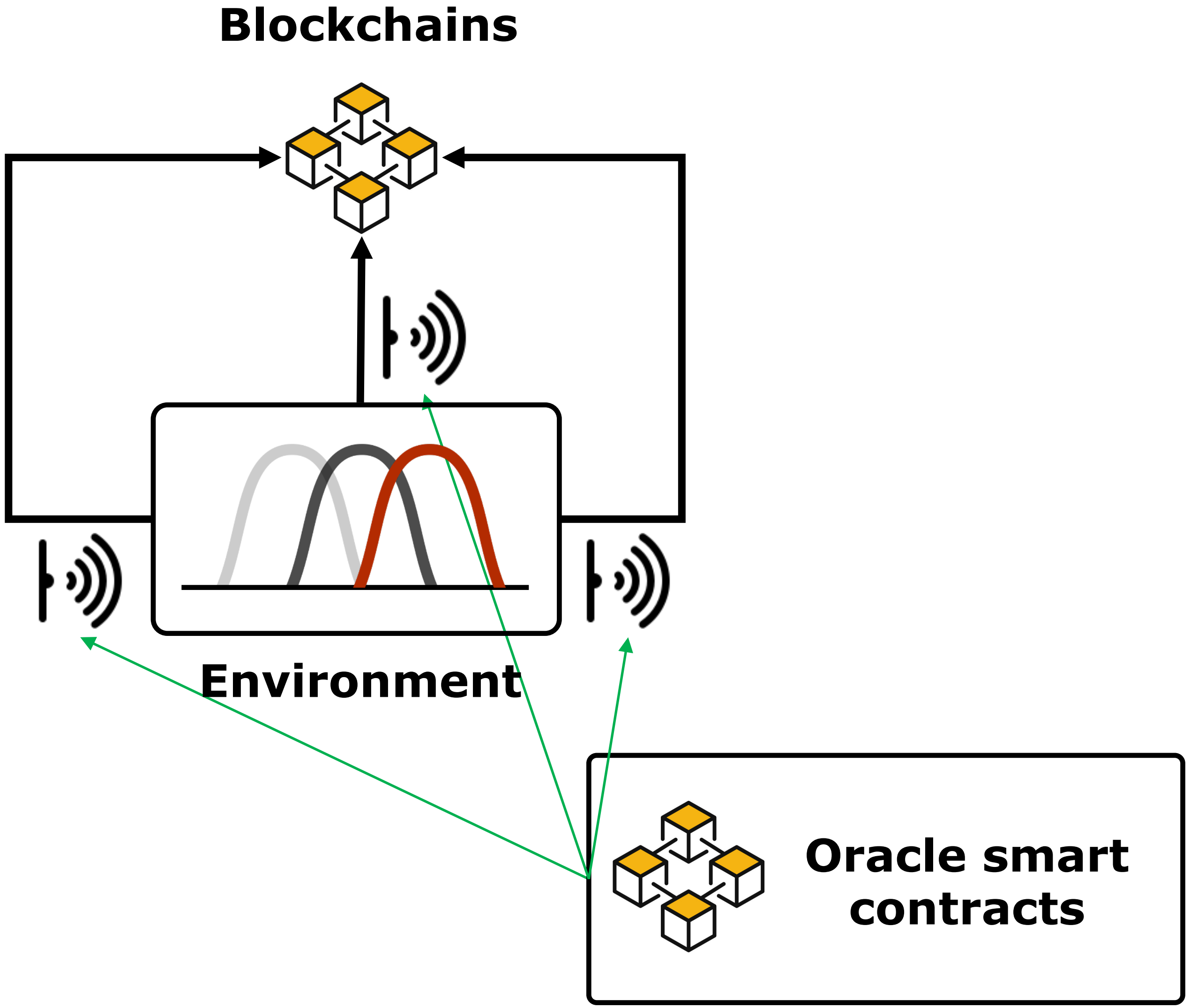
ACon^2: Adaptive Conformal Consensus for Provable Blockchain Oracles

