



Yex Lab



ETH
SHANGHAI

Batch Swap

DeFi & AMM



Chainlink



ChainIDE
Swift, Simple, Smart



PROBLEM

Slippage

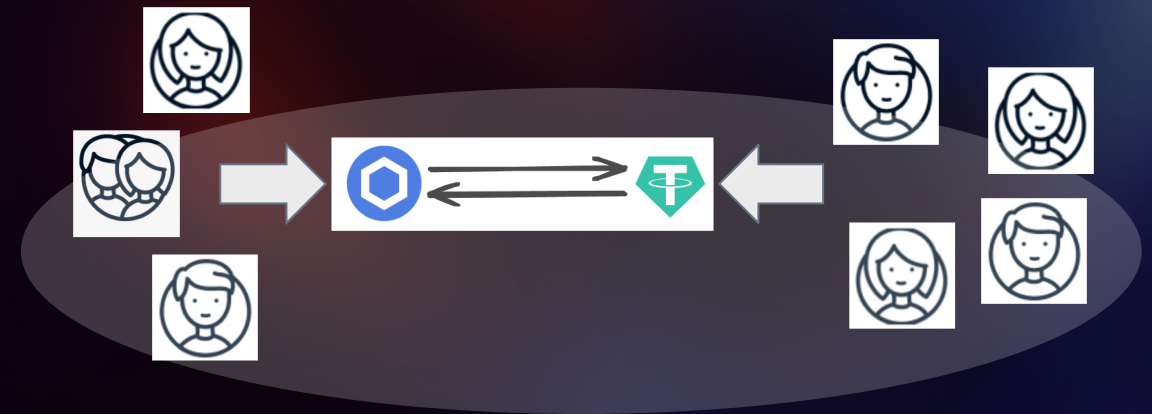
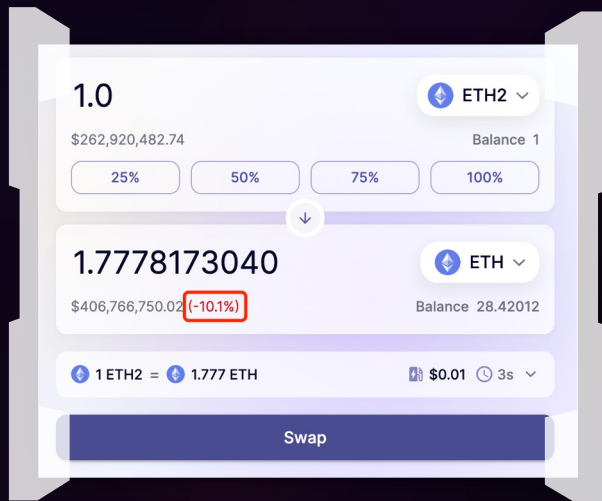
When the depth of liquidity is shallow, or the user's swap amount is large, AMM will get a huge slippage. This is common on many small DEXs.

LOADING

SOLUTION

How to reduce slippage when liquidity is shallow ?

A direct swap between two demands is always the easiest way.





PROBLEM

Sandwich Attack

- Arbitrage bot places their own two transactions around a victim's transaction with the intention of manipulating the price and profiting from the user.

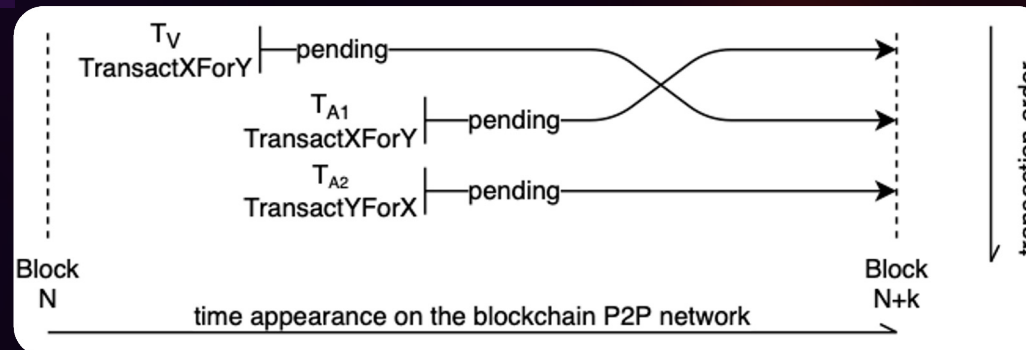
LOADING

SOLUTION



How to implement a order-independent swap?

