Elements of DeFi

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

Professor Pramod Viswanath

Princeton University

Lecture 9

Oracles

Last lecture: MEV and DeFi

- Ethereum allows proposer freedom to reorder
- Examples of MEV: Frontrunning, Sandwiching, JIT liquidity, etc.
- MEV as a centralizing force
- Priority gas auctions, Flashbots auctions
- Proposer-Builder separation
- Decentralized builders

This Lecture: Oracles

- Importing off-chain data
  - Token prices (e.g., BTC price for a BTC-ETH AMM on Ethereum)
- Price oracles
  - Oracle enabled DeFi applications
- Oracles designs
- Security, cost of manipulation and incentives
  - Dispute resolution

Data access for smart contracts

- Smart contracts access data stored within the chain
  - access state storage
- Accessing data on-chain is **secure**
  - Due to **consensus**: state data is created by transactions and nodes have consensus on the order of transactions

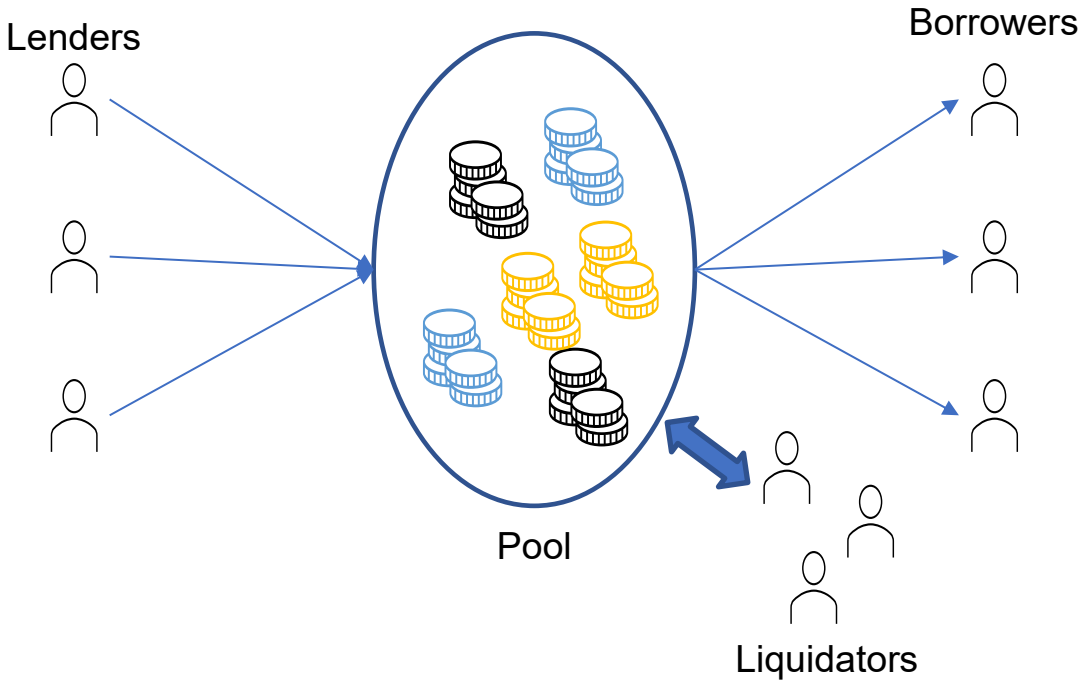
- Accessing data **outside** the blockchain requires additional infrastructure – **Oracles**
- Oracles can be thought of as any blockchain's "**internet connection**"

Need for importing external data

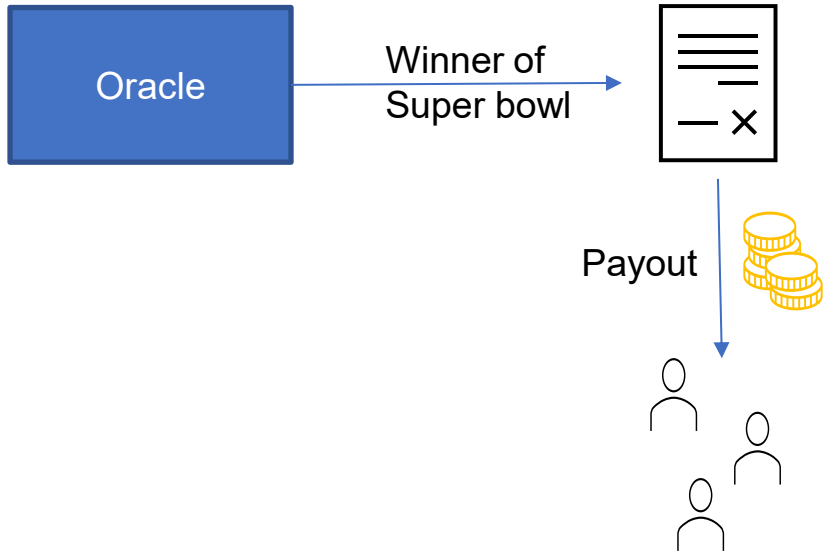
- Limited storage of on-chain data: can’t run the whole internet
- Need a reliable source of external events
  - Who won the super bowl?
  - Which flights were cancelled?
- Need to know state of other ledgers such as:
  - Other blockchains
  - Government land records
- Source of randomness

Oracle enabled DeFi applications

Borrow-lending protocols:
Enables liquidations of loans if collateral price drops

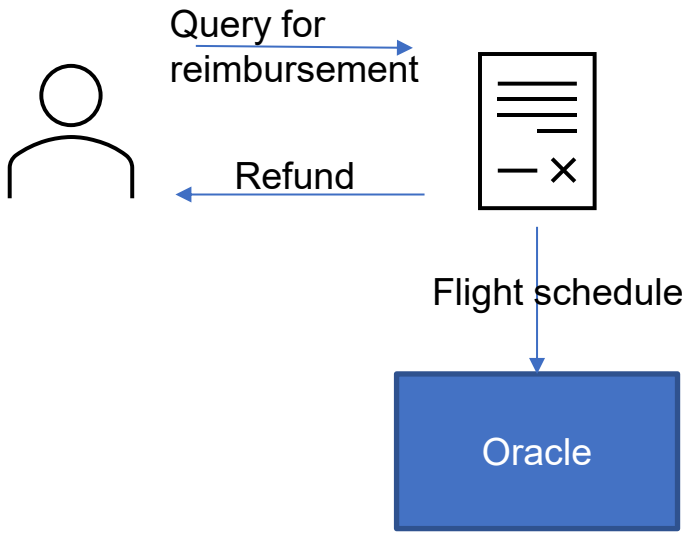


Betting markets:
Enables the betting contract to know the final result of an event

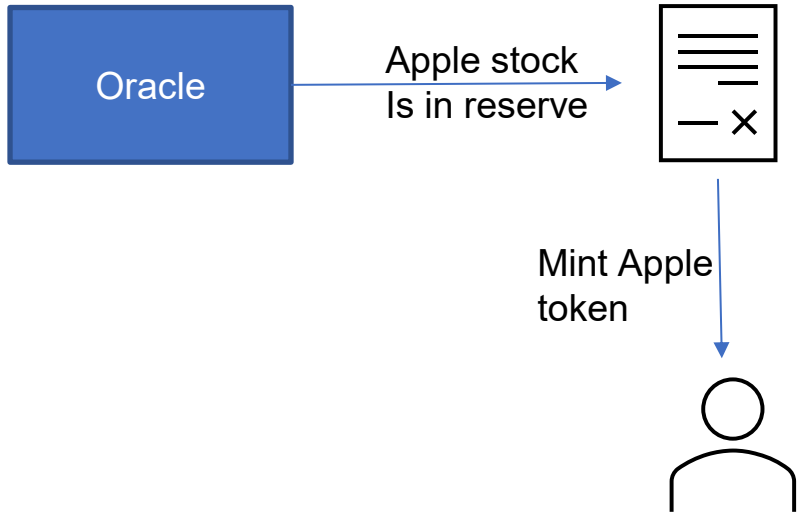


Oracle enabled DeFi applications

Flight insurance:
Enables contract to keep track of flight schedules

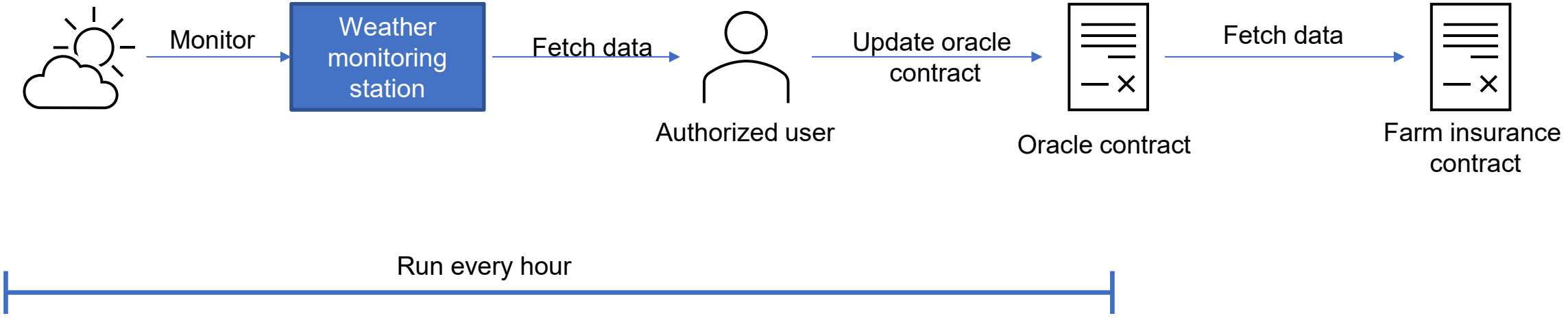


Real world asset synthetics:
Enables tokenization of real-world asset by proving ownership



