The Invention

Money is a thing you earn by the sweat of
your brow
And that's how it should be.
Or you can steal it, and go to jail;
Or inherit it, and be set for life;
Or win it on the pools, which is luck;
Or marry it, which is what I did.
And that is how it should be, too.
But now this idea's come up
Of inventing money, just like that.
I ask you, is nothing sacred?

Courtesy of ChatGPT

Elements of DeFi

https://web3.princeton.edu/elements-of-defi/

Professor Pramod Viswanath

Princeton University

Lecture 1. What is DeFi?

DeFi is tokenized finance on decentralized platforms

Decentralized platforms

Blockchains are decentralized digital trust platforms

This is a mouthful, so let us unpack it.

Trust

Human success is based on flexible cooperation in large numbers. This requires trust

Evolution of Trust over human history

A Decentralized Platform?

- A decentralized NYSE and NASDAQ?
- Decentralized Amazon, eBay, YouTube?
- Incentives aligned with consumers and resource providers?
- No need for a trusted middle party and limited rent-seeking?

Such is the siren song of blockchains.

Tokenization

- Converting a tangible/intangible asset into a digital format
- Can be fungible (“currency”) or not (“an image or a video clip”)
- Awfully similar to **securitization**
  - Key is the **missing trusted middle party**

Tokenized Finance

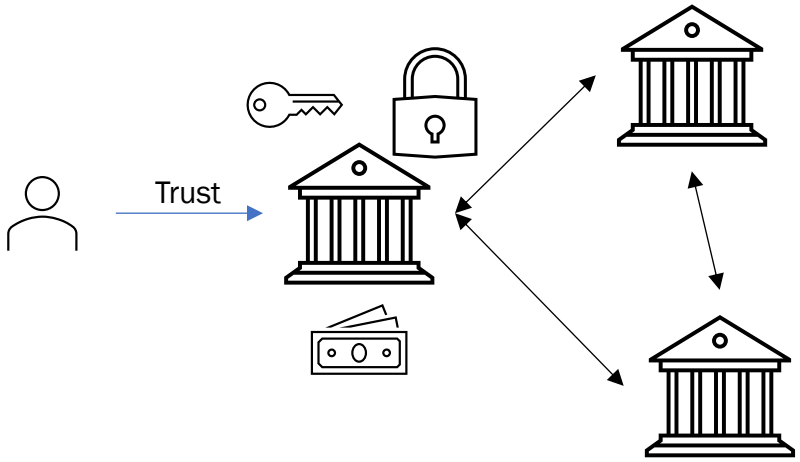
- Commerce – buying, selling
- Market places – exchanges
- Options, derivatives – financial instruments
- Borrowing, lending – banks

How is this any different from traditional finance?

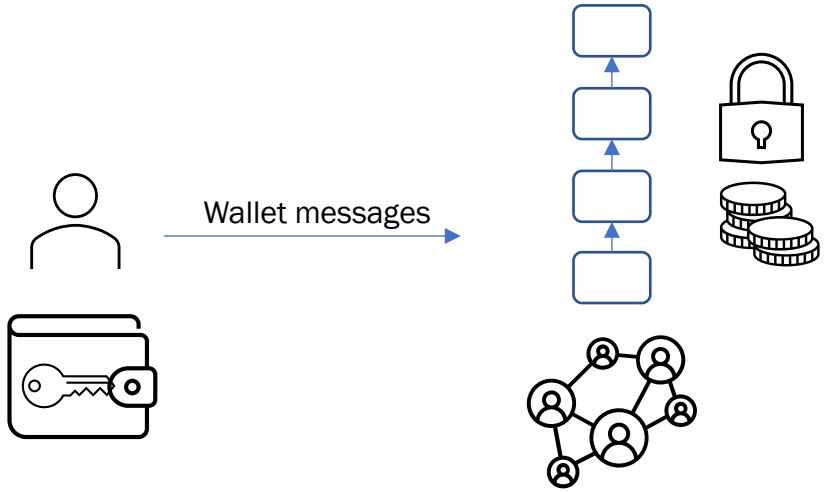
TradFi vs DeFi

DeFi is Non-custodial

- Users control ownership of their assets



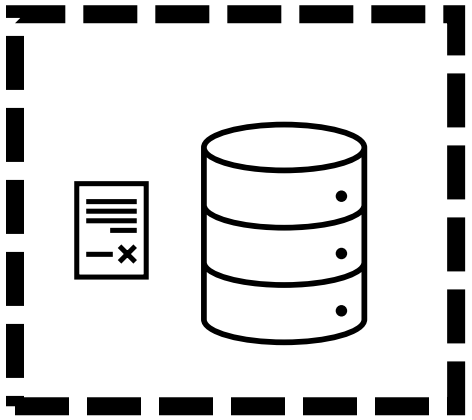
Flow of assets in control of the institution



