Tokenomics & Mechanism Design: Designing Token Economies

Standalone Technical Lecture

Prof. Dr. Joerg Osterrieder

University Lecture Series

March 5, 2026

Lecture Roadmap

1. Token Fundamentals → 2. Bonding Curves → 3. Incentive Design → 4. Token Design Framework → 5

Learning Objectives

- Classify tokens by function (utility, governance, security)
- Analyse supply models and their economic implications
- Derive bonding-curve pricing mathematics
- Apply game theory to incentive alignment
- Design a token economy from first principles

Prerequisites

- Lessons 1–5: Blockchain fundamentals, smart contracts, DeFi
- Basic familiarity with Ethereum and ERC-20 tokens

Durat

90 minutes — 5 sections — ˜55 frames — Prerequisite: Lessons 1–5

Table of Contents

Navig

through 5 sections covering token fundamentals to case studies and pitfalls

Learning Objectives

By the end of this lecture, you will be able to:

1. **Analyze** token supply models (fixed, inflationary, deflationary) and velocity sinks
2. **Calculate** bonding curve prices using linear, polynomial, and Bancor formulas
3. **Apply** mechanism design principles (Nash equilibrium, Schelling points) to token systems
4. **Design** a token using the 7-step framework (utility, distribution, vesting, launch)
5. **Evaluate** real-world tokenomics through UNI, MKR/DAI, CRV, and LUNA/UST case studies

Bloom

taxonomy levels: Remember → Understand → Apply → Analyze → Evaluate → Create

Section 1: Token Fundamentals & Supply Economics

Token types, supply mechanics, and valuation fundamentals

What Is a Token?

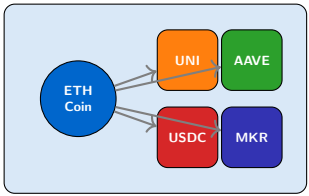
Definition

A **token** is a digital asset on a blockchain representing a unit of value, utility, or ownership right within a specific ecosystem.

Token vs. Coin

Property	Coin	Token
Own blockchain	✓	×
Native asset	✓	×
Built on another chain	×	✓
Smart contract based	×	✓

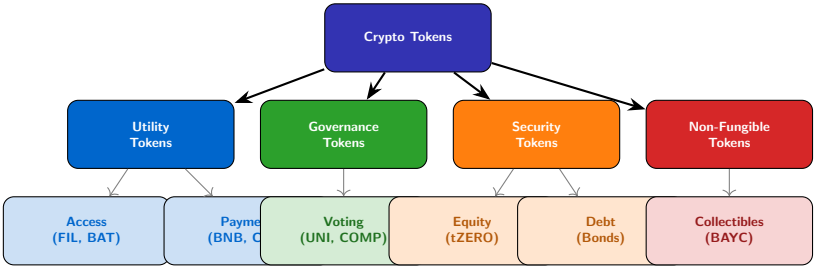
Blockchain Ecosystem



Token

are programmable assets – coins are native currencies of their own blockchain

Token Taxonomy

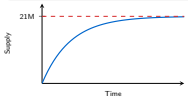


The SEC's Howey Test determines whether a token qualifies as a security – implications for compliance

Token Supply Models

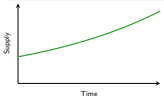
Fixed Supply

- Hard cap on total tokens
- Deflationary pressure
- Example: BTC (21M cap)



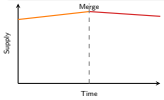
Inflationary

- Continuous new token minting
- Funds staking rewards
- Example: DOT (~10%/yr)



Deflationary

- Burn mechanisms reduce supply
- EIP-1559 base fee burn
- Example: ETH (post-Merge)



Suppl

model is the single most important tokenomic decision – it defines long-term value dynamics

Inflation & Deflation Mechanics

Inflationary Mechanisms (Faucets)

- **Block rewards:** New tokens per block (BTC, ETH pre-Merge)
- **Staking rewards:** Minted to incentivise validators
- **Liquidity mining:** Rewards for LP providers
- **Airdrops:** Free distribution to grow user base

Deflationary Mechanisms (Sinks)

- **Fee burns:** EIP-1559 burns base fees (ETH)
- **Buyback & burn:** Protocol buys and destroys tokens (BNB)
- **Slashing:** Validators lose staked tokens for misbehaviour
- **Usage burns:** Tokens consumed on use (LUNA pre-crash)

Key Metric

Real yield = Staking APY − Inflation rate
If inflation > yield, holders lose purchasing power.

Equilibrium

Net emission = Minting − Burning
ETH targets net emission ≈ 0 ("ultrasound money").

Sustainable tokenomics balances faucets (emission) and sinks (burns) for long-term stability

Market Cap & Valuation Metrics

Key Formulas

$$\text{Market Cap} = \text{Price} \times \text{Circulating Supply} \quad (1)$$

$$\text{FDV} = \text{Price} \times \text{Max Supply} \quad (2)$$

$$\text{MC/FDV Ratio} = \frac{\text{Circulating Supply}}{\text{Max Supply}} \quad (3)$$

Why FDV Matters

- Low MC/FDV ratio $\Rightarrow$ large future dilution
- Token unlocks create selling pressure
- Always compare MC **and** FDV when evaluating projects

Token	MC ($B)	FDV ($B)	Ratio
BTC	1,200	1,200	100%
ETH	400	400	100%
SOL	80	95	84%
ARB	3.2	12.8	25%
OP	2.5	11.0	23%

Warning

Low MC/FDV tokens face significant sell pressure as locked tokens unlock over time.

FDV reveals the "true" valuation – a $3B MC with $13B FDV means 77% of tokens are still locked

The Token Velocity Problem

Equation of Exchange (Fisher)

$$M \times V = P \times Q$$

- M = token supply (monetary base)
- V = velocity (turnover rate)
- P = price level
- Q = quantity of goods/services

The Problem

If V is high (tokens are not held), then M (and thus token price) must be low to satisfy PQ.

High velocity = low token value.

