

SCDO Laboratory · TECH PR · UNIT 05

Automated Contract Ledgers for AI Agents · Next-Gen Smart Payments

DeFi Legos: Money Blocks in Contracts

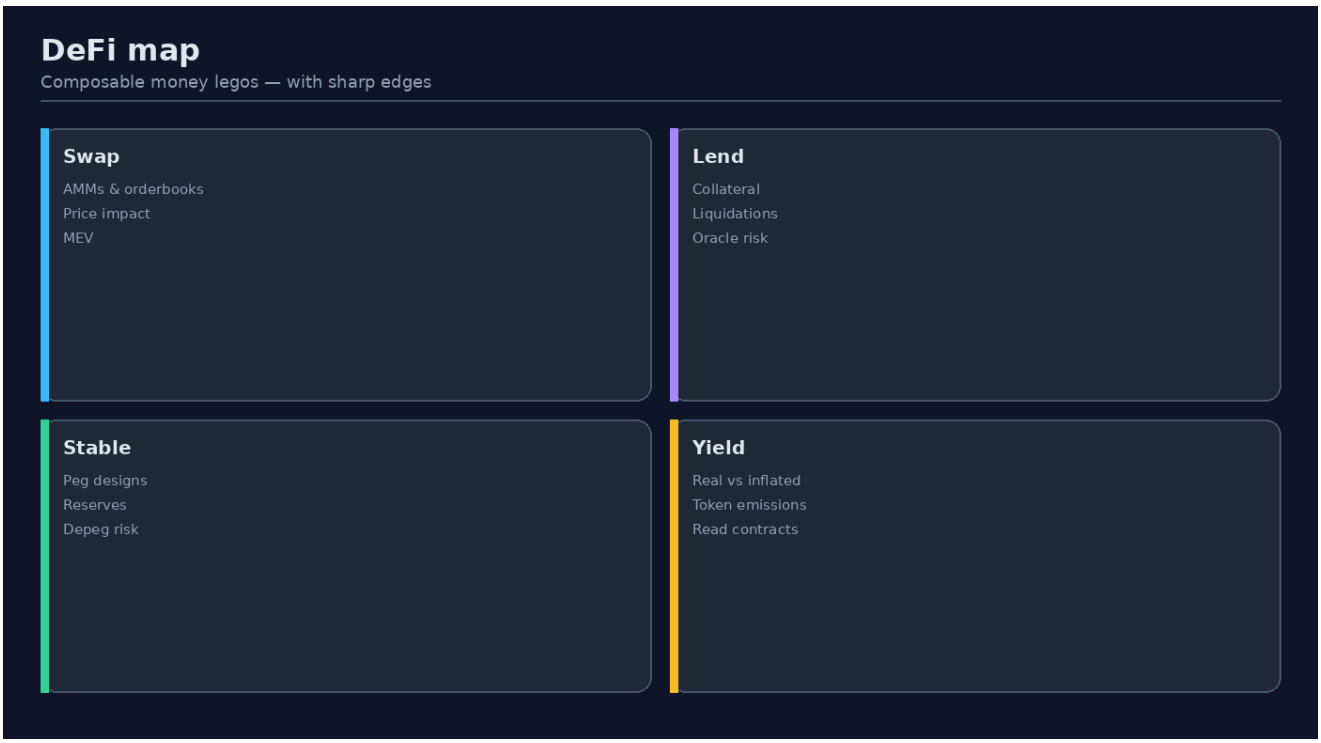
CEX/DEX, liquidity, and risk boundaries · Ying Willam Zhang · 2026

> Disclaimer: This primer is for education only — not investment, legal, or tax advice.

5. DeFi

SCDO Lab · Web3 Primer for Newcomers v2 · English edition
DeFi = decentralized finance: smart-contract Lego for swaps, lending, market-making, and more. Useful—and scary.
No protocol white-paper dumps; do not worship TVL. **Not investment advice, and not a yield tutorial.**

What is DeFi?



DeFi (Decentralized Finance): on public chains (and L2s), open or verifiable smart contracts offer pieces of traditional finance—swaps, lending, liquidity provision for fees, derivatives—while reducing "must open an account and trust one broker's backend."

You usually need:

- A self-custody wallet (or a custodial entry whose risks you understand);
- Some native coin for Gas;
- Literacy about what a signature authorizes.