Strawman oracle design

Consider an oracle providing weather in Princeton

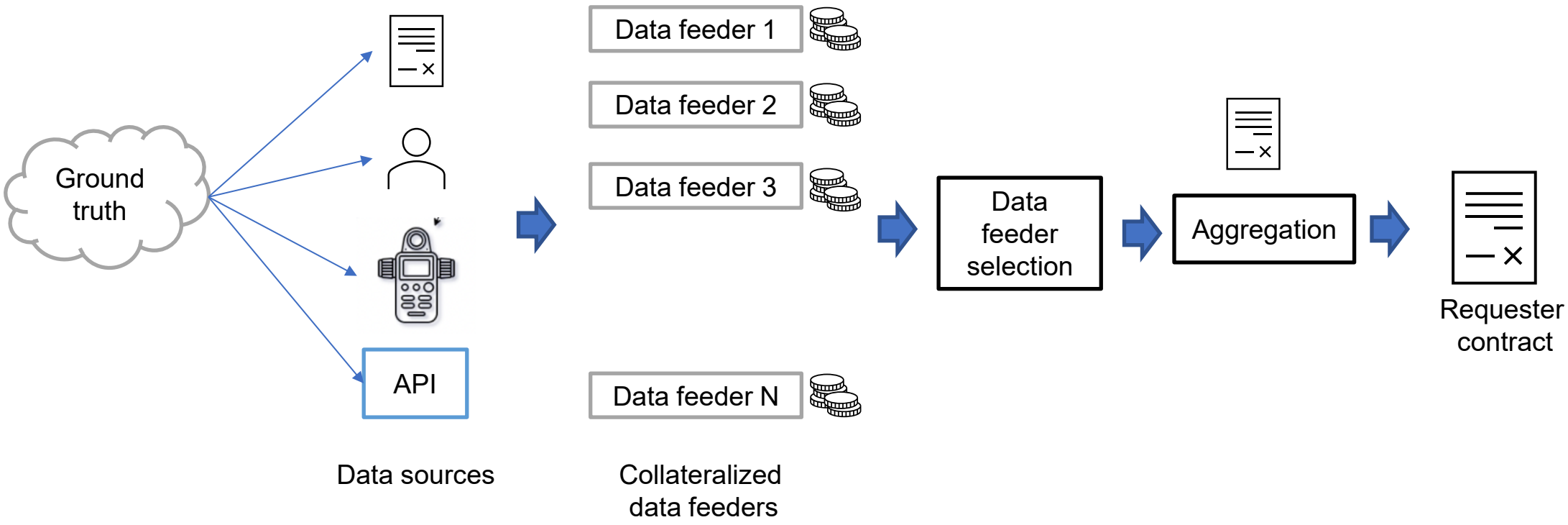


A single authorized user is responsible for updating the state of an oracle contract that stores weather data

Security vulnerabilities

- The single weather monitoring station might malfunction
- The authorized user may go offline resulting in stale data
- The authorized user can act adversarially -- input incorrect data
- Objective:
  - Remove single point of failure
  - Ensure robust data aggregation
  - Ensure reliable updates

General oracle architecture



Ground truth

- External data to be gathered by the oracle
- Ground truth should be visible to all participants in the oracle system
- Oracle is used if importing ground truth to the blockchain in a provable manner is either:
  - Impossible – Weather data
  - Expensive – State of another public blockchain

Data sources

- Measure and store ground truth

- Depending on the type of ground truth
  - Noise in measurements is tolerated – different weather monitoring stations
  - Noise may not be tolerated – winner of a publicized game, state of a finalized ledger

- Examples: Sensors, humans, other smart contracts, databases

Data feeder

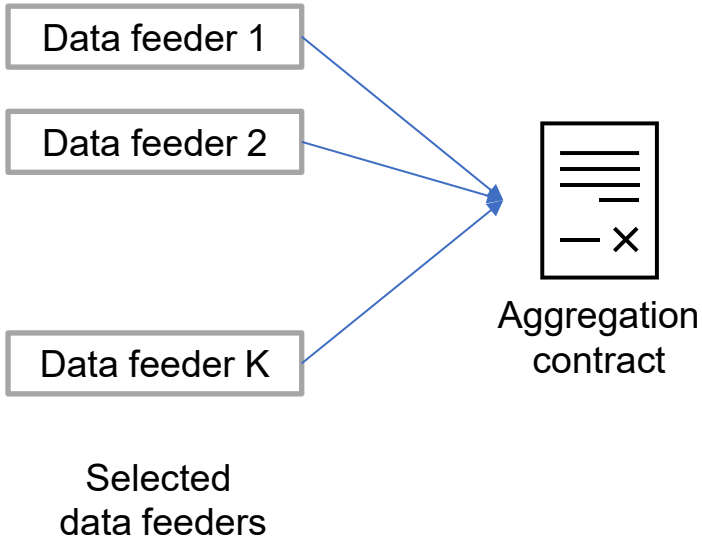
- Reports off-chain data to on-chain oracle contracts
- Incentivized by collateralization with staking rewards proportional to collateral or reputation
- Collateralization prevents sybil attacks
- Data feeder reporting may be periodic or triggered by an on-chain request

Data feeder selection

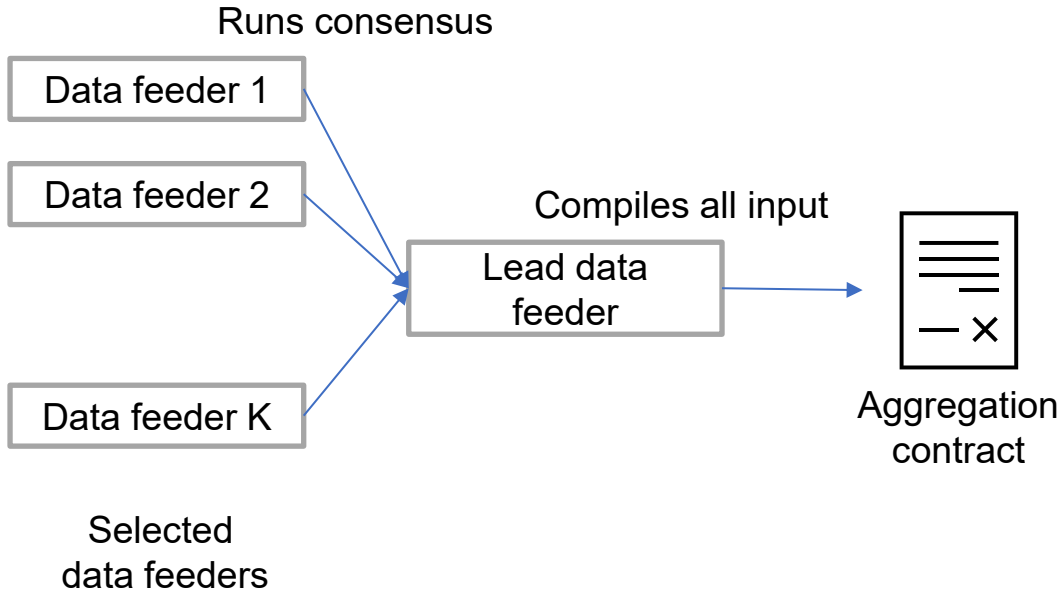
- The process of selecting what data-feeders report
- Selection needed for reputation incentivization and reducing on-chain transaction load
- Centralized selection: Restricts to a selected set of data feeders
- Decentralized selection: Random selection proportional to collateral/reputation

Aggregation

- Oracle contract receives a lot of reports from data feeders
- All inputs need to be aggregated to be used by a DeFi contract
- Two types of input reporting:



Direct reporting



Off-chain reporting

Aggregation: Robust statistics

- How to aggregate input:

- Option 1: Mean – easy to manipulate
- Princeton temperature: [32, 31, 32, 33, 150] -> Mean = 55.5 F

