Decentralized Finance (DeFi)

A Standalone Mini-Course

BSc Blockchain Course

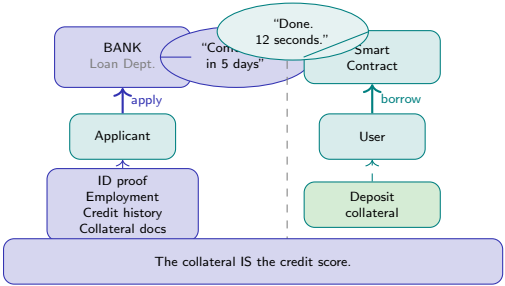
Why Would You Lend Money to a Stranger Without Asking Their Name?

Traditional lending starts with a question: who are you? A bank demands identity documents, employment history, a credit score built over years, and the right address in the right country. Millions of people worldwide fail these filters before a single number is evaluated.

DeFi asks a different question:

- What if collateral replaced identity? Deposit assets that exceed the loan value and borrow instantly – no name, no credit score, no opening hours.
- What if a smart contract replaced the loan officer? Rules encoded in public code execute automatically when conditions are met.
- What if the protocol ran 24 hours a day, every day, for anyone with an internet connection?

The insight at the heart of DeFi: *collateral is the credit score*. You do not prove who you are – you prove you have put something at stake.



DeFi does not ask who you are – it asks what you have put at stake. Collateral replaces credit history; code replaces the loan officer.

DeFi = deposit collateral, borrow instantly, 24/7, no identity check required.

What Happened to Your Money the Last Time a Bank Failed?

You have probably never seen a bank run in person. But millions of people in Cyprus (2013), Greece (2015), Lebanon (2019), and elsewhere watched ATMs run dry and accounts freeze while regulators decided how much of their money they would get back.

Think Before We Continue – Three Prompts

1. **Have you ever been unable to access your own money?** A frozen account, a failed card, a closed branch, a bank holiday that stranded you. How did that feel – and who did you call? Write down the institutions that were between you and your funds.

2. **Have you ever had money in an exchange or platform that collapsed?** In November 2022, FTX – one of the world's largest crypto exchanges – froze withdrawals and filed for bankruptcy overnight. Customers lost billions. The funds were held by FTX, not by the customers. "Not your keys, not your coins" is not a slogan; it is a description of what happened.

3. **What is the difference between a bank bail-in and a bail-out?** In a bail-in (Cyprus 2013), depositors' savings above the insured limit were converted to bank equity to recapitalise the bank. Their money became shares – without their consent. How much of your savings are protected by deposit insurance where you live?

DeFi emerged partly as a response to exactly these failures. Keep these examples in mind as we explore whether the cure introduces new problems.

Custodial risk is real: FTX, Celsius, Voyager – CeFi failures that DeFi's non-custodial model aims to prevent.

What Makes DeFi Different from Your Banking App?

Four financial models – same goal, very different rules:

Feature	Traditional Bank	Fintech App	CeFi Exchange	DeFi Protocol
Identity required	Yes (KYC/AML)	Yes	Yes	None
Operating hours	Business days	24/7 (app)	24/7	24/7
Custody of funds	Bank	Bank/partner	Exchange	User (wallet)
Fees set by	Regulator/board	Company	Company	Algorithm
Permissionless	No	No	No	Yes
Transparent rules	Partial	Partial	Partial	Fully public

The pattern: Read the DeFi column. Every row shows a property that other models restrict or hide. DeFi is the only column where all five constraints are removed simultaneously – at the cost of recourse when things go wrong.

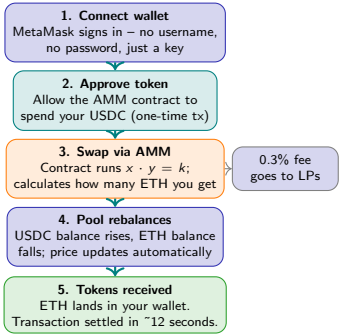
Three defining pillars of DeFi:

- **Permissionless:** Anyone with a wallet address can interact with any protocol. No account application, no geographic restriction, no credit check. A farmer in rural Kenya and a hedge fund in London access the same smart contract at the same fee.
- **Non-custodial:** Your private key controls your assets at all times. The protocol never holds your funds; it holds the logic for what can happen to them. You cannot be "frozen out" by an administrator.
- **Composable:** Protocols are open APIs. One protocol's output is another's input – "money legos" that developers combine without asking permission. Yearn Finance routes deposits through Aave, which uses Chainlink prices, all on Ethereum.

DeFi is not a faster bank – it is a different contract: you trade recourse and customer support for permissionless access and self-custody.

Permissionless + non-custodial + composable = the three pillars that define DeFi.

Follow One DeFi Trade: From Wallet to Liquidity Pool and Back



What is actually happening at each step:

1. Your wallet is your identity. Connecting it is signing a message with your private key – nothing is sent to any server. The protocol sees only your address.

2. Approvals are a safety mechanism: you explicitly allow a specific contract to move a specific amount. Approving does not move funds; it just unlocks the door.

