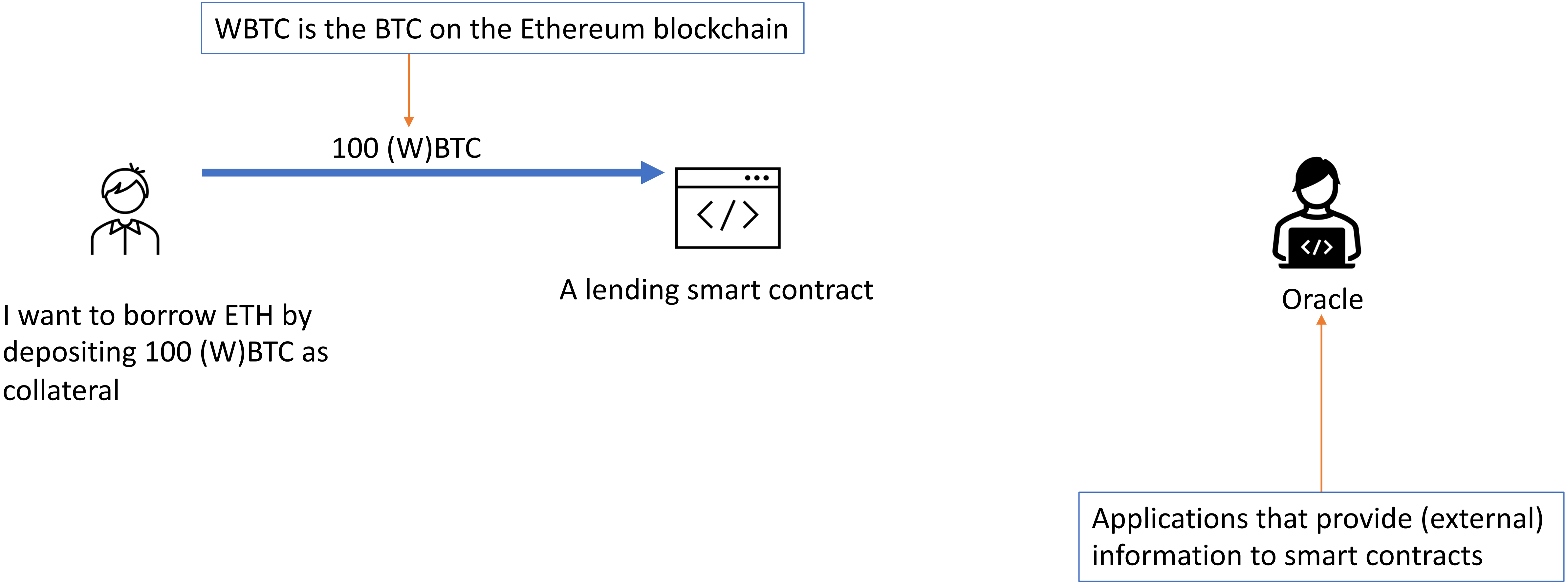
Robust (Decentralized) Oracle Design

Leifu Zhang

The Hong Kong University of Science and Technology (Guangzhou)

July 2024 @ CMID

Oracle and its problem



WBTC is the BTC on the Ethereum blockchain

100 (W)BTC

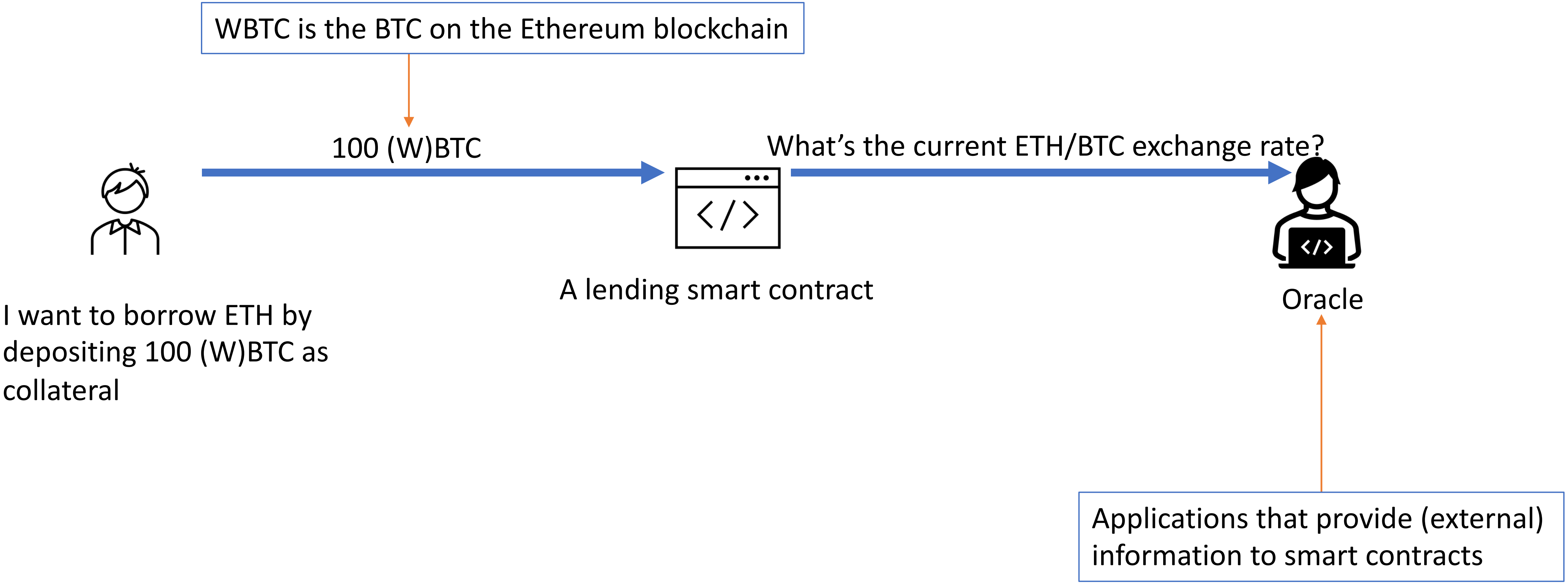
I want to borrow ETH by depositing 100 (W)BTC as collateral