- group a batch of swaps together and executing at the same time is order-independent.
- In addition, choosing AMM and swapping in the same one transaction can also avoid attackers.





BATCH ACTION

Crypto Wiki:

01

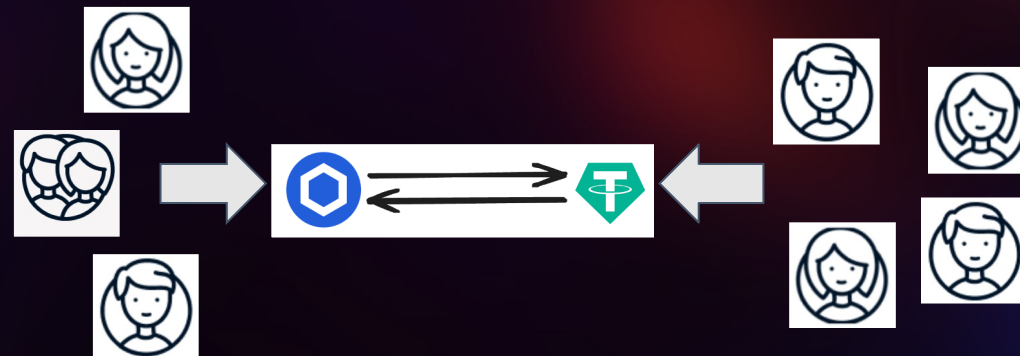
Individual orders are grouped together into a batch and executed at the same time.

02

The same clearing price is assigned to all orders within one batch.

03

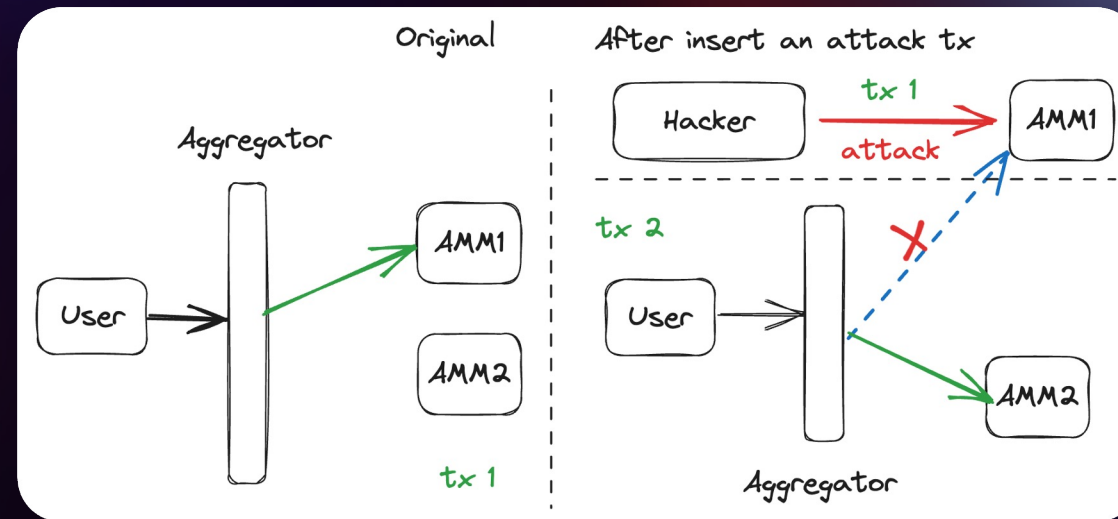
Trading in batch auctions helps guarantee fair price discovery and avoid MEV(Sandwich Attack).






