#10 Automated Market Makers (AMMs)

Lecture Notes for CS190N: Blockchain Technologies and Security November 3, 2025

The foundation of decentralized finance (DeFi) rests on the promise of open, programmable money. While core crypto assets like Ethereum (ETH) and Bitcoin (BTC) are revolutionary, their inherent volatility makes them challenging to use as a stable "unit of account" or a reliable medium of exchange. It's like trying to build a financial application with a measuring tape that unpredictably stretches and shrinks. While the stablecoins discussed in Lecture 10 address the issue of value volatility, a new challenge emerges: how to provide efficient, continuous trading liquidity for these assets and the broader crypto market without relying on traditional, centralized order books?

The order book model relies on buyers and sellers submitting limit orders, requiring a centralized entity to match trades. Implementing this on-chain presents numerous challenges, including high gas fees, inefficiency, and scalability issues. To solve this fundamental problem, the core innovation of decentralized exchanges (DEXs), Automated Market Makers (AMMs), was born. An AMM is a smart contract that holds a reserve pool of two or more tokens and uses a predefined mathematical formula (an "invariant") to automatically determine the price and execute trades. This model provides continuous, permissionless on-chain liquidity without a central party or an order book. This lecture will delve into three primary AMM designs, their underlying mathematics, and their respective trade-offs and use cases.

1 CONSTANT-SUM MARKET MAKER (CSMM): A THEORETICAL IDEAL

1.1 The Linear Invariant

The starting point for exploring AMM design is to consider the simplest possible pricing mechanism. The Constant-Sum Market Maker (CSMM) is one such model, which maintains a simple linear invariant:

$$x + y = k \tag{1}$$

where x and y represent the reserves of two tokens (X and Y), and k is a constant that remains unchanged when no liquidity is added or removed. Graphically, this invariant is represented by a straight line with a slope of -1. Intuitively, it means that for every increase in one token's reserve, the other token's reserve must decrease by an equal amount to keep the sum constant.

1.2 The Promise of Zero Slippage

The most appealing feature of the CSMM model is its promise of "zero slippage". When a trader deposits Δx of token X to receive token Y, the new reserves will be $x' = x + \Delta x$ and $y' = y - \Delta y$. To maintain the invariant, the new reserves must satisfy:

$$(x + \Delta x) + (y - \Delta y) = k \tag{2}$$

Because $x + y = k$, we can cancel x and y from both sides of the equation to get:

$$\Delta x - \Delta y = 0 \Rightarrow \Delta y = \Delta x \tag{3}$$

This derivation shows that no matter the trade size, Δx, the trader will always receive an equal amount of token Y at a fixed 1:1 exchange rate. In other words, the price offered by the pool is constant, and trades generate no price impact. This is ideal for traders, as they can execute any size trade at a perfectly predictable price, right up until one of the pool's reserves is exhausted.

1.3 The Fatal Flaw: Fragile, Finite Liquidity

While the CSMM model is mathematically perfect, it has a fatal flaw in practice. Its core advantage, a perfect, fixed price, is also its inherent, unsustainable weakness. The fundamental problem with this model is its inability to react to external market price changes.

Suppose the tokens X and Y in the pool are initially trading at a 1:1 ratio on an external market, but for some reason, the external price deviates, for example, to 1.1 Y per X. A savvy arbitrageur will immediately spot a risk-free profit opportunity. They will continuously swap token Y for token X at the fixed 1:1 rate. Since the pool's price never changes to reflect the external market shift, the arbitrageur will continue this trade until all of token X in the reserve is completely drained. Once a reserve is depleted, the pool becomes useless and can no longer provide any liquidity. Thus, a pure CSMM is almost never used alone, as it faces a massive risk of being completely drained unless the tokens have an unbreakable, perfectly synchronized peg with the external market.

2 CONSTANT-PRODUCT MARKET MAKER (CPMM): THE GENERAL-PURPOSE SOLUTION

2.1 The Hyperbolic Invariant

To solve the liquidity depletion problem of CSMM, a more robust AMM model was proposed and pioneered by Uniswap v2: the Constant-Product Market Maker (CPMM). The core of the CPMM is its invariant:

$$x \cdot y = k \tag{4}$$

Unlike the linear relationship of CSMM, CPMM maintains a constant product of the two token reserves. The graph of this invariant is a hyperbola whose unique characteristic is that it never intersects the axes. This visual property directly reflects the model's core design: no matter how large a trade is, the pool's reserves of either token can never be fully exhausted, thus providing "infinite range" liquidity.

