#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 [12].

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

- **The Core Idea:** DeFi (Decentralized Finance) is an attempt to build a global, open alternative to the traditional financial system. Instead of relying on intermediaries like banks and brokerages, it uses smart contracts on public blockchains (mostly Ethereum) to create financial services that are transparent, accessible to anyone, and run 24/7 [4, 12].
- **Trust in Code, Not Companies:** The system is designed to be **trustless**. You don't need to trust a CEO not to misuse your funds; you only need to trust that the open-source code will execute as written. It's also **permissionless**, meaning anyone with an internet connection can use it without asking for approval [12].
- **Why Now? The FTX Example:** The collapse of the centralized exchange FTX in 2022, where billions in customer funds vanished inside a corporate "black box," highlighted the problem DeFi aims to solve. While FTX failed, DeFi protocols operated without interruption because their rules and assets were transparently managed on-chain [12].

2 COMPOSABILITY: THE POWER OF ‘MONEY LEGOS”

- **The Superpower of DeFi:** The core design principle of DeFi is **composability**. Each protocol is like a Lego brick with a standard connector. The output of one protocol can be seamlessly plugged in as the input to another [12].
- **Stacking the Legos:** This allows for incredible innovation. For example, you can take a stablecoin (Lego 1), deposit it into a lending protocol to earn interest (Lego 2), and then use the interest-bearing token you receive as collateral in another protocol (Lego 3). This "stacking" creates new financial products that would be impossible in the siloed world of traditional finance [12].
- **Permissionless Innovation:** Because the system is open, anyone can build a new "Lego" and connect it to the existing stack without asking for permission. This has led to a Cambrian explosion of financial experimentation.

3 STABLECOINS: THE BEDROCK OF THE SYSTEM

- **The Problem:** Native cryptocurrencies like ETH and BTC are too volatile to be used for everyday finance. Imagine taking out a loan where the value of your debt could double overnight.
- **The Solution: Stablecoins** are tokens designed to hold a stable value, usually pegged 1:1 to the US dollar. They are the "digital cash" of the blockchain, providing a reliable unit of account for everything else in DeFi.

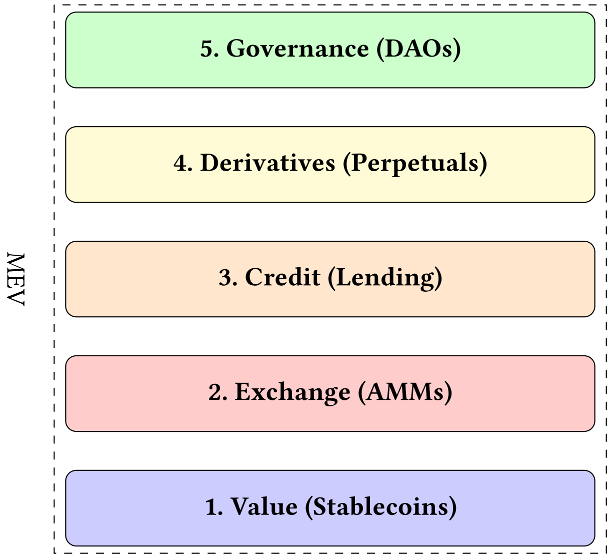
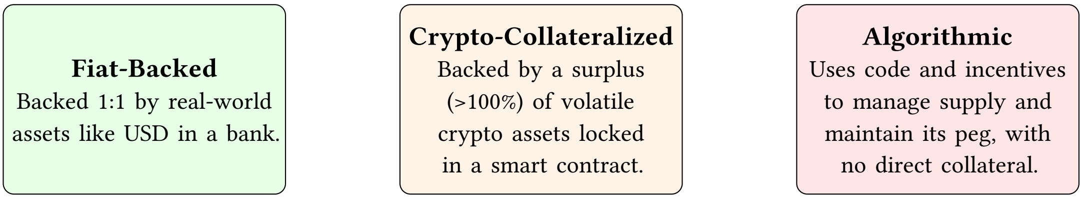


Fig. 1. The DeFi Stack, with each layer building upon the one below it. MEV is an emergent force that affects all layers.

- **How They Work:** There are three main designs for maintaining the peg:
  - **Fiat-Backed:** Each token is backed by one real dollar held in a bank account (e.g., USDC, USDT) [6].
  - **Crypto-Collateralized:** Backed by a surplus of other crypto assets locked in a smart contract. The system is overcollateralized to absorb price shocks (e.g., MakerDAO's DAI) [11].
  - **Algorithmic:** Use code and economic incentives to automatically adjust supply and demand to maintain the peg (historically the riskiest model).


Fiat-Backed
Backed 1:1 by real-world assets like USD in a bank.

Crypto-Collateralized
Backed by a surplus (>100%) of volatile crypto assets locked in a smart contract.

Algorithmic
Uses code and incentives to manage supply and maintain its peg, with no direct collateral.

Fig. 2. The three primary models for stablecoin design.

4 AUTOMATED MARKET MAKERS (AMMS): THE ROBOT MARKET MAKER

- **The Problem:** Traditional exchanges use an **order book**, where buyers and sellers are matched. This is slow, expensive, and difficult to implement on a blockchain. How can you trade assets efficiently in a decentralized way?
- **The Solution: Automated Market Makers (AMMs)**. Instead of an order book, an AMM is a smart contract that holds a pool of two tokens. Anyone can trade directly with this pool.

