DeFi

Decentralized Finance

Thierry Sans

TradFi (Traditional Finance) **vs.** DeFi (Decentralized Finance)

TradFi

- Centralized
- Many intermediaries (brokers, marker makers, clearing houses, exchanges)
- More or less transparency (depends on regulations and oversight)
- KYC (Know Your Customer)

DeFi

- Decentralized
- No intermediaries (from wallet to smart contract exchanges directly)
- Fully transparent (data and code written in clear on the blockchain)
- Permissionless

Bridging DeFi and TradFi

Two operations bridge the gap between DeFi and TradFi

- **On-Ramp**
  Purchasing cryptocurrency with actual FIAT* currency
- **Off-Ramp**
  Selling cryptocurrency to get actual FIAT* currency

* FIAT is government-issued currency like CAD, USD, EURO

DeFi Summary

- Decentralized Exchanges (a.k.a Automated Market Makers)
- DeFi Staking
- Price Discovery Through Arbitrage
- Borrowing and Lending
- Flash Loans
- Stablecoins
- Yield Farming

Decentralized Exchanges

a.k.a Automated Market Makers

[Recap] ERC-20 Tokens

A fungible token is a smart contract that maintains all user balances

```
mapping(address => uint256) balances
```

ERC-20 is a standard API for fungible tokens

```
function transfer(address to, uint256 value) returns (bool)
function transferFrom(address from, address to, uint256 value) returns (bool)
function approve(address spender, uint256 value) returns (bool)

function totalSupply() view returns (uint256)
function balanceOf(address owner) view returns (uint256)
function allowance(address owner, address spender) view returns (uint256)
```

Concept of Exchange (a.k.a market maker)

An exchange converts one currency to another given an exchange rate

How is the exchange rate defined ?

- It can be set arbitrary (unfair market)
- It can be calculated dynamically based on supply/demand (fair market)

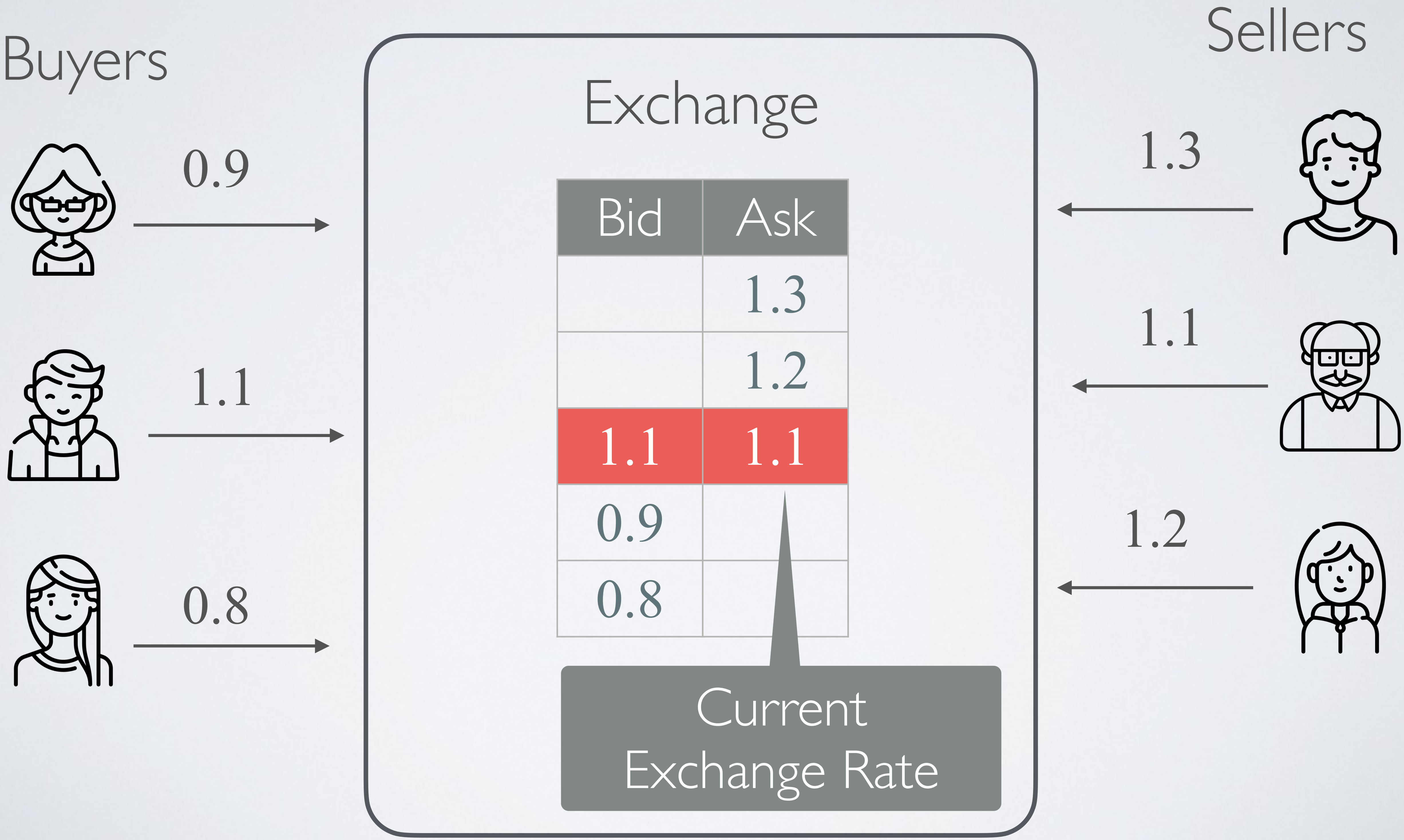
But how to calculate an exchange rate dynamically?