A lending smart contract

Oracle

Applications that provide (external) information to smart contracts

Oracle and its problem



WBTC is the BTC on the Ethereum blockchain

100 (W)BTC

What’s the current ETH/BTC exchange rate?

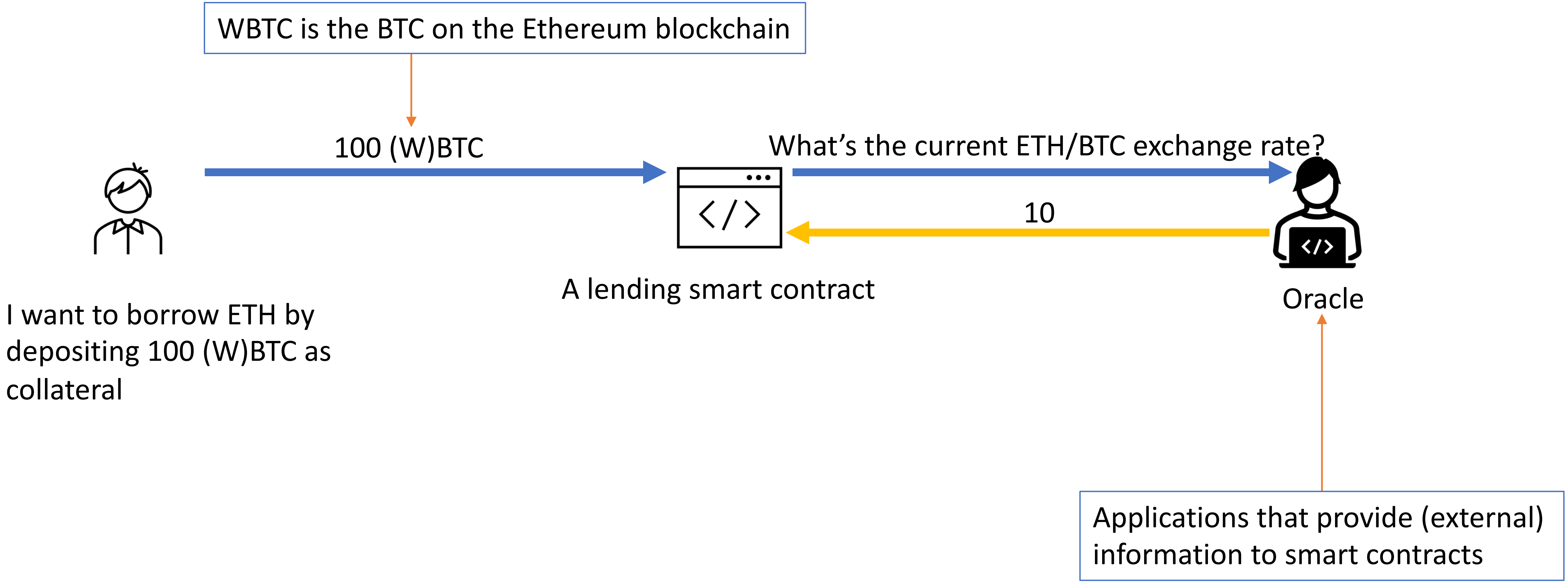
I want to borrow ETH by depositing 100 (W)BTC as collateral

A lending smart contract

Oracle

Applications that provide (external) information to smart contracts

Oracle and its problem



WBTC is the BTC on the Ethereum blockchain

100 (W)BTC

What’s the current ETH/BTC exchange rate?