Sangdon Park Osbert Bastani Taesoo Kim

Georgia Tech Penn University of Pennsylvania POSTECH

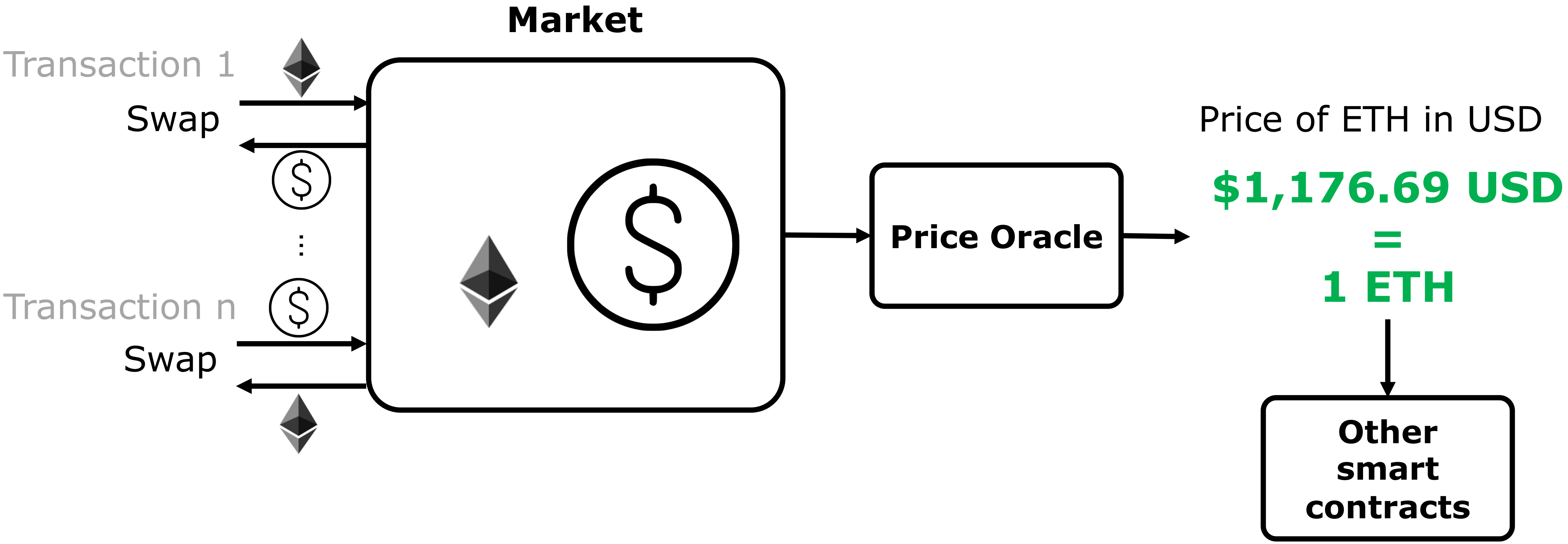
Oracle Smart Contracts in Blockchains

"Sensors" of Blockchains



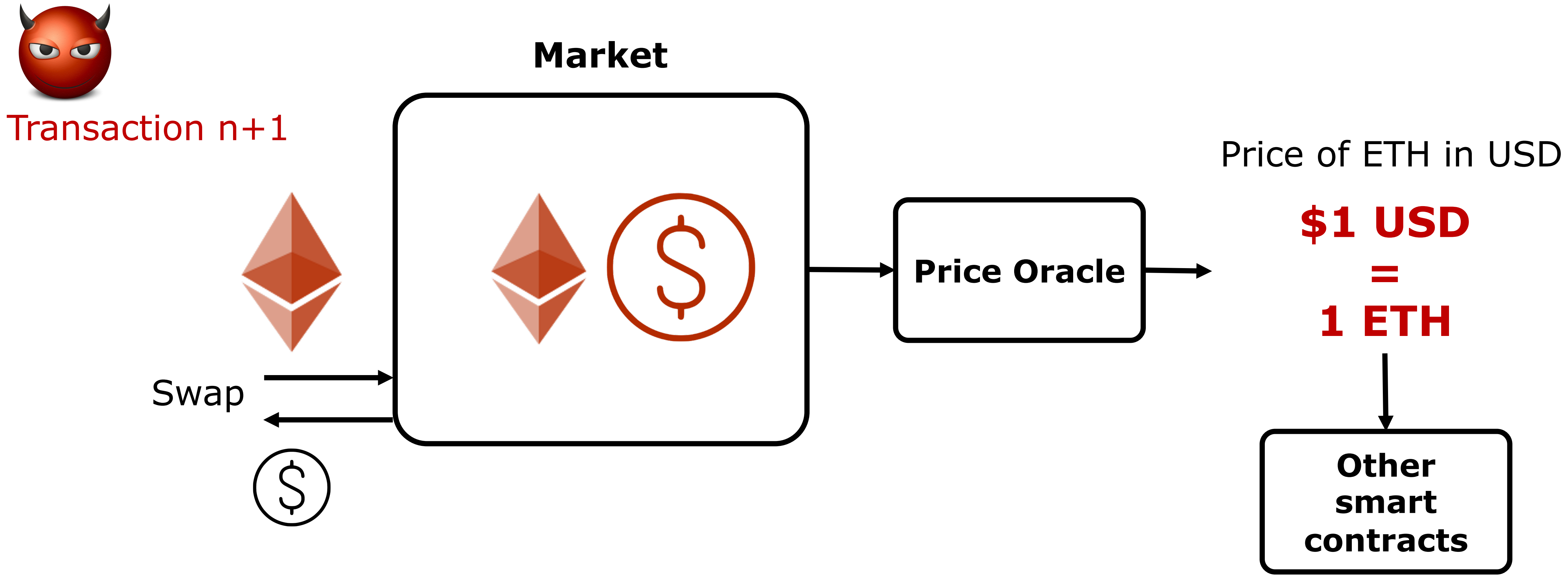
An Example of Oracle Smart Contracts

Price Oracle



An Example of Oracle Smart Contracts

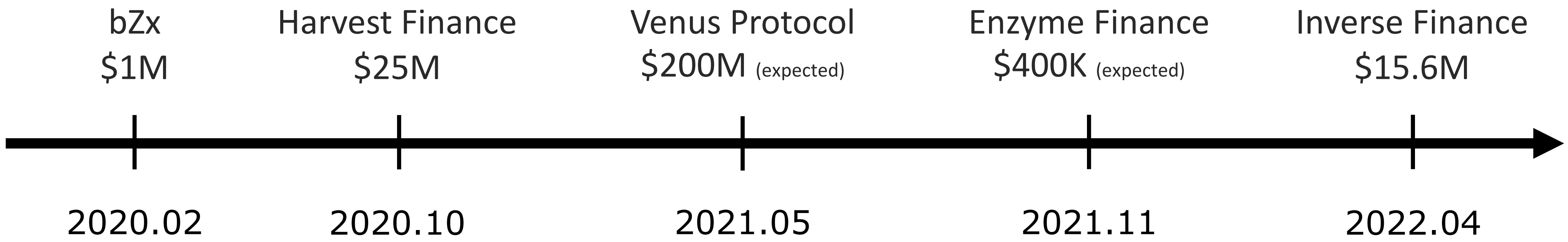
Price Oracle



Called **Oracle Manipulation**

Oracle Manipulation Is Serious

Price Oracle Manipulation on Decentralized Finance (DeFi) Protocols in Ethereum



bZx
$1M
2020.02

Harvest Finance
$25M
2020.10

Venus Protocol
$200M (expected)
2021.05

Enzyme Finance
$400K (expected)
2021.11

Inverse Finance
$15.6M
2022.04

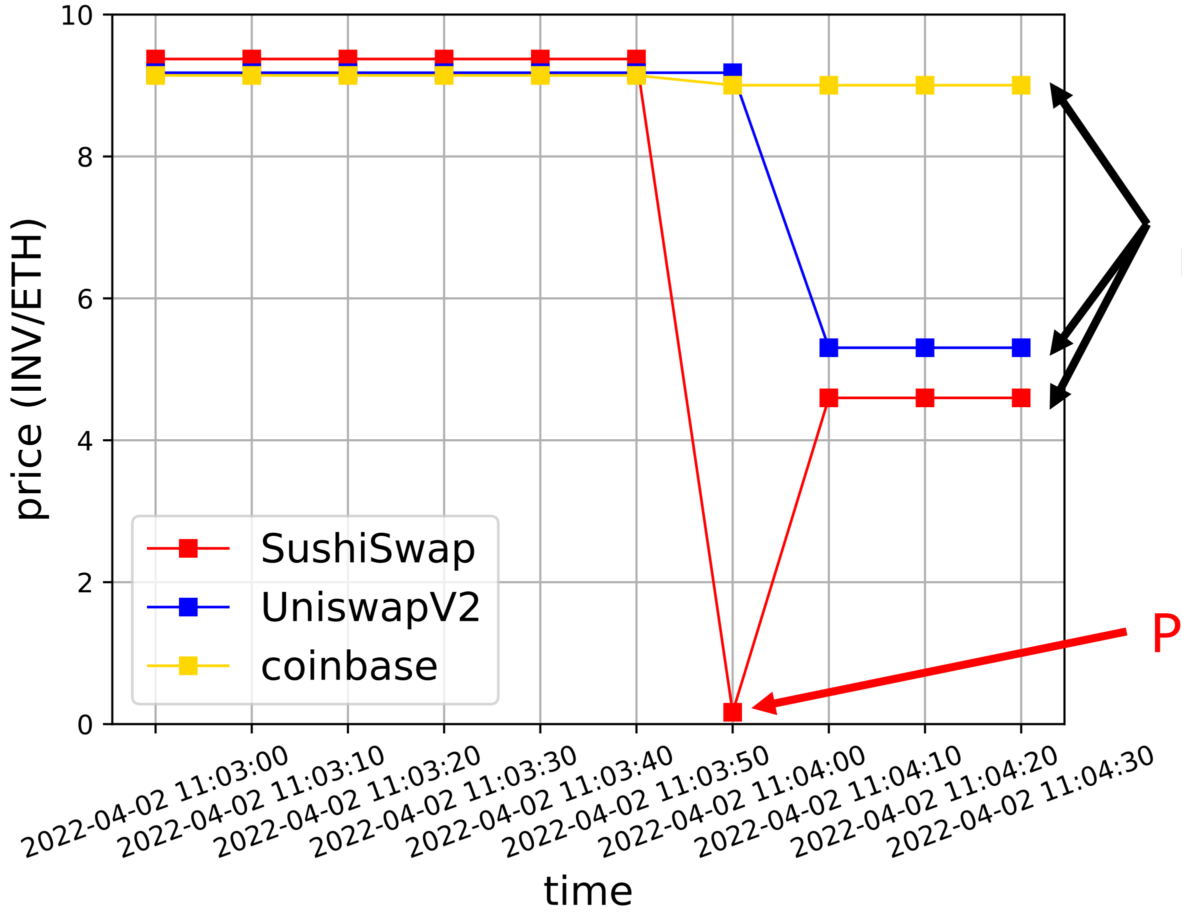
Oracle manipulation should be rigorously addressed!