Where it came from

Bitcoin proved on-chain assets; Ethereum contracts made money rules programmable. Late 2010s through 2020's "DeFi Summer," AMMs and lending exploded; then bubbles, hacks,

stablecoin storms, regulatory pressure. By **2026** DeFi is calmer: more institutional and RWA (real-world asset) talk—but **contract risk and user-ops risk never left**.

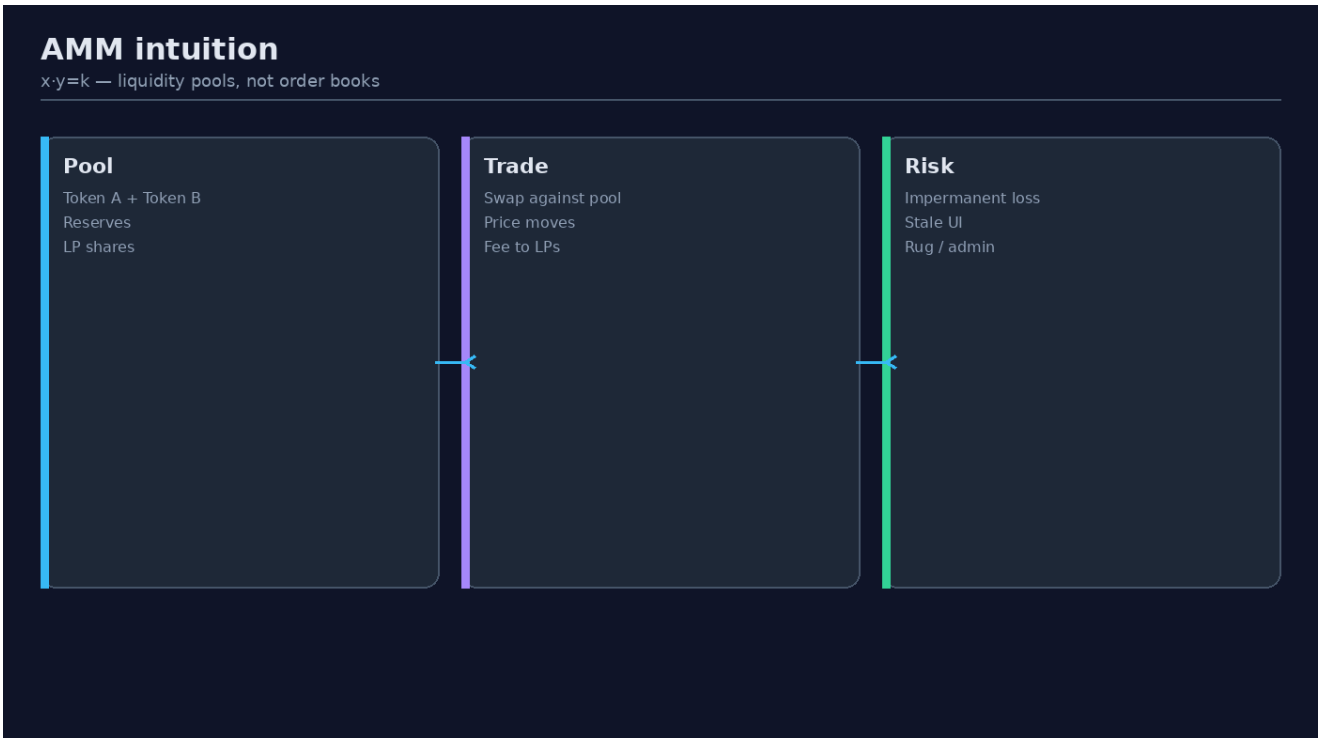
Traits (double-edged)

Trait	Benefit	Cost
Permissionless access	Wallet → try	Scammers deploy fake contracts too
Composability	Protocols call each other like Lego	Risk contagion; one pit topples a stack
Transparency	Parameters and positions inspectable	Transparent ≠ you understand; MEV can sandwich you
Global 24/7	No market close	No support rollback; wrong sign stays wrong

What still blocks mainstream adoption?

UX (Gas, bridges, seeds), compliance (stablecoins and on/off-ramps), security (hacks and phishing), education (impermanent loss and liquidation jargon). Do not believe “DeFi already replaced banks.”