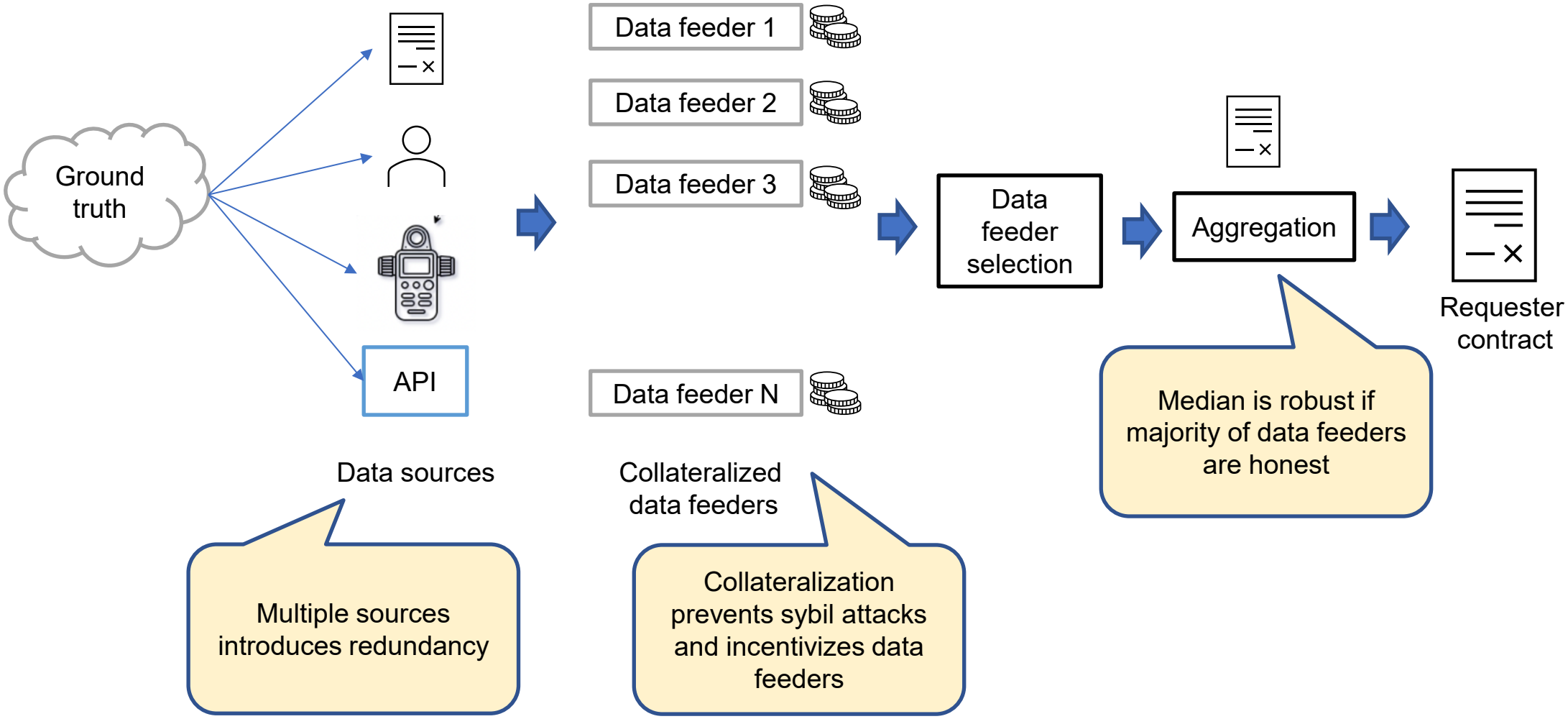
- Option 2: Median – Robust to changes by minority adversaries
- Princeton temperature: [32, 31, 32, 33, 150] -> Median = 32

- Option 3: Mode – Used for non-numerical data
- Flight status: [on-time, on-time, on-time, on-time, delayed] -> on-time

Dispute phase (optional)

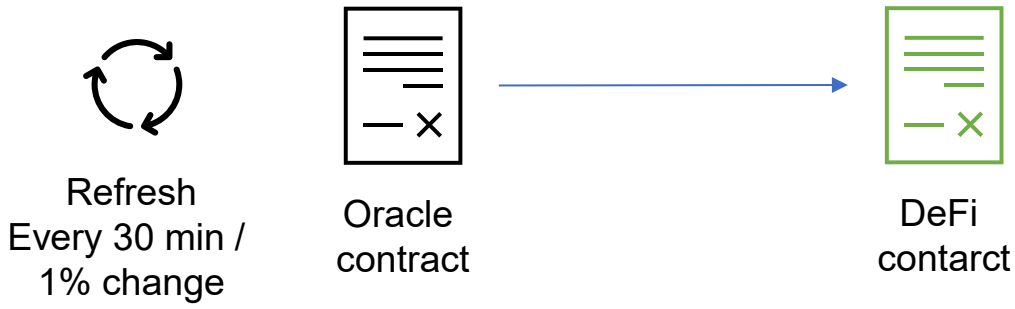
- Dispute can be reported within a time-frame to revert data
- Dispute phase involves utilizing an expensive data feeding option such as:
  - Select a larger set of data feeders
  - Provide proofs of inclusion, finalization on another chain
- Successful dispute may penalize original data feeders and reward challengers
- Penalty may involve slashing data feeder collateral