Source: https://rekt.news/

Closer Look At Price Manipulation

Inverse Finance Incident

Inverse Finance
$15.6M attack on
2022.04



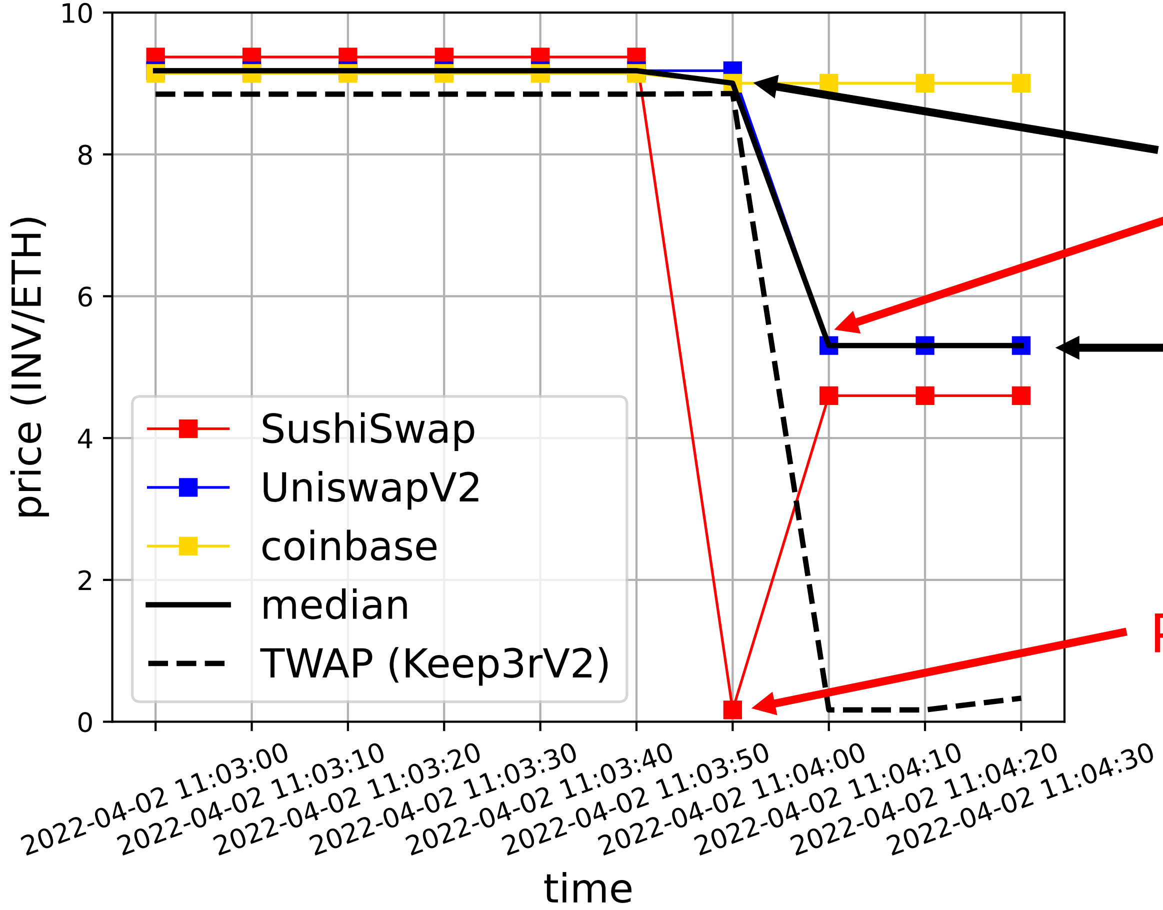
Can we leverage multiple markets?