- some people wants to sell token T_A to buy T_B
- other people wants to sell token T_B to buy T_A

➡ an exchange connects buyers and sellers together

✓ The exchange rate is the result of this dynamic process

Order Book-based approach (commonly used in TradFi)



CEX - Centralized Exchange

Can you create a platform that implements an automated order book-based exchange?

➡ Yes, build a platform with :

- a backend to collect user orders
- a wallet to collect money (escrow transaction)

◉ Limitation : centralized approach!
Users must trust the backend to do the right thing and to be always available

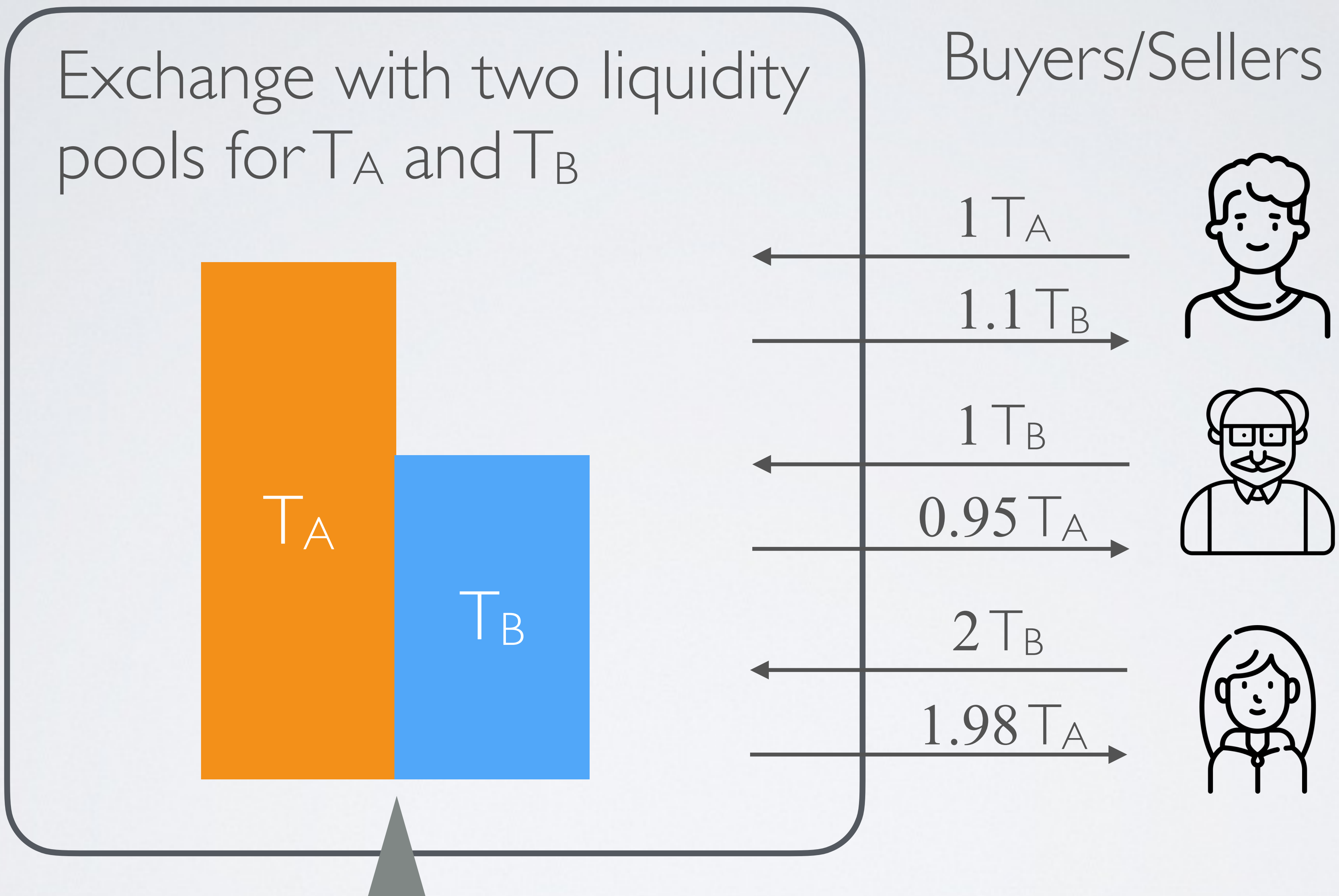
Decentralized version of an order book-based exchange

Can you write a smart contract that implements an automated order book-based exchange?

