L06 — Decentralized Finance (DeFi)

Cheatsheet

DeFi Overview

Core Definition

DeFi = Financial services built on public blockchains without traditional intermediaries.
Key pillars: permissionless, transparent, composable, non-custodial.

Composability ("Money Legos") — Protocols can be stacked and combined freely; each layer builds on layers below enabling rapid innovation.

Permissionless — Anyone with a wallet can participate; no KYC, no credit check, no business hours.

Non-custodial — Users retain control of their private keys and assets; no bank holds funds on their behalf.

The DeFi Stack (bottom to top):

1. *Settlement*: blockchain (Ethereum, Solana)
2. *Asset*: tokens, stablecoins, wrapped assets
3. *Protocol*: AMMs, lending smart contracts
4. *Application*: dApp front-ends
5. *Aggregation*: cross-protocol routing services

Automated Market Makers (AMMs)

Constant Product Formula

$$x \cdot y = k$$

x = reserve of token A, y = reserve of token B, k = invariant. Buying A decreases x, forces y up to preserve k. Larger trades $\Rightarrow$ more **slippage**.

Numerical example: Pool with 100 ETH + 200,000 USDC $\Rightarrow k = 2 \times 10^7$. Buying 1 ETH costs $\approx$ \$2,020 ($\approx$1% slippage).

Liquidity Provision:

- Deposit equal value of both tokens; receive LP tokens.
- Earn trading fees (typically 0.3%).
- Burn LP tokens to withdraw share of pool.

Uniswap v2 — standard $x \cdot y = k$ over full price range.

Uniswap v3 — *concentrated liquidity*: LPs choose a custom price range $[p_a, p_b]$, earning higher fees but exposed to more impermanent loss if price leaves the range.

Curve — optimized for stablecoin pairs; uses a hybrid invariant ($x \cdot y = k + x + y = \text{const}$) for very low slippage near peg.

Impermanent Loss (IL)

IL Formula

$$IL = \frac{2\sqrt{r}}{1+r} - 1, \quad r = \frac{P_{\text{new}}}{P_{\text{initial}}}$$

IL is always ≤ 0; loss is *symmetric*: price doubling and price halving both give $IL \approx -5.7\%$.

r (price ratio)	IL
0.25 (price $\times$0.25)	-20.0%
0.50 (price halved)	-5.7%
1.00 (unchanged)	0%
2.00 (price doubled)	-5.7%
4.00 (price $\times$4)	-20.0%

"Impermanent" because the loss reverses if price returns to entry; it becomes *permanent* upon withdrawal.

Lending Protocols (Aave, Compound)

Depositors (lenders): supply assets $\rightarrow$ earn *supply APY* (variable, paid by borrowers).

Borrowers: deposit overcollateral ($\geq$ 150% of loan value) $\rightarrow$ borrow up to *collateral factor* $\rightarrow$ pay *borrow APY*.

Utilization rate U = Total Borrowed/Total Supplied. Interest rates increase steeply above a "kink" (typically $U = 80\%$) to ensure withdrawal liquidity.

Aave Interest Rate

$$R = R_0 + \frac{U}{U_{\text{opt}}} R_1 + \max\left(0, \frac{U - U_{\text{opt}}}{1 - U_{\text{opt}}}\right) R_2$$

Health Factor

$$HF = \frac{\sum \text{Collateral}_i \times \text{LiqThreshold}_i}{\text{TotalBorrows}}$$

$HF < 1 \Rightarrow$ position can be liquidated.

Liquidation Cascade

Trigger: collateral value falls until $HF < 1.0$.

Process: liquidator repays portion of debt, receives collateral at a 5–10% discount (liquidation bonus), automated and permissionless.

Cascade spiral:

Liquidation $\rightarrow$ forced selling $\rightarrow$ price drop $\rightarrow$ more liquidation

Scale: \$350M+ liquidated within hours during sharp crashes (e.g., May 2021, Nov 2022).

Oracles

Oracle Problem

Blockchains cannot natively read off-chain data. Oracles bridge this gap by supplying price feeds, rates, and event outcomes to smart contracts.

Chainlink: decentralised oracle network; node operators stake LINK, earn rewards for accurate data, get slashed for deviations.

TWAP (Time-Weighted Average Price): average price over a time window; harder to manipulate than spot price but slower to update.

Flash loan oracle attack: borrow large amount $\rightarrow$ manipulate spot price in low-liquidity pool $\rightarrow$ trigger liquidation or exploit $\rightarrow$ repay; all in one transaction. TWAP and multi-source aggregation defend against this.

Yield Farming

Definition: Moving assets across protocols to maximize returns.

Yield sources:

- Trading fees from LP positions
- Supply APY from lending protocols
- Protocol token rewards (liquidity mining)
- Governance token distributions

APY vs. APR: APY compounds continuously; APR does not. $APY = (1 + APR/n)^n - 1$.

Risks: impermanent loss, smart contract exploits, reward token price crash, rug pulls. Sustainable yield is typically 5–20% APY; $> 100\%$ signals very high risk.

Stablecoins in DeFi

Type	Example	Collateral
Fiat-backed	USDT, USDC	USD in banks (1:1)
Crypto-backed	DAI	ETH/WBTC ($\geq$150%)
Algorithmic	UST (failed)	Seigniorage (none)

DAI (MakerDAO): Mint DAI by locking ETH into a Maker Vault; pay stability fee; repay DAI to unlock collateral. Peg maintained by arbitrage: if DAI $>$ \$1, mint & sell; if DAI $<$ \$1, buy & burn.

Terra/UST collapse (May 2022): reflexive design, no real collateral; \$60B market cap wiped in days. Lesson: algorithmic stablecoins carry extreme tail risk.

DEX vs. CEX Comparison

Aspect	CEX	DEX
Custody	Exchange holds	Self-custody
Identity	KYC required	Pseudonymous
Hours	Often 24/7	Always 24/7/365
Settlement	Off-chain (fast)	On-chain (mins)
Liquidity	Order book	AMM / pools
Risk	Counterparty	Smart contract

Gas Fees & EIP-1559

Gas — unit measuring computational effort on the EVM.

Transaction fee = Gas Used $\times$ Gas Price (Gwei). 1 Gwei $= 10^{-9}$ ETH.

EIP-1559 (London, Aug 2021):

- *Base fee*: algorithmically set, **burned**; adjusts to target 50% block fullness.
- *Priority fee* (tip): paid to validator.
- More predictable costs; reduces first-price bidding wars; makes ETH deflationary at high usage.

Flash Loans

Definition

Uncollateralised loans that must be **borrowed and repaid within a single transaction**. If repayment fails, the entire transaction reverts — zero default risk for the protocol.

Legitimate use cases:

- DEX arbitrage (capture price discrepancies risk-free)
- Collateral swap (change collateral type without new capital)
- Self-liquidation (close own position cheaply)

Attack vectors:

- Oracle manipulation (inflate spot price, exploit lending protocol)
- Governance attacks (borrow tokens, vote, repay in one tx)
- Reentrancy combined with flash loan

Invented by Aave; fee typically 0.05–0.09%.

Key DeFi Metrics

Metric	Meaning
TVL	Total Value Locked: sum of crypto assets deposited in a protocol
Volume	24h trading value across DEX pools
Fees	Protocol revenue; distributed to LPs / token holders
APY	Annual yield including compounding
APR	Annual yield excluding compounding
U	Utilization rate = Borrowed / Supplied
HF	Health Factor; liquidation when $HF < 1$
IL	Impermanent loss borne by LPs