#8 DeFi Overview: Money Legos

Lecture Notes for CS190N: Blockchain Technologies and Security October 27, 2025

This lecture provides a top–down introduction to Decentralized Finance (DeFi) and its core design principle: composability. We begin with a system overview, then ground the stack in its most basic financial asset: USD-pegged stablecoins. With assets in hand, we study trading via automated market makers (AMMs), which enable decentralized exchange (DEX) and on-chain price discovery. Leveraging these prices, we examine collateralized lending markets and then extend to higher-order combinations of lending and trading through perpetual futures (perps). We conclude with two cross-cutting themes that shape safety and governance in DeFi: MEV (Maximal Extractable Value) as a security/economic risk, and DAOs as the mechanism for protocol evolution. Throughout, we emphasize how each layer snaps into the next, stablecoins → AMMs → lending → perps, illustrating why DeFi's "Money Legos" matter for both functionality and risk.

1 INTRODUCTION: WHAT IS DEFI AND WHY DOES IT MATTER?

- **DeFi (Decentralized Finance):** An open financial system built on public blockchains (mostly Ethereum) enabling peer-to-peer financial services (lending, borrowing, trading) through smart contracts, without traditional intermediaries (banks, exchanges).
- **Trustless & Permissionless:** Users interact directly via code on a transparent ledger. No need to trust a CEO or centralized institution. Anyone with an internet connection can access services; transactions are public and verifiable.
- **Cost and Risk Reduction:** Removing middlemen can lower fees and counterparty risk. Code-enforced rules mean less room for hidden insolvency or fraud.
- **Example – FTX Collapse (2022):** Centralized exchange FTX failed and customers lost billions in a "black box" failure. In contrast, DeFi protocols continued operating transparently. In the week after FTX's collapse, decentralized exchange (DEX) trading volume more than doubled (from $20B to $50B) as users flocked to trustless, on-chain alternatives.
- **Core Promise of DeFi:** An **"open, free, and fair"** global financial system. This lecture is a high-level overview of how DeFi's modular building blocks ("Money Legos") snap together to create this system.

2 COMPOSABILITY: THE POWER OF "MONEY LEGOS"

- **Composability:** DeFi protocols are interoperable modules. Output of one protocol can serve as input to another, enabling complex combinations.
- **Money Legos Analogy:** Each DeFi primitive (stablecoins, exchanges, loans, etc.) is like a Lego brick with standard connections. You can stack them in any order to build new financial products (e.g., deposit a stablecoin into a lending pool, use the interest-bearing token as collateral elsewhere, etc.).
- **Permissionless Innovation:** Anyone (developers or users) can mix and match protocols without seeking permission. This open architecture allows for rapid, creative experimentation and new products (like flash loans or automated yield strategies).
- **Resilience and Agility:** The modular design is *antifragile*: if one brick fails, others can often replace it or route around the failure, similar to swapping Lego pieces. The whole ecosystem can adapt without a single point of failure.

3 STABLECOINS: DIGITAL CASH AS THE FOUNDATION

- **Definition:** Stablecoins are crypto tokens designed to maintain a stable value (usually pegged 1:1 to USD). They function as "digital cash" on blockchains, providing a reliable unit of account.
- **Role in DeFi:** Act as the base currency for the ecosystem. Almost all trading pairs and loans in DeFi use a stablecoin (so users aren't exposed to extreme volatility). They let people "use dollars" on-chain.
- **Types of Stablecoins:**
  - **Fiat-backed:** Like USDC or USDT, each token is (supposedly) backed by real USD in a bank.
  - **Crypto-collateralized:** Like MakerDAO's DAI, backed by overcollateralized crypto assets locked in a smart contract.
  - **Algorithmic:** Rely on code/incentives to adjust supply (e.g. Terra's UST was an example, though algorithmic coins can be risky).
- **Example – MakerDAO's DAI:** Users lock ETH or other crypto as collateral in Maker's smart contract and borrow DAI against it. DAI stays near $1.00. If collateral value falls too much, the smart contract auto-sells (liquidates) collateral to cover the loan, preserving stability.
- **Importance:** Without stablecoins, it's hard to do commerce or credit on-chain because crypto prices swing wildly. Stablecoins give DeFi "dollar-like" money: deposits, loans, and trades can all be denominated in (approximately) $1 tokens.

4 AUTOMATED MARKET MAKERS (AMMS): TRADING VIA CODE

- **Decentralized Exchanges (DEX) with AMMs:** Traditional trading uses order books, but AMMs replace that with smart contract pools. Anyone can swap tokens by interacting with the pool, without a human market-maker.
- **Liquidity Pools:** Each AMM pool holds two tokens (e.g., ETH and DAI). Liquidity providers deposit equal-value amounts into the pool and earn fees when traders swap tokens.
- **Automated Pricing Formula:** Commonly, AMMs use the constant product formula ($x \times y = k$). If you buy one token (reducing x), the price automatically goes up (increasing y) so that the product k stays constant. This adjusts prices in response to trading.
- **Trading Process:** Traders swap Token A for Token B directly with the pool. As a token gets bought (and its reserve decreases), the pool raises its price for the next trader, and vice versa if it's sold.
- **Vending Machine Analogy:** Imagine a candy vending machine that raises the price of candy as it gets low on stock. Similarly, an AMM's formula automatically changes prices as supply levels shift.
- **Advantages:** Always-available liquidity (you don't need a specific counterparty), transparent pricing (algorithmic), no permissions or approvals needed. These pools provide the on-chain price feeds for other protocols.