➡ Technically yes but **no in practice** because of gas

- Matching (i.e ordering) buy/sell orders is expensive
- Placing, withdrawing and fulfilling orders is expensive

A Better Approach : Liquidity Pools



Current Exchange Rate is calculated based on the pool levels

Dynamic pricing using the Constant Product Market Maker

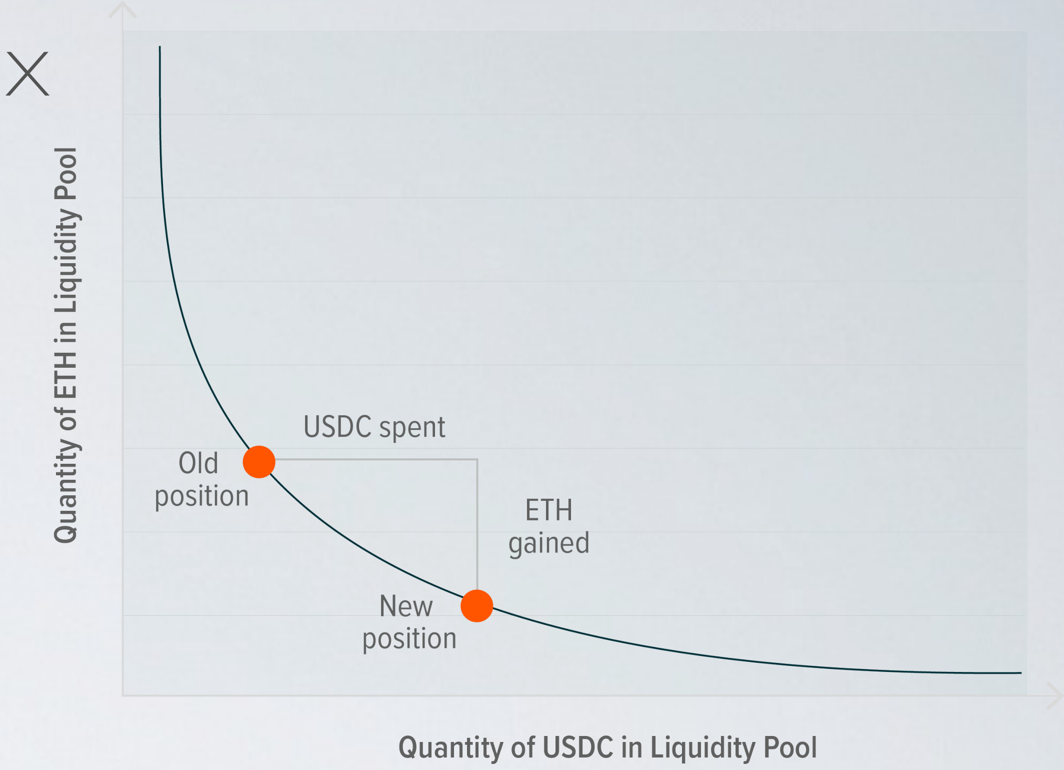
The Constant Product Market Maker is about maintaining a value **k** constant between two liquidity pools

$$\mathbf{k} = \mathbf{vol}(T_A)\ \mathbf{x}\ \mathbf{vol}(T_B)$$

➡ Using this constant, we can calculate swap values i.e what quantity of T_B must be withdrawn when adding adding a given quantity of T_A to keep **k** constant (and vice versa)

✓ This determines the exchange rate

source: Global X



Calculating the exchange rate

- Swapping **a** amount of T_A for **b** amount of T_B

  Since $vol(T_A) \times vol(T_B) = (vol(T_A) + a) \times (vol(T_B) - b)$

  Then $b = (a \times vol(T_B)) / (a + vol(T_A))$

- Swapping **b** amount of T_B for **a** amount of T_A

  Since $vol(T_A) \times vol(T_B) = (vol(T_A) - a) \times (vol(T_B) + b)$

  Then $a = (b \times vol(T_A)) / (b + vol(T_B))$

A liquidity pool cannot be emptied

Example of exchange rate evolution

Swap Order	Out	Rate (T_B/T_A)	vol(T_A)	vol(T_B)	k
			12	10	120
4 T_A	2.5 T_B	0.625	16	7.5	120
4 T_A	1.5 T_B	0.375	20	6	120
4 T_B	8 T_A	0.5	12	10	120
2 T_B	2 T_A	1	10	12	120
6 T_A	4.5 T_B	0.75	16	7.5	120

Side Effects of the Dynamic Pricing

When a user submits an exchange transaction,
the actual exchange may varies depending on other transactions executed before

➡ Slippage (common to TradFi and DeFi)
Difference between the exchange rate when quoted and the actual one when executed

✓ Most DEXes implement a slippage protection mechanism that allow users to specify a slippage tolerance limit

➡ Sandwich Attack a.k.a front-running attack (specific to DeFi)
An attacker can monitor transactions in the mempool and emit concurrent transactions that will take advantage of dynamic exchange rate

✓ Some DEXes implement swap protection mechanism (e.g *Uniswap* v4)

Slippage Example

Beforehand

- When Alice wants to do a swap, the pool contains 12 T_A and 10 T_B
- So she gets quoted that swapping 4 T_A will get her 2.5 T_B (0.62 exchange rate)
- She submits the swap transaction to the mempool **allowing 20% slippage**

Scenario #1

- Bob submits a swap request for **1 T_A** at the same time (i.e within the same block)
- However, Bob's transaction is executed before Alice's changing the levels of liquidity polls and moving the current exchange rate down
- When Alice's request is executed, she actually gets 2.17 T_B (0.54 exchange rate)

✓ The slippage is 15% (0.62 / 0.54 ~ 1.15) and the swap is executed

Scenario #2

- Bob submits a swap request for **2 T_A** at the same time (i.e within the same block)
- When Alice's request is executed, she actually gets 1.90 T_B (0.48 exchange rate)