Oracle security



Oracle interaction models

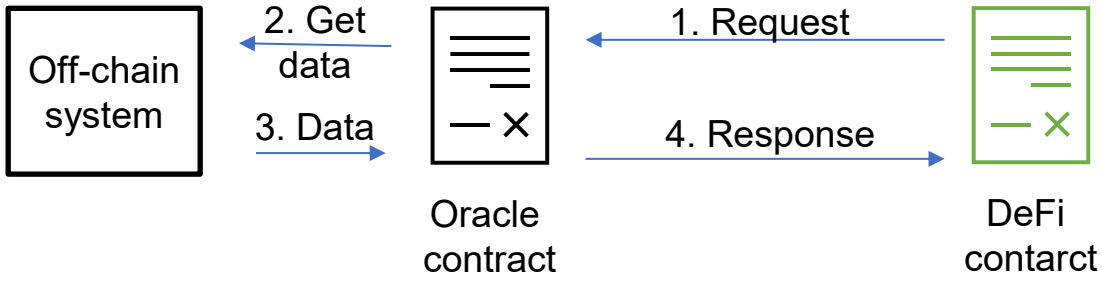
Feed



Used by most Price feed oracles

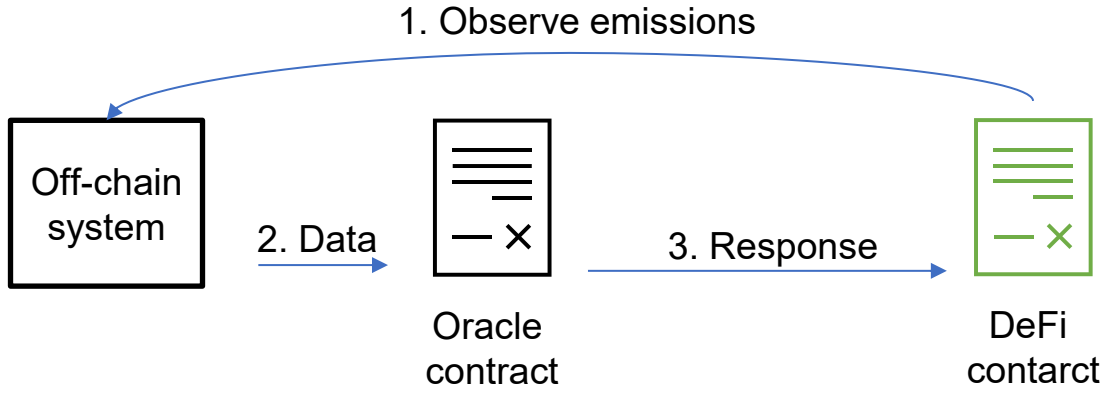
Oracle interaction models

Request-Response



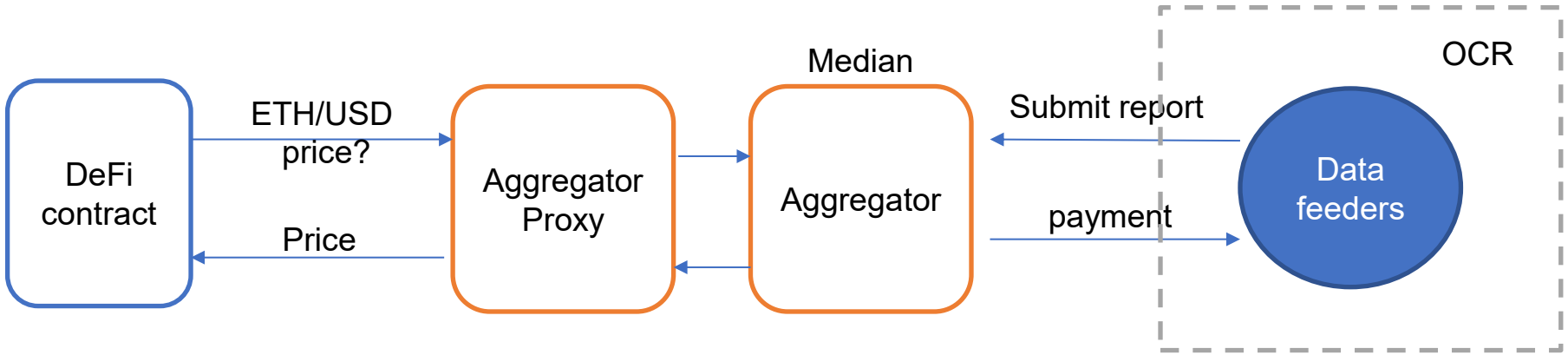
Similar to client-server API

Subscribe-Response



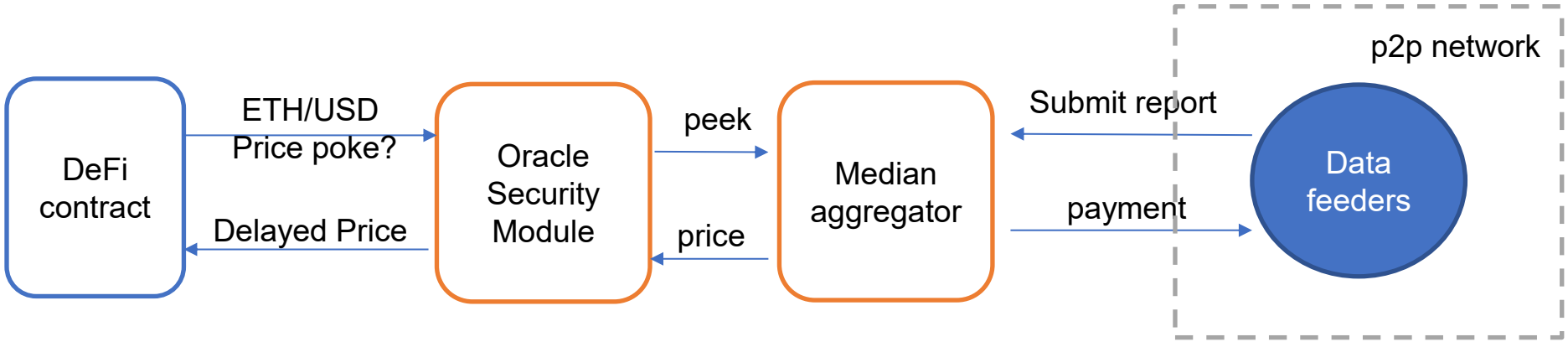
Subscription is pre-arranged

ChainLink price feed oracle design



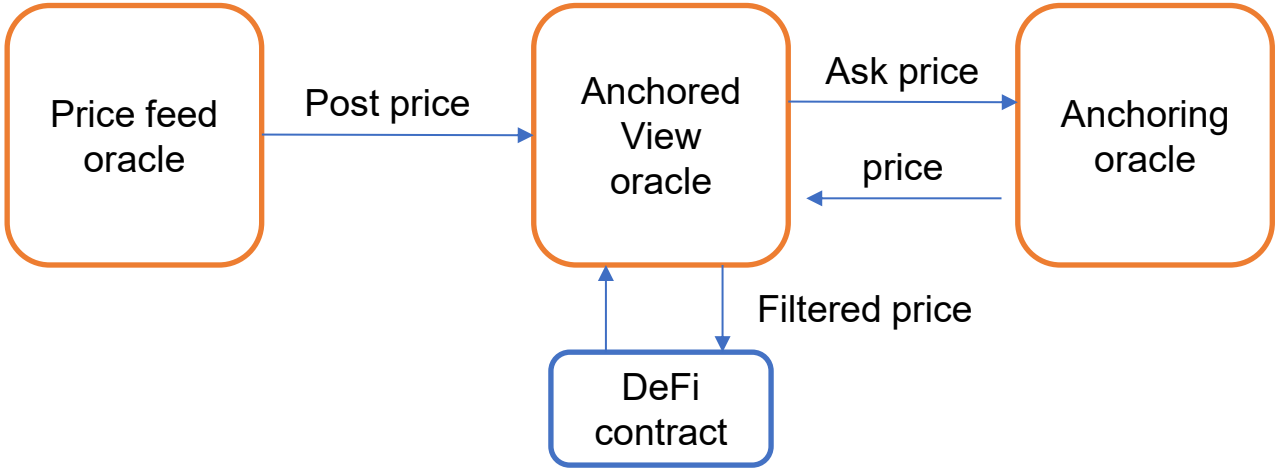
- Reports are submitted at fixed intervals or when price deviates a threshold percentage from last reported price
- Data feeders maintain a consensus amongst themselves and the leader reports data to the aggregator (off-chain reporting)

MakerDAO oracle design



- Oracle Security module reveals a delayed price to ensure that oracle attack can be constrained within Median aggregator
- DeFi contracts can choose to get the more secure delayed data via the *poke()* call or a less secure current data using a *peek()* call

Compound oracle design



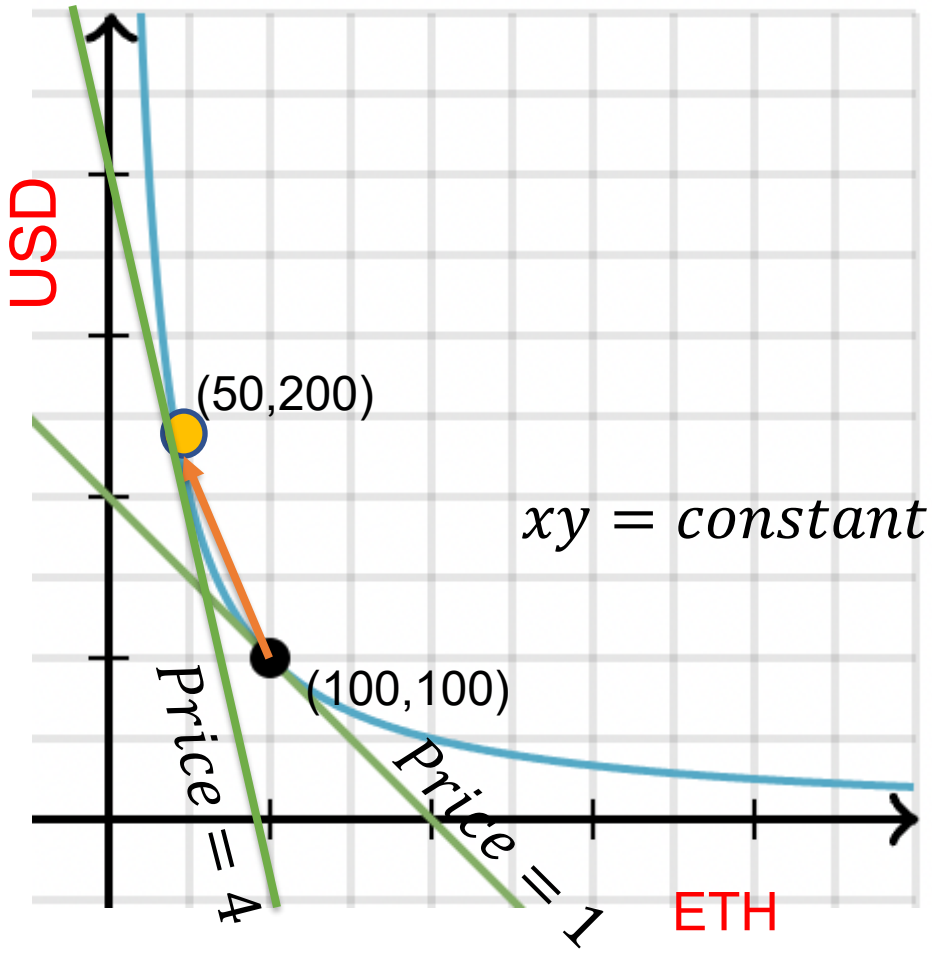
- If (Price feed posted price close to anchoring oracle price):
  - Filtered price = Price feed posted price
- else:
  - Filtered price = anchoring oracle price
- Anchoring oracle is typically an on-chain AMM (protection against price feed oracle attacks)

AMMs as price oracles

- AMMs maintain price between two assets by arbitrage
- Example:
  - If ETH/USD price is below the off-chain market value, buy ETH and sell it off-chain
  - If ETH/USD price is above the off-chain market value, buy ETH off-chain and sell it on the AMM
- Arbitrageurs add information of off-chain price on-chain through this process
- We can use this as a price-feed oracle
- Covered in detail in next