Velocity Reduction Strategies

1. **Staking:** Lock tokens for rewards (reduces circulating supply)
2. **Governance:** Require holding to vote (time-lock)
3. **Burn-and-mint:** Users burn tokens for services
4. **Work tokens:** Stake to earn right to perform work
5. **veCRV model:** Lock for up to 4 years for boosted rewards

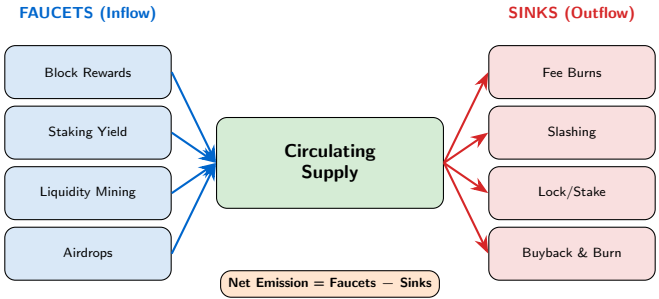
Design Principle

Good tokenomics creates reasons to **hold**, not just **use and sell**.

Kyle

Samani (Multicoin Capital): "Velocity is the killer of token value" – design sinks to counteract

Token Sinks & Faucets Framework



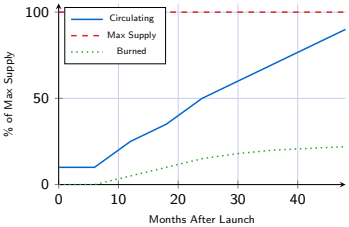
A healthy token economy maintains equilibrium between inflows (faucets) and outflows (sinks)

Circulating Supply Dynamics

Supply Categories

- **Total Supply:** All tokens that exist
- **Max Supply:** Maximum that can ever exist
- **Circulating Supply:** Tokens freely tradeable
- **Locked Supply:** Vesting, staking, or burned

$$\text{Circulating} = \text{Total} - \text{Locked} - \text{Burned}$$



Moni

unlock schedules – large supply releases often correlate with price drops

Halving & Emission Schedules

Bitcoin Halving Model

Block reward halves every 210,000 blocks (˜4 years):

$$R_n = \frac{50}{2^n} \text{ BTC per block}$$

Halving	Year	Reward
0	2009	50 BTC
1	2012	25 BTC
2	2016	12.5 BTC
3	2020	6.25 BTC
4	2024	3.125 BTC

Alternative Emission Models

- **Linear decay:** Reward decreases by fixed amount each epoch
- **Tail emission:** Minimum reward forever (Monero: 0.6 XMR/block)
- **Demand-based:** Emission adjusts to network usage (Algorand)
- **Epoch-based:** Discrete reduction at milestones (Solana: -15%/yr)

Design Trade-off

Aggressive emission $\Rightarrow$ fast bootstrap but dilution
Conservative emission $\Rightarrow$ slow growth but value preservation

Stock

to-flow ratio increases with each halving – scarcity narrative drives price cycles

Real Yield vs. Inflationary Yield

Two Sources of DeFi Yield

- **Real Yield:** Revenue generated by actual protocol activity (trading fees, interest, liquidation penalties) distributed to token holders.
- **Inflationary Yield:** New tokens minted and distributed as rewards – effectively diluting existing holders to subsidise new users.

$$\text{Real Yield} = \frac{\text{Protocol Revenue to Holders}}{\text{Token Market Cap}} \times 100\%$$

$$\text{Effective APY} = \text{Nominal APY} - \text{Inflation Rate}$$

Comparison

Dimension	Real Yield	Inflationary
Source	Protocol fees	Token emission
Sustainable?	Yes	No
Dilutive?	No	Yes
Typical APY	3–15%	50–1,000%+
Example	GMX, MKR	Early SUSHI
Value signal	Revenue > 0	Emission > 0

The Sustainability Test

If a protocol's yield disappears when token emissions stop, it was **never real yield** – it was a temporary subsidy funded by dilution.

Real Yield Protocols

- **GMX:** 30% of trading fees $\rightarrow$ GMX stakers in ETH/AVAX
- **MakerDAO:** Stability fees buy and burn MKR
- **Lido:** 5% of staking rewards to LDO treasury

DeFi

Llama tracks "Real Yield" separately from inflationary APY – always check the source of returns

Section 1 Summary: Token Fundamentals

Key Concepts

1. Tokens are programmable assets on existing blockchains
2. Four main types: utility, governance, security, NFT
3. Supply model (fixed/inflationary/deflationary) is the core design choice
4. Market Cap vs. FDV reveals dilution risk
5. Token velocity inversely affects token value

Design Checklist

- ✓ What type of token? (utility, governance, hybrid)
- ✓ Fixed or variable supply?
- ✓ What are the faucets? (how tokens enter circulation)
- ✓ What are the sinks? (how tokens leave circulation)
- ✓ What incentivises holding vs. selling?

Next Section

⇒ **Bonding Curves & Pricing Mechanisms:** Mathematical foundations for automated token pricing.

Token

is the "constitution" of a token economy – get fundamentals right before mechanism design

Section 2: Bonding Curves & Pricing Mechanisms

Automated pricing, bonding curve mathematics, and AMM design

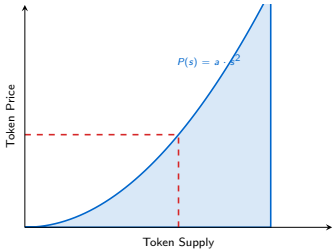
What Is a Bonding Curve?

Definition

A **bonding curve** is a mathematical function that defines the relationship between a token's price and its supply. Tokens are minted on purchase and burned on sale via a smart contract.

Properties

- **Deterministic:** Price is a function of supply
- **Continuous:** Always liquid, no order book needed
- **Autonomous:** No market maker required
- **Transparent:** Price curve is public and immutable



Bond

curves enable "automatic market making" without counterparties – pioneered by Bancor in 2017

Linear & Polynomial Bonding Curves

Linear Curve

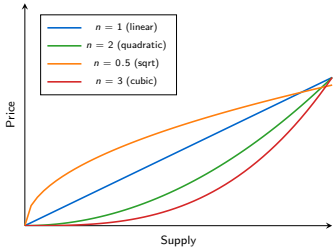
$$P(s) = m \cdot s + b$$

- Price increases linearly with supply
- Constant price sensitivity
- Simple but may grow too fast

Polynomial Curve

$$P(s) = a \cdot s^n$$

- $n < 1$: Sublinear (early buyers benefit less)
- $n = 1$: Linear
- $n > 1$: Superlinear (early buyers benefit more)



Highe

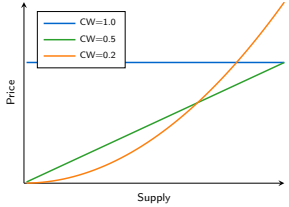
exponent n rewards early adopters more aggressively – choose n based on incentive goals

The Bancor Formula

Continuous Token Model

The Bancor protocol introduced the **Connector Weight** (CW), also called Reserve Ratio:

$$P = \frac{\text{Reserve Balance}}{\text{Token Supply} \times CW}$$



Purchase Price Calculation

Tokens received for depositing d into reserve:

$$T = S_0 \left[\left(1 + \frac{d}{R_0} \right)^{CW} - 1 \right]$$

where S_0 = current supply, R_0 = current reserve.