◉ The slippage is 30% (0.62 / 0.48 = 1.30) and the swap is not executed

Sandwich Attack Example

- Alice submits a transaction to the mempool to swap 4 T_A with a 20% slippage
- Mallory monitors the mempool and **sees Alice's transaction**
- Mallory immediately submits two transactions :
    1. swap 1.2 T_A **(high tip)**
    2. swap 0.9 T_B (low tip)
- Transactions are executed as follows:
    1. Mallory's transaction (high priority) **swaps 1.2 T_A** into 0.9 T_B
    2. Alice's transaction (medium priority) swaps 4 T_A into 2.12 T_B (which is just within the 20% slippage limit)
    3. Mallory's transaction (low priority) swaps 0.9 T_B **into 1.98 T_A**

➡ Mallory **pockets 0.78 T_A** (risk free) with two simple transactions

Simple DEX Example

```
    function swap(address _fromToken, uint256 _amountIn) external returns (uint256 amountOut) {
        require(_amountIn > 0, "Amount must be greater than zero");
        require(_fromToken == address(token1) || _fromToken == address(token2), "Invalid token");

        bool isToken1 = _fromToken == address(token1);
        IERC20 from = isToken1 ? token1 : token2;
        IERC20 to = isToken1 ? token2 : token1;
        uint256 reserveIn = isToken1 ? reserve1 : reserve2;
        uint256 reserveOut = isToken1 ? reserve2 : reserve1;

        // deduct the fee from in
        uint256 amountMinusFee = (_amountIn * (FEE_DIVISOR - FEE_PERCENT)) / FEE_DIVISOR;

        // calculate the amount of token to swap out
        amountOut = (amountMinusFee * reserveOut) / (reserveIn + amountMinusFee);

        // update the reserves
        if (isToken1) {
            reserve1 += _amountIn;
            reserve2 -= amountOut;
        } else {
            reserve2 += _amountIn;
            reserve1 -= amountOut;
        }
        // transfer the tokens from user to contract
        require(from.transferFrom(msg.sender, address(this), _amountIn), "Swap transfer in failed");
        // transfer the tokens from contract to user
        require(to.transfer(msg.sender, amountOut), "Swap transfer out failed");
    }
```

Deduct the fees

Calculate the swap

Update the pools

Transfer the tokens

DEX Staking

Incentive for Liquidity Pool Providers

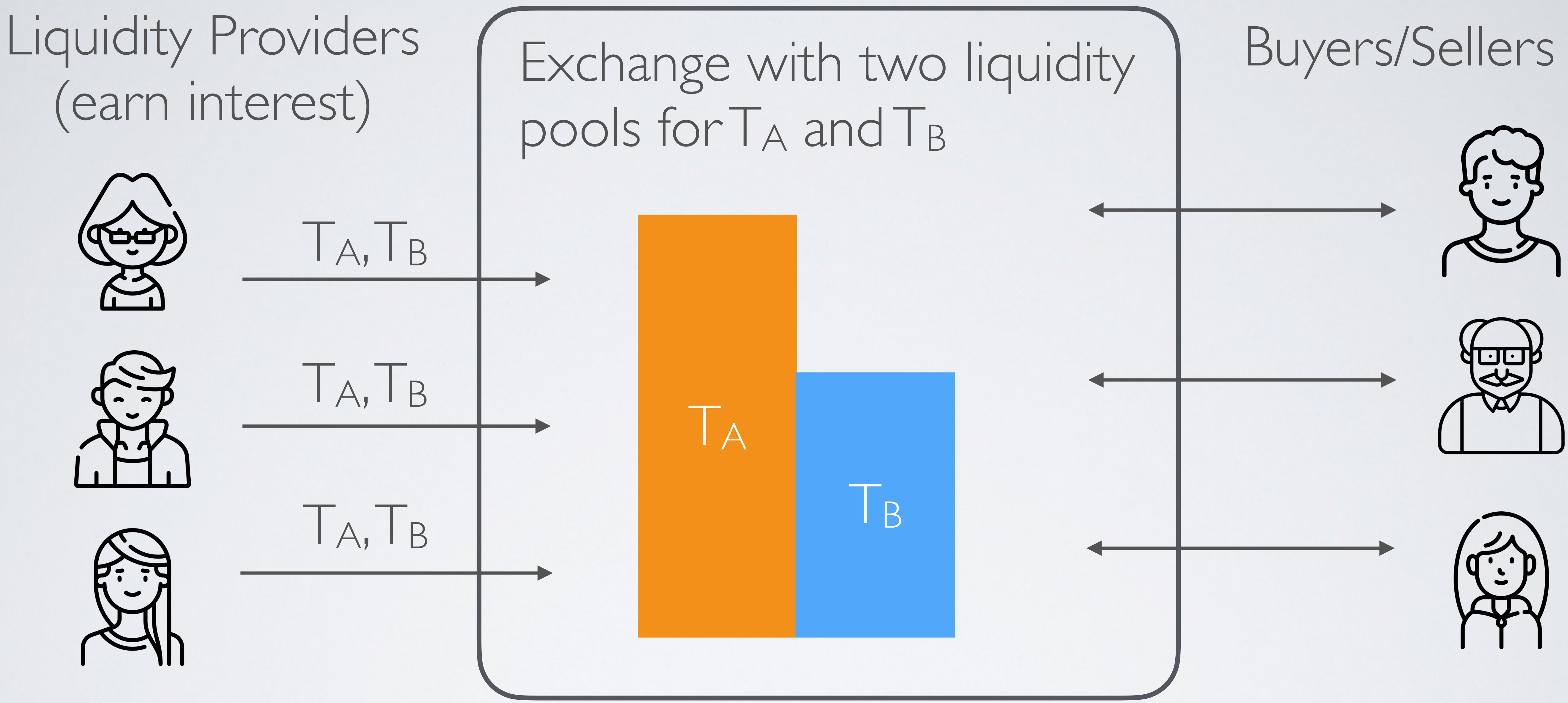
To be efficient, liquidity pools must stash large volumes of cryptocurrencies to absorb a great quantity of possibly unbalanced transactions

So what is the incentive to stake into DEX liquidity pools?