- **How It Works:** The price is set by a simple mathematical formula, most commonly the **constant product formula ($x \cdot y = k$)**. When you buy a token from the pool, its supply (x) decreases, so the formula automatically increases its price for the next person [2, 3].
- **The Vending Machine Analogy:** Think of an AMM like a smart vending machine. It holds two types of snacks. As people buy more of one snack, the machine automatically raises its price to reflect its increasing scarcity, while lowering the price of the other. It's always ready to trade, 24/7.

5 LENDING PROTOCOLS: THE DIGITAL PAWN SHOP

- **The Problem:** How do you create a credit market where people can lend and borrow from strangers without trusting them?
- **The Solution: Overcollateralized lending**. Protocols like Aave and Compound allow users to borrow assets only if they first lock up collateral that is worth more than the loan [1, 10].
- **How It Works:** A user deposits an asset (e.g., $1,000 of ETH) into a lending pool. They can then borrow another asset (e.g., $750 of USDC) against it. Because the loan is overcollateralized, there is a safety buffer.
- **Automatic Liquidation:** If the value of the collateral drops (e.g., the price of ETH crashes) and gets too close to the value of the loan, the smart contract automatically sells the collateral to repay the loan. This protects the lenders from losing money.
- **The Digital Pawn Shop Analogy:** It works just like a pawn shop. You give the shop a valuable item (collateral) and get cash (a loan). If you don't pay back the loan, the shop keeps your item. In DeFi, this entire process is automated by code.

6 DERIVATIVES AND PERPETUALS: ADVANCED FINANCIAL TOOLS

- **The Problem:** Simple buying and selling isn't enough for a sophisticated financial market. Traders need tools to hedge risk and make leveraged bets on price movements.
- **The Solution: On-chain derivatives**, with **perpetual futures (perps)** being the most popular. A perpetual is a futures contract that never expires, allowing traders to hold a leveraged long or short position indefinitely.
- **How It Works:** The price of the perpetual is kept in line with the actual asset price through a mechanism called the **funding rate**. This is a small fee paid between long and short traders to incentivize them to balance the market [5, 8].
- **Why It Grew:** After the failure of centralized giants like FTX, on-chain perpetual exchanges like dYdX and GMX saw massive growth as traders sought transparent, non-custodial alternatives where their funds couldn't be misused.

7 GOVERNANCE AND MEV: THE RULES OF THE GAME

- **Governance (DAOs):** Who makes the rules for these protocols? The answer is a **DAO (Decentralized Autonomous Organization)**. Governance tokens (like UNI, AAVE, MKR) give holders the right to vote on proposals to upgrade the protocol. This allows the community, not a central company, to steer the future of the system.
- **MEV (Maximal Extractable Value):** This is the "invisible tax" of DeFi. Because all pending transactions are visible in a public mempool, sophisticated bots and block producers can reorder or insert their own transactions to capture profit [7, 9].
- **Examples of MEV:** A bot sees your large trade on Uniswap, buys the token just before you to drive up the price, lets your trade execute at a worse price, and then sells immediately

after for a risk-free profit (a "sandwich attack"). Another bot races to be the first to liquidate an underwater loan to claim the bonus.

- **The Double-Edged Sword:** While some MEV is harmful to users, other forms, like arbitrage between exchanges and liquidations, are essential for keeping the ecosystem efficient and safe. Mitigating the negative effects of MEV is one of the biggest ongoing challenges in blockchain research.

REFERENCES

[1] Aave Protocol. 2025. Aave Documentation. https://docs.aave.com/faq/ Accessed: 2025-10-01.

[2] Hayden Adams, Noah Zinsmeister, and Dan Robinson. 2020. Uniswap v2 Core. https://uniswap.org/whitepaper.pdf Accessed: 2025-10-01.

[3] Guillermo Angeris and Tarun Chitra. 2020. Improved Price Oracles: Constant Function Market Makers. https://arxiv.org/abs/2003.10001 Accessed: 2025-10-01.

[4] Andreas M. Antonopoulos and Gavin Wood. 2018. *Mastering Ethereum: Building Smart Contracts and DApps.* O'Reilly Media.

[5] BitMEX. 2016. Perpetual Contracts Guide. https://www.bitmex.com/app/perpetualContractsGuide Accessed: 2025-10-01.

[6] Circle Internet Financial. 2025. USDC: A Regulated Stablecoin. https://www.circle.com/en/usdc Accessed: 2025-10-01.

[7] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. In *2020 IEEE Symposium on Security and Privacy (SP).* 910–927. doi:10.1109/SP40000.2020.00040

[8] dYdX Foundation. 2025. How dYdX Funding Rates Work. https://docs.dydx.exchange/ Accessed: 2025-10-01.

[9] Flashbots. 2025. Flashbots: Research and Tools for MEV. https://docs.flashbots.net/ Accessed: 2025-10-01.

[10] Robert Leshner and Geoffrey Hayes. 2019. Compound: The Money Market Protocol. https://compound.finance/documents/Compound.Whitepaper.pdf Accessed: 2025-10-01.

[11] Maker Foundation. 2017. The Dai Stablecoin System. https://makerdao.com/whitepaper/ Accessed: 2025-10-01.

[12] Fabian Schär. 2021. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review* 103, 2 (2021), 153–174. doi:10.20955/r.103.153-74 Accessed: 2025-10-01.