3. The AMM is a formula, not a person. The constant-product rule ($x \cdot y = k$) determines the price. Larger swaps move the curve more – this is slippage.

4. Every swap rebalances the pool automatically. As ETH becomes scarcer in the pool, its price rises. Arbitrageurs align this with external market prices.

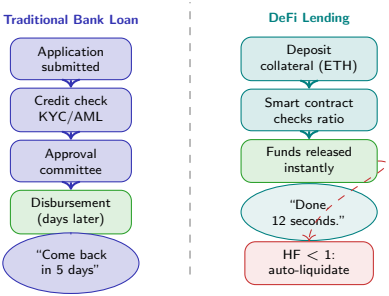
5. Settlement is atomic: either the full swap completes in one block or the transaction reverts entirely. There is no partial execution.

The entire process involves no human counterparty, no order book, and no credit relationship.

A DeFi swap is a call to a public function in a smart contract. The "exchange" is a formula; the "market maker" is a pool of tokens locked by liquidity providers who earn fees.

AMM = automated market maker; LP = liquidity provider; $x \cdot y = k$ = the constant-product pricing rule.

How Can a Smart Contract Replace a Bank's Entire Lending Department?



The key substitutions:

- **Loan officer → Smart contract:** The contract holds the rules. It cannot be bribed, go on holiday, or apply inconsistent judgment. If your collateral ratio is above the threshold, the borrow executes.
- **Credit score → Collateral ratio:** You deposit assets worth more than you borrow. The excess is the bank's protection. No employment history required.
- **Collections department → Liquidation bot:** If your collateral value drops below the threshold, an automated liquidation occurs within the same block. There is no negotiation window.

Health factor:

$$HF = \frac{\text{Collateral} \times \text{Liq. Threshold}}{\text{Debt}}$$

When $HF < 1$, liquidation is triggered automatically.

The smart contract does not trust the borrower – it holds their collateral. Rules execute mechanically; outcomes are deterministic. There is no loan officer because there is no judgment required.

Collateral replaces identity; the health factor replaces the collections department; liquidation bots replace the courts.

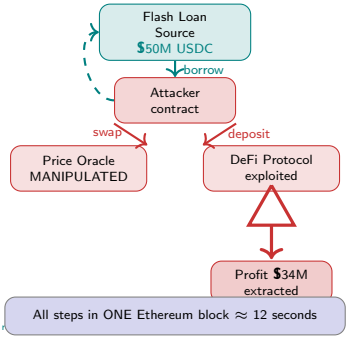
The Pool Drained in Twelve Seconds – A Flash Loan Exploit in Slow Motion

Flash loans: uncollateralised borrowing for one block A flash loan lets anyone borrow millions of dollars with zero collateral, provided the entire amount is repaid within the same Ethereum transaction. If repayment fails, the whole transaction reverts – as if it never happened. This is legitimate; it powers arbitrage and liquidations.

The exploit playbook (Harvest Finance, 2020):

1. Borrow $50M USDC via flash loan from Uniswap – no collateral, zero cost.
2. Swap a large fraction to USDT on Curve – the pool's price oracle is now manipulated because the exchange detects a huge temporary imbalance.
3. Deposit into Harvest at the manipulated (favourable) price – receive more fToken shares than the real value would justify.
4. Swap back: restore Curve pool; fTokens are now worth more relative to the manipulated baseline.
5. Withdraw profit, repay $50M flash loan. Net profit: $34M. Transaction time: 7 minutes.

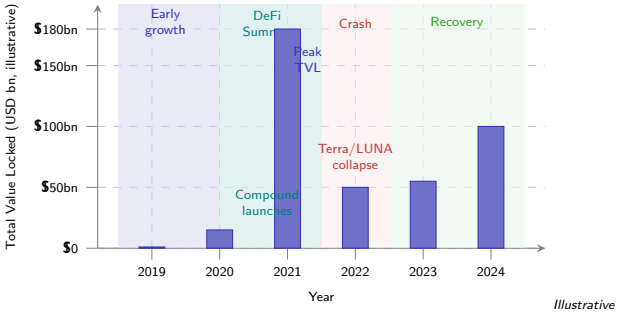
The code performed exactly as written. The design relied on a price oracle that an attacker with enough capital could move.



Flash loan exploits are not hacks of cryptography – they are economic attacks on design assumptions. The fix: use time-weighted average prices (TWAP) instead of spot prices for sensitive operations.

Flash loan attacks exploit oracle design, not encryption – TWAP oracles (Chainlink, Uniswap V3) reduce this risk.

How Did DeFi Grow from One Million to One Hundred Billion Dollars?



Illustrative

TVL trend based on published DeFi Pulse and DefiLlama data. Not investment advice.