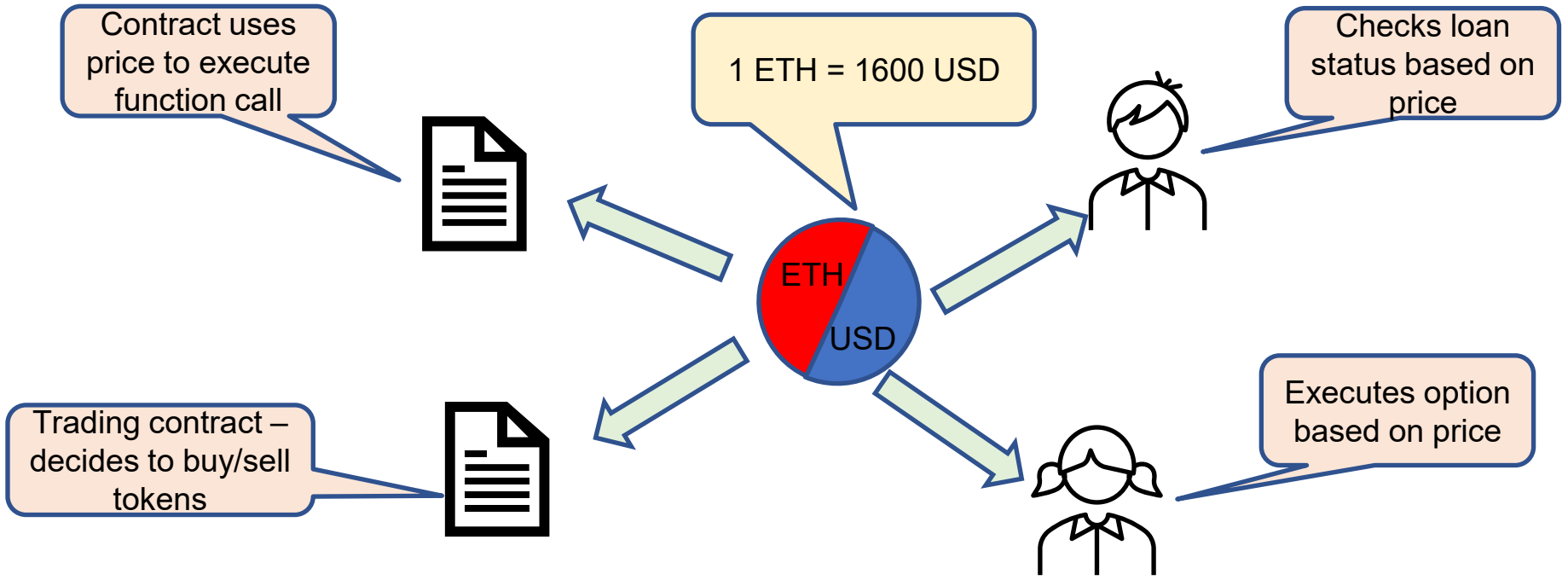
AMMs as price oracles

- Can DeFi elements serve as accurate price reporters?
- CFMMs! - reserves move to match price
- Use the aggregate data across multiple CFMMs
- What ensures that the prices stay in line?



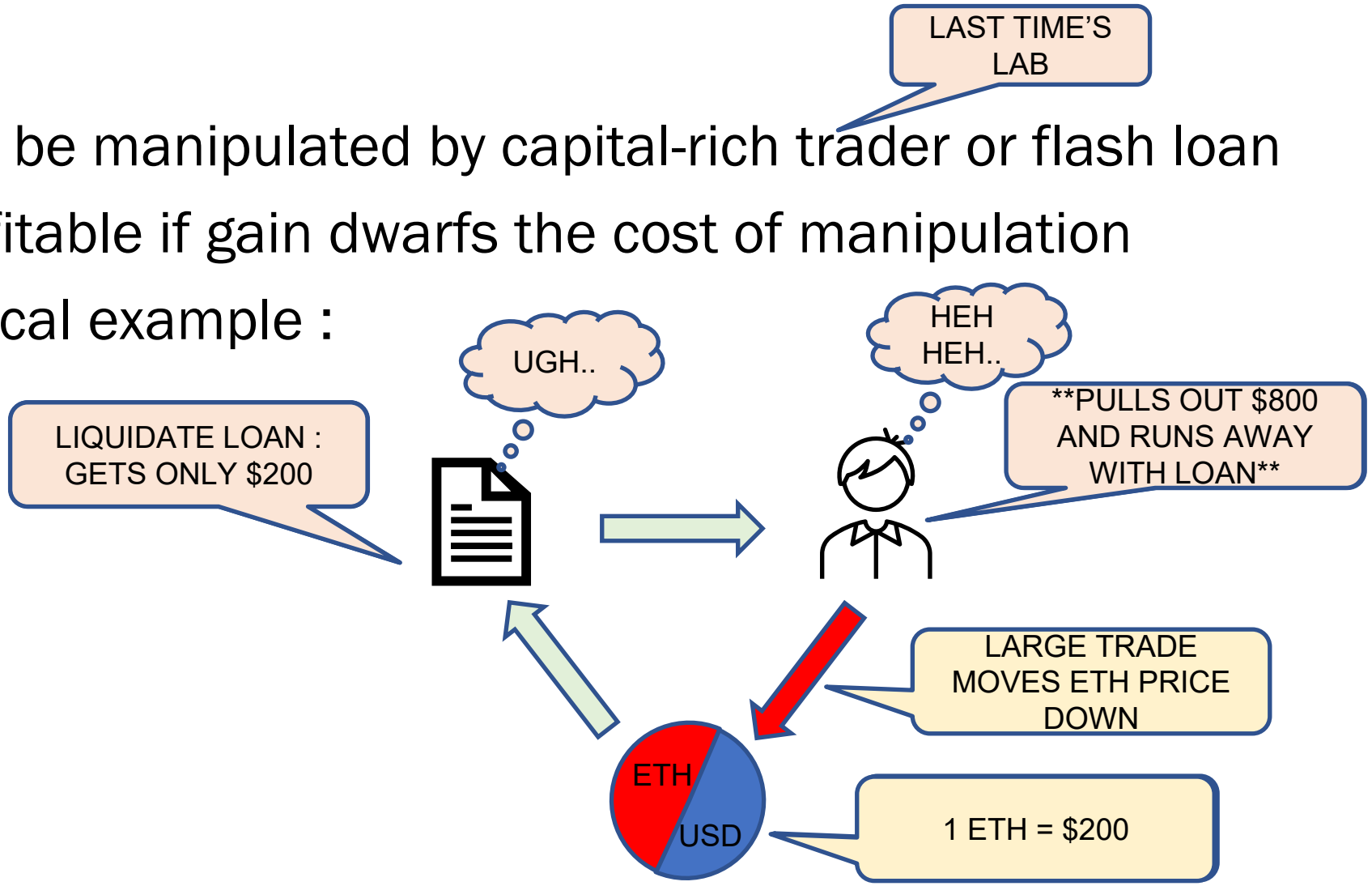
Strawman price oracle

- Naïve way : Query price of CFMM and use it for your purposes
- Problem?



Security vulnerability of strawman oracle

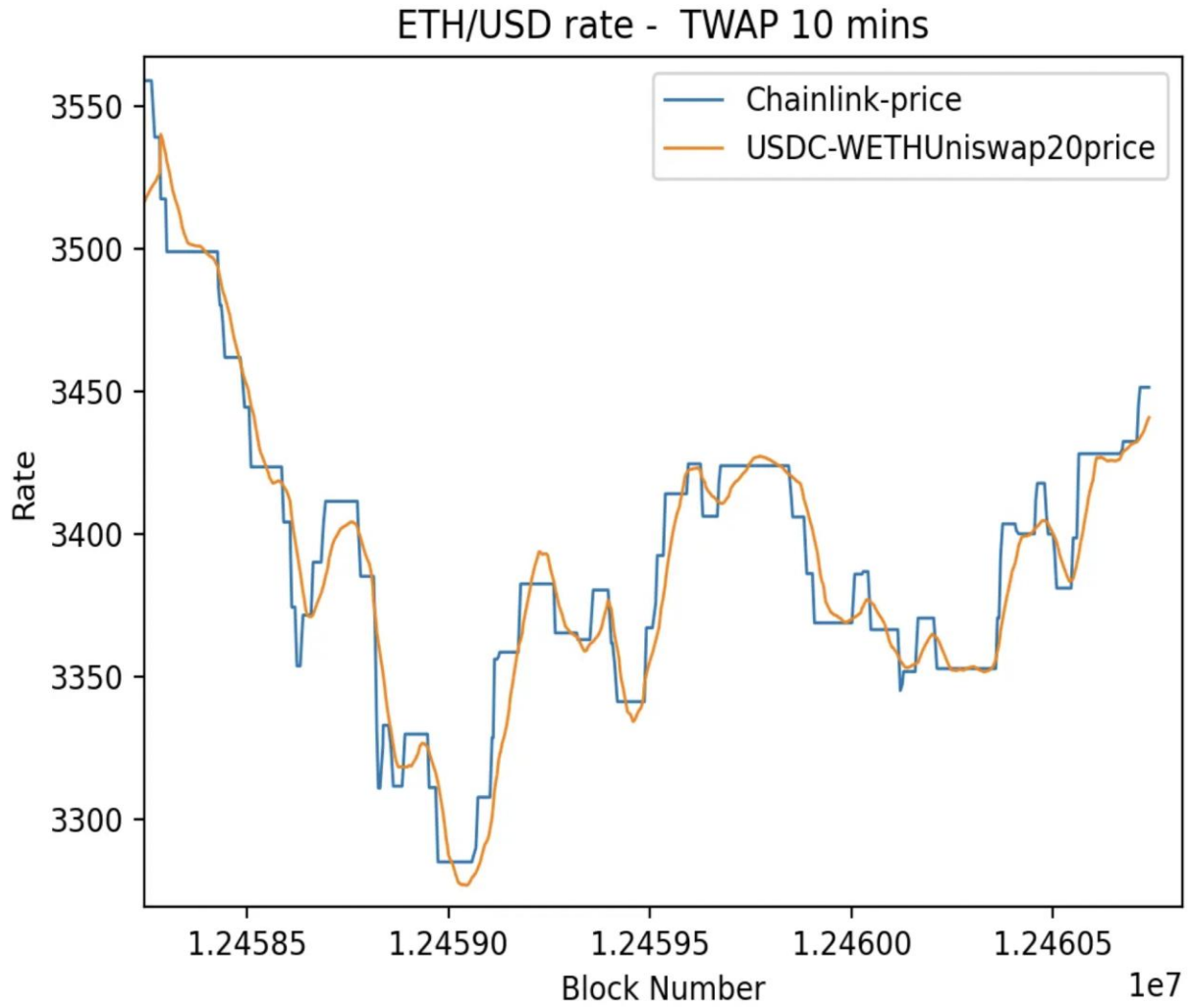
- Can be manipulated by capital-rich trader or flash loan
- Profitable if gain dwarfs the cost of manipulation
- Typical example :