10

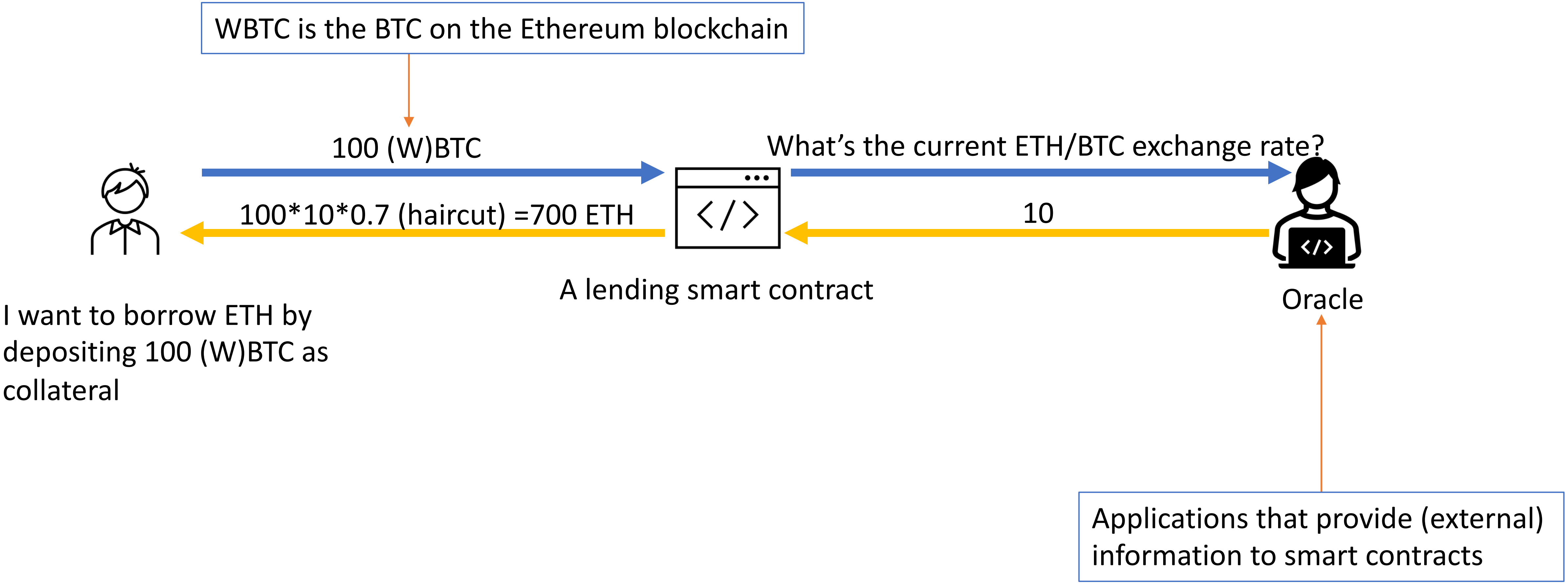
I want to borrow ETH by depositing 100 (W)BTC as collateral

A lending smart contract

Oracle

Applications that provide (external) information to smart contracts

Oracle and its problem



WBTC is the BTC on the Ethereum blockchain

100 (W)BTC

100*10*0.7 (haircut) =700 ETH

What’s the current ETH/BTC exchange rate?

10

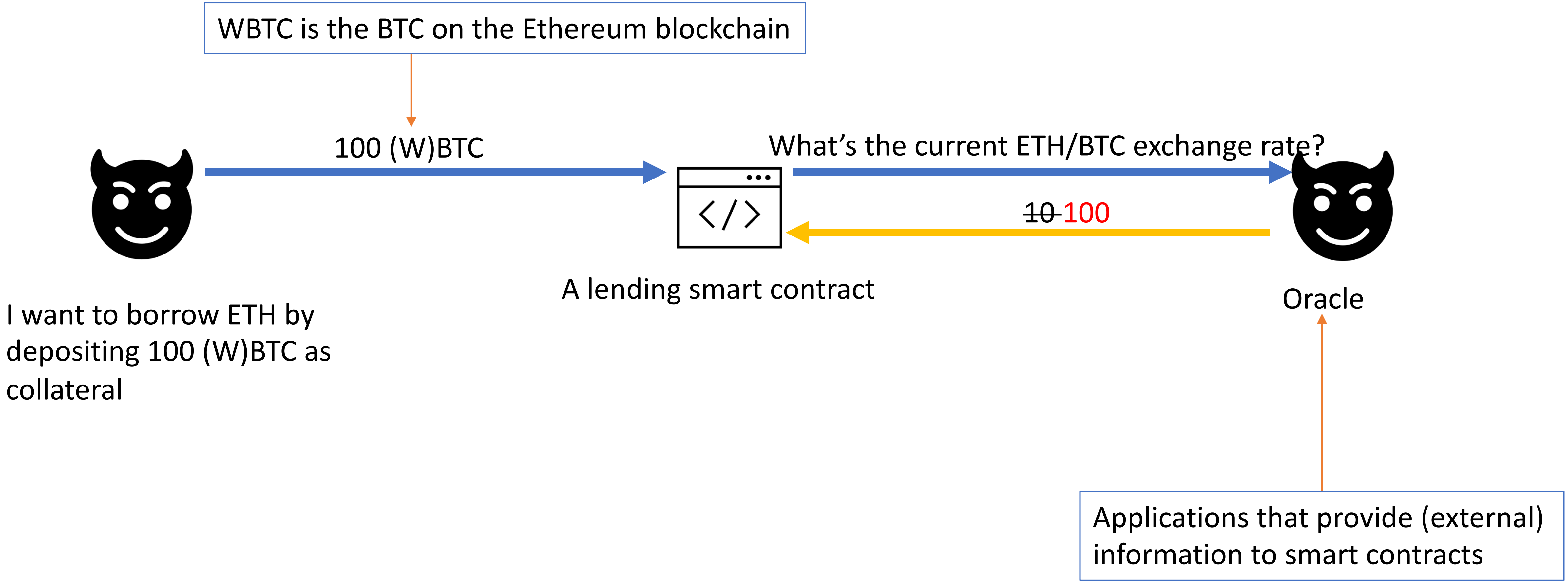
A lending smart contract

Oracle

I want to borrow ETH by depositing 100 (W)BTC as collateral

Applications that provide (external) information to smart contracts

Oracle and its problem



WBTC is the BTC on the Ethereum blockchain

100 (W)BTC

What’s the current ETH/BTC exchange rate?