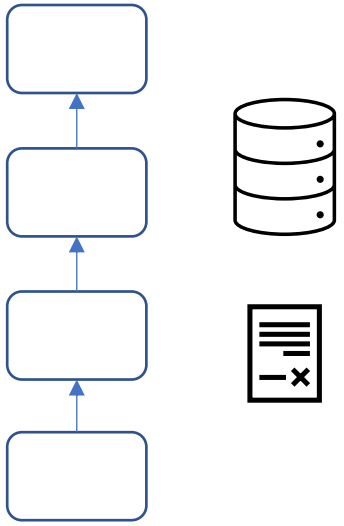
Flow of assets in control of the owner

DeFi is Openly-auditable

- Transparent execution logic of financial instruments and marketplaces



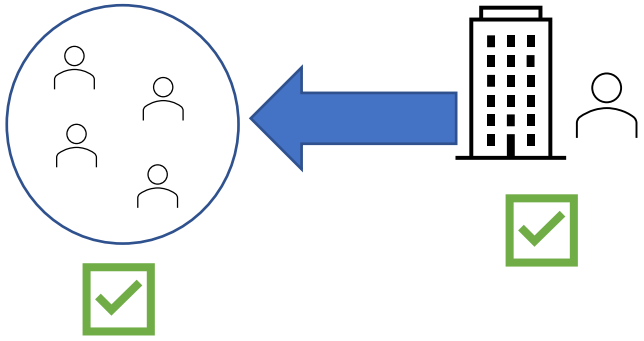
Database and its execution in a closed database, secured by regulation and audits



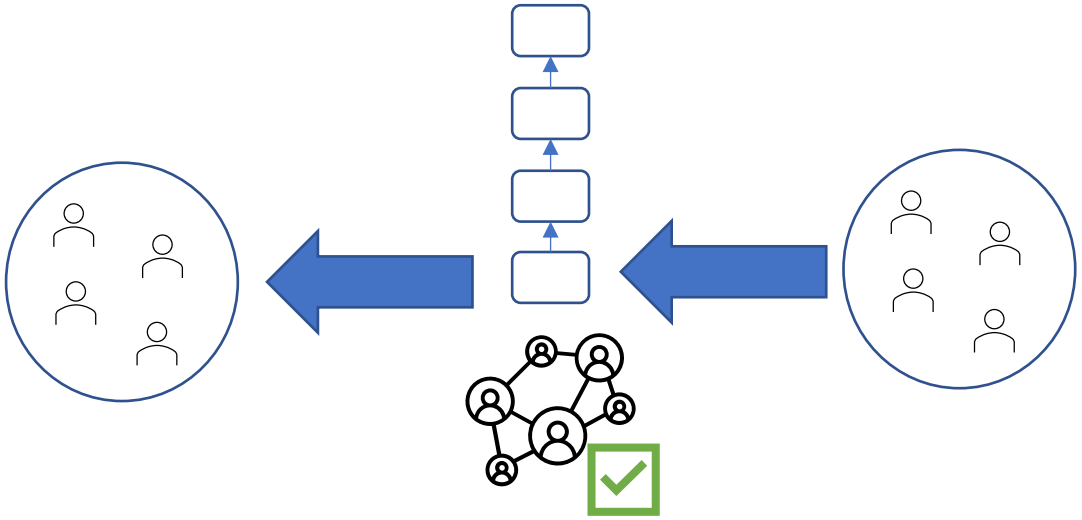
Anyone can check if the contract is programmed as expected and behaves as promised

DeFi is Permissionless

- Anyone can participate and interact with contracts
  - Wallets hold tokens and allow interaction with the blockchain
- Smart contract “regulates” that assets are managed as promised



