333$ tokens/month. Total: $3 \times 83{,}333 = \mathbf{250{,}000}$ tokens.
- (b) At month 30: $30 - 6 = 24$ months of vesting completed. $24 \times 83{,}333 = \mathbf{2{,}000{,}000}$ tokens (fully vested).

Example: Problem 4 — Token Velocity

Question: A DeFi lending protocol has $10M in annual transaction volume. The governance token has a circulating supply of 1,000,000 tokens. If velocity $V = 5$ (each token changes hands 5 times per year on average), what is the implied token price from the equation of exchange? What happens to implied price if velocity drops to 2?

Solution:

$$P_{\text{token}} = \frac{\text{Transaction Volume}}{V \times \text{Supply}}$$

- $V = 5$: $P = \frac{\$10{,}000{,}000}{5 \times 1{,}000{,}000} = \$2.00$
- $V = 2$: $P = \frac{\$10{,}000{,}000}{2 \times 1{,}000{,}000} = \$5.00$

Lower velocity (e.g., from staking incentives that lock tokens) implies higher per-token price for the same protocol usage. This illustrates why well-designed tokenomics actively discourage holding velocity.

Key Takeaways

1. **Token types**: Utility, governance, security, stablecoin, and LP tokens have distinct purposes and regulatory profiles. The Howey Test determines whether a token is a security in the US.
2. **Supply models**: Fixed cap creates digital scarcity (Bitcoin); inflation funds security but dilutes holders; burns can create net deflation; elastic/algorithmic models carry stability risks.
3. **Bitcoin's monetary policy**: Total supply of 21M BTC is derived from a geometric series. Halvings halve block rewards every 210,000 blocks. The stock-to-flow ratio captures scarcity but is not a reliable price predictor.
4. **Distribution matters**: Fair launches maximise decentralisation; ICOs provide development capital but concentrate supply. Airdrop criteria shape who becomes a long-term token holder.
5. **Vesting aligns incentives**: Cliff + linear vesting over 3–4 years prevents team/investor dumping. On-chain enforcement removes trust in the issuer.
6. **Stablecoin architectures**: Fiat-backed (custodial risk), crypto-collateralised (over-collateralisation absorbs volatility), and algorithmic (reflexivity risk). UST's collapse illustrates the bank-run dynamic in algorithmic designs.
7. **Valuation tools**: Market cap, FDV, FDV/MC ratio, and the velocity equation ($MV = PQ$) provide complementary perspectives. A high FDV/MC ratio signals future dilution; high velocity undermines token value accrual.
8. **Burns and buybacks**: EIP-1559 makes Ethereum deflationary during high usage; BNB auto-burn follows a formula. Burns are generally tax-neutral for holders versus fee distributions.

Further Reading

- Buterin, V. (2021). *On Collusion*. Personal blog. https://vitalik.eth.limo/general/2019/04/03/collusion.html
  Analyses coordination failures in token-based governance.
- Samani, K. (2017). *Understanding Token Velocity*. Multicoin Capital. https://multicoin.

capital/2017/12/08/understanding-token-velocity/

- Cochrane, J. H. (2022). *Cryptocurrencies and Monetary Theory*. Hoover Institution Working Paper. Discusses stablecoin economics from a monetary theory perspective.
- Do Kwon / Terraform Labs. *Terra White Paper* (historical document). For post-mortem analysis see: Clements, R. (2022). *Built to Fail: The Inherent Fragility of Algorithmic Stablecoins*. Wake Forest Law Review.
- Messari.io: *Token Analyst* research reports on individual project tokenomics. https://messari.io/
- Token Terminal. *Protocol revenue and P/F ratios*. https://tokenterminal.com/
- EIP-1559 specification: https://eips.ethereum.org/EIPS/eip-1559