Slippage

Large purchases move along the curve, paying progressively higher prices. This is inherent slippage.

CW Interpretation

- $CW = 1$: Constant price (stablecoin)
- $CW = 0.5$: Linear price increase
- $CW < 0.5$: Superlinear (steep curve)

innovation: algorithmic liquidity without counterparties – foundation of modern AMMs

Augmented Bonding Curves (ABC)

Concept (Commons Stack)

Augmented bonding curves add a **funding pool** alongside the reserve pool:

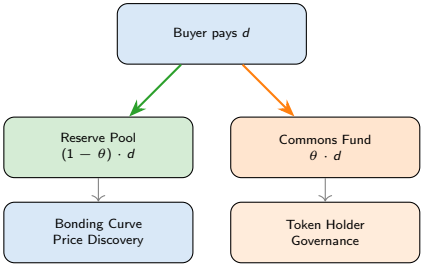
- A percentage of each purchase goes to a **commons fund**
- Fund is governed by token holders
- Creates sustainable funding for public goods

Split Mechanism

On each buy of amount d:

- $(1 - \theta) \cdot d \rightarrow$ Reserve (backs token value)
- $\theta \cdot d \rightarrow$ Commons Fund (project treasury)

Typical $\theta = 0.1$ to 0.3 (10–30% to commons).



ABCs

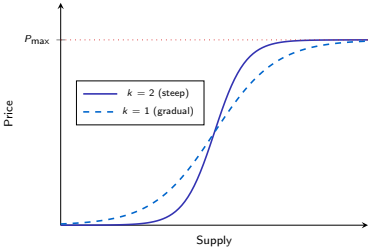
align speculation with public goods funding – "skin in the game" for ecosystem development

Sigmoid & S-Curve Pricing Models

Sigmoid Bonding Curve

$$P(s) = \frac{P_{\max}}{1 + e^{-k(s - s_0)}}$$

- Price starts low, grows rapidly, then plateaus
- $P_{\max}$: maximum price ceiling
- s_0: midpoint of growth
- k: steepness parameter



When to Use Sigmoid

- Early access at low cost
- Natural price ceiling prevents bubbles
- Ideal for capped ecosystems

Sigm

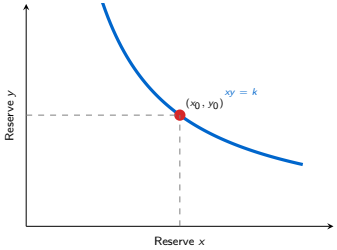
curves are well-suited for tokens that should reach a stable equilibrium price over time

Constant Product AMM (Uniswap Model)

Invariant Formula

$$x \cdot y = k$$

- x: reserve of token A
- y: reserve of token B
- k: constant product invariant



Marginal Price

$$P = \frac{dy}{dx} = \frac{y}{x}$$

Trading Δx tokens in, receiving:

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

Unisv

$xy = k$ **is the most widely deployed bonding curve – over $1T cumulative volume**

Comparing Bonding Curve Types

Property	Linear	Polynomial	Bancor	Sigmoid
Formula	$ms + b$	as^n	$\frac{R}{S \cdot CW}$	$\frac{P_{\max}}{1+e^{-k(s-s_0)}}$
Price ceiling	No	No	No	Yes
Early-adopter reward	Moderate	Tunable (n)	Tunable (CW)	High
Complexity	Low	Low	Medium	Medium
Slippage	Predictable	Variable	Variable	Low at extremes
Use case	Simple tokens	DAO tokens	DEX reserves	Capped ecosystems

Design Guidance

Match curve type to your token's purpose:

- Fair distribution $\rightarrow$ Linear or sqrt
- Reward early adopters $\rightarrow$ Polynomial ($n > 1$)
- Sustainable funding $\rightarrow$ Augmented Bancor

Common Mistake

Using a steep polynomial curve ($n \geq 3$) creates excessive early-adopter advantage, resembling a Ponzi scheme. Regulators scrutinise this.

No single curve is "best" – the right choice depends on your distribution goals and regulatory context

Bonding Curve: Solidity Implementation

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

contract LinearBondingCurve {
    uint256 public totalSupply;
    uint256 public reserveBalance;
    uint256 public slope = 1e15; // price slope in wei

    mapping(address => uint256) public balances;

    // Price = slope * totalSupply
    function currentPrice() public view returns (uint256) {
        return slope * totalSupply / 1e18;
    }

    // Buy tokens: cost = slope * (s1^2 - s0^2) / 2
    function buy() external payable {
        uint256 s0 = totalSupply;
        // Solve for tokens: area under linear curve
        uint256 tokens = sqrt(2 * msg.value / slope + s0 * s0) - s0;
        totalSupply += tokens;
        reserveBalance += msg.value;
        balances[msg.sender] += tokens;
    }