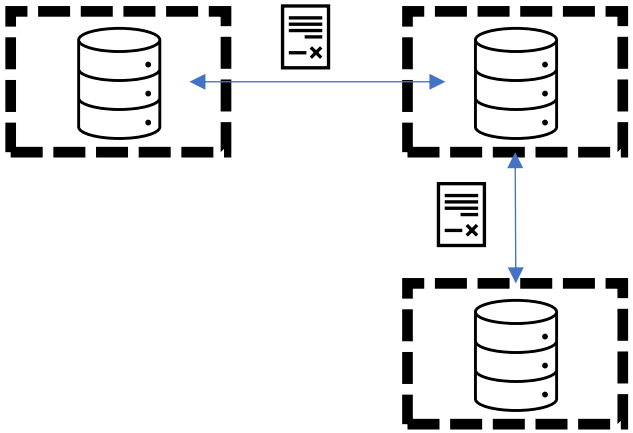
Only trusted entities can participate



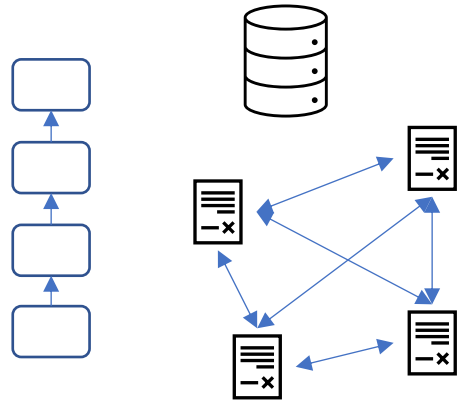
Anyone can participate, smart contracts provide trust

DeFi is Composable

- Interoperability across financial instruments



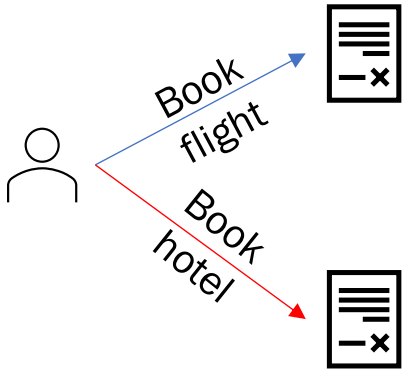
Siloed databases restricts interoperability



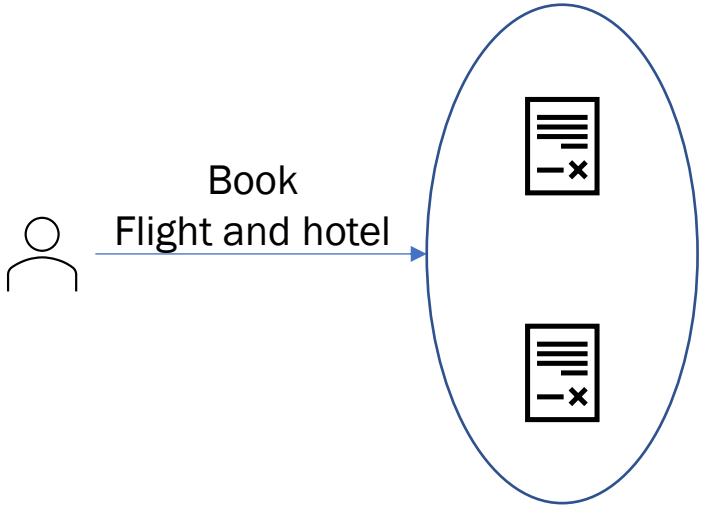
Contracts share state and can call each other while executing a transaction

DeFi is Atomic

- Option to add - **all or none** logic of execution for transactions interacting with multiple instruments



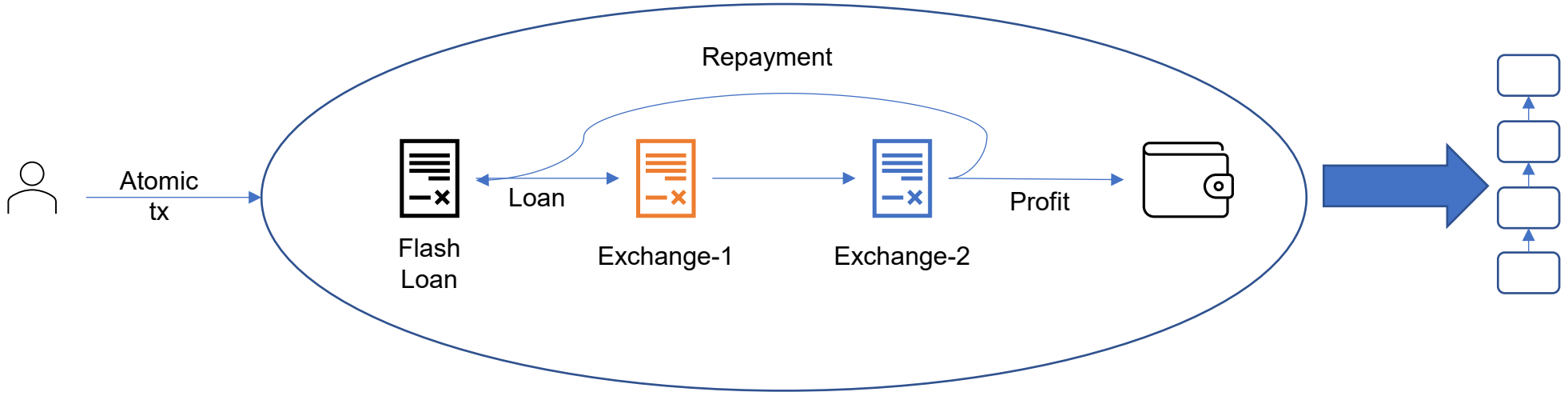
One operation might suceed and the other might fail