2.2 The Trade-Off of Infinite Liquidity

The CPMM design cleverly links the trade price to the current state of the pool's reserves. When a trader adds Δx of token X to the pool, the new reserves will be $x' = x + \Delta x$ and $y' = y - \Delta y$. To maintain the invariant, the following condition must be met:

$$(x + \Delta x)(y - \Delta y) = k = xy \tag{5}$$

Solving for Δy, we can find the amount of token Y the trader receives:

$$y - \Delta y = \frac{xy}{x + \Delta x} \Rightarrow \Delta y = y - \frac{xy}{x + \Delta x} \tag{6}$$

To simplify further, we can find a common denominator for the right side:

$$\Delta y = \frac{y(x + \Delta x) - xy}{x + \Delta x} = \frac{xy + y\Delta x - xy}{x + \Delta x} \tag{7}$$

Finally, we get the output formula:

$$\Delta y = \frac{\Delta x \cdot y}{x + \Delta x} \tag{8}$$

This formula shows that the amount of token Y a trader receives is always less than what they would get if they traded at the initial price of y/x. As Δx increases, the denominator $x + \Delta x$ also gets larger, causing the ratio of Δy to Δx to become progressively smaller. This is the inherent price impact of the CPMM model.

2.3 Understanding Slippage and Price Impact

In CPMM, the trade price is not constant. The marginal price (or instantaneous rate) is the slope of the hyperbola at a given reserve point, represented as $P_{X\to Y} = \frac{y}{x}$. This ratio changes in real-time with every trade.

Slippage is defined as the difference between the average execution price a trader receives and the marginal price at the start of the trade. For a CPMM, the larger the trade size, the greater the price impact, leading to a greater deviation between the effective price and the marginal price. This price impact is not a flaw but a crucial safety mechanism. When the pool's price deviates from the external market, arbitrage trades become profitable, continuing until the pool's internal y/x ratio aligns with the global market price. This built-in feedback loop ensures that the CPMM pool's quoted price accurately reflects market changes over time.

Let's consider a concrete example to quantify slippage. Assume a Uniswap v2 pool with initial reserves of 50 million USDC and 50 million DAI. A trader wants to swap 1 million USDC for DAI.

- **Initial State:** $x = 50,000,000$, $y = 50,000,000$.
- **Invariant:** $k = x \cdot y = (50,000,000)(50,000,000) = 2.5 \times 10^{15}$.
- **Post-Trade Reserves:** The trader deposits $\Delta x = 1,000,000$ USDC, making the new USDC reserve $x' = 51,000,000$.
- **Calculate New DAI Reserve:**

$$y' = \frac{k}{x'} = \frac{2.5 \times 10^{15}}{51,000,000} \approx 49,019,607.84 \tag{9}$$

- **Calculate DAI Received:**

$$\Delta y = y - y' = 50,000,000 - 49,019,607.84 \approx 980,392.16 \text{ DAI} \tag{10}$$

- **Calculate Effective Price:**

$$\text{Effective Price} = \frac{\text{Output DAI}}{\text{Input USDC}} = \frac{980,392.16}{1,000,000} \approx 0.9804 \tag{11}$$

- **Calculate Price Impact:**

$$\text{Price Impact} = \frac{\text{Initial Price} - \text{Effective Price}}{\text{Initial Price}} = \frac{1.0 - 0.9804}{1.0} \approx 1.96\% \tag{12}$$

Compared to CSMM's zero slippage, the CPMM model introduces significant price impact in exchange for its robustness and infinite liquidity. However, it is this "exponentially worse" price curve that ensures the AMM can function securely even with large trades and prevents the pool from being drained, solving the fundamental flaw of the CSMM.

3 HYBRID CONSTANT-FUNCTION MARKET MAKER (CFMM): CURVE'S STABLESWAP

3.1 Combining the Best of Both Worlds: The StableSwap Invariant

While CPMM is a general-purpose and robust AMM model, it is inefficient for certain asset types, such as stablecoins like USDC and DAI. These assets are designed to maintain a fixed 1:1 price, but as the example above shows, a CPMM would incur nearly 2% slippage on even a moderately sized trade. To solve this problem, Curve Finance introduced an innovative model specifically for stablecoins, StableSwap.

StableSwap is a Constant-Function Market Maker (CFMM) that aims to combine the low-slippage benefits of CSMM with the infinite-liquidity safety of CPMM. Its invariant formula for a two-token pool is quite complex, reflecting this hybrid design:

$$A(x+y)+D=AD+\frac{D^3}{4xy} \tag{13}$$

This formula cleverly combines the linear term from CSMM, $A(x+y)$, with the product term from CPMM, $\frac{D^3}{4xy}$. Here, x and y are the token reserves, D represents the total liquidity, and A is a critical parameter known as the **Amplification Coefficient**.