    function sqrt(uint256 x) internal pure returns (uint256) {
        uint256 z = (x + 1) / 2;
        uint256 y = x;
        while (z < y) { y = z; z = (x / z + z) / 2; }
        return y;
    }
}
```

Produ

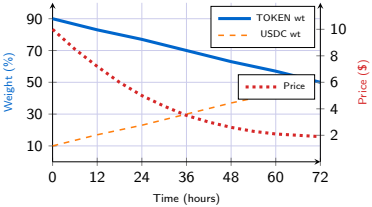
contracts need SafeMath, reentrancy guards, and proper ERC-20 compliance

Liquidity Bootstrapping Pools (LBPs)

Mechanism (Balancer LBP)

A **Liquidity Bootstrapping Pool** shifts token weights over time, creating a Dutch-auction-style price discovery:

- Start with high project-token weight (e.g., 90/10 TOKEN/USDC)
- Gradually shift to balanced ratio (e.g., 50/50) over 24–72 hours
- Price starts high and naturally decreases if no one buys
- Buyers set their own entry price by choosing when to buy



Balancer Weighted Pool Price

$$P = \frac{B_{\text{ref}} / w_{\text{ref}}}{B_{\text{token}} / w_{\text{token}}}$$

As w_{token} decreases from 0.9 to 0.5 and w_{ref} increases from 0.1 to 0.5, the denominator grows relative to the numerator, driving price down.

Anti-Bot & Anti-Whale Properties

- Bots buying early pay maximum price (self-penalising)
- Large buys push price up, rewarding patient small buyers
- No front-running advantage – price declines naturally

Balar

LBPs have launched 100+ tokens including Perpetual Protocol, Radicle, and HydraDX

Section 2 Summary: Bonding Curves

Key Concepts

1. Bonding curves create deterministic price-supply relationships
2. Linear, polynomial, Bancor, and sigmoid are the main types
3. Reserve ratio (CW) controls curve steepness in Bancor model
4. Augmented curves fund public goods via split mechanism
5. $xy = k$ (Uniswap) is the most deployed bonding curve

Mathematical Toolkit

$$P_{\text{linear}} = m \cdot s + b \tag{4}$$

$$P_{\text{poly}} = a \cdot s^n \tag{5}$$

$$P_{\text{bancor}} = R/(S \cdot CW) \tag{6}$$

$$P_{\text{sigmoid}} = P_{\max}/(1 + e^{-k(s-s_0)}) \tag{7}$$

$$P_{\text{uniswap}} = y/x \tag{8}$$

Next Section

⇒ **Incentive Design & Game Theory:** How to align stakeholder incentives using mechanism design.

Bond curves are the mathematical backbone of token pricing – choose wisely for your use case

Section 3: Incentive Design & Game Theory

Mechanism design, staking incentives, and Nash equilibria in token systems

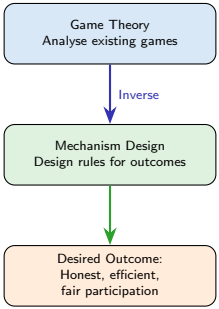
Mechanism Design: The Inverse Game Theory

Definition

Mechanism design is the engineering side of game theory: instead of analysing existing games, we *design* rules so that rational agents produce desired outcomes.

Key Properties

- **Incentive compatibility:** Truthful behaviour is optimal
- **Individual rationality:** Participation is voluntary and beneficial
- **Budget balance:** Mechanism doesn't require external funding



Leoni

Hurwicz, Roger Myerson, Eric Maskin won the 2007 Nobel Prize for mechanism design theory

Nash Equilibrium in Token Systems

Staking Game: Payoff Matrix

Two validators decide whether to **Stake honestly** or **Attack**:

		Validator B	
		Stake	Attack
Val. A	Stake	5, 5	2, 7
	Attack	7, 2	−10, −10

Without Slashing

(Attack, Attack) is tempting → Prisoner's dilemma. Both defect, both lose.

With Slashing Penalty

Adding slashing (−20 for attack detected):

	Stake	Attack
Stake	5, 5	5, −13
Attack	−13, 5	−30, −30

Nash Equilibrium

With slashing, **(Stake, Stake)** becomes the dominant strategy. Rational validators always stake honestly.

Slash

transforms the game from Prisoner's Dilemma to one where cooperation is the Nash equilibrium

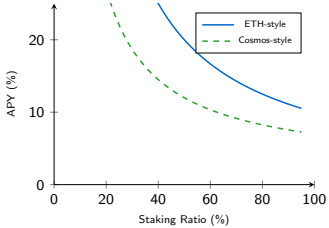
Staking Incentive Design

Reward Function

Validator reward per epoch:

$$R_v = R_{\text{base}} \cdot \frac{S_v}{\sum_i S_i} \cdot (1 + \beta \cdot \text{uptime}_v)$$

- S_v: validator's stake (proportional share)
- R_{base}: total rewards per epoch
- β: uptime bonus factor



Key insight: APY decreases as more stake joins → self-regulating equilibrium.

Slashing Conditions

- **Double signing:** Sign two blocks at same height (−5%)
- **Downtime:** Offline for extended period (−0.1%/epoch)
- **Surround vote:** Contradictory attestations (−100%)

Ether

targets 27% staking ratio – rewards adjust dynamically to maintain this equilibrium

Tragedy of the Commons in Token Governance

The Problem

- Governance is a **public good**: everyone benefits, few contribute
- Rational token holders free-ride: holding is profitable, voting is costly
- Result: low participation, plutocratic outcomes

Solutions

1. **Delegation:** Token holders delegate votes to experts (dPoS-like)
2. **Quadratic voting:** Cost $= (\text{votes})^2$, reduces whale dominance