Perform action only if both operations succeed; else revert

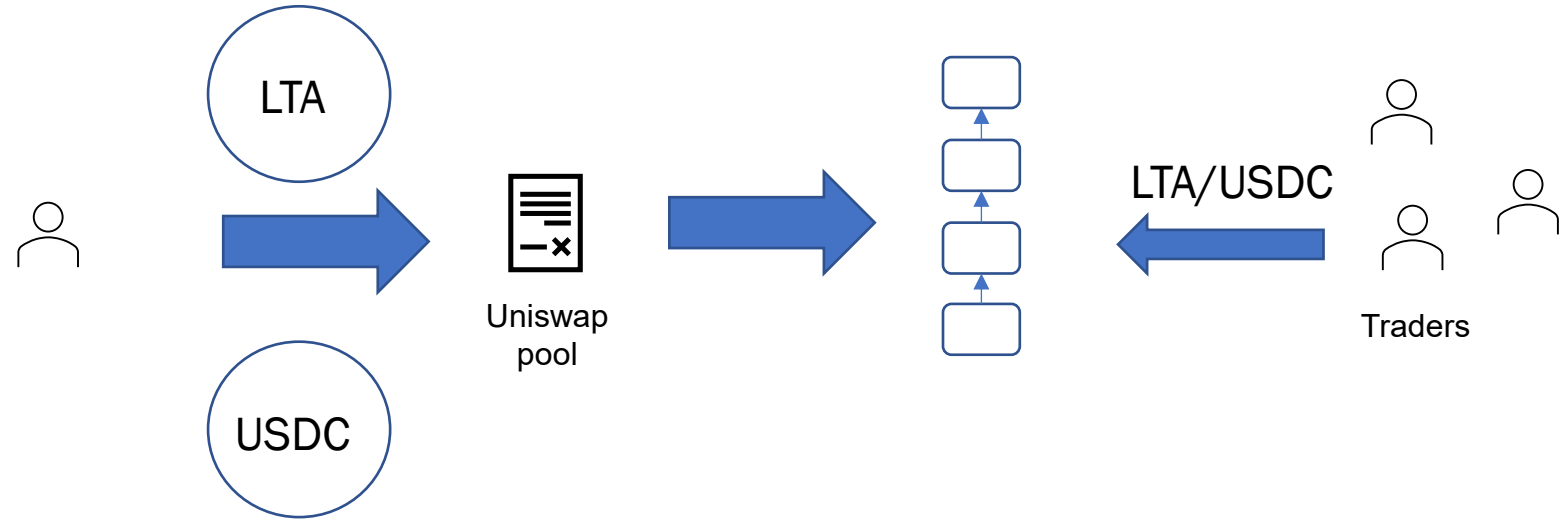
Use case: Flash loan arbitrage

- Two exchanges have a difference in price:
  - TradFi: Need to be a capital rich institution to extract arbitrage value
  - DeFi: Anyone can take a very large capital loan (with no collateral), perform arbitrage, earn money and return capital, in a **single transaction**



Use case: Market for low volume assets

- Need to set up a market for a low volume fungible asset:
  - TradFi: Centralized order-book exchanges don't work due to lack of market making
  - DeFi: Anyone can create liquidity pool for the low volume asset and ensure availability of market



Nine elements of DeFi

1. Token transfers: native blockchain transactions
2. Market making via smart contracts
3. Oracles: importing external data
4. Borrow/Lending: banking functionality
5. Cross border finance: bridges, wrapped tokens
6. Stable coins: tying tokens to fiat
7. Synthetics and Perpetuals: self-adapting financial instruments
8. NFT: digital collectibles
9. DAO: tokenized governance