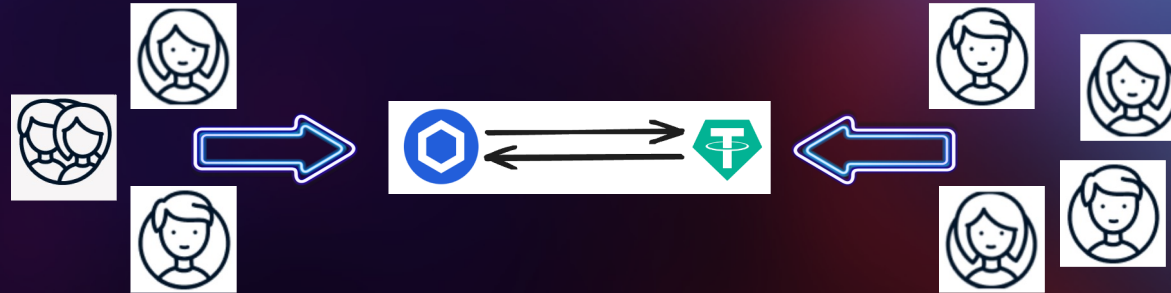
Aggregate more than 2 AMMs through on-chain contracts, execute routing algorithms and swap in the same transaction to avoid attacks.

The swap is always fair unless the attacker attacks all AMMs at the same time.



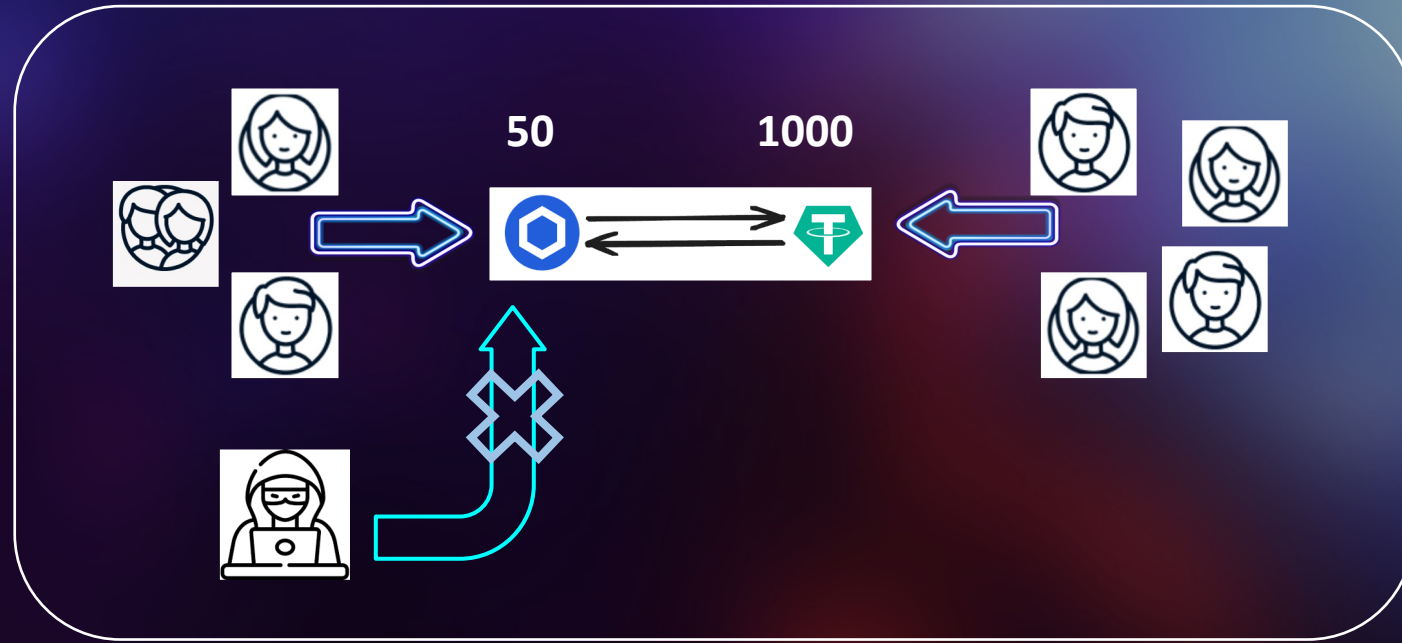
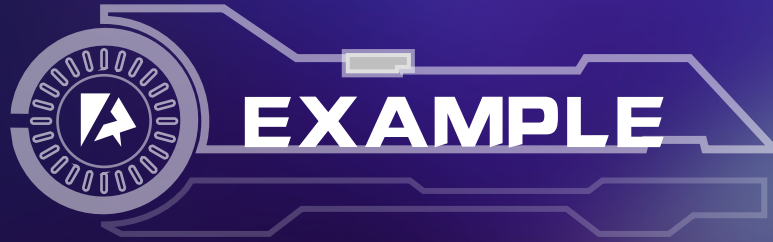