3. **Conviction voting:** Voting power grows over time (Gardens)
4. **Vote-escrowed:** Lock tokens for boosted governance power (veCRV)
5. **Incentivised voting:** Rewards for participation (OP RetroPGF)

Real-World Data

Protocol	Avg. Turnout
Uniswap	3–5%
Compound	5–10%
Aave	2–4%
MakerDAO	10–15%

Quadratic Voting Cost

$$\text{Cost}(n) = n^2 \text{ tokens for } n \text{ votes}$$

1 vote = 1 token, 10 votes = 100 tokens.

Low

governance turnout is the #1 challenge in DAO design – mechanism design must incentivise participation

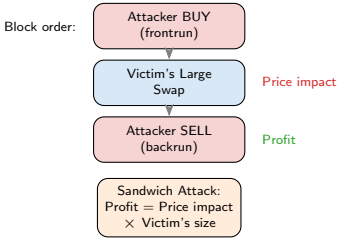
MEV and Strategic Behaviour

Maximal Extractable Value (MEV)

MEV = profit extracted by reordering, inserting, or censoring transactions within a block.

MEV Strategies

- **Frontrunning:** Insert tx before a known large trade
- **Backrunning:** Insert tx after an oracle update
- **Sandwich attack:** Buy before, sell after a victim's trade
- **Liquidation:** Race to liquidate undercollateralised positions



Flash

estimates $600M+ MEV extracted on Ethereum – mechanism design must account for strategic actors

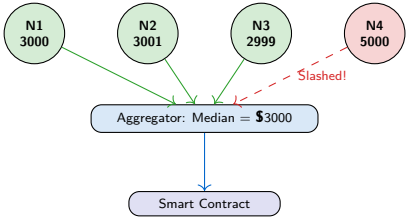
Schelling Points & Coordination Games

Schelling Point

A **Schelling point** (focal point) is a solution people converge on without communication, because it seems natural or obvious.

Oracle Design Example (Chainlink)

- N oracle nodes independently report ETH/USD price
- Honest reporting is the Schelling point
- Outliers are penalised (slashed)
- Median value is accepted as "truth"



Reward Function

$$R_i = \begin{cases} R_{\text{base}} & \text{if } |p_i - \tilde{p}| < \epsilon \\ -S_{\text{slash}} & \text{otherwise} \end{cases}$$

Schel

point mechanisms underpin oracle networks, prediction markets, and dispute resolution systems

Token-Curated Registries (TCRs)

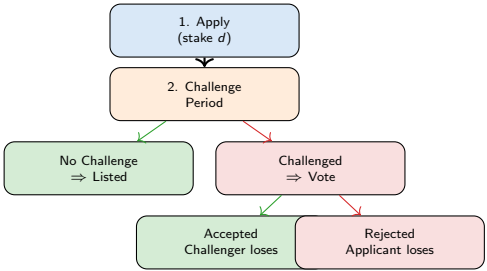
Mechanism

A **TCR** is a decentralised list curated by token holders:

1. Applicant stakes tokens to apply for listing
2. Challenge period: anyone can challenge by staking
3. If challenged $\rightarrow$ token-weighted vote
4. Winner keeps loser's stake (incentive alignment)

Game-Theoretic Incentives

- **Applicants:** Only apply if genuinely qualified (risk losing stake)
- **Challengers:** Only challenge bad applications (risk losing stake)
- **Voters:** Vote honestly (earn share of loser's stake)



TCRs

demonstrate how skin-in-the-game via staking creates self-policing communities

Incentive Failure Modes

Mercenary Capital

- Liquidity providers chase highest APY
- Leave immediately when rewards decrease
- Destabilises protocol TVL
- Solution: time-locked rewards, veCRV model

Sybil Attacks on Airdrops

- Create thousands of wallets
- Qualify each for airdrop criteria
- Dump tokens immediately
- Solution: identity verification, retroactive criteria

Governance Attacks

- Flash loan to acquire voting power
- Pass malicious proposal in single tx
- Example: Beanstalk $182M governance attack (2022)
- Solution: time-locks, vote-escrow, snapshot voting

Death Spirals

Reflexive feedback loops where falling price triggers more selling:

1. Price drops → collateral under-backed
2. Liquidations fire → more selling pressure
3. Confidence collapses → bank run
4. Example: UST/LUNA May 2022

Every incentive mechanism has attack vectors – adversarial thinking is essential in tokenomic design

Quadratic Voting & Quadratic Funding

Quadratic Voting (QV)

In standard token voting, 1 token = 1 vote $\Rightarrow$ plutocratic.

QV: Cost to cast v votes = v^2 tokens.

$$\text{Cost}(v) = v^2 \quad \Rightarrow \quad v = \sqrt{\text{tokens spent}}$$

- Buying 1 vote costs 1 token, 2 votes cost 4, 10 votes cost 100
- Reduces whale dominance: a whale with 10,000 tokens gets 100 votes, not 10,000
- Expresses *preference intensity* – voters can allocate more to issues they care about

QV Comparison

Tokens	1-token-1-vote	QV ($\sqrt{}$)
1	1	1
100	100	10
10,000	10,000	100
1,000,000	1,000,000	1,000

Quadratic Funding (Gitcoin Grants)

Matching formula from Buterin, Hitzig & Weyl (2019):

$$F_i = \left(\sum_{j=1}^{n} \sqrt{c_{ij}} \right)^2$$

where c_{ij} is contributor j's donation to project i.

Key property: Many small contributions are amplified more than few large ones.

Example: Project A gets \$1 from 100 people; Project B gets \$100 from 1 person.

- Direct total: both receive \$100
- QF matching: $A = (100 \times \sqrt{1})^2 = \$10{,}000$; $B = (1 \times \sqrt{100})^2 = \$100$
- Project A receives 100$\times$ more matching – reflecting broader support

Challenges