~~10~~ 100

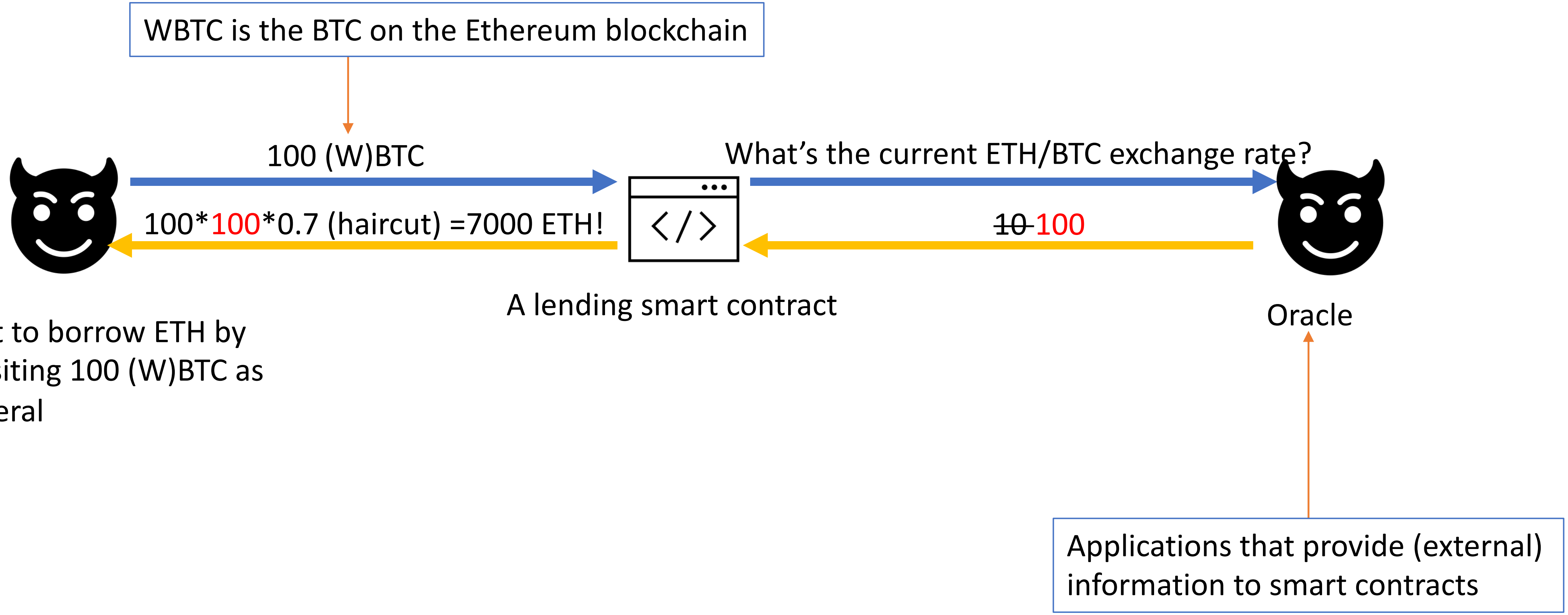
A lending smart contract

Oracle

I want to borrow ETH by depositing 100 (W)BTC as collateral

Applications that provide (external) information to smart contracts

Oracle and its problem



WBTC is the BTC on the Ethereum blockchain

100 (W)BTC

100*100*0.7 (haircut) =7000 ETH!

What's the current ETH/BTC exchange rate?