➡ Have a fee for every swap transaction and reward liquidity pool providers (0.30% on *Uniswap* for instance)

◉ This is "DEX Staking"
(not be confused with "Consensus Layer Staking" in PoS)

Liquidity Providers



➡ The liquidity providers provide both T_A and T_B and are rewarded from fees collected on every swap

Liquidity Token

Liquidity providers must **add or withdraw T_A and T_B** from/to the pools **while preserving the ratio** (i.e the exchange rate)

➡ Have a token T_L that represents the contribution to the liquidity pools

✓ `addingLiquidity` mints T_L tokens representing the amount of of tokens T_A and T_B deposited by the user to the pools

✓ `removeLiquidity` burns T_L tokens allowing the user to withdraws the corresponding amount of tokens T_A and T_B (plus interest generated from fees collected during staking period)

Example

Call	Returns	vol(T_A)	vol(T_B)	real(T_A)	real(T_B)
addLiq(12, 10)	14,400 T_L	12	10	12	10
addLiq(6, 5)	7,200 T_L	18	15	18	15
swap(2.06 T_A)	1.5 T_B	20	13.5	20.06	13.5
swap(4.635 T_B)	5 T_A	15	18	15.06	18.135
rmLiq(7,200 T_L)	5.02 T_A 6.045 T_B	10	12	10.04	12.09

```
    function addLiquidity(uint256 amount1, uint256 amount2) external {
        require(amount1 > 0 && amount2 > 0, "Amounts must be greater than zero");

        uint256 correctAmount2;
        uint256 liquidityMinted;
        // check if the reserves are empty
        if (reserve1 == 0 && reserve2 == 0) {
            // if empty, the amount of token 1 and 2 set pool ratio (a.k.a the exchange rate)
            correctAmount2 = amount2;
            // and the amount of lpToken to mint is (amount1* amount2)^2
            liquidityMinted = amount1 * amount2 * amount1 * amount2;
        } else {
            // calculate the right amount of token2 to add to preserve the liquidity pool ratio
            correctAmount2 = (amount1 * reserve2) / reserve1;
            require(amount2 >= correctAmount2, "Insufficient token2 amount provided");
            amount2 = correctAmount2;
            // calculate the amount of lpToken to mint
            liquidityMinted = amount1 * lpToken.totalSupply() / reserve1;
        }

        uint256 amount1ToPay = amount1;
        uint256 amount2ToPay = correctAmount2;

        uint256 token1Reward;
        uint256 token2Reward;
        (token1Reward, token2Reward) = calculateReward(msg.sender);
        amount1ToPay -= token1Reward;
        amount2ToPay -= token1Reward;

        // mint the lpToken
        lpToken.mint(msg.sender, liquidityMinted);
        isStaking[msg.sender] = true;

        // update rewardPerTokenPaid
        rewardPerToken1Paid[msg.sender] = rewardPerToken1;
        rewardPerToken2Paid[msg.sender] = rewardPerToken2;

        // update the reserves
        reserve1 += amount1;
        reserve2 += correctAmount2;

        // transfer the funds from user to contract
        require(token1.transferFrom(msg.sender, address(this), amount1ToPay), "Token1 transfer failed");
        require(token2.transferFrom(msg.sender, address(this), amount2ToPay), "Token2 transfer failed");
    }
```

```
    function removeLiquidity(uint256 lpAmount) external {
        require(lpAmount > 0, "Invalid LP token amount");
        require(lpToken.balanceOf(msg.sender) >= lpAmount, "Insufficient LP balance");

        // calculate the amounts of token1 and token 2
        uint256 totalSupply = lpToken.totalSupply();
        uint256 amount1 = (lpAmount * reserve1) / totalSupply;
        uint256 amount2 = (lpAmount * reserve2) / totalSupply;

        uint256 token1Reward;
        uint256 token2Reward;
        (token1Reward, token2Reward) = calculateReward(msg.sender);

        // update rewardPerTokenPaid
        rewardPerToken1Paid[msg.sender] = rewardPerToken1;
        rewardPerToken2Paid[msg.sender] = rewardPerToken2;

        // update the reserves
        reserve1 -= amount1;
        reserve2 -= amount2;

        // burn the lpTokens
        lpToken.burn(msg.sender, lpAmount);
        isStaking[msg.sender] = (lpToken.balanceOf(msg.sender) > 0);

        // transfer the funds from contract to user
        require(token1.transfer(msg.sender, amount1 + token1Reward), "Token1 transfer failed");
        require(token2.transfer(msg.sender, amount2 + token2Reward), "Token2 transfer failed");
    }
```