Uniswap: AMM for newcomers



What it is

Uniswap is a flagship **DEX** protocol in the Ethereum ecosystem: instead of a centralized order book matching buyers and sellers, it uses **liquidity pools** + **pricing formulas** (automated market makers, AMMs).

Plain:

- People deposit two tokens into a pool (become LPs);
- Traders swap A for B; the pool adjusts price by algorithm;
- LPs take **impermanent loss** risk from price moves and may earn trading fees.

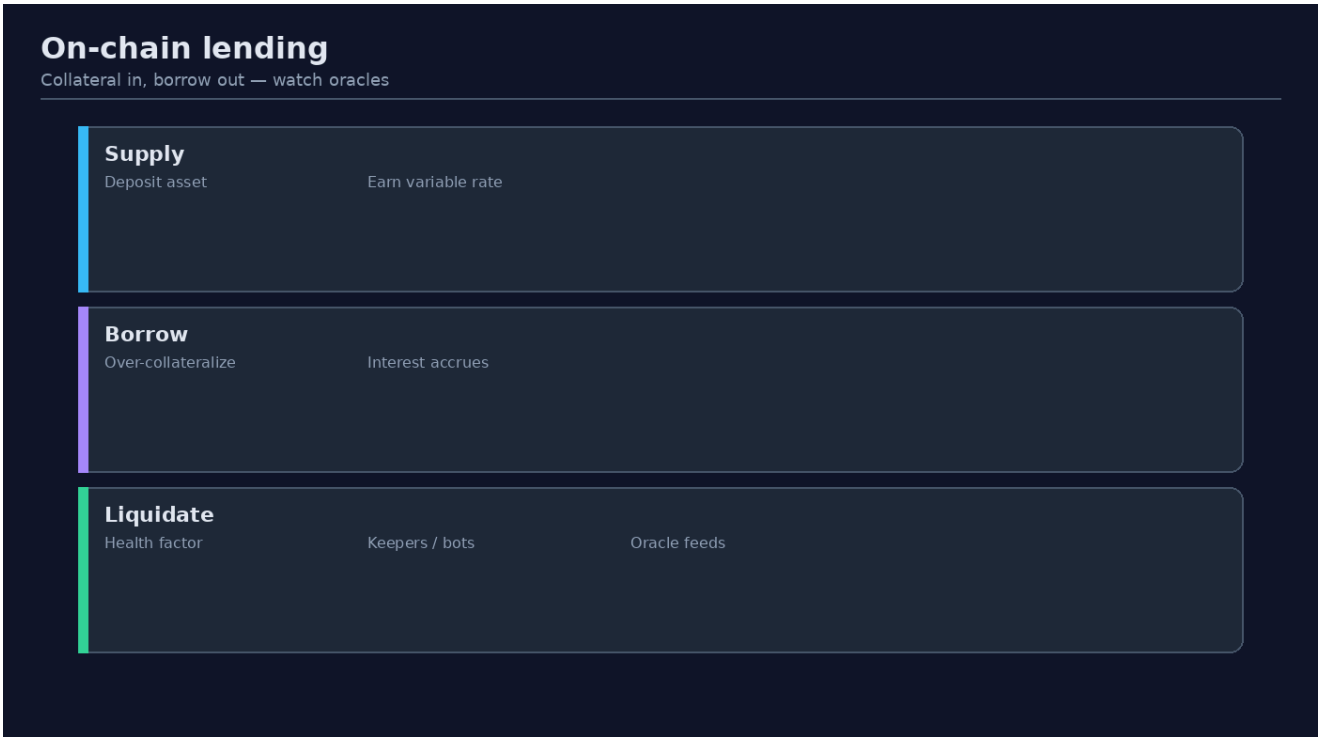
Versus CEXes

- You often trade while self-custodying keys (frontends still phish);
- No classic “deposit to exchange account” layer (unless you already sit on an exchange);
- Price forms from pools and arbitrageurs; extreme markets can produce huge slippage.

Mental model when using

1. Correct network (Ethereum L1 or an L2 deployment).
2. Clear pair, slippage, fee tier.
3. First token approval to a router—be cautious; smaller allowances when possible.
4. Tiny test swap; large size may split or seek better routes.
5. Versions and fee tiers change—trust the UI and explorer of the moment, not memorized numbers.