- Sybil attacks: split one identity into many to game matching
- Collusion: coordinated voting rings
- Solutions: Gitcoin Passport, MACI (anti-collusion infrastructure)

Hitzig & Weyl, "Liberal Radicalism" (2019) – QF has distributed \$50M+ via Gitcoin to public goods

Buter

Section 3 Summary: Incentive Design

Key Concepts

1. Mechanism design engineers rules for desired outcomes
2. Slashing transforms games to make honesty dominant
3. Staking APY self-regulates via supply/demand
4. Quadratic voting reduces plutocratic governance
5. Schelling points enable decentralised consensus

Failure Modes to Watch

- Mercenary capital (short-term LPs)
- Flash loan governance attacks
- Sybil attacks on airdrops
- Death spirals (reflexive loops)
- MEV extraction by block producers

Next Section

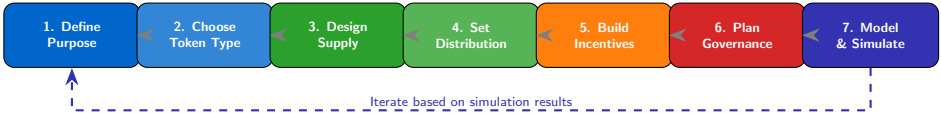
$\Rightarrow$ **Token Design Framework:** Step-by-step methodology for designing your own token economy.

Good mechanism design assumes all participants are rational and self-interested – then proves honesty is optimal

Section 4: Token Design Framework

Systematic methodology for designing sustainable token economies

Token Design Methodology: 7-Step Framework



1. What problem does the token solve?
2. Utility, governance, or hybrid?
3. Fixed, inflationary, or deflationary supply?
4. Fair launch, ICO, airdrop, or mining?
5. What rewards holding? What penalises misbehaviour?
6. Who decides what? How do votes work?
7. Agent-based simulation before launch

Token design is iterative – simulate extensively before deployment because smart contracts are immutable

Value Capture Mechanisms

How Tokens Capture Value

1. **Fee capture:** Protocol fees flow to token holders (Sushi, Curve)
2. **Buyback & burn:** Revenue buys and destroys tokens (BNB)
3. **Work token:** Must stake to earn right to perform work (LINK, GRT)
4. **Collateral:** Token used as collateral in the system (MKR, AAVE)
5. **Access:** Token required to use platform features (FIL, AR)

Mechanism	Example	Strength
Fee sharing	CRV	Direct yield
Buyback/burn	BNB	Deflationary
Work token	LINK	Demand-driven
Collateral	MKR	Systemic need
Access gate	FIL	Usage-driven

The "Governance Only" Trap

Tokens with *only* governance rights struggle to capture value. Governance alone is not enough demand driver.

Stron

value capture = strong reason to buy & hold – without it, tokens trend toward zero

Token Distribution Strategies

Distribution Methods

- **Fair Launch:** No pre-mine, no VC allocation (BTC, YFI)
- **ICO/IDO:** Public sale at fixed or dynamic price
- **Airdrop:** Free distribution to early users (UNI, ENS)
- **Liquidity Mining:** Earn tokens by providing liquidity
- **VC Rounds:** Seed, Series A, etc. with vesting

Distri

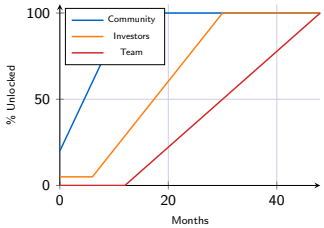
determines who controls the network – prioritise community allocation for decentralisation

Vesting Schedules & Cliff Periods

Vesting Terminology

- **TGE (Token Generation Event):** Initial token creation
- **Cliff:** Period before any tokens unlock
- **Linear vesting:** Tokens unlock gradually over time
- **TGE unlock:** Percentage available immediately

Stakeholder	TGE	Cliff	Vesting
Team	0%	12 mo	36 mo linear
Investors	5%	6 mo	24 mo linear
Community	20%	0	12 mo linear
Advisors	0%	6 mo	24 mo linear



team vesting signals commitment – investors scrutinise vesting schedules for alignment

Token Vesting: Solidity Implementation

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

import "@openzeppelin/contracts/token/ERC20/IERC20.sol";

contract TokenVesting {
    IERC20 public token;
    address public beneficiary;
    uint256 public start;
    uint256 public cliff;     // cliff duration in seconds
    uint256 public duration;  // total vesting duration
    uint256 public released;

    constructor(IERC20 _token, address _beneficiary,
                uint256 _cliff, uint256 _duration) {
        token = _token;
        beneficiary = _beneficiary;
        start = block.timestamp;
        cliff = _cliff;
        duration = _duration;
    }

    function releasable() public view returns (uint256) {
        return vestedAmount() - released;
    }

    function vestedAmount() public view returns (uint256) {
        uint256 total = token.balanceOf(address(this)) + released;
        if (block.timestamp < start + cliff) return 0;
        if (block.timestamp >= start + duration) return total;
        return total * (block.timestamp - start) / duration;
    }

    function release() external {
        uint256 amount = releasable();
        require(amount > 0, "Nothing to release");
```