The risk Behind Staking a.k.a Impermanent Loss

When liquidity provider deposits 10 T_A and 5 TB, the exchange rate is 2

➡ So the amount deposited is worth **20 T_A when staking**

When the liquidity providers withdraws the whole stake for 14 T_A and 3.5 T_B and the exchange rate is 4

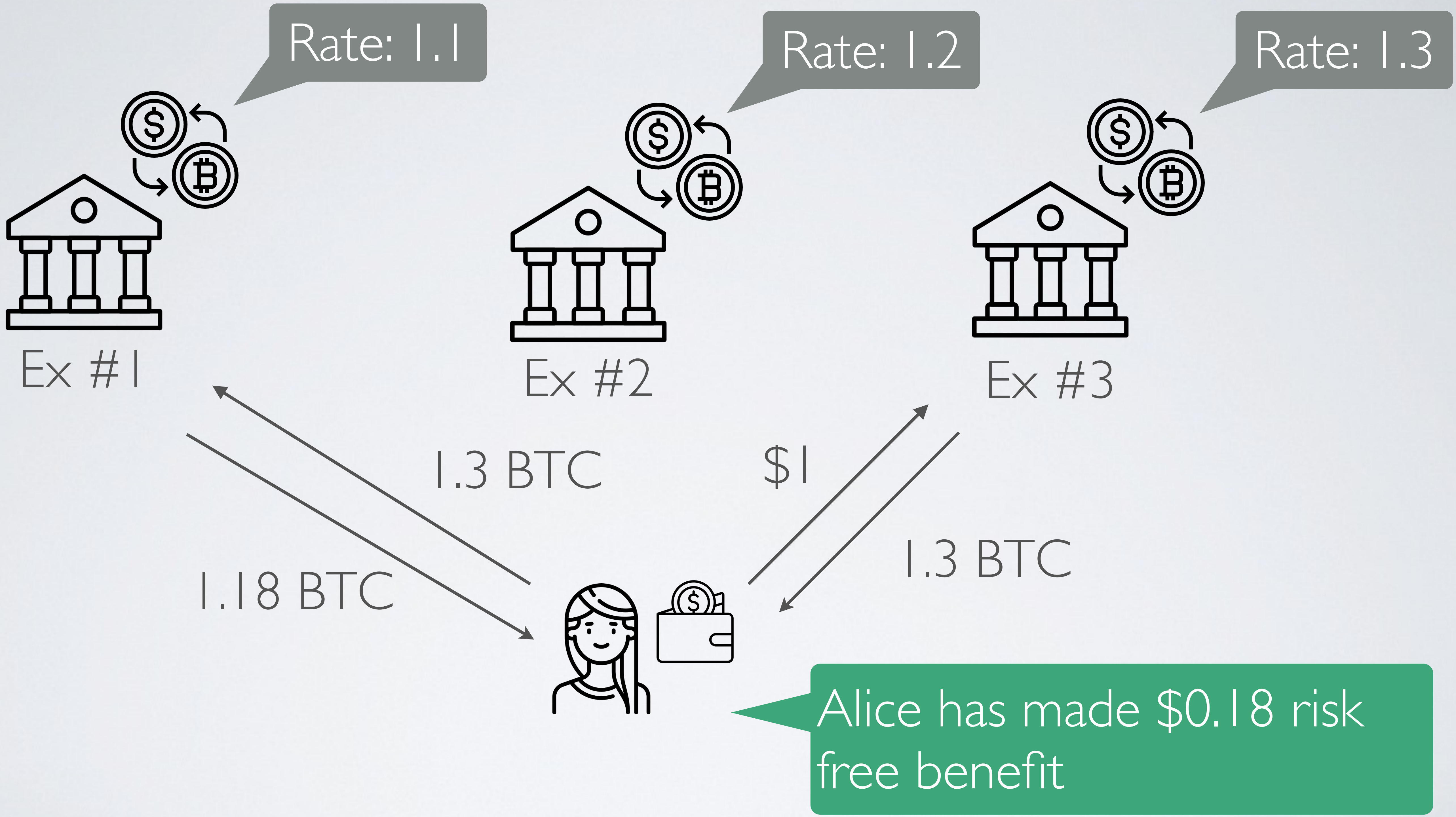
➡ This amount is worth **28 T_A after withdrawing**

However, the **initial stake is now worth 30 T_A without staking**

- This is an **impermanent loss**
  It is an unrealized loss until the liquidity provider withdraws its stake

Automatic Price Discovery

In a decentralized world



➡ Alice can repeat the operation over and over while there are exchanges with different rates

The concept of Arbitrage

Arbitrage (common to TradFi and DeFi)

Exploiting price differences between markets

➡ Traders do take advantage of rate differences between exchanges to make risk-free profits

Automatic Price Discovery resulting from Arbitrage

As traders take advantages of arbitrage, the market as a whole move to a state where no one can make these profits (also called *Nash Equilibrium*)