Lending: Aave-class protocols (with risks)



What they do

Like an “on-chain pawnshop + money market”:

- **Depositors** supply assets and earn interest;
- **Borrowers** post collateral and borrow other assets;
- If collateralization fails on price moves, **liquidation** sells collateral to keep the system solvent.

Aave is a long-standing major lending protocol (peers exist). Experiments like GHO are ecosystem extensions—newcomers learn collateralized borrow/repay before stablecoin issuance details.

Risks you must understand

1. **Liquidation:** collateral falls or debt rises; liquidations add penalties.
2. **Smart-contract risk:** bugs, oracle manipulation.
3. **Rates and utilization:** when money is scarce, rates spike.
4. **Nested asset risk:** collateral that is itself another DeFi receipt stacks risk.
5. **Ops risk:** wrong network, wrong allowance, misread health factor.

Flash loans: borrow-and-repay in one tx for arbitrage/liquidation—advanced tools, not “uncollateralized forever loans for the masses.” “Risk-free flash-loan riches” is usually a scam or hidden complexity.

Curve and stable pools (compact)

Curve-class protocols excel at low-slippage swaps among **similar assets** (various stablecoins, related derivatives) and grew complex reward/governance/bribe markets (historically Convex and peers).

Newcomer takeaways:

- Stables can depeg; pools can lose;
- “Stable” is a design goal, not a law of physics;
- High yields often come from token incentives—when incentives end, APY collapses.

Skip memorizing full bribe-war history; advanced readers can dig later.

LP and token logic

Providing liquidity is not “bank deposit interest”:

1. You deposit assets and receive an LP receipt (often another token).
2. Traders pay fees; you share by share.
3. When relative prices move hard, what you withdraw may underperform simply holding—**impermanent loss (IL)**.
4. If farm rewards stack on top, count reward-token dump pressure into real yield.

Mindset: first ask “is this pool sensible without reward tokens,” then “how long can rewards last.”

How to read TVL

TVL (Total Value Locked): sum of asset valuations locked in a protocol’s contracts. Media loves rankings.

How to read:

- **Useful:** scale and relative heat;
- **Not gospel:** recursive collateral can inflate, prices distort, competitors game numbers;
- **Disaggregate:** what assets? free exit? audits and multisig posture?

One line: **TVL is one thermometer, not a full medical report.**

Synthetic assets (principles)

Synthetics: use collateral and oracles to tokenize exposure to some price (stocks, FX, crypto indexes).

Usual pieces:

1. Collateral;
2. Debt / synthetic position;
3. Price feeds (oracles);
4. Liquidation and stability mechanisms.

The hard part is always **information input**: chains do not know real-world prices unless someone feeds them. Wrong or manipulated feeds make synthetics absurd. Dai, sUSD, and peers trade different assumptions—compare decentralization, censorship resistance, and reliance on real-world custody; do not compare slogans only.

Ten newcomer anti-pit rules

1. Cross-check official sites and contract addresses from multiple sources.
2. Minimize allowances; revoke regularly.
3. Do not max leverage if you do not understand health factors.
4. Stablecoins: reserves and issuer risk matter more than a “USD” ticker.
5. Assume high APR is unsustainable.
6. Someone should clearly explain upgrade rights, multisigs, timelocks.
7. Separate pits: principal loss, IL, liquidation penalties, token → zero.
8. Exchange “support” and Telegram DMs are not official.
9. Tax and local compliance are your responsibility.
10. Use sims/tiny size as tuition—not rent money.

Stablecoins: DeFi’s blood—and a risk source

Without a relatively stable unit of account, lending and trading shake. Rough types:

- **Fiat-backed / custodial:** company + bank-account narratives; watch reserve transparency and freeze policy.
- **Crypto-collateralized:** more on-chain collateral; complex markets; extremes can depeg.
- **Algorithmic / hybrid:** history of blow-ups; “algorithm guarantees forever $1” raises alarms.

In DeFi, a “USD-named token” ≠ bank dollars. Ask: who can freeze? where are reserves? how do oracles price?