~~10~~ 100

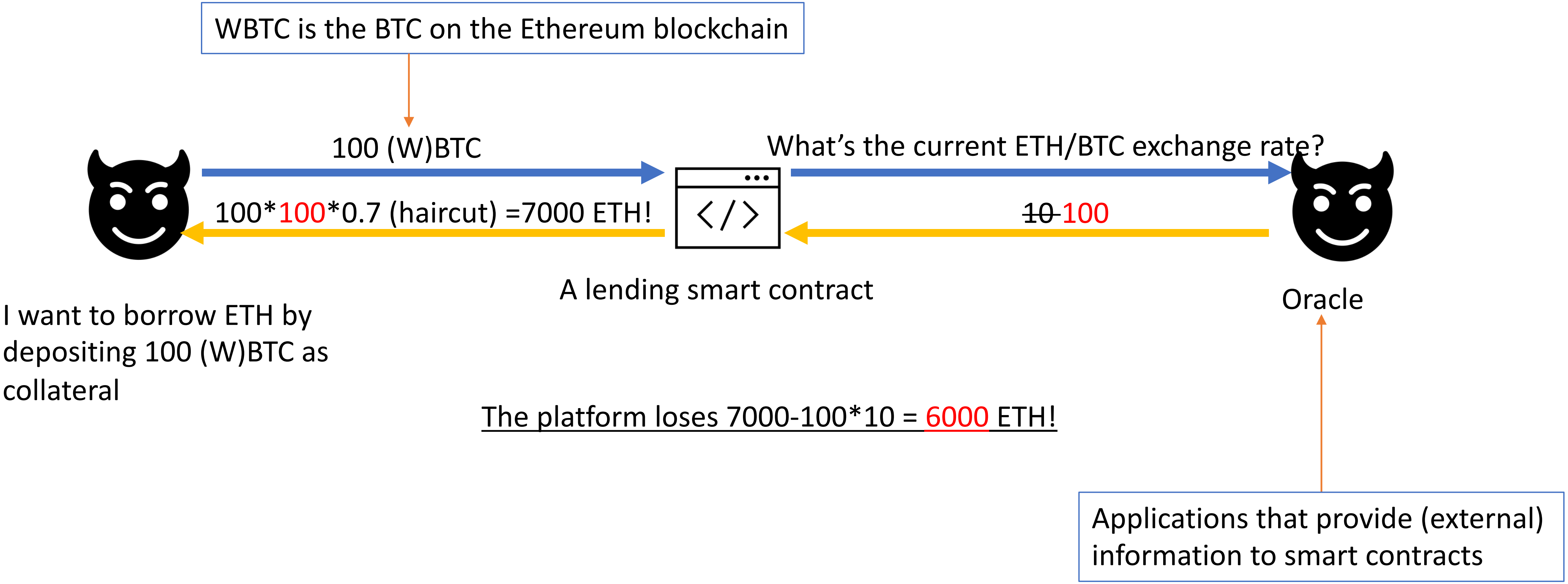
A lending smart contract

Oracle

I want to borrow ETH by depositing 100 (W)BTC as collateral

Applications that provide (external) information to smart contracts

Oracle and its problem



WBTC is the BTC on the Ethereum blockchain

100 (W)BTC

What’s the current ETH/BTC exchange rate?

100*100*0.7 (haircut) =7000 ETH!