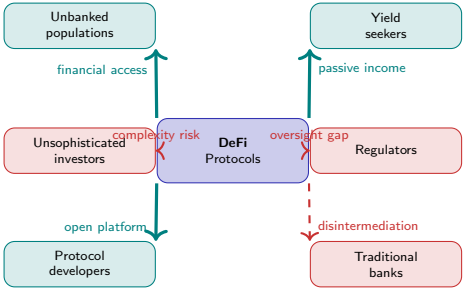
Four phases, four different dynamics:

- **Early growth (pre-2020):** Uniswap V1, MakerDAO CDP, and a handful of experimental lending protocols. TVL under $1bn. Primarily developers and cryptographers.
- **DeFi Summer (2020):** Compound introduced "yield farming" – earning governance tokens by depositing. Copycat protocols proliferated. TVL jumped from $1bn to $15bn in months. Retail capital flooded in.
- **Crash (2022):** Terra/LUNA algorithmic stablecoin collapsed to zero in 72 hours, wiping $40bn. FTX bankruptcy in November destroyed CeFi trust. DeFi TVL fell 70%.
- **Recovery (2023–24):** Institutional DeFi (Aave Arc, Spark Protocol), real-world asset tokenization, and regulatory clarity in some jurisdictions drove renewed TVL growth toward $100bn.

TVL measures locked collateral, not profit. A rising TVL can reflect genuine adoption or reflexive leverage – depositing borrowed tokens as collateral to borrow more.

TVL = Total Value Locked – the sum of all assets deposited in DeFi smart contracts. A flawed but widely used metric.

Who Benefits When Anyone Can Be a Bank – And Who Gets Hurt?



Who gains:

- **Unbanked (1.4bn worldwide):** A mobile wallet and internet access replaces a branch visit. Stablecoins enable savings without currency devaluation exposure.
- **Yield seekers:** Liquidity providers earn trading fees proportional to pool share. Lenders earn interest set by supply/demand curves, not bank policy.
- **Developers:** Composable, open-source infrastructure. Launch a protocol without regulatory approval or banking partnership.

Who bears new risks:

- **Unsophisticated investors:** Complex token mechanics, high gas fees during stress, and no recourse when exploited.
- **Regulators:** Pseudonymous, borderless, 24/7 protocols resist existing AML/KYC frameworks.
- **Traditional banks:** Payment and lending revenue under long-run pressure from zero-marginal-cost protocols.

The same property – permissionless access – empowers the unbanked and exposes the unsophisticated. DeFi is not inherently good or bad; its impact depends on who uses it and whether they understand the risks.

Decentralization redistributes power and risk simultaneously – access gains and recourse losses travel together.

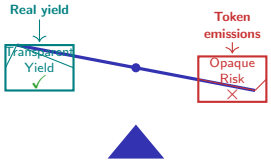
Three Rules That Separate Real DeFi Yield from Unsustainable Promises

Before committing capital to any DeFi protocol, apply these three rules:

Rule 1 **Real yield comes from fees, not token emissions.** Trading fees, borrowing interest, and liquidation bonuses are revenues generated by real economic activity. Token emissions are new tokens printed and handed to depositors – the yield is the inflation of another holder's position. Ask: "If the governance token price goes to zero tomorrow, does this protocol still pay a return?"

Rule 2 **If the APY exceeds 100%, ask where the money comes from.** Sustainable yield in any market is bounded by the productivity of the underlying capital. APYs of 500%+ are almost always subsidised by token emissions or Ponzi mechanics. The question is not whether the yield is possible today but whether it can persist when new capital stops arriving.

Rule 3 **"Not your keys, not your coins" applies to DeFi too.** Any yield-bearing position that requires depositing into a custodial interface reintroduces the risk DeFi claims to eliminate. Check: does the contract have an admin key? Is there a timelock? Can the team drain the pool unilaterally?



Red flags:
- Anonymous team
- Unaudited contracts
- APY from emissions only
- No timelock on admin keys

Quick score: 3 rules pass → investigate further. Any rule fails → treat as speculative capital only.

Evaluating DeFi yield is the same as evaluating any investment yield: trace the source. If you cannot find a clear economic activity generating the return, someone else is paying for your yield – until they stop.

Rule 1: fees not emissions. Rule 2: trace the source of APY. Rule 3: verify custody and admin key controls.

Your Challenge

Read the case below. Apply the three rules from the previous slide.

Case: Cross-Border Remittance via DeFi Stablecoins

Situation: A fintech startup plans to offer cross-border remittances from Western Europe to sub-Saharan Africa using USDC stablecoins on Ethereum L2. The sender converts EUR to USDC at the point of origin; the recipient converts USDC to local currency at the destination. Current fee: 6% (bank wire + currency conversion). Proposed DeFi fee: 0.5%. Settlement time drops from 3–5 days to 30 seconds.

Apply the three rules. Fill in the table:

Rule	Pass / Fail / Partial?	Reasoning (one sentence)
Rule 1: Yield from fees, not emissions?	.....	.....
Rule 2: APY source traceable?	.....	.....
Rule 3: Non-custodial / admin keys time-locked?	.....	.....

Discuss with your neighbour (4 minutes):

- What risks does the recipient face that the sender does not? (Think: custody, local liquidity, stablecoin de-peg.)
- What regulatory challenges arise in each jurisdiction? Which rule of the three is hardest to verify for this use case?
- Would you recommend this system to a low-income migrant worker with limited crypto literacy? What safeguards would you require first?

Real-world DeFi applications must balance permissionless efficiency against user protection, regulatory compliance, and local liquidity constraints.