Price manipulation

Mitigation of Price Manipulation

Median of Multiple Oracles

Inverse Finance
$15.6M attack on
2022.04



✓ Simple

✓ Robust

✗ Affected, but no anomaly signal

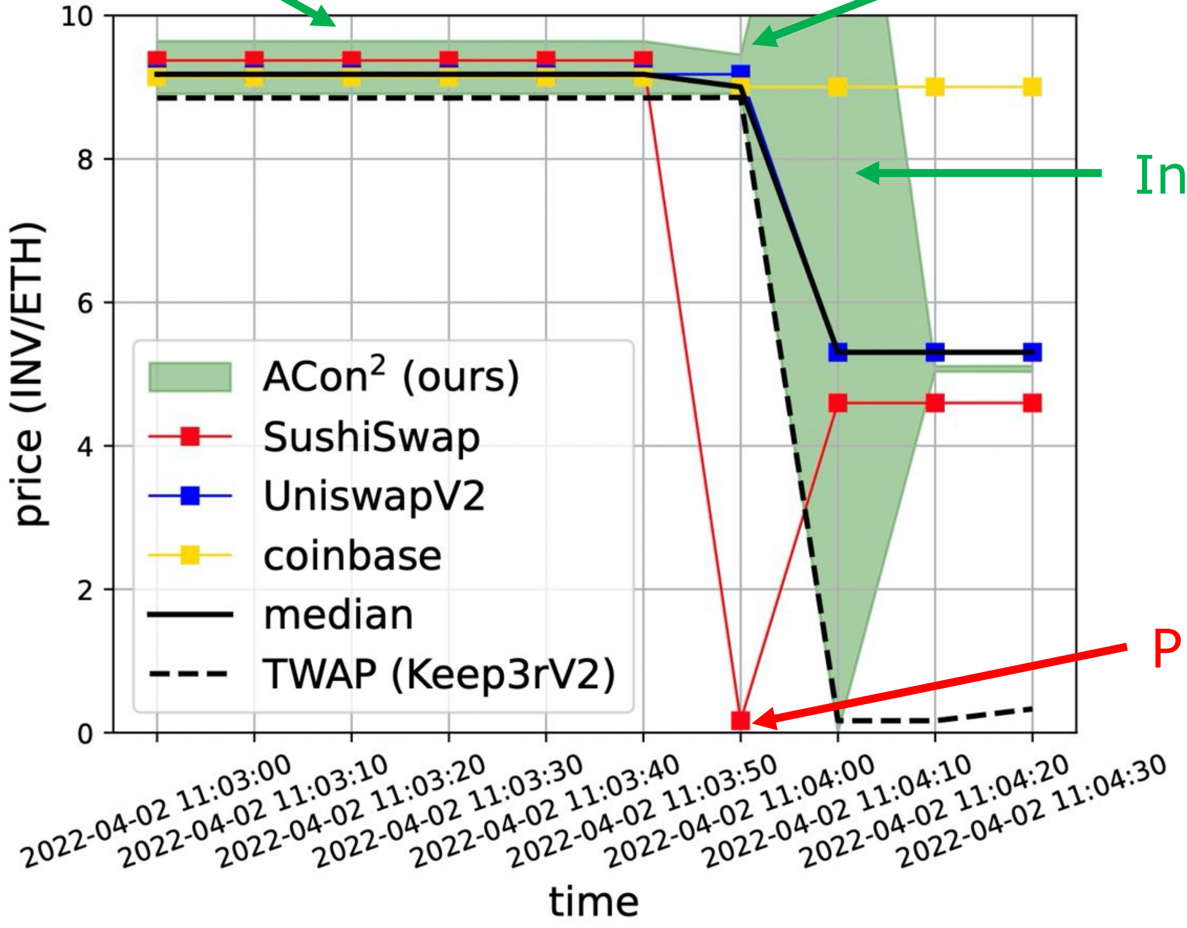
median

Price manipulation

Median mitigation works but less informed

→ Uncertainty helps more informed decision

Idea: Leverage Uncertainty for Consensus!



Closely predict price ranges

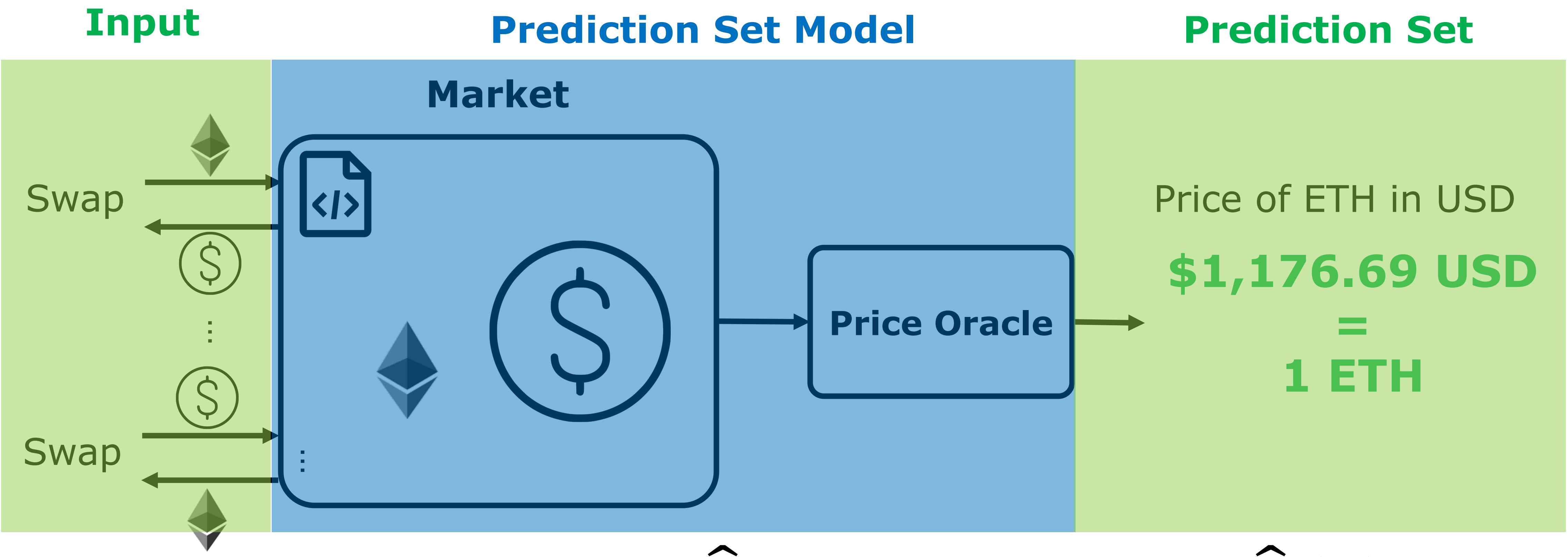
Make consensus

Inform an anomaly signal

Price manipulation

How to Represent Uncertainty?