TWAP feed

TIME WEIGHTED AVERAGE PRCING

- Need to make price robust to manipulation
- Take weighted average over recent history
- Costlier to manipulate – why?
- Cannot use “flash” loans



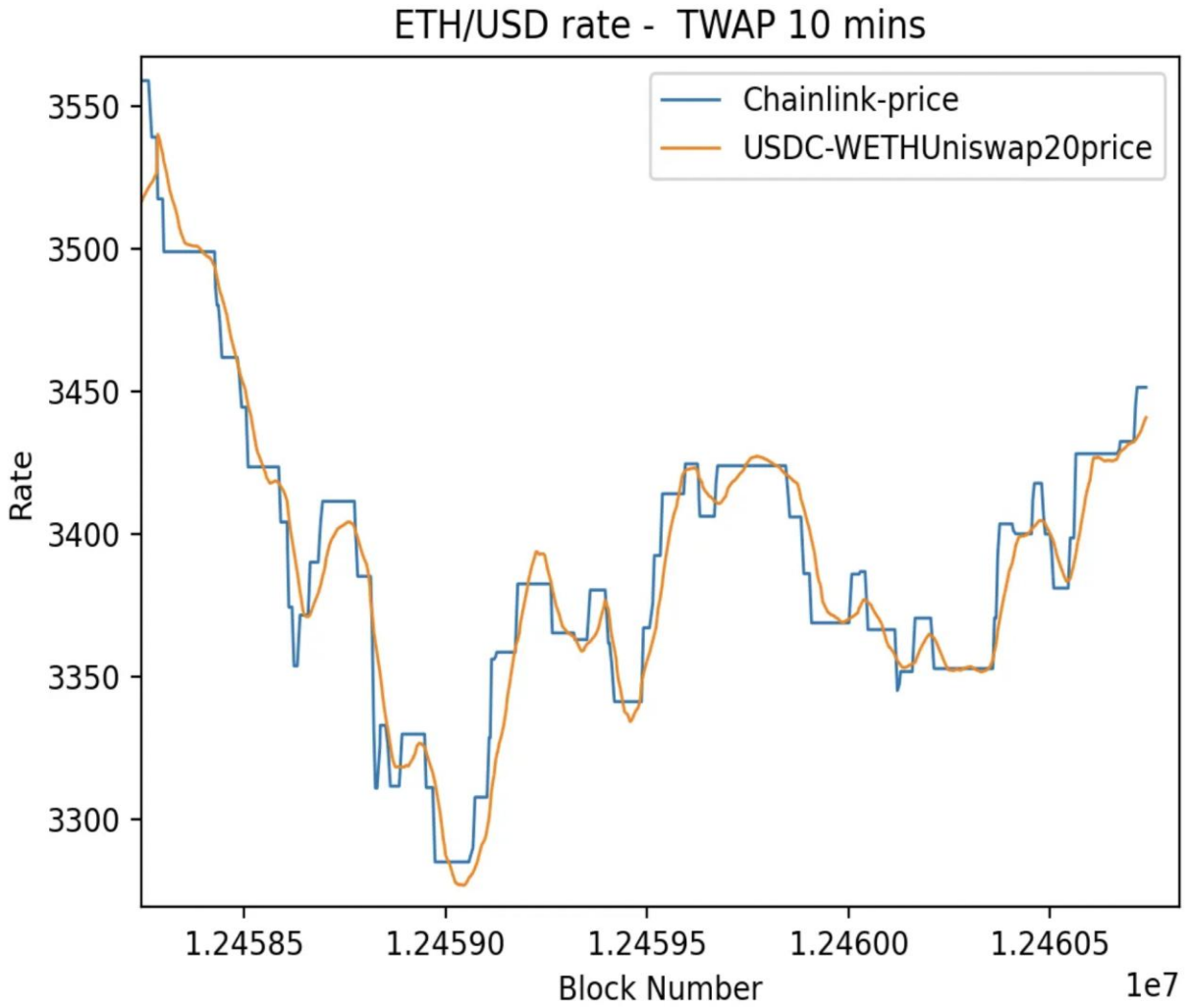
TWAP feed

TIME WEIGHTED AVERAGE PRCING

What's wrong with it?

- Tradeoff?
  - Accuracy vs Manipulability

- TWAP price is more robust but not as fresh as AMM price
- Market coverage limited by one AMM
- Thinly traded/illiquid tokens still easy to manipulate



VWAP feed

VOLUME WEIGHTED AVERAGE PRCING

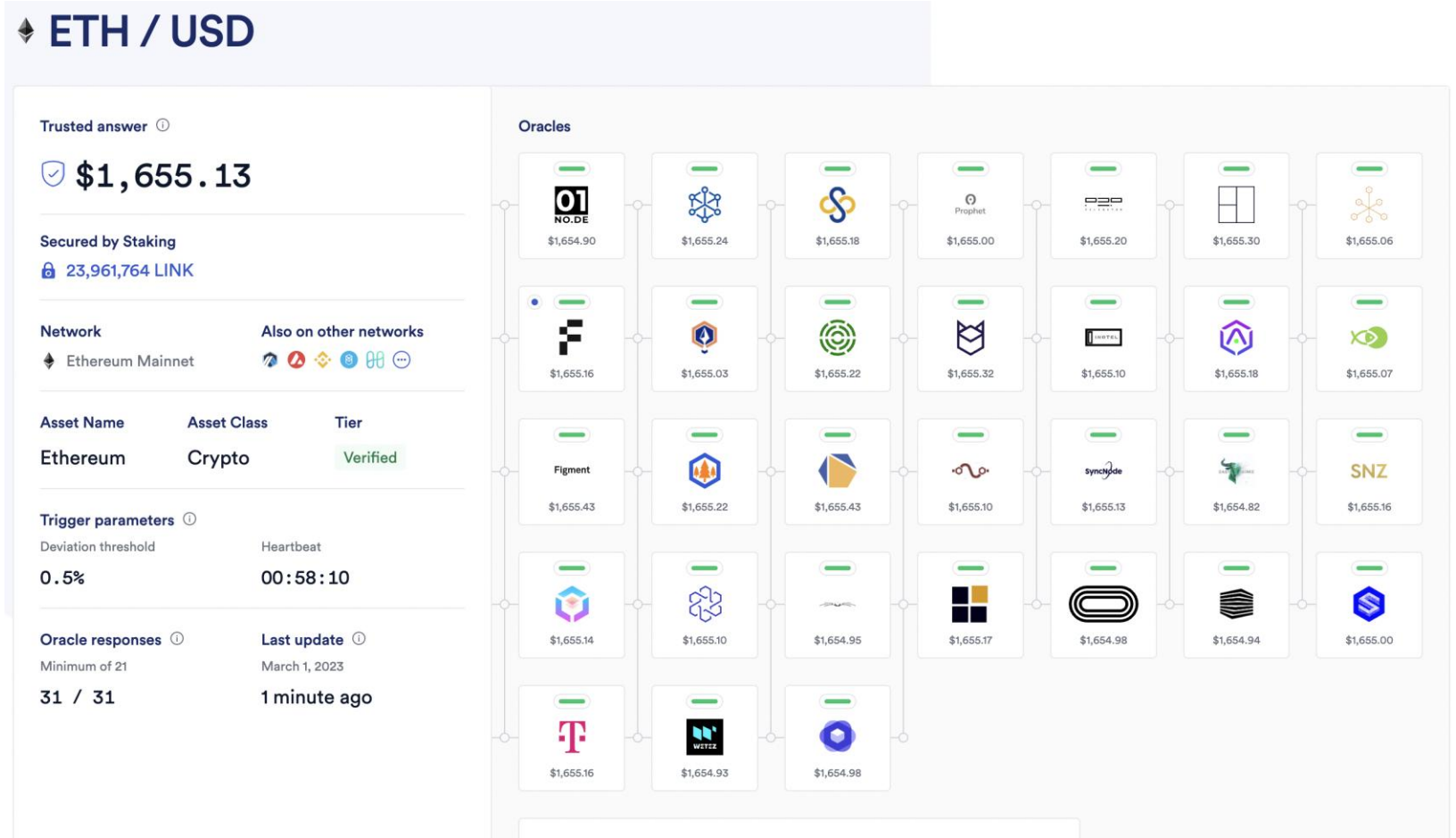
- Need to ensure freshness *and* robustness to manipulation
- Aggregate data from multiple AMMs and weight them by trade volume or liquidity

$$P^t_{oracle} = \frac{\sum_{exchanges} v_i^t P_i^t}{\sum_{exchanges} v_i^t}$$

- Provides market coverage
- No tradeoff between freshness and accuracy
- Need to change market price everywhere for successful manipulation