3.2 The Role of the Amplification Coefficient (A)

The amplification coefficient A is the key tuning lever in the StableSwap model. A higher A value makes the invariant curve much flatter around the equilibrium point (i.e., when $x \approx y$), causing its behavior to more closely resemble a constant-sum model. This results in extremely low slippage for trades in most scenarios (i.e., when stablecoin prices remain close to 1:1).

StableSwap's innovation lies in its approach to liquidity. Instead of distributing liquidity evenly across the entire price range like CPMM, it uses the amplification coefficient to **concentrate** the vast majority of its liquidity around the expected stablecoin peg point (e.g., 1:1). This concentration strategy significantly boosts capital efficiency, allowing for large trades to be executed with minimal price impact.

When the pool's asset ratio begins to seriously imbalance, the invariant curve transitions from its flat, linear-like segment to a CPMM-style hyperbolic shape. This mechanism ensures that the pool will not be completely drained even in a market panic or extreme imbalance, preserving the safety features of the constant-product model. Thus, StableSwap perfectly achieves its design goal: providing near-zero slippage around the peg while retaining an infinite range of liquidity for extremes.

4 CASE STUDY: UNISWAP V2 VS. CURVE FOR STABLECOIN SWAPS

4.1 The Problem of General-Purpose Design

This case study highlights the key differences between a general-purpose AMM model (Uniswap v2's CPMM) and a purpose-built AMM model (Curve's StableSwap CFMM). While Uniswap v2 is a cornerstone of DeFi due to its simple, universal, and powerful design, its CPMM invariant is not optimized for all asset types. For a volatile pair like ETH/BTC, the CPMM curve is ideal because it provides liquidity across the entire price range. However, for stablecoins like USDC/DAI, where the price is expected to be fixed, the CPMM's generality leads to inefficiency and high slippage.

4.2 Quantitative Comparison: Re-examining the $1M Swap

Let's re-examine the trade of swapping 1 million USDC for DAI, assuming the pool's initial reserves are 50 million USDC and 50 million DAI. By analyzing each AMM model, we can quantify their performance differences on the same trade.

- **CPMM (Uniswap v2):**
  - As calculated in section 3.3, a 1 million USDC trade would result in an output of approximately 980,392 DAI.
  - The effective price is about 0.9804 DAI/USDC, a drop of roughly 1.96% from the ideal 1:1 price.
- **CSMM (Constant-Sum):**

  - Theoretically, this model would yield exactly 1,000,000 DAI with zero price impact. However, as discussed, this pool is unsafe in reality and could be drained by arbitrageurs.
- **StableSwap (Curve):**
  - Due to its high amplification coefficient, the StableSwap curve is extremely flat near the equilibrium point, behaving almost like a CSMM.
  - For this 1 million USDC trade, it would yield an output very close to 1,000,000 DAI, for example, approximately 999,990 DAI.
  - The resulting slippage is negligible, around 0.001%.

4.3 Table: Slippage Comparison Analysis

The table below visually summarizes the results of the three AMM models on the same stablecoin trade, clearly demonstrating their respective performance and design trade-offs.

AMM Model	Output (DAI)	Effective Price (DAI/USDC)	Price Impact (vs. 1.0)
CPMM ($x \cdot y = k$)	~980,392	~0.9804	~1.96% ↓
CSMM ($x + y = k$)	1,000,000	1.0000	0%
Curve StableSwap	~999,990	~0.99999	~0.001% ↓

5 CONCLUSION: THE EVOLUTION OF AMM DESIGN

The evolution from CSMM to CPMM and then to CFMM is not just a progression in mathematical formulas but a maturation of AMM design philosophy from simple to complex, and from general to specialized. Each model represents an exploration of different design trade-offs:

- **Constant-Sum (CSMM)** pursues a perfect, fixed price but at the cost of unsustainable, finite liquidity.
- **Constant-Product (CPMM)** abandons the fantasy of a fixed price in exchange for the powerful ability to provide liquidity across any price range. It uses predictable slippage to ensure the protocol's resilience, making it the ideal general-purpose solution for most volatile assets.
- **Constant-Function (CFMM)** represents the specialization and optimization of AMMs. It recognizes the unique nature of stablecoins and, through a hybrid model, concentrates liquidity where it is most needed. This design provides near-CSMM trading efficiency while retaining the security of the CPMM.