EXAMPLE



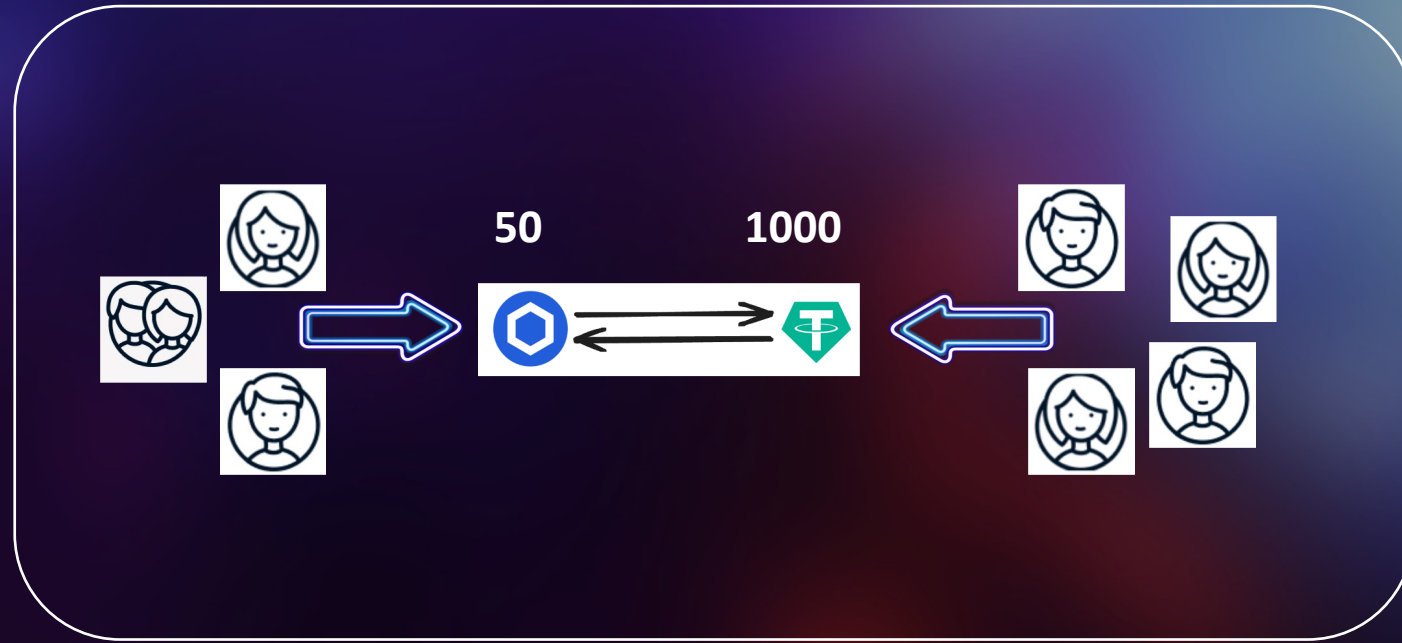
Random users pay tokens and require another token.
A Batch of orders will execute together.

There is no CFMM, no Slippage in this step.