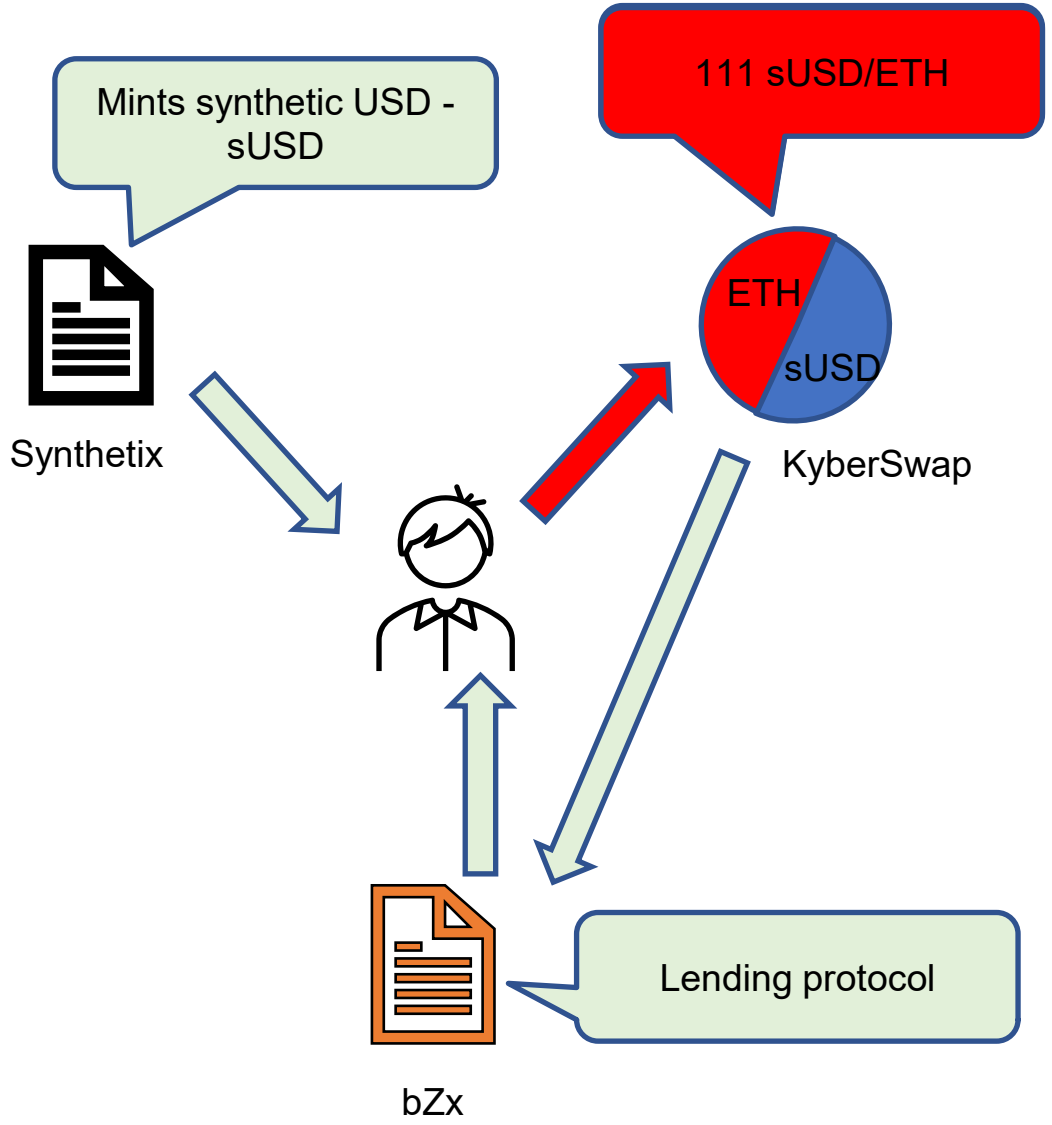
VWAP feed

- E.g. Chainlink – uses multiple exchange and protocol price sources



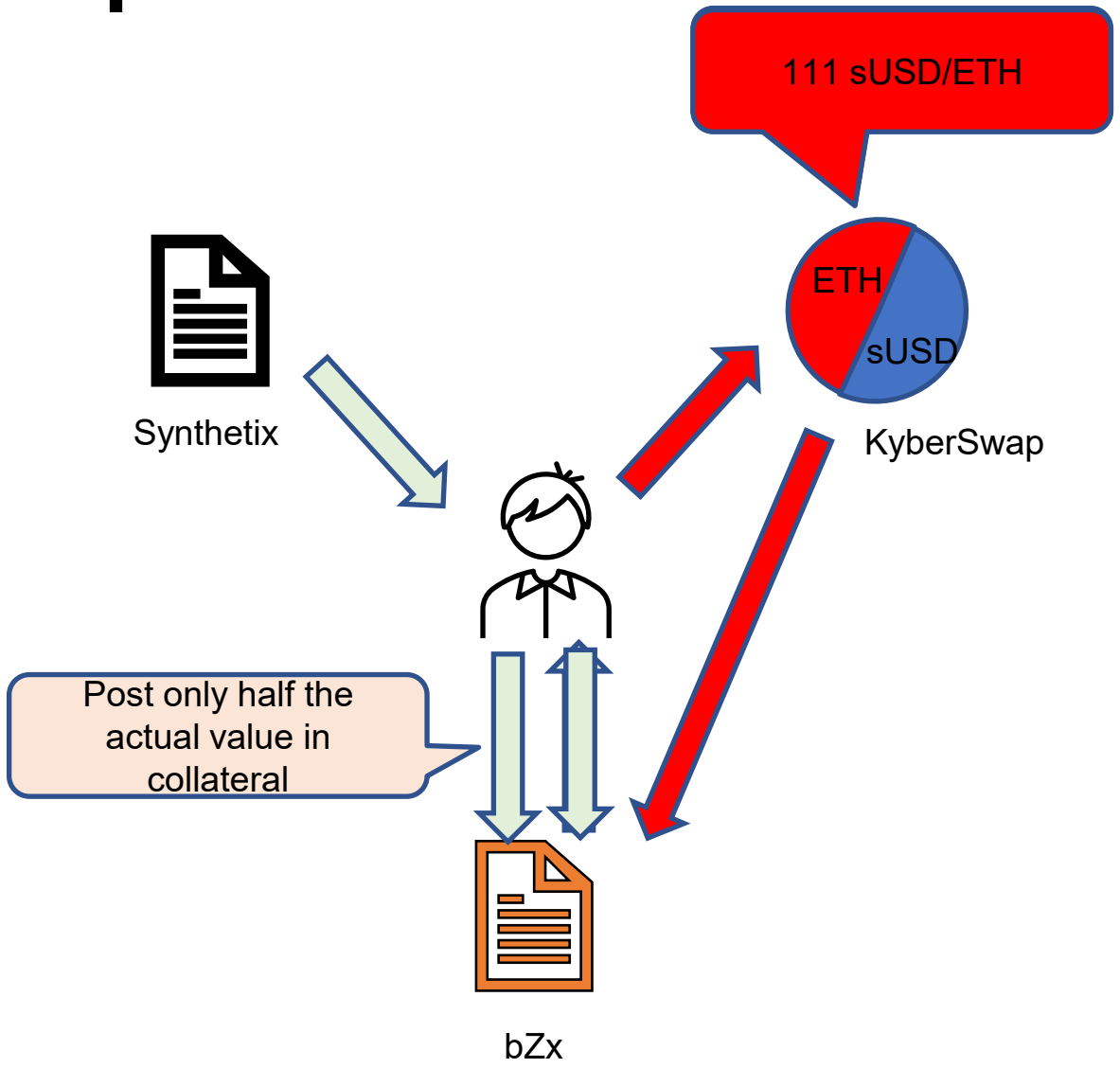
Attacks: BzX Oracle manipulation -2020

- Step 1 : Borrow 7500 ETH from bZX – promise to repay in same block (flash loan)
- Step 2 : Sell 900 ETH on Kyber pool
- Step 3 : Get 943k sUSD for 3518 ETH on Synthetix