5 LENDING PROTOCOLS: ROBO-BANKS AND ALGORITHMIC CREDIT

- **Concept:** Protocols like Compound or Aave let anyone lend crypto assets to earn interest, or borrow assets by providing collateral, all through smart contracts instead of a bank.
- **How It Works:** You deposit an asset (e.g., DAI or ETH) into the lending pool. Lenders receive tokens representing their stake, earning interest. Borrowers lock up collateral (usually >100% of loan value) and receive a loan (often in stablecoins).

- **Overcollateralization:** Loans are always overcollateralized (e.g., borrowing up to 75–80% of collateral value). If collateral value falls (because market price dropped), the protocol automatically liquidates enough collateral to repay the loan, protecting lenders.
- **Interest Rates:** Rates float based on supply and demand in the pool. If many people borrow and liquidity is low, the interest rate goes up; if many people lend, the rate falls.
- **"Robo-Bank" Analogy:** Think of it like a global automated pawn shop. You lock your crypto as collateral (like pawning an item) and instantly get a loan (in crypto). Pay back the loan plus interest to retrieve your collateral, or else the contract sells it.
- **Composability:** Lending protocols rely on stablecoins (for loans) and price oracles/DEXs (to set prices for collateral). In turn, they supply interest-bearing tokens (like cTokens or aTokens) that can be used elsewhere in DeFi.

6 DERIVATIVES AND PERPETUALS: ON-CHAIN ADVANCED INSTRUMENTS

- **Derivatives Overview:** These are contracts deriving value from underlying assets. In DeFi, this includes futures, options, synthetic assets, etc., used for hedging or speculation.
- **Perpetual Futures (Perps):** A popular derivative on-chain. Unlike traditional futures, perpetuals have no expiration date. Prices track the spot market via a funding rate mechanism that periodically balances longs and shorts.
- **Mechanics:** Traders can go long or short an asset with leverage. The protocol adjusts the contract price toward the actual market price through funding payments. If demand to long exceeds demand to short (or vice versa), funding rates incentivize traders to take the opposite side.
- **On-Chain Perpetuals:** Protocols like dYdX, GMX, Synthetix (Kwenta) have launched decentralized perpetual exchanges. After centralized venues like FTX failed, these on-chain perpetual DEXs saw huge growth in volume and users, as traders sought transparent, non-custodial platforms.
- **Benefits:** Like other DeFi products, on-chain derivatives offer transparency (anyone can inspect open interest, collateral, and trades) and censorship-resistance (no exchange can freeze your account as long as collateral requirements are met).
- **Other Derivatives:** Beyond perps, DeFi has on-chain options (e.g., Opyn, Lyra), synthetic asset platforms (e.g., Synthetix's synths for stocks or commodities), and prediction markets (e.g., Augur). These are built on top of the basic stack of coins, AMMs, and lending.

7 GOVERNANCE AND MEV: EMERGENT PROPERTIES OF THE DEFI STACK

- **Governance (DAOs and Tokens):** Major DeFi protocols often issue governance tokens (like COMP, UNI, MKR). Holders use these tokens to vote on protocol parameters and upgrades (e.g., interest rates, fee changes, code upgrades). This forms a DAO (Decentralized Autonomous Organization) for each protocol.
- **Decentralized Decision-Making:** Instead of a central CEO or board, protocol changes are proposed by community members and approved by token-holder votes. This "open governance" allows the community to steer the protocol, though it also raises questions about low participation and large holders having outsized influence.
- **Importance of Governance:** It's the mechanism that lets DeFi systems evolve and respond to problems. For example, MakerDAO holders vote to set the DAI stability fee; Uniswap token holders could vote to change the protocol's fee rate. Without governance, protocols would remain static or be controlled by a few developers.
- **MEV (Maximal Extractable Value):** A side-effect of DeFi's transparent, public transaction pools. Miners/validators (or bots) can reorder or insert transactions in a block to capture extra

profit. This includes front-running large trades, sandwich attacks on AMMs, or capturing liquidation bonuses.

- **Examples of MEV:** If someone tries to swap a large amount on Uniswap, a bot might see it in the mempool and buy the token first (front-run) and sell after the big order (back-run), pocketing the price difference. Liquidation bots compete to be first to grab a liquidated collateral, snatching potential discounts.
- **Implications of MEV:** It's often called an "invisible tax" because these opportunities drain value from regular users. It can also impact consensus (e.g., miners prioritizing MEV over fair ordering). The community is developing solutions (like Flashbots auctions, Fair Ordering services, or Ethereum's Proposer-Builder Separation) to mitigate negative effects.