~~10~~ 100

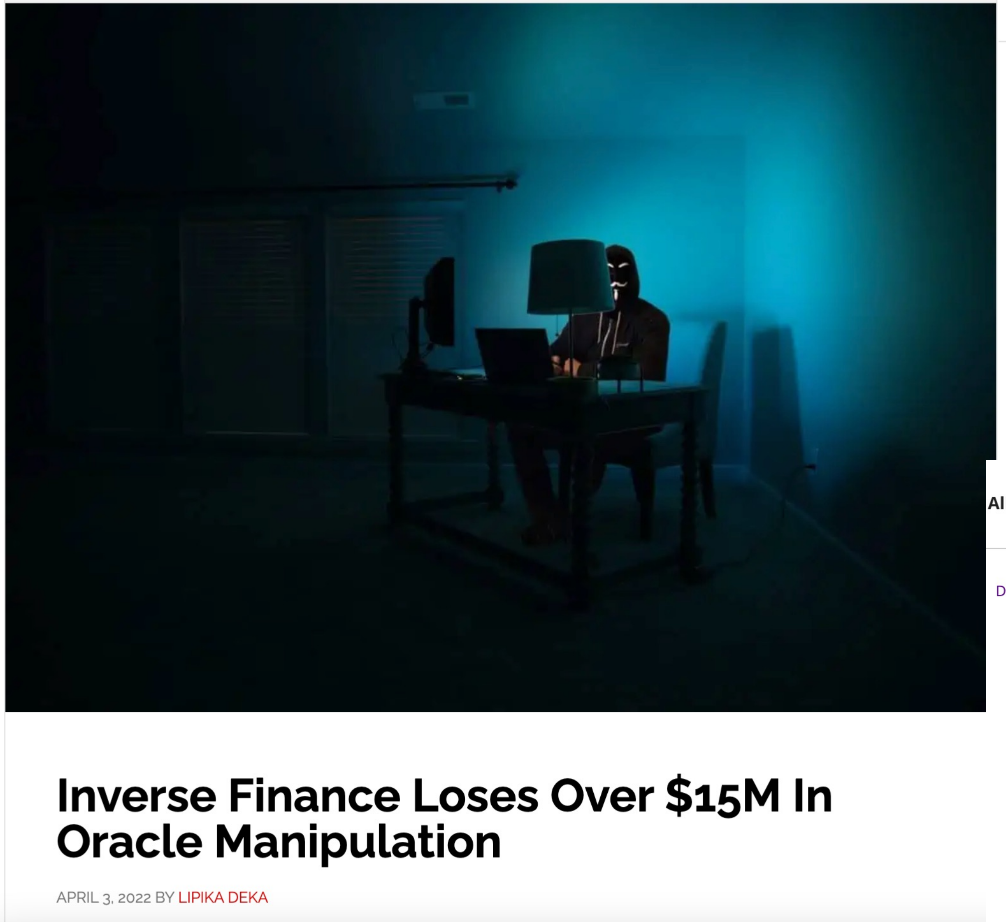
A lending smart contract

I want to borrow ETH by depositing 100 (W)BTC as collateral

Oracle

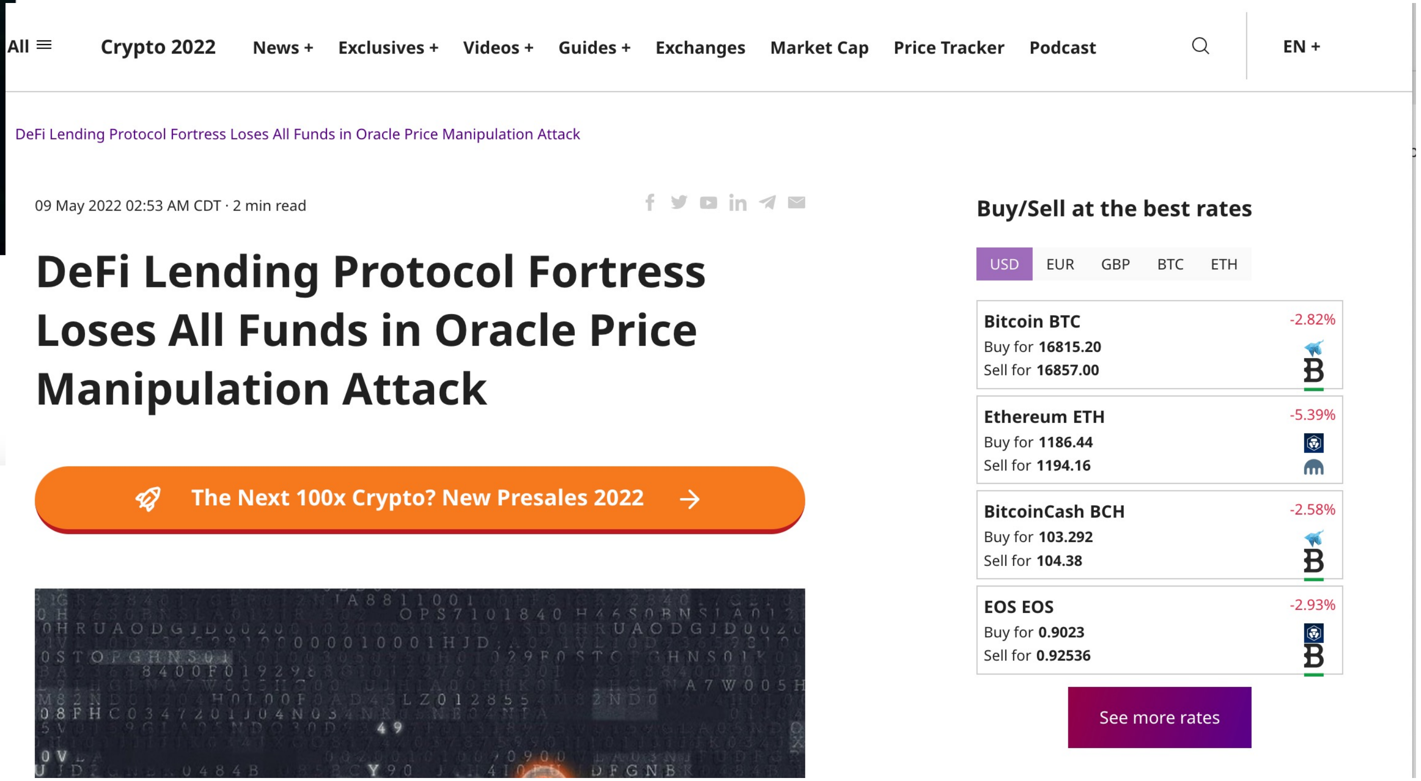
The platform loses 7000-100*10 = 6000 ETH!

Applications that provide (external) information to smart contracts



Inverse Finance Loses Over $15M In Oracle Manipulation

APRIL 3, 2022 BY LIPIKA DEKA



DeFi Lending Protocol Fortress Loses All Funds in Oracle Price Manipulation Attack

09 May 2022 02:53 AM CDT · 2 min read

DeFi Lending Protocol Fortress Loses All Funds in Oracle Price Manipulation Attack

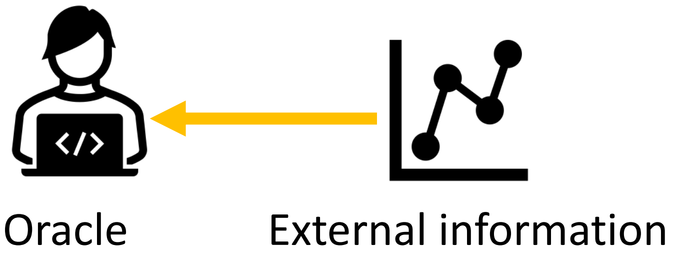
Buy/Sell at the best rates

Bitcoin BTC	Buy for 16815.20 Sell for 16857.00	-2.82%
Ethereum ETH	Buy for 1186.44 Sell for 1194.16	-5.39%
BitcoinCash BCH	Buy for 103.292 Sell for 104.38	-2.58%
EOS EOS	Buy for 0.9023 Sell for 0.92536	-2.93%

Sources: https://www.tronweekly.com/inverse-finance-loses-15m-oracle-manipulation/
https://cryptonews.com/news/defi-lending-protocol-fortress-loses-all-funds-oracle-price-manipulation-attack.htm

The importance of oracles

- Oracles are the cornerstone of DeFi
  - Decentralized lending platforms
  - Prediction markets
  - Insurance contracts
  - NFT games
  - (Many) stablecoins
  - …



The oracle problem

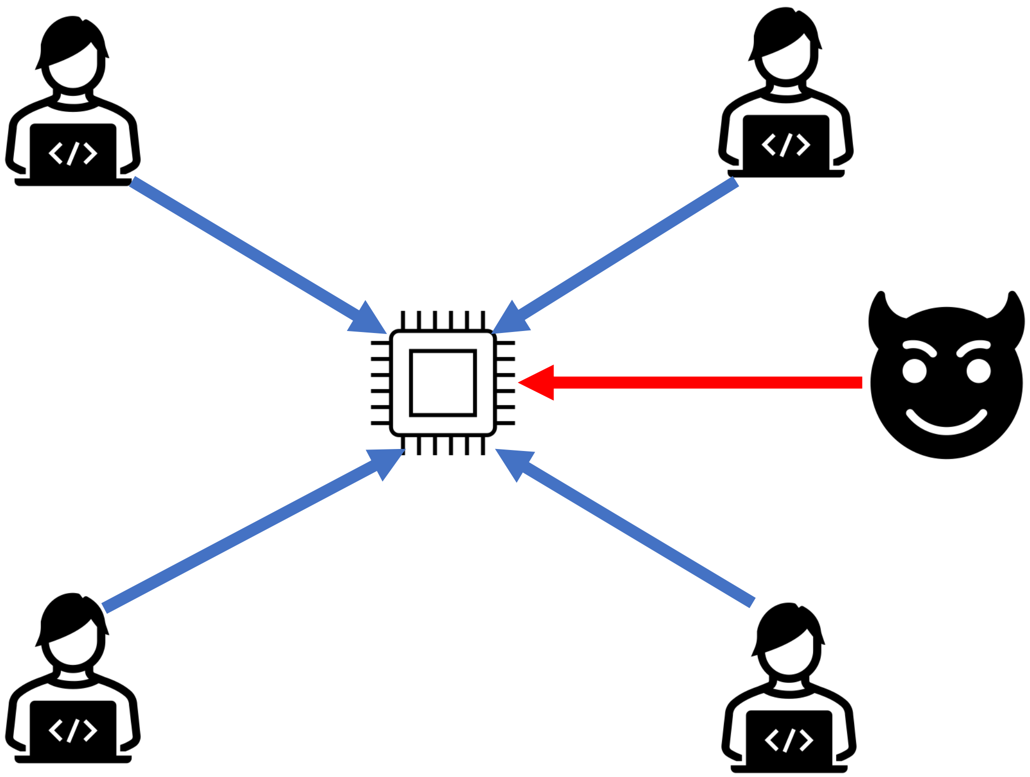
- How can we ensure the information provided by oracles is accurate?