Oracle Smart Contract = Prediction Set Model in ML



Input

Prediction Set Model

Prediction Set

Market

Swap

Swap

Price Oracle

Price of ETH in USD

$1,176.69 USD

=

1 ETH

x_t

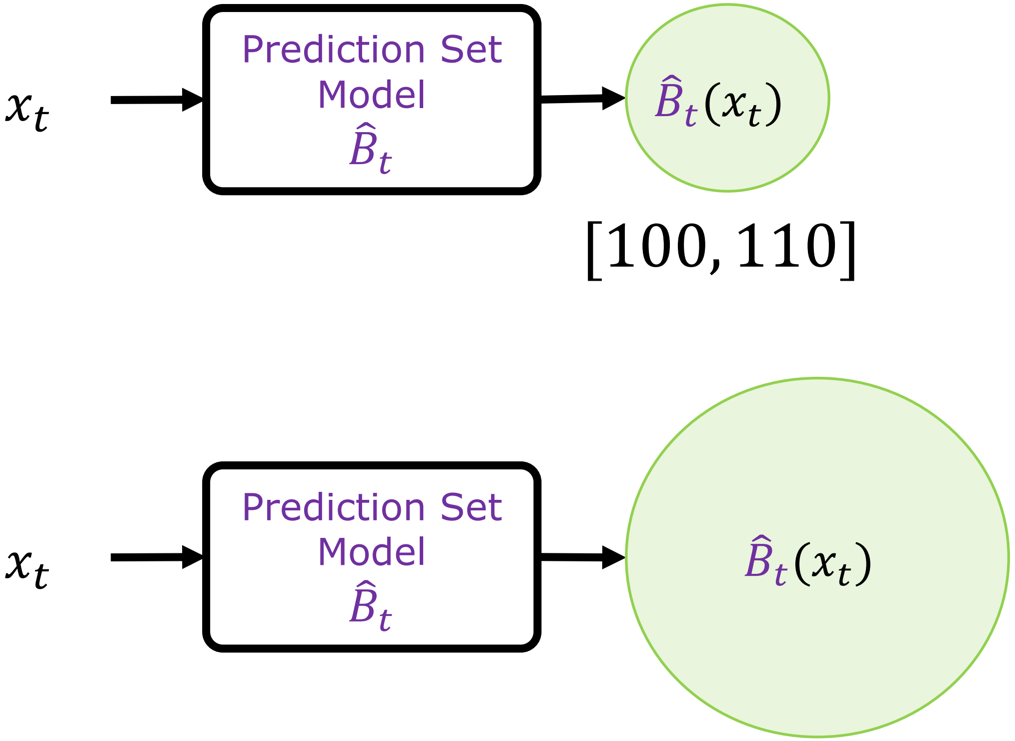
$\hat{B}_t$

$\hat{B}(x)$

e.g., $[1{,}175.1, 1{,}190.5]$

Uncertainty = Set Size

Prediction set



x_t

Prediction Set Model $\hat{B}_t$

$\hat{B}_t(x_t)$

$[100, 110]$

More uncertain

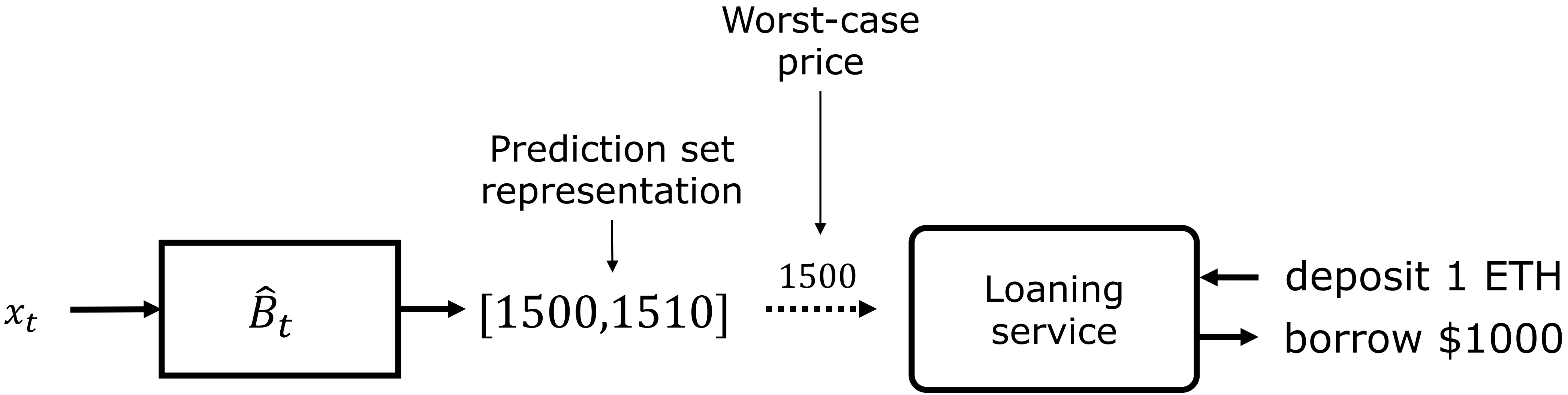
x_t

Prediction Set Model $\hat{B}_t$

$\hat{B}_t(x_t)$

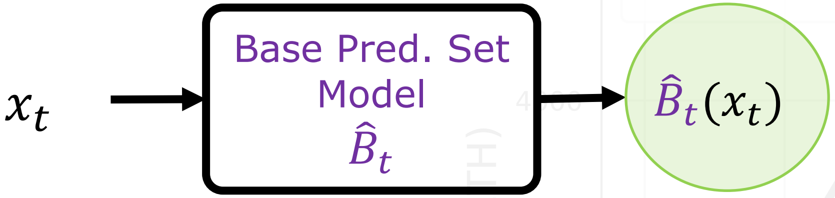
$[100, 500]$

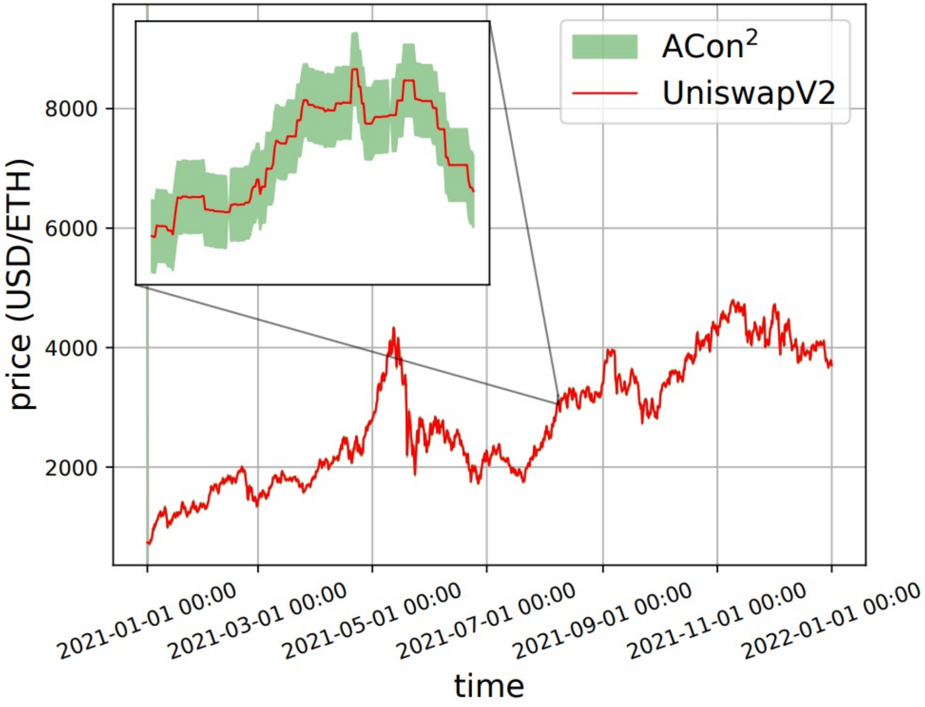
Is Prediction Set Representation Compatible?