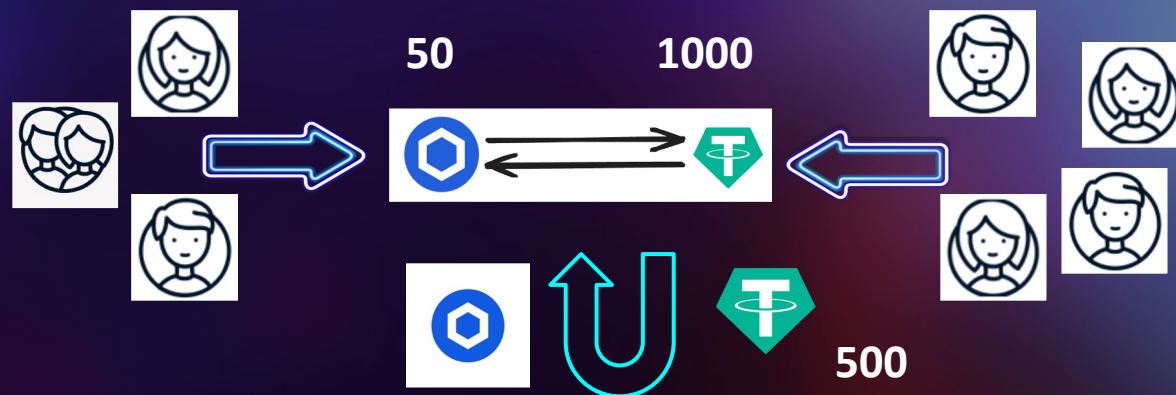
Because everyone's final **clearing price is the same** which is order-independent. So arbitrageurs can't attack on the price by ranking the TXs.

EXAMPLE

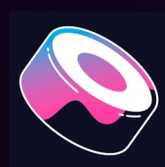


- We assume that there are **1000 USDT** and **50 LINK** in this batch.
- We assume the **market price** of LINK (easily obtained through the **Chainlink Price Oracle**) is **10 USDT** at this time.

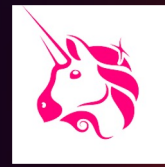
EXAMPLE



$$= \text{amount_usdt} - \text{amout_link} * \text{price_link}$$

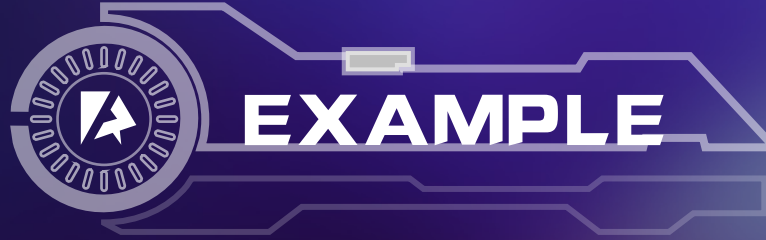


or

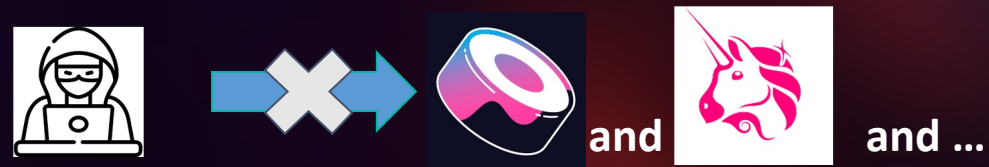
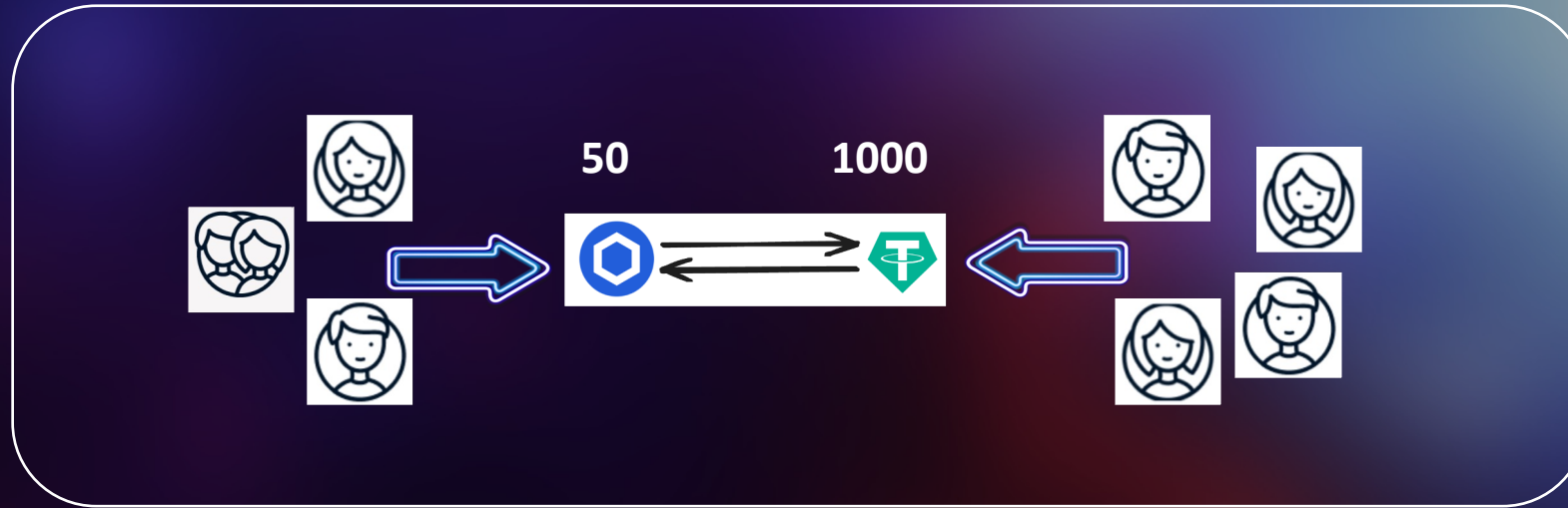