➡ All exchanges converge to the same rate
a.k.a the market price

✓ This process is called **automatic price discovery**

Borrowing and Lending

Concept of Lending Market

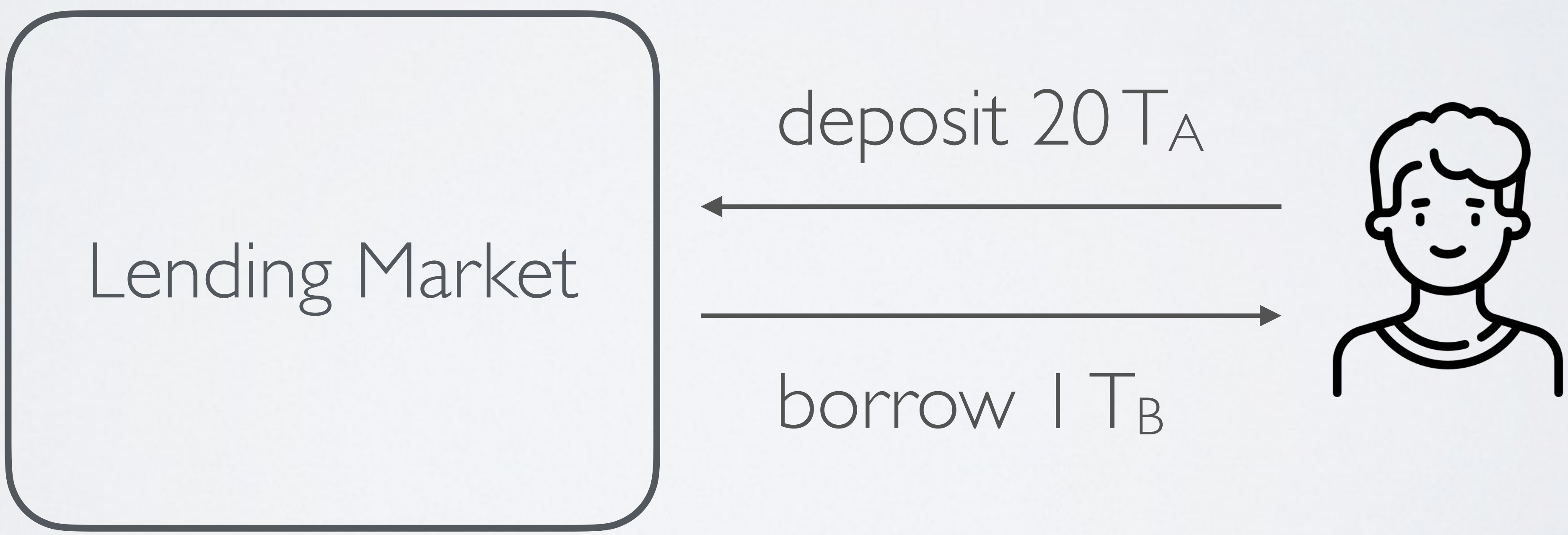
Lenders make money available to borrow and earn interest

Borrowers can take out a loan and repay it with interest before maturity date

The concept of collateral

What if a lender defaults on a loan?

➡ When taking out a loan, the lender must deposit a **collateral** i.e assets that serve as a security deposit



Undercollaterized vs overcollaterized

Undercollaterized
Borrower must provide a collateral that is less than the value of the loan

$$\text{val(collateral)} < \text{val(loan)}$$

Overcollaterized
Borrower must provide a collateral that is more than the value of the loan

$$\text{val(collateral)} > \text{val(loan)}$$

- Problem : over time the value of the loan might increase compared to the value of the collateral (because of exchange rate)
  - ➡ An undercollaterized loan might become further undercollaterized
  - ➡ An overcollaterized loan might become undercollaterized

Collateral factor

Throughout the whole loan period, the value of collateral must not fall below a threshold called **collateral factor**

➡ i.e $\mathrm{val(collateral)} \times k > \mathrm{val(loan)}$ must remain true

This factor is usually

- >1 for undercollaterized loan
- <1 for overcollaterized loan

The role of collateral

After taking a loan, two things can happen:

1. The lender repays the loan with interest
   - ➡ Collateral is returned
2. The lender defaults (i.e does not repay before maturity date)
   - ➡ The loan is **liquidated** (i.e repaid with collateral) with a penalty
3. Before maturity date, the value of collateral falls under
   - ➡ The loan is **liquidated** with a penalty

CeFI vs DeFI

CeFi - both undercollaterized and overcollaterized lending schemes are common (enabled by laws and regulations)

- e.g mortgage (overcollaterized)
- e.g credit card (undercollaterized)

DeFi - only overcollaterized lending schemes are common

- e.g *Aave*, *Compound*, *Curve Finance*

Example of Overcollaterized Loan

A borrower deposits **$15, 000 USDC** as collateral to borrow **5 ETH** (priced at $2,000 USD each) in lending market with:

- Collateralization required: 1.5 (150%)
- Collateralization factor: 1.2 (120%)
- Penalty: 0.1 (10%)
- Interest rate: 0.05 (5%)

What can happen:

- Either the borrower repays 5,25 ETH and $15,000 USDC are returned
- Or the borrower defaults when 1 ETH is $2,200 USDC, $12,100 USDC (worth 5.5 ETH) are liquidated and $2,900 USDC are returned to the borrower
- Or ETH rises above $2,400 (10,000*1.2/5), $13,200 USDC are liquidated and $1,800 USDC are returned to the borrower