✓ Compatible

Learning Uncertainty
Challenge 1: Natural Shift Over Time

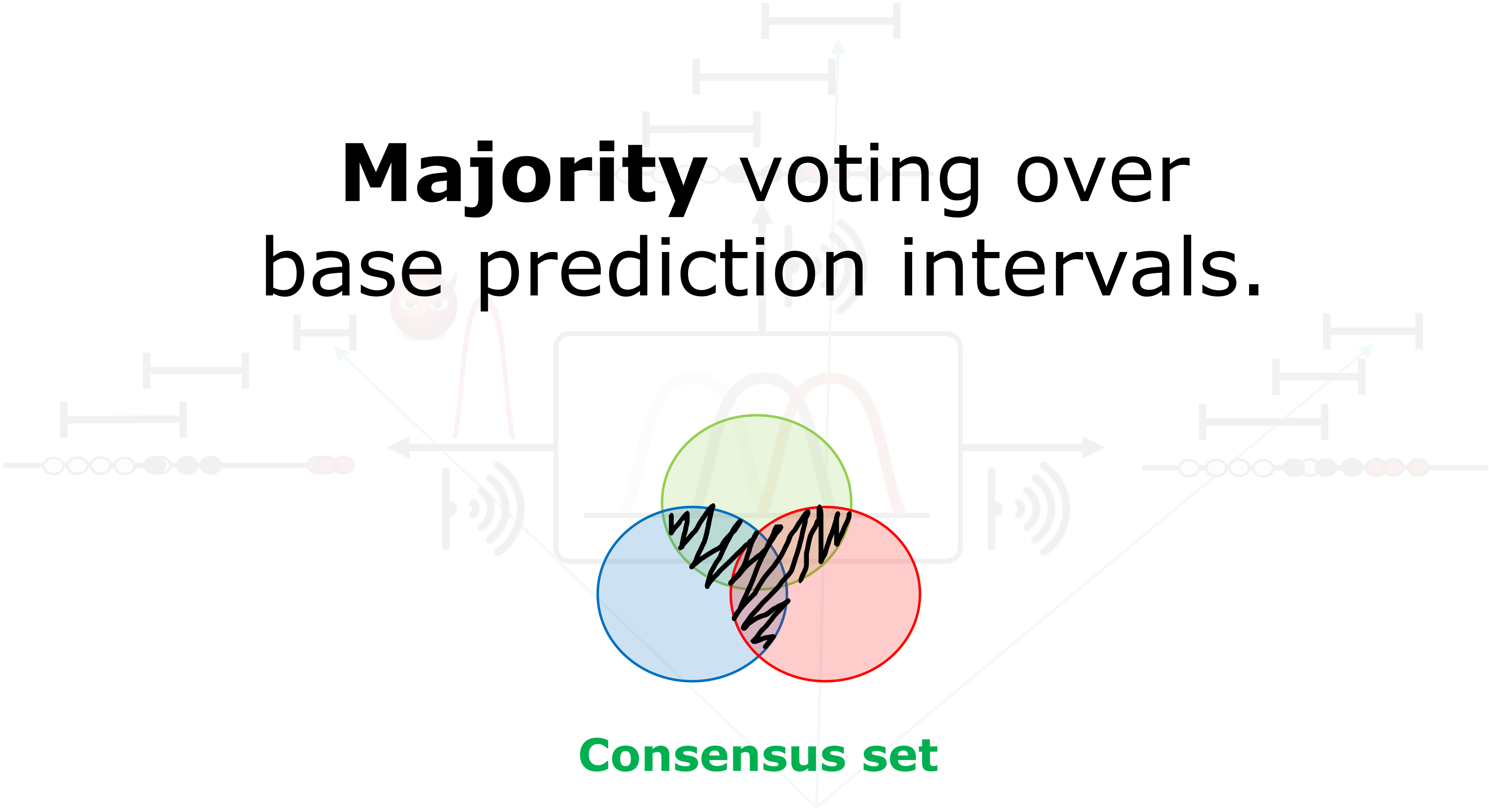




Use **adaptive conformal prediction**.

Learning Uncertainty
Challenge 2: Adversarial Manipulation

Majority voting over
base prediction intervals.



Consensus set

How to make consensus among prediction intervals
with a correctness guarantee?