or ... ?


- The excess **500 USDT** needs to swap in a AMM.
- The contract compares the best AMM to swap.



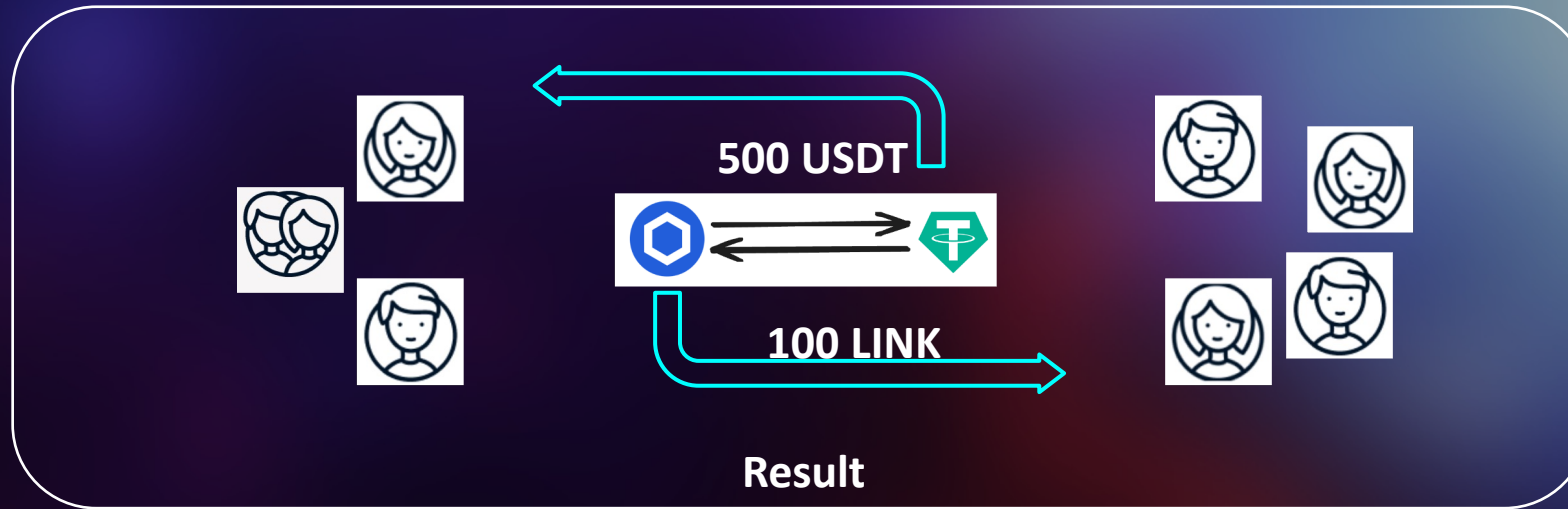
EXAMPLE



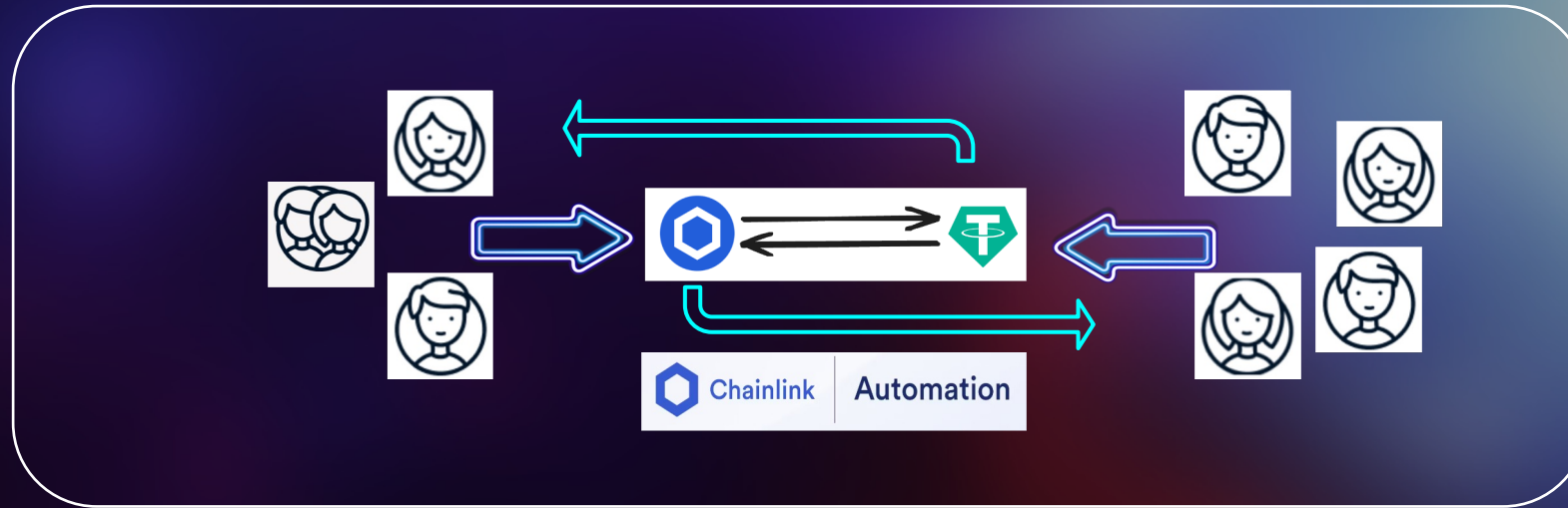
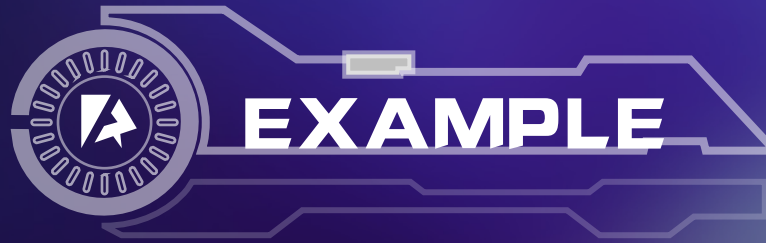
- The hacker should attack all AMMs at the same time to operate the price.
- The more aggregated AMMs, the harder they attack.



EXAMPLE



- The same clearing price is assigned to all orders within one batch.



Chainlink Automation is the infrastructure of batch swap:

- Create a time window and check that the swap volume and timestamp in a batch meet the requirements.
- Calculate the best price AMM then to do swap for tokens to balance demand.
- Automatic distribution tokens - users do not need to wait for results and claim token, token will be automatically withdrawn to users' account.

Thanks to all our Contributors

Contributors



@Taki13579



@0x_xiaotian



@chris2lauu



@punk2sang



@0xXiaoChen

THANK YOU



Yex Lab



ETH
SHANGHAI



Chainlink



ChainIDE
Swift, Simple, Smart