The oracle problem

- How can we ensure the information provided by oracles is accurate?
- Single source → single point of failure

The oracle problem

- How can we ensure the information provided by oracles is accurate?
- Single source → single point of failure → decentralization!



Research question 1

- Q: Can we find a robust compensation mechanism?

Definition

A compensation mechanism is robust if, under that mechanism, there is an equilibrium in which truthful reporting is the unique optimal response for strategic nodes regardless of the adversary's strategy.

Research question 1

- Q: Can we find a robust compensation mechanism?

Definition
A compensation mechanism is robust if, under that mechanism, there is an equilibrium in which truthful reporting is the unique optimal response for strategic nodes regardless of the adversary's strategy.

- A: Without identifying an honest node, generally no
- Takeaway: "A" limit of decentralization

Research question 2

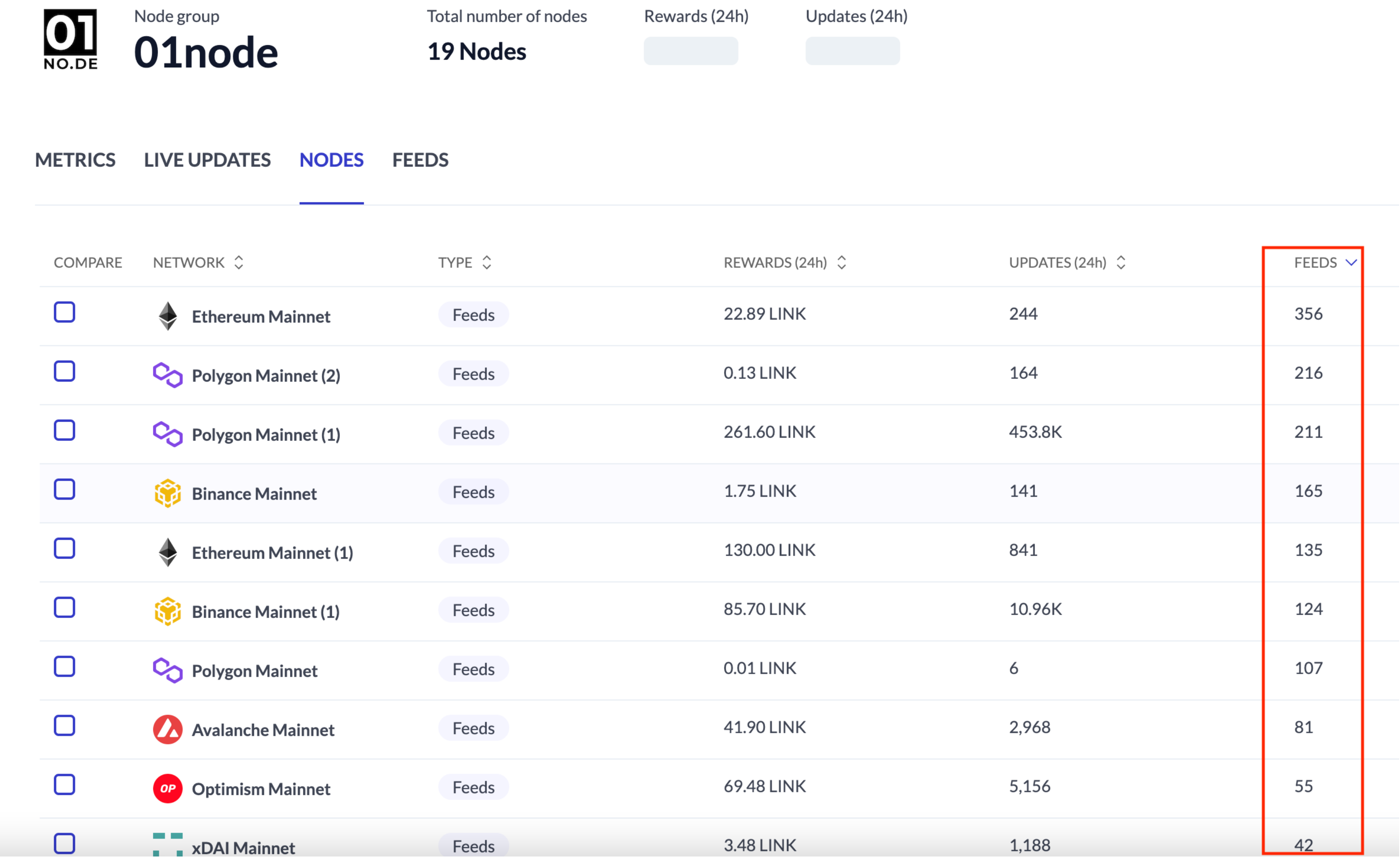
- Q: What is the optimal way to aggregate information under the worst-case scenario?