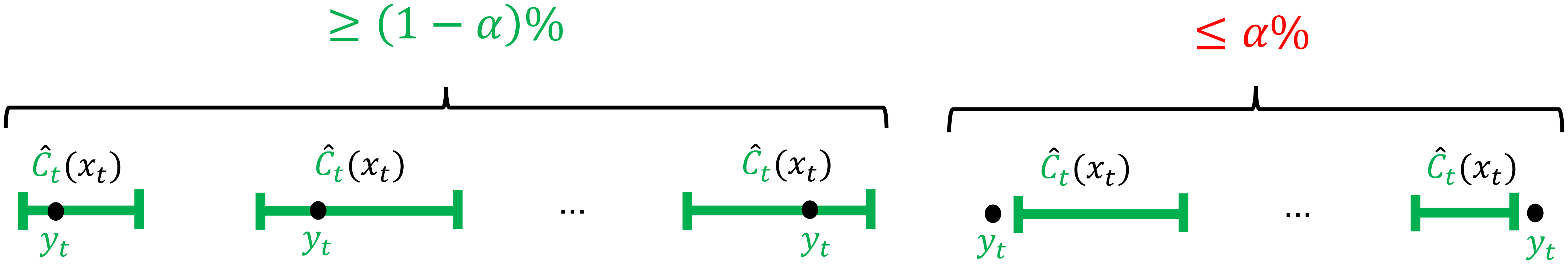
Correctness Guarantee

Provide Trustworthiness on Consensus Sets

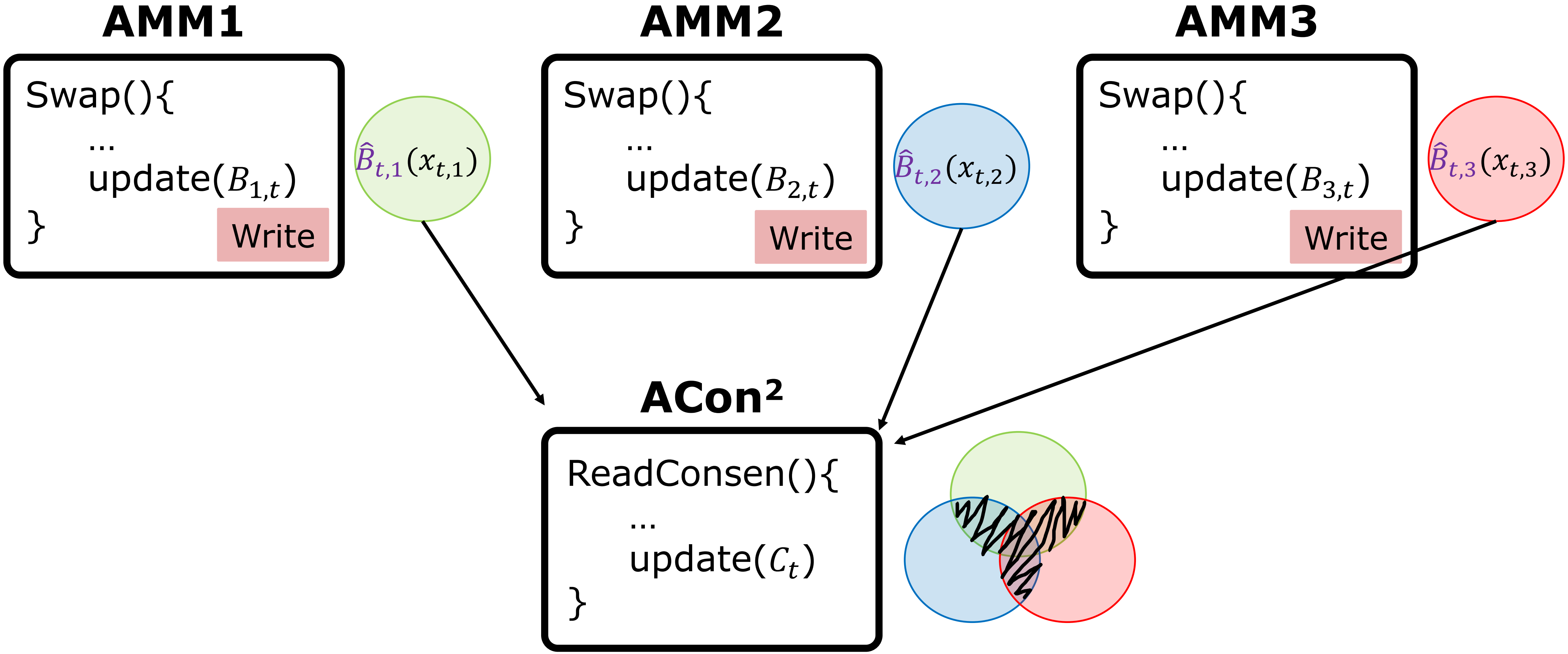
Theorem (informal). Under some assumptions, the consensus learner is approximately correct, i.e.,

$$\frac{1}{T}\sum_{t=1}^{T} \mathbb{I}\left(y_t \in \hat{C}_t(x_t)\right) \gtrsim 1-\alpha$$

TRUSTWORTHY
TRUSTWORTHY
TRUSTWORTHY



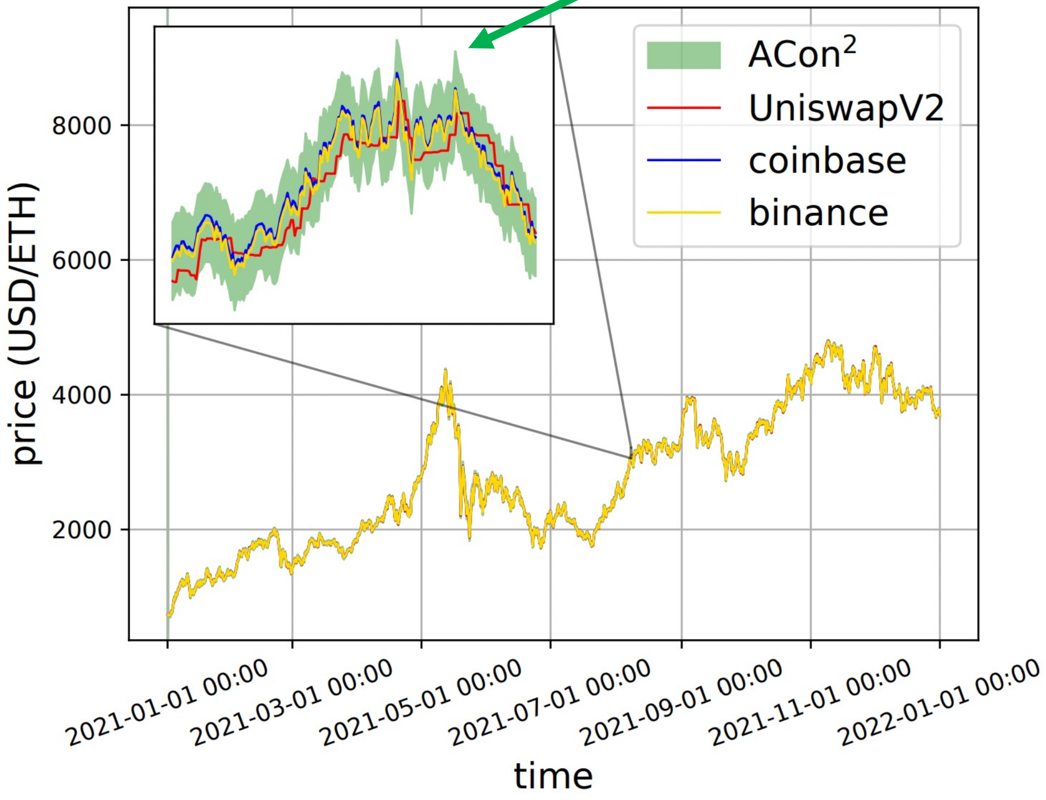
How to Implement ACon^2 in Ethereum?