DeFi elements are smart contracts

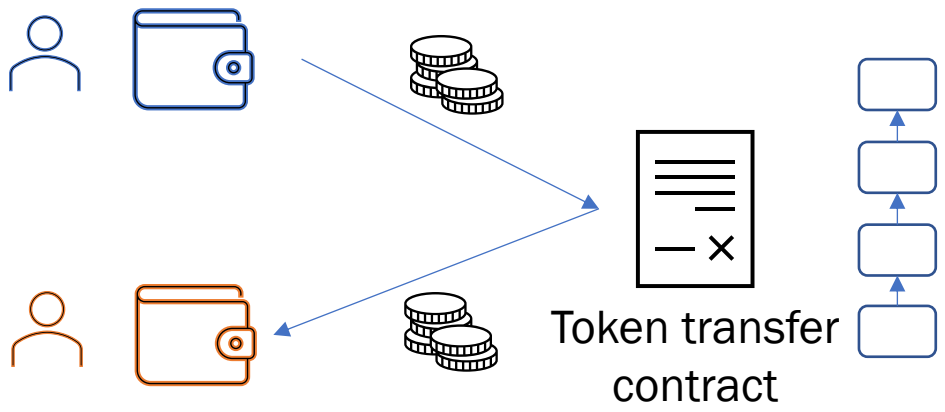
- Each element implemented via smart contracts
- Smart contracts “manage” the input/output of the tokens
- Smart contracts “regulate” the logic of the DeFi element

The underlying blockchain ledger maintains the time sequence ordered contract operations