Attacks: BzX Oracle manipulation

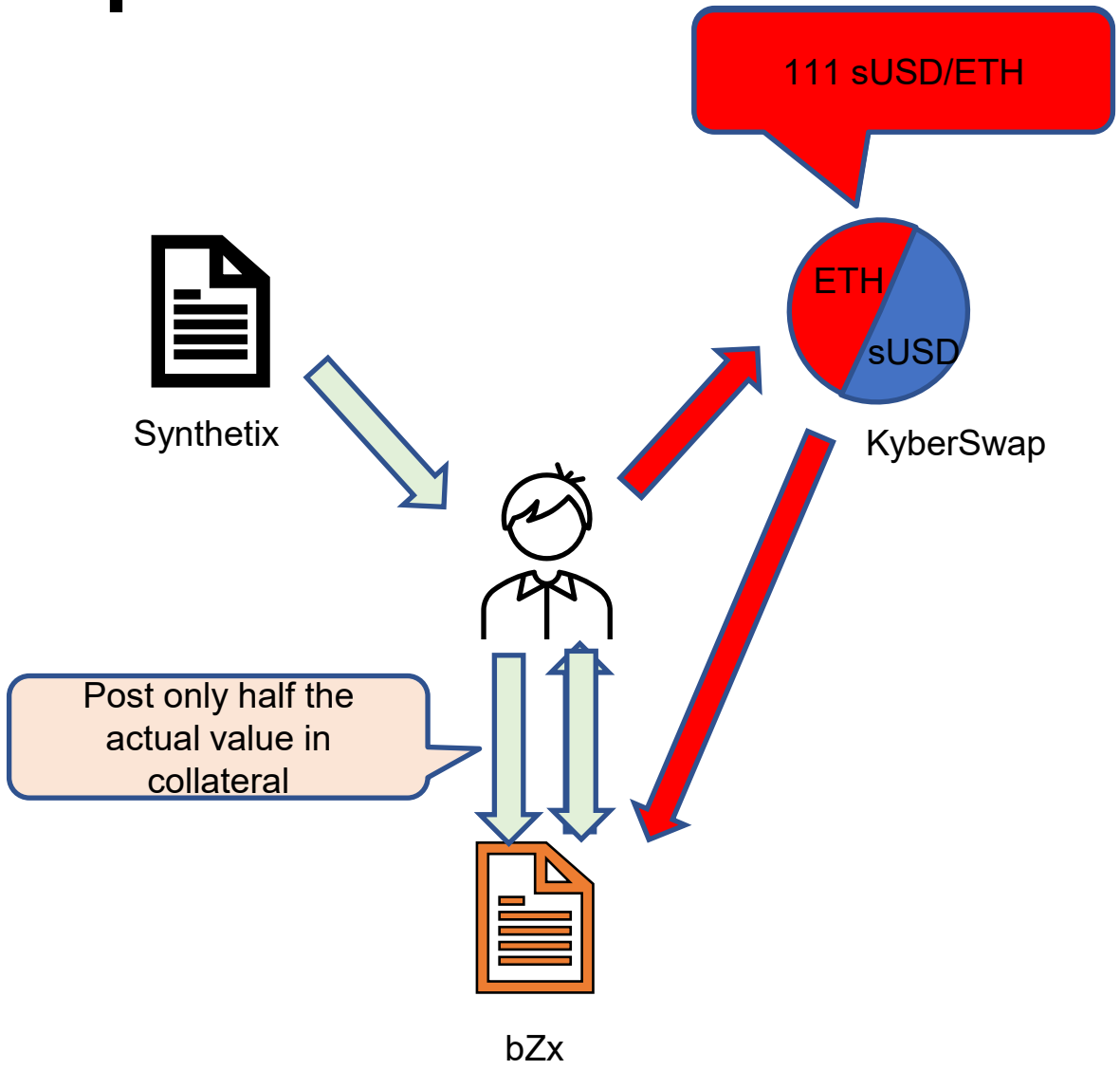
- Step 4 : Borrow 6796 ETH from bZX – post collateral which is priced through Kyber – 1099k sUSD
- Step 5 : Repay 7500 ETH flash loan
- Step 6 : Run away with 2378 ETH profit!



Attacks: BzX Oracle manipulation

Main flaws exploited?

- Lending relied on only one AMM as oracle
- Oracle lacked sufficient liquidity
- sUSD Token very thinly traded



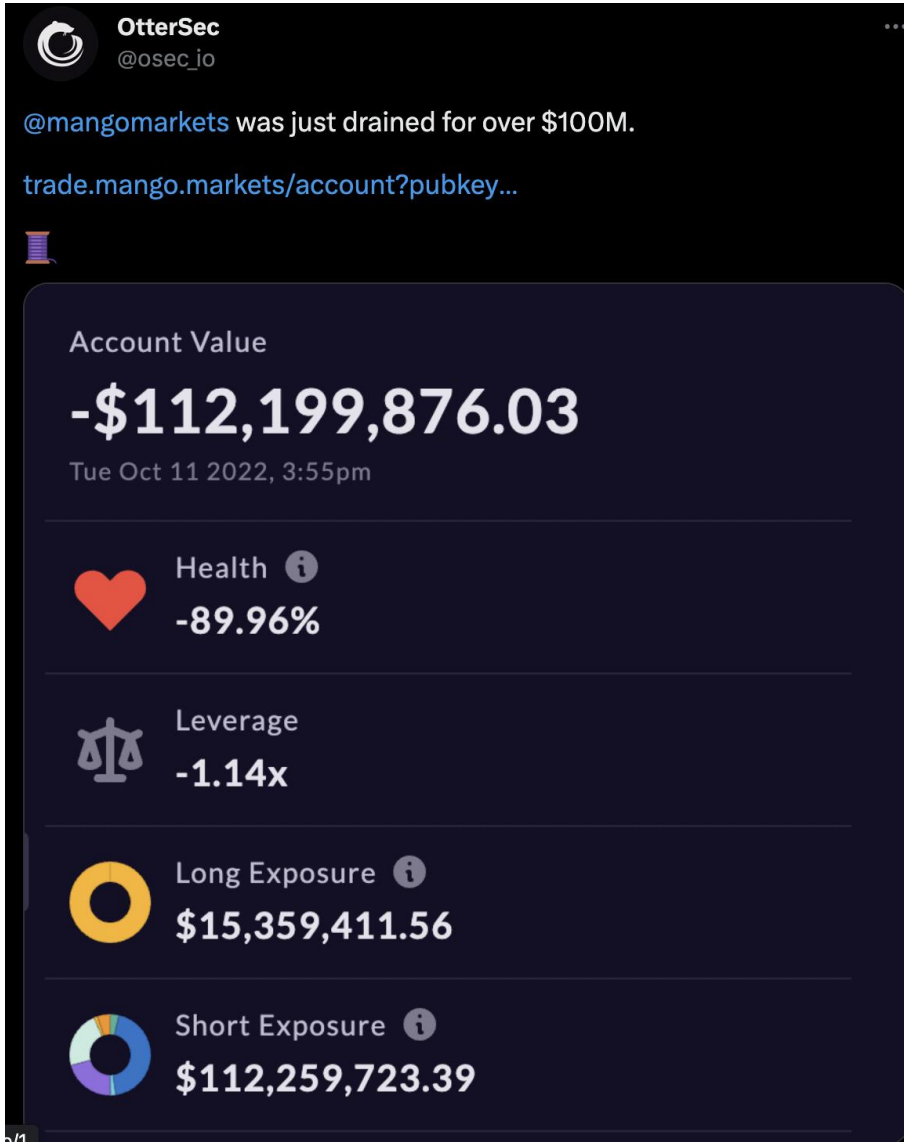
Attacks: Mango attack - 2022

- Similar attack happened on the thinly traded MNGO token of the Mango lending protocol on Solana

- Attack :
  - Drive up MNGO price to make it valuable on an AMM
    - AMM was the sole oracle for the Mango lending protocol
  - Borrow large amount of USDC by posting MNGO as collateral
  - Run away with USDC
  - Over $100M stolen

Attacks: Mango attack - 2022

- Attacker confessed on twitter, agreed to pay back
- Mango DAO refuses deal – sues attacker for “unlawful bargaining”
- Arrested by FBI in Dec 2022 on counts of commodities fraud and manipulation
- SEC, CFTC added charges of market manipulation as well
- First person to be arrested for manipulating a decentralized market



Open problems

- Formalized cost and profit analysis
- Dispute resolution for cross-chain oracles
- Multi-block MEV attacks – price manipulation of oracles easier if proposer controls multiple blocks in a row
- Legal framework around DeFi attacks?
- Privacy preserving Oracles?

LECTURE ENDS