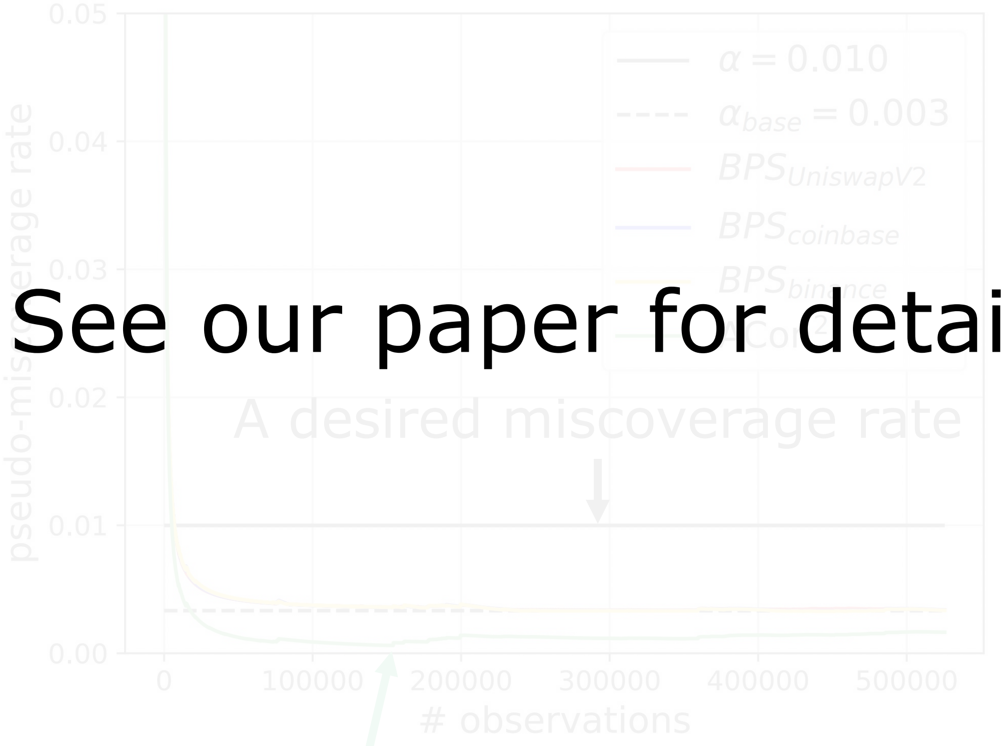


AMM: Automated Market Maker

Evaluation Under Natural Shift

Consensus sets closely follow





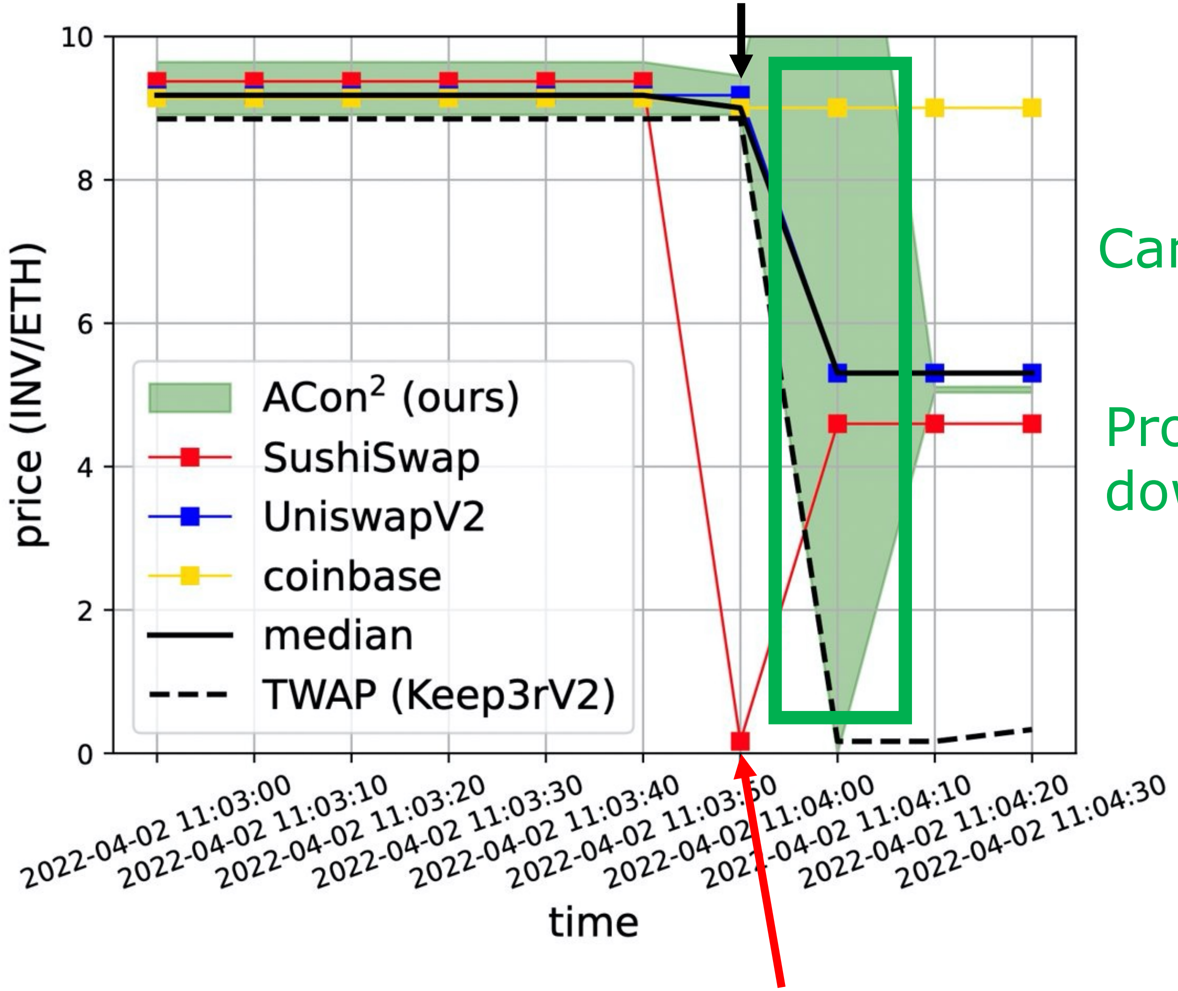
See our paper for details!

Satisfy the desired miscoverage guarantee

Evaluation Under Adversarial Manipulation

Price manipulation could be avoidable

Inverse Finance
$15.6M attack on
2022.04



Make consensus

Cannot make consensus

↓

Provide an alarm to downstream applications

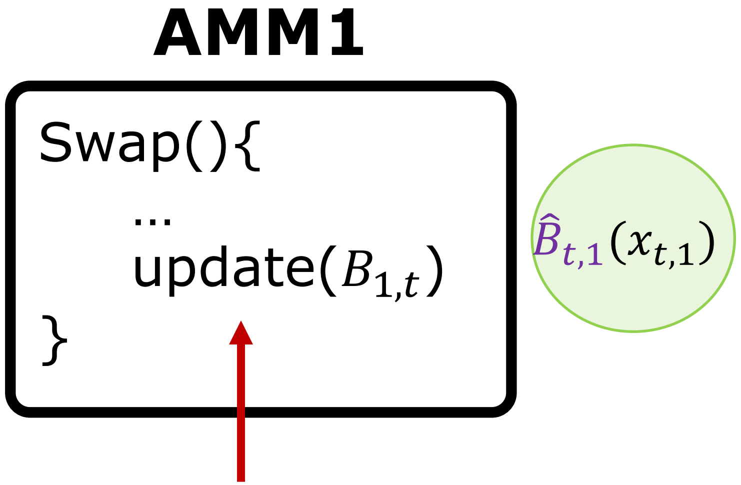
Price manipulation

Limitations

? “Identical label distribution” assumption

→ Can we relax this assumption?

? Higher transaction fee for learning



```
Swap(){
    …
    update($B_{1,t}$)
}
```

Expensive (e.g., $30.8)

→ Can we find an Ethereum friendly learning algorithm?

Take-home Message

ACon^2 aims **trustworthy oracle smart contracts,** backed by **machine learning theory.**

https://github.com/sslab-gatech/ACon2

Georgia Tech

Penn UNIVERSITY of PENNSYLVANIA

POSTECH