Element 1: Native Blockchain Transactions

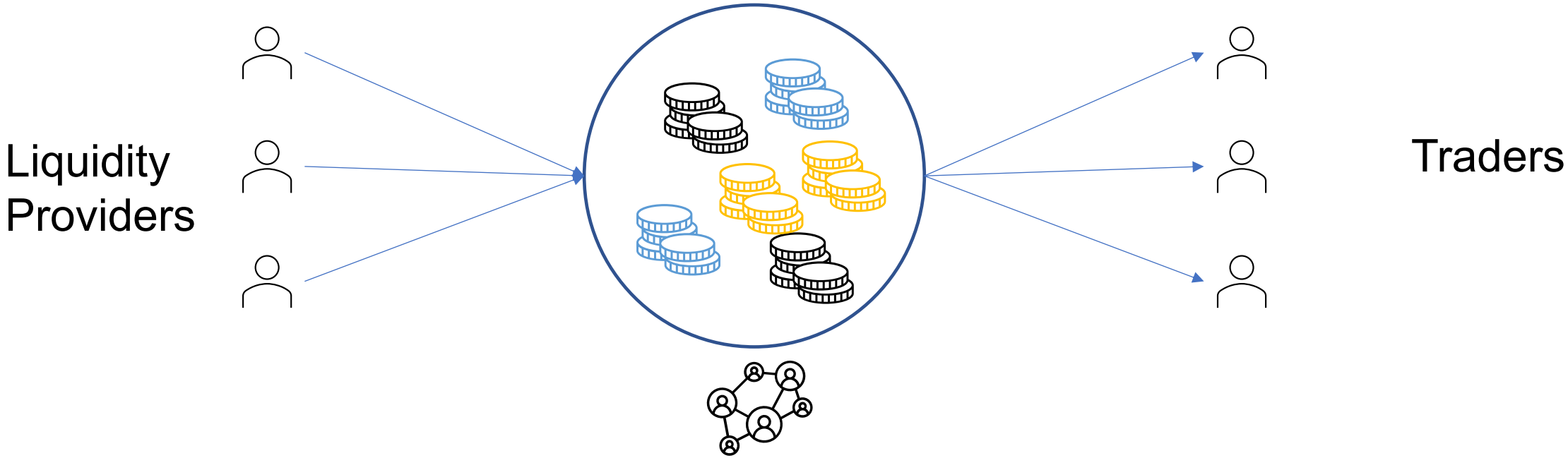
Token transfer

- No intermediaries, direct access via the blockchain
- Sending and receiving



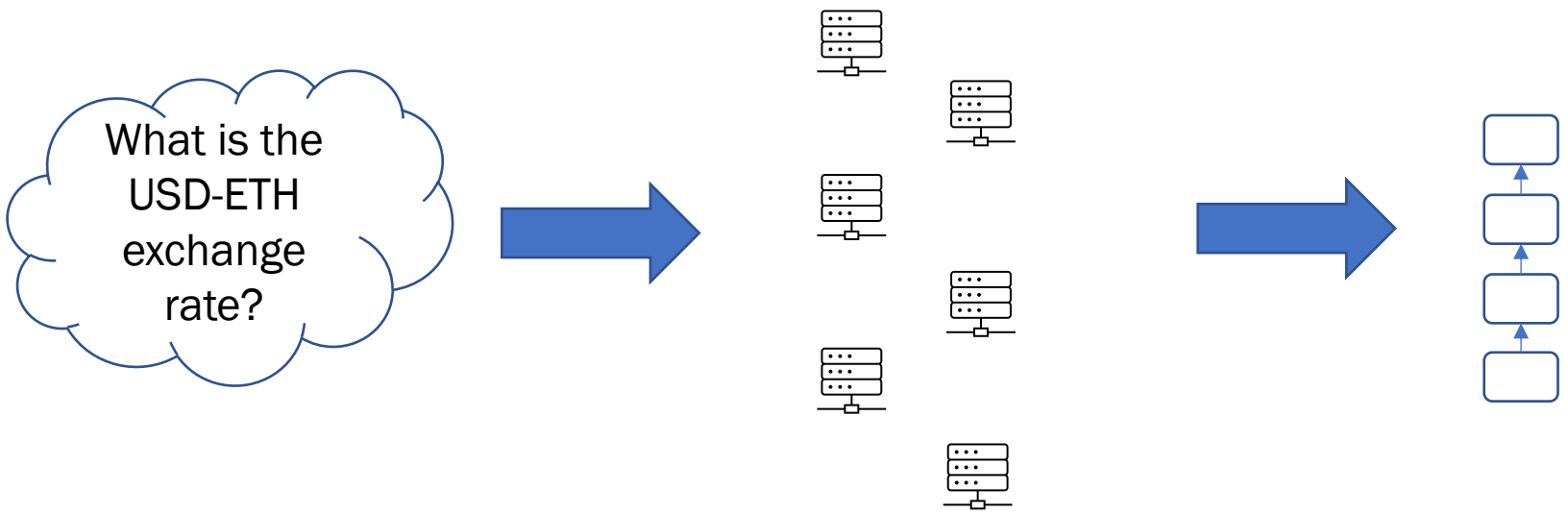
Element 2: Market Making

- Swapping Tokens
  - Market making via smart contracts
  - Liquidity providers and traders interact via the contract
- Peer-to-pool-to-peer Mechanism



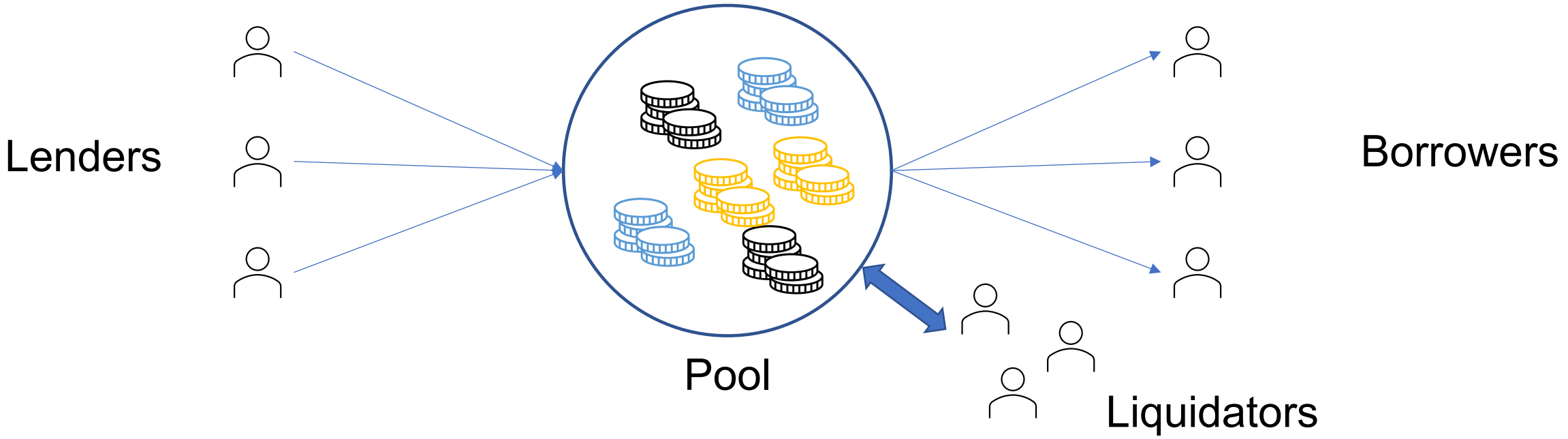
Element 3: Oracles

- A set of nodes import off-chain data into the blockchain
- Robust statistics ensure accuracy of data