MEV and your fill price

Miners/validators/searchers may front-run, sandwich, or reorder. Wallet “expected fill” is not guaranteed. Protections include sensible slippage, private tx rails (advanced), avoiding huge sweeps of thin pools. You need not become an MEV researcher—know the **public mempool is not a charity ball**.

Governance tokens and the “voting power illusion”

Many protocols issue governance tokens. Holding ≠ you alone control the treasury. Look at quorums, delegation, multisigs, emergency switches. Treating gov tokens as “dividend stocks” disappoints; treating them as **coordination tools** + **speculative assets** is more honest.

Abstract ops flow (no specific frontend)

1. Dedicated browser profile and wallet.
2. Confirm network and contracts (multi-source).
3. Tiny swap; confirm receipt.
4. If LPing: stress IL at ±30%/±50% price moves.
5. If lending: set liquidation alerts; do not max.
6. After ops, review allowances; revoke unused.
7. Bookkeep (future you will thank you for taxes).

Regulation and geography (principles)

Jurisdictions differ on DEX frontends, stablecoins, and staking ads. Some regions change frontend access; some require KYC entries. This book does not teach “how to dodge local rails”—only: **tech is global; law is local.**

When people say “smart money”

On-chain whale addresses are visible; that does not mean you should copy-trade. Fake deposits, scam pads, and wash trades can perform. Analytics are tools; without situational awareness they become reverse indicators.

Composition risk: when Lego falls

Composability means your yield may nest four layers—deposit receipts re-collateralized, farmed, rewards sold into another debt. Each layer has contract and oracle risk. Bull

markets call this “capital efficiency”; bears call it “dominoes.”

Practical: draw your position dependency graph. If unclear, cut leverage and layers. Protocol “safety modules” / insurance funds buffer some risk—they are not infinite policies. “One-click strategy vaults” outsource complexity to strategists—you also trust them and their contracts.

Another hidden risk is **liquidity illusion:** high TVL with circular same-asset staking; real exits slip hard. Probe depth with sims or tiny size before large exits.

Treat DeFi as a toolbox: swap when you need to swap, lend when you need to lend, then reduce exposure. Chasing max APY all day usually sells volatility and tail risk to yourself.

FAQ (DeFi)

Q: Is impermanent loss losing principal?
A: It is an opportunity gap vs “just hold”; asset quantities change on exit; extremes hurt.

Q: Audited = safe?
A: Audits reduce risk; they do not erase it—also watch permissions and dependencies.

Q: Where does high APY come from?
A: Often token subsidies or high risk; when subsidies stop, so does the rate.

Q: Can I just hold stables for interest?
A: Still contract, issuer, and depeg risk; rates also move.

Q: Wallet shows fake tokens?
A: Ignore; do not click fake “claim” pages.

Liquidity, price discovery, and where newcomers sit

AMMs let anyone LP—and move market-making risk from desks to retail LPs. You earn fees (and maybe rewards) and pay adverse selection: informed flow trades when it hurts you. Thin pools amplify impact; deep pools may thin your fee share per trade. Fee tiers and concentrated ranges (where supported) are specialist work—novices start with full-range tiny size or simply swap.

Lending markets hand rates to supply/demand algorithms. High utilization raises deposit rates and borrowing costs—that is a feature. Danger is longing collateral while borrowing another asset; flash crashes liquidate faster than your fingers. Treat health factor as a seatbelt, not a high-score challenge.

Yield aggregators auto-compound. They save time and amplify contract/strategy risk. Ask: if the strategist vanishes, can you still exit? timelocks? admin mint rights? Write answers in notes—more responsible than APY screenshots on social media.

DeFi turns part of global capital markets into 24/7 permissioned Lego. It does not erase risk; it reallocates risk and information. You see on-chain data; counterparties see your positions. Transparency is double-edged: auditable and huntable.

Chapter wrap

1. DeFi is on-chain financial Lego; core is contracts and collateral liquidation—not a magic printer.
2. Uniswap teaches AMMs; lending teaches liquidation; Curve teaches “stable isn’t always stable.”
3. LPs face impermanent loss; TVL can mislead.
4. Synthetics live on oracles and collateral, not pretty names.
5. Next: **NFT and the metaverse**—pull unique credentials out of financial Lego and cool the 2021 foam.

(End of Chapter 5 · v2 English edition · SCDO Lab)