Simple Staking: Solidity Implementation

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

import "@openzeppelin/contracts/token/ERC20/IERC20.sol";

contract SimpleStaking {
    IERC20 public stakingToken;
    uint256 public rewardRate = 100; // tokens per second
    uint256 public lastUpdateTime;
    uint256 public rewardPerTokenStored;
    uint256 public totalStaked;

    mapping(address => uint256) public staked;
    mapping(address => uint256) public rewards;
    mapping(address => uint256) public userRewardPerToken;

    function stake(uint256 amount) external updateReward(msg.sender) {
        totalStaked += amount;
        staked[msg.sender] += amount;
        stakingToken.transferFrom(msg.sender, address(this), amount);
    }

    function withdraw(uint256 amount) external updateReward(msg.sender) {
        totalStaked -= amount;
        staked[msg.sender] -= amount;
        stakingToken.transfer(msg.sender, amount);
    }

    modifier updateReward(address account) {
        rewardPerTokenStored = rewardPerToken();
        lastUpdateTime = block.timestamp;
        rewards[account] = earned(account);
        userRewardPerToken[account] = rewardPerTokenStored;
        _;
    }

```

Token Launch Checklist

Pre-Launch

- ✓ Token purpose and value proposition defined
- ✓ Supply model and emission schedule set
- ✓ Distribution allocations finalised
- ✓ Vesting schedules for all stakeholders
- ✓ Smart contracts audited (2+ auditors)
- ✓ Legal opinion on token classification
- ✓ Agent-based simulation completed

Launch Day

- ✓ Liquidity pool seeded
- ✓ Token contract verified on Etherscan
- ✓ Initial distribution executed
- ✓ Governance forum live

Post-Launch Monitoring

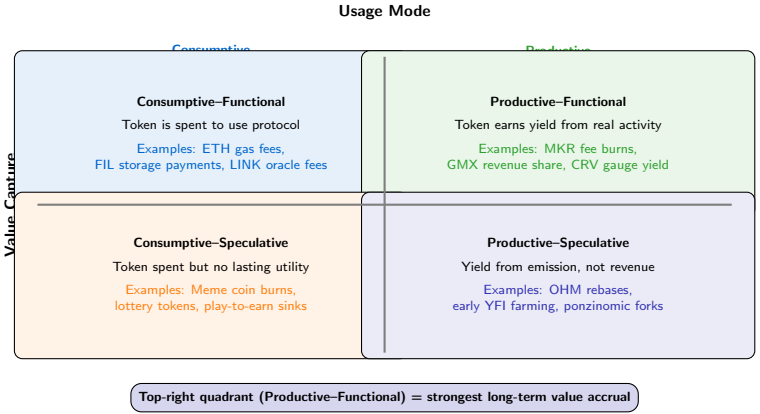
- ✓ Token velocity tracking
- ✓ Holder distribution (Gini coefficient)
- ✓ Governance participation rate
- ✓ TVL and usage metrics
- ✓ Unlock schedule calendar public

Common Launch Mistakes

1. Too much TGE unlock (dumping)
2. No liquidity depth (volatile price)
3. Unclear value capture mechanism
4. Team allocation too high ($>25\%$)

A token launch is like an IPO – meticulous preparation and transparent communication are essential

Token Utility Matrix



Kyle

Samani (Multicoin Capital): classify tokens along these axes before investing – functional + productive = durable value

Regulatory Considerations in Token Design

Howey Test (SEC – U.S.)

A token is a **security** if it satisfies ALL four prongs:

1. Investment of money
2. In a common enterprise
3. With expectation of profits
4. Derived from efforts of others

Implication: Tokens with passive yield from a team's work likely qualify as securities.

Global Regulatory Landscape

Jurisdiction	Approach
U.S. (SEC)	Case-by-case Howey test; enforcement-driven
EU (MiCA)	Comprehensive framework; asset-referenced & e-money tokens regulated from 2024
Singapore (MAS)	Payment tokens exempt; security tokens under SFA
Switzerland (FINMA)	3-tier classification: payment, utility, asset tokens
UAE (VARA)	Activity-based licensing; sandbox regime

Security vs. Utility

- **Utility:** Required to use the protocol (e.g., gas, access)
- **Security:** Purchased for profit expectation (e.g., revenue share)
- **Hybrid:** Many tokens exhibit both characteristics

Design Implications

- Decentralisation can move token outside Howey ("sufficiently decentralised")
- Vesting, lockups, and progressive decentralisation reduce security risk
- Always obtain legal opinion **before** TGE

Regu

classification determines listing eligibility, investor base, and compliance costs – get it right early

Tokenomics Red Flags for Investors

Warning Checklist

	Red Flag
✗	Insider allocation $> 30\%$ of total supply
✗	No vesting schedule for team/investor tokens
✗	Unlimited supply with no burn or sink mechanism
✗	Team tokens unlocked at TGE
✗	No clear value accrual to token holders
✗	FDV/MC ratio $> 10\times$ (extreme future dilution)
✗	Yields funded by emissions, not revenue
✗	Anonymous team with no audit

Healthy Tokenomics Indicators

	Green Flag
✓	Community allocation $\geq 50\%$
✓	12–48 month vesting with cliff
✓	Real yield from protocol revenue
✓	Multiple independent audits
✓	Transparent on-chain treasury
✓	Active governance participation

Quick Heuristic

Score each red flag as -1 and each green flag as $+1$. If total score < 0, **investigate further** before investing. If ≤ -3, **avoid**.

"If you can't find the sucker at the table, you're the sucker" – apply this to tokenomics due diligence

Section 4 Summary: Token Design Framework

7-Step Framework

1. Define purpose (why does the token exist?)
2. Choose type (utility, governance, hybrid)
3. Design supply (fixed, inflationary, deflationary)
4. Set distribution (fair launch, ICO, airdrop)
5. Build incentives (staking, burns, rewards)
6. Plan governance (voting, delegation, time-locks)
7. Model & simulate (agent-based testing)

Solidity Patterns Covered

- Linear bonding curve contract
- Token vesting with cliff and linear unlock
- Synthetix-style staking rewards

Next Section

⇒ **Case Studies & Pitfalls:** Real-world tokenomics analysis of UNI, MKR, CRV, and lessons from failures.

Theo

meets practice – the next section examines how leading protocols implement these principles

Section 5: Case Studies & Pitfalls

Real-world tokenomics successes, failures, and lessons learned

Case Study: UNI – Governance Token Design

Token Overview

Property	Value
Type	Governance
Max Supply	1 billion UNI
Distribution	60% community, 21.5% team
Launch	Sept 2020 (retroactive airdrop)
Value Capture	Governance only (fee switch pending)

Strengths

- Retroactive airdrop rewarded genuine users
- 400 UNI to 250K+ addresses ("fair" distribution)
- Strong brand and community loyalty

Weaknesses

- **No fee switch:** UNI holders don't earn protocol fees
- **Low turnout:** 3–5% governance participation
- **Whale dominance:** Top 10 wallets control 40%+ voting power
- **2% annual inflation** after 4-year distribution

Lessons Learned

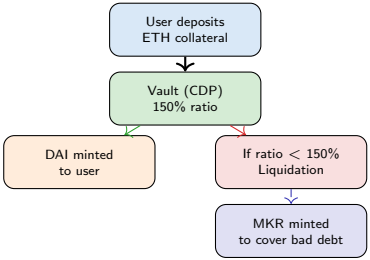
- Governance-only tokens struggle with value capture
- Retroactive airdrops create strong initial distribution
- Delegation helps but doesn't solve low turnout

UNI's fee switch debate highlights the tension between protocol growth and token holder returns