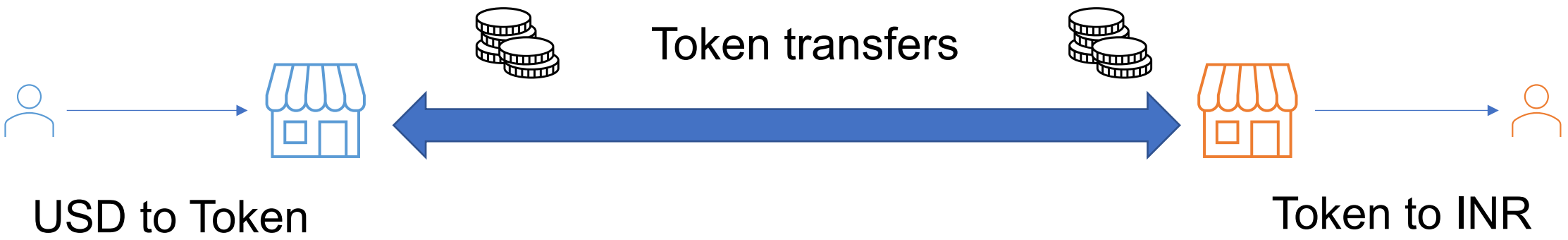
Element 4: Borrowing and Lending

- Deposit asset into the pool to earn interest
- Borrow assets collateralized by the deposited asset and pay interest



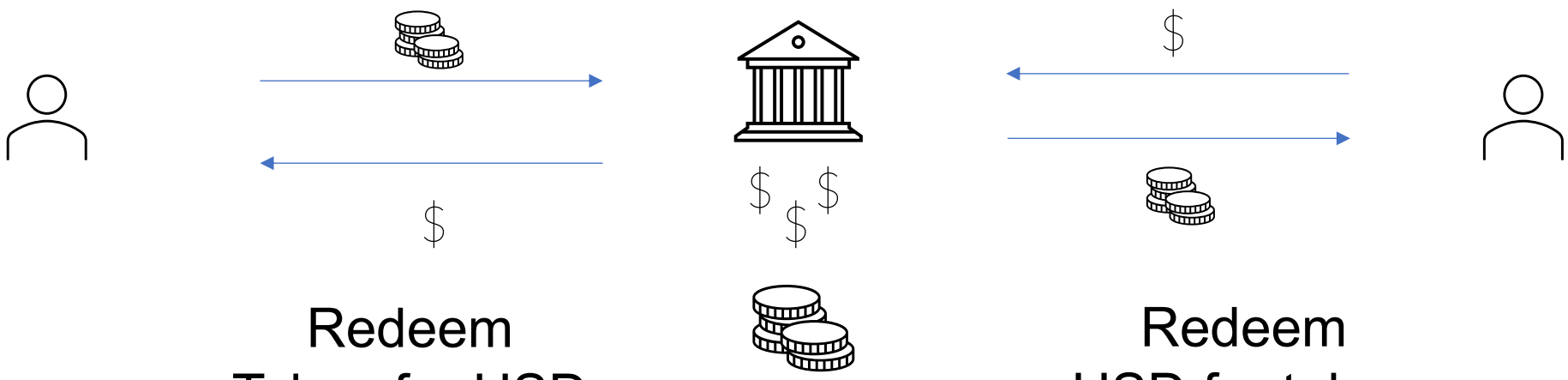
Element 5: Cross Border Transactions

- Token transfers on blockchains have the same security properties across different countries



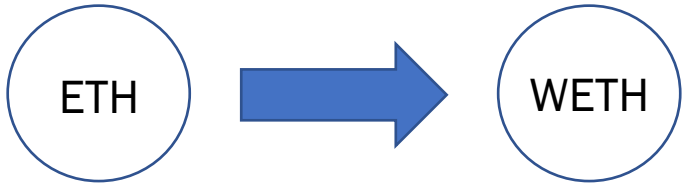
Element 6: Stable Coins

- Token's value can be pegged to the value of a fiat currency through a variety of reserve mechanisms

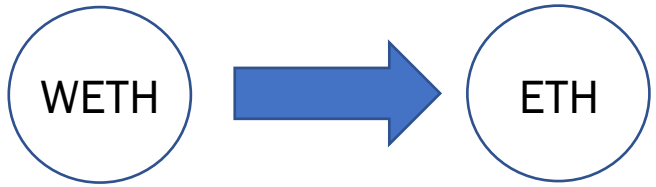


Element 7: Synthetics and Perpetuals

- Generate tokens whose value
  - Tracks value of another token
  - Tracks a value “derived” from another token