Why overcollateralized borrowing makes sense

Why taking an overcollaterized loan when you can just exchange the collateral

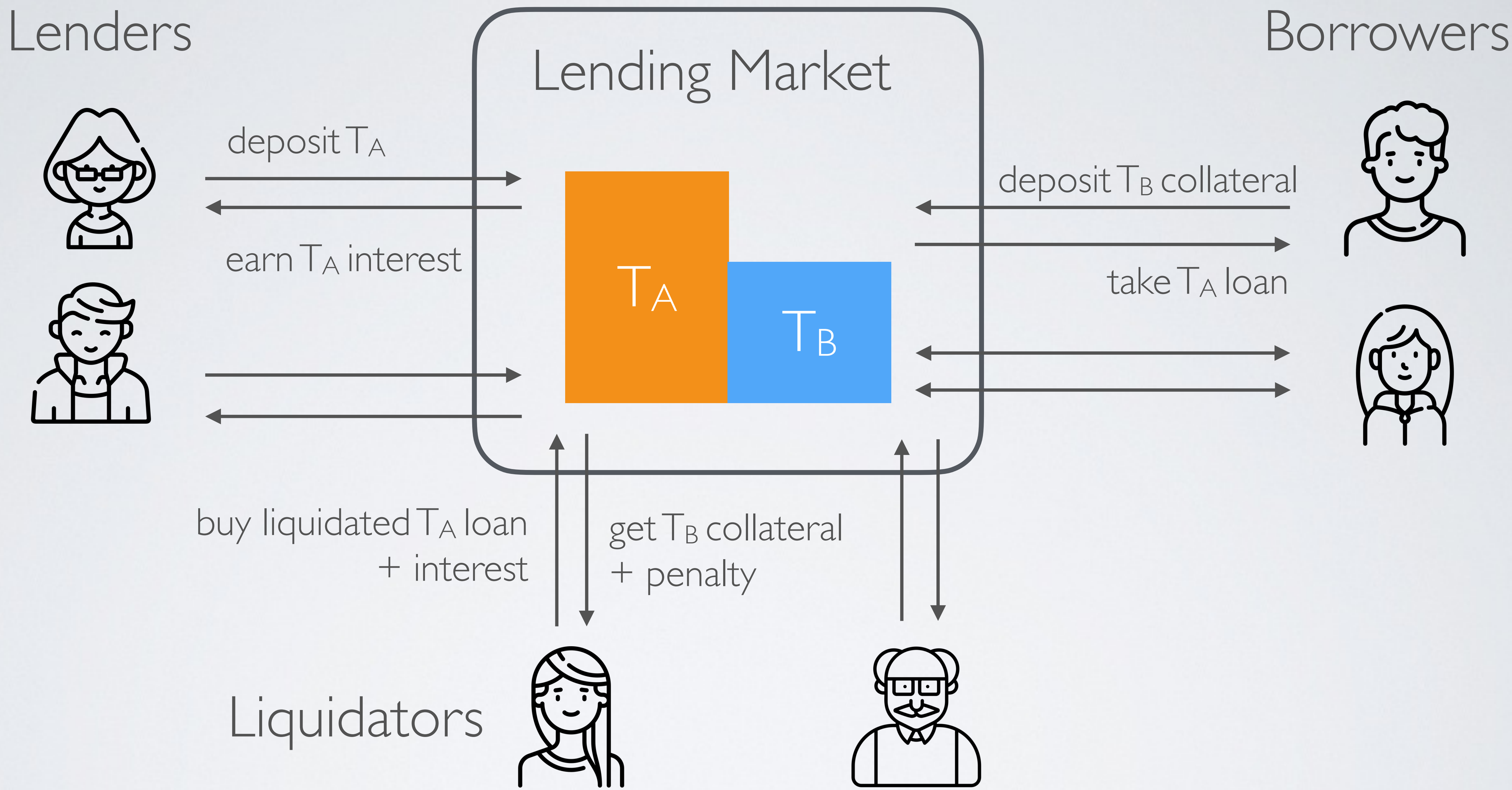
➡ In a nutshell : **shorting**
i.e betting that the value of an asset will go down

Example

1. Borrow 5 ETH (1 ETH - $2,000) with $15,000 collateral
2. and sell it right away to cash out $10,000
3. Wait for ETH to decrease to $1,500 and buy back 5.5 ETH for $7,875
4. Repays 5.25 ETH and get the full collateral back

✓ The borrower pockets $2,125

Implementing a DeFi Lending Market



➡ The liquidators are important to make sure the T_A pool does dry up when borrowers are defaulting

Linear Variable Interest Rate

When the **supply of T_A is low**, raise interest rate to

- decrease the demand of loans
- and increase the incentive for lenders to stake T_A

➡ Have a interest rate that depends on the utilization of the T_A pool

Utilization ratio $U = \text{totalBorrow} / \text{totalDeposit}$

Borrow rate $R = \text{baseRate} + U$

✓ The interest rate varies on every deposit, loan and liquidation transactions

Slopped Variable Interest Rate

Used in common DeFI Lending Markets such as AAVE and Compound

Same idea but the goal is to reach an optimal pool utilization (usually 80% by empirical model)

➡ The model takes into account how fast the interest rate should varies (a.k.a **slope**) to reach the optimal utilization rate

- **Slope1** defines how the borrow rate increases as utilization rises up to the optimal utilization rate (to incentivize borrowing)
- **Slope2** Defines how sharply the borrow rate increases after the optimal utilization point (to penalize borrowing)

$$\text{Borrow Rate} = \begin{cases} \text{Base Rate} + U \times \text{Slope}_1, & \text{if } U \leq U_{opt} \\ \text{Base Rate} + \text{Slope}_1 + \frac{U - U_{opt}}{1 - U_{opt}} \times \text{Slope}_2, & \text{if } U > U_{opt} \end{cases}$$