Case Study: MKR/DAI – Dual-Token System

Dual-Token Architecture

- **DAI:** Stablecoin pegged to $1 (user-facing)
- **MKR:** Governance + recapitalisation token



MKR Tokenomics

- **Fee revenue:** Stability fees paid in DAI, used to buy and burn MKR
- **Backstop:** If system insolvent, new MKR is minted (dilution penalty)
- **Governance:** MKR holders set risk parameters

Key Innovation

MKR holders bear the downside risk (dilution in crisis) and earn the upside (burn from fees). This aligns incentives for good governance.

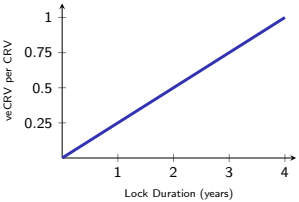
Make

pioneered the dual-token model – MKR aligns governance with risk bearing

Case Study: CRV – Vote-Escrowed Tokenomics (veCRV)

veCRV Mechanism

- Lock CRV for 1 week to 4 years → receive veCRV
- veCRV = non-transferable, decays linearly to zero
- More lock time = more voting power and yield boost



veCRV Formula

$$\text{veCRV} = \text{CRV} \times \frac{t_{\text{remaining}}}{t_{\text{max}}}$$

where $t_{\text{max}} = 4$ years. Locking 100 CRV for 4 years gives 100 veCRV; for 1 year gives 25 veCRV.

The Curve Wars

Protocols bribe veCRV holders to direct CRV emissions to their pools. Convex Finance controls 40%+ of veCRV.

Benefits

- Up to 2.5× yield boost for LPs
- Voting power over CRV emissions (gauge weights)
- Share of 50% of protocol trading fees

veCR

solved mercenary capital – long-term lockers govern the protocol, reducing velocity

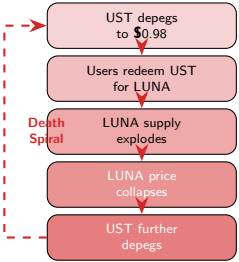
Case Study: LUNA/UST – The $40B Death Spiral

Algorithmic Stablecoin Mechanism

- UST peg maintained by mint/burn with LUNA
- $1 UST can always be redeemed for $1 of LUNA
- If UST $< \$1$: burn UST, mint LUNA (arbitrage profit)
- If UST $> \$1$: burn LUNA, mint UST

What Went Wrong (May 2022)

1. Large UST sell-off $\rightarrow$ UST depegged to $0.98
2. Arbitrageurs burned UST, minted massive LUNA
3. LUNA supply exploded: 350M $\rightarrow$ 6.5 trillion
4. LUNA price collapsed $\rightarrow$ UST further depegged
5. Reflexive death spiral: both assets $\rightarrow$ $0



LUNA is the most expensive tokenomics failure in history – $40B in value destroyed in 72 hours

Comparing Real-World Token Models

Dimension	UNI	MKR	CRV	LUNA	ETH
Type	Governance	Gov + Backstop	Gov + Yield	Collateral	Native coin
Supply	1B fixed	Elastic	3.03B max	Elastic	No cap
Value capture	Weak	Strong	Strong	Reflexive	Fee burn
Velocity sink	Delegation	Burn	veLock	Stake	Stake
Distribution	Airdrop	Sale	Mining	Sale	Mining
Governance	Direct vote	Direct vote	Gauge vote	Validators	–
Resilience	High	High	High	Failed	High

Success Patterns

- Multiple value capture mechanisms
- Aligned incentives (skin in the game)
- Velocity sinks (staking, locking)
- Gradual token unlock

Failure Patterns

- Reflexive/circular value backing
- Unsustainable yield promises
- Concentrated token holdings
- No intrinsic demand driver

Study

both successes and failures – the difference often lies in the robustness of value capture

Common Tokenomics Pitfalls

1. Ponzi Dynamics

- Returns funded by new entrants, not real yield
- Steep bonding curves that only reward early buyers
- **Red flag:** "guaranteed" yields $>$ 100% APY

2. Governance Capture

- Whales accumulate voting power
- Pass proposals benefiting insiders
- **Red flag:** Top 10 addresses hold $>$50% supply

3. Emission Cliff

- High initial rewards attract users
- Rewards drop sharply $\rightarrow$ users leave
- TVL collapses, token price follows

4. Insufficient Liquidity

- Thin order books cause extreme volatility
- Large holders cannot exit without crashing price
- **Solution:** Ensure deep initial liquidity

5. Regulatory Risk

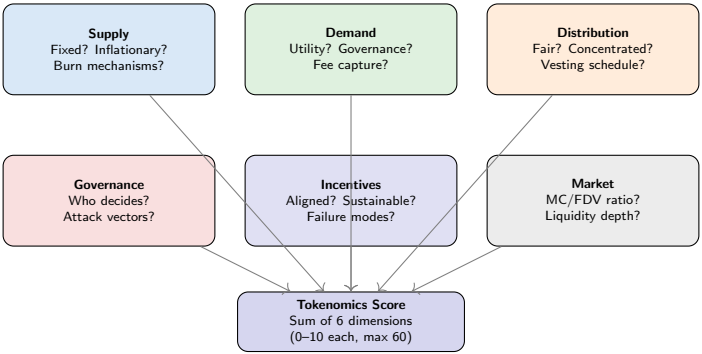
- Token classified as unregistered security
- SEC enforcement actions (XRP, LBRY)
- **Mitigation:** Legal opinion before launch

Due Diligence Questions

- Where do the yields come from?
- Who bears the risk?
- What happens if price drops 80%?
- Is the token actually needed?

"If you can't explain where the yield comes from, you are the yield" – crypto investing wisdom

Tokenomics Analysis Framework



Use this 6-dimension framework to systematically evaluate any token's economic design

The Future of Tokenomics

Emerging Trends

1. **Real-World Assets (RWA):** Tokenised treasuries, real estate, commodities
2. **Account abstraction:** Gas-free token interactions (ERC-4337)
3. **Soulbound tokens (SBTs):** Non-transferable identity/reputation
4. **Dynamic NFTs:** Token properties that evolve based on on-chain data
5. **Restaking:** EigenLayer-style shared security tokenomics

Regulatory Evolution

- EU MiCA framework (effective 2024)
- SEC vs. Ripple precedent
- "Sufficiently decentralised" doctrine
- Compliance-by-design tokenomics

Research Frontiers

- Agent-based token simulation (cadCAD, TokenSPICE)
- Formal verification of token mechanisms
- Cross-chain tokenomics and bridge design
- AI-assisted mechanism design

Token

is a young field – the best designs of the next decade haven't been invented yet

Lecture Summary & Key Takeaways

5 Sections Covered

1. **Token Fundamentals:** Types, supply models, velocity
2. **Bonding Curves:** Linear, polynomial, Bancor, sigmoid, $xy = k$
3. **Incentive Design:** Game theory, staking, slashing, MEV
4. **Design Framework:** 7-step methodology, vesting, launch
5. **Case Studies:** UNI, MKR, CRV, LUNA failures

Golden Rules of Tokenomics

1. Design for rational, self-interested actors
2. Create sinks to reduce velocity
3. Align incentives: skin in the game
4. Never back a token with itself (no reflexivity)
5. Simulate before deploying
6. Start with "Does this need a token?"

Solidity Patterns

- Linear bonding curve (mint/burn)
- Token vesting with cliff
- Synthetix-style staking rewards

Further Reading

- Vitalik Buterin: "Token Sales" (2017)
- Placeholder VC: "Cryptonetwork Governance"
- Gauntlet: cadCAD simulation framework

The best tokenomics creates systems where selfish behaviour produces collective benefit

Thank you!

Questions & Discussion

Key Question to Take Away:

"For any token you encounter, ask:

Where does the value come from, and who bears the risk?"

Conta

joerg.osterrieder@university email — Course materials available on GitHub Pages