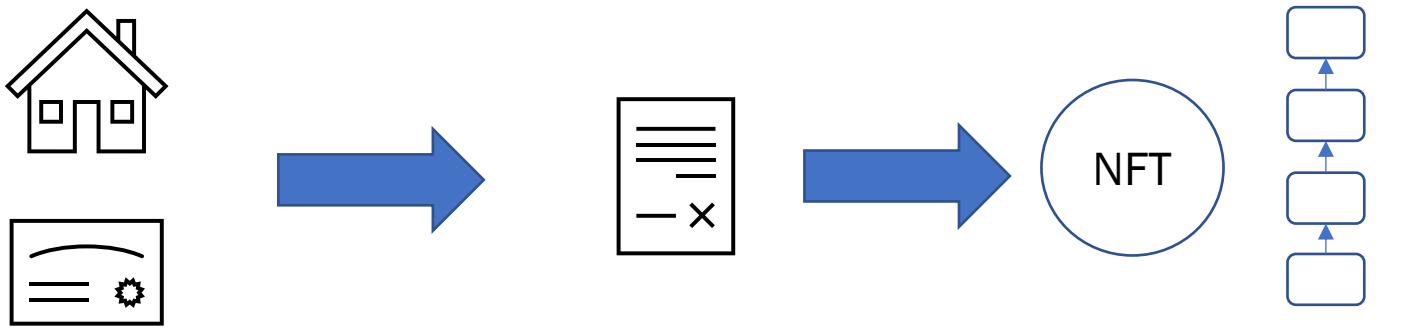
Deposit ETH mint WETH



Burn WETH get ETH

Element 8: Non-Fungible Tokens (NFT)

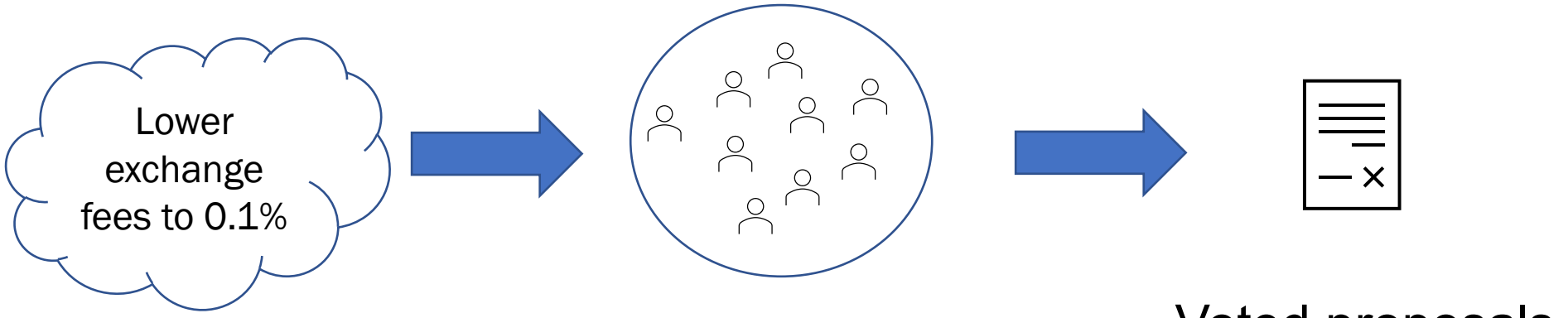
- Representation of unique asset on-chain
- Supports variety of functions on that asset
  - Asset transfers
  - Asset splits, sale commissions, sale tracking



Contract mints
House ownership
NFT

Element 9: Decentralized Governance (DAO)

- Contracts and protocols can be managed by a decentralized organization
- Protocol updates can be voted on by organization members
- Anyone can join the organization in a sybil resistant way



Structure of the Course

Each class meeting is divided into two components:

- Lecture
  - Slides, oral presentation of the material
  - Outcome: a conceptual and theoretical understanding of the material
- Lab
  - In-class, hands-on activity
  - Largely on public blockchains
  - Outcome: hands-on, practical experience on major blockchain platforms

Grading

The grading is conducted via three components:

- Lab participation – 56%
  - In-class activity, students expected to come prepared for the lab
  - Attendance is mandatory for the lab (cannot be done offline).
  - Some slack: need to attend at least 14 labs (out of roughly 20)
- Smart Contract Programming -- 24%
  - Outside the class activity
  - Solidity programming of core DeFi elements
  - Some slack: need to complete the first 3 out of 5 assignments
- Final project– 20%
  - 5-page report on one of the DeFi elements, due after dean's date
  - In-class project presentation (last few lectures of the semester)