Research question 2

- Q: What is the optimal way to aggregate information under the worst-case scenario?

- Key observations:
  1. Obtaining consensus = unsupervised learning with contaminated data
  2. The popular aggregating method ignores the multi-dimensional structure of decentralized oracles---each node usually covers many cryptocurrencies

The multi-dimensional structure



Node group

01node

Total number of nodes

19 Nodes

Rewards (24h)

Updates (24h)

COMPARE	NETWORK	TYPE	REWARDS (24h)	UPDATES (24h)	FEEDS
□	Ethereum Mainnet	Feeds	22.89 LINK	244	356
□	Polygon Mainnet (2)	Feeds	0.13 LINK	164	216
□	Polygon Mainnet (1)	Feeds	261.60 LINK	453.8K	211
□	Binance Mainnet	Feeds	1.75 LINK	141	165
□	Ethereum Mainnet (1)	Feeds	130.00 LINK	841	135
□	Binance Mainnet (1)	Feeds	85.70 LINK	10.96K	124
□	Polygon Mainnet	Feeds	0.01 LINK	6	107
□	Avalanche Mainnet	Feeds	41.90 LINK	2,968	81
□	Optimism Mainnet	Feeds	69.48 LINK	5,156	55
□	xDAI Mainnet	Feeds	3.48 LINK	1,188	42

Source: https://market.link/nodes/568cedcc-46f3-49e4-84c7-a9d7d5e23a0d/nodes

Research question 2

- Q: What is the optimal way to aggregate information under the worst-case scenario?

- A: A filtering algorithm can dramatically improve the consensus by utilizing this multi-dimensional structure
  - Adversarial nodes which look “normal” in every single dimension could be detected from a “global” view
  - Approaching the theoretical limit

Related literature

- Oracle design
  - F. Zhang et al. (2016), F. Zhang et al. (2020), Breidenbach et al. (2021)
  - Contribution: 1) “A” limit of decentralization; 2) connecting machine learning to oracle design

- Information elicitation
  - McCarthy (1956), Savage (1971), Prelec (2004), Miller et al. (2005), P. Zhang and Chen (2014), Lambert (2019), Gao et al. (2019)
  - Contribution: Getting an impossible result under the adversarial environments

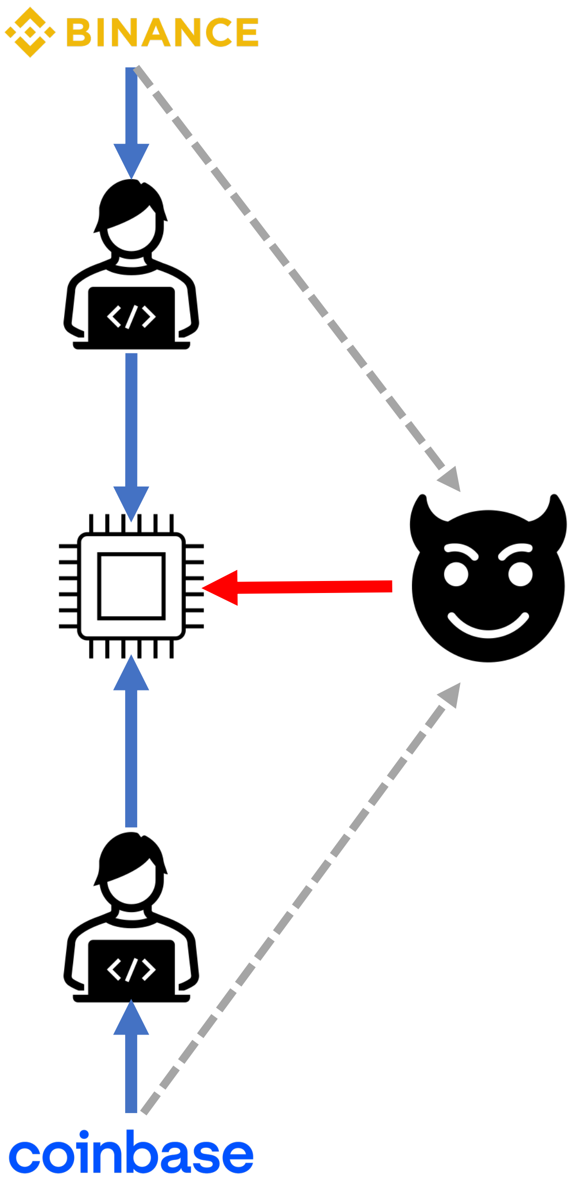
- Manipulation in traditional capital markets
  - Gandhi et al. (2019), A. Zhang (2022)
  - Contribution: Shedding light on designing replacements for the London Inter-Bank Offered Rate (LIBOR)

- Byzantine fault tolerance
  - Lamport et al. (1982), Amoussou-Guenou et al. (2021), Halaburda et al. (2021)

- Machine learning
  - Lai et al. (2016), Diakonikolas et al. (2016, 2017, 2019), Charikar et al. (2017), Zhu et al. (2022)

Setting

- n (a large number of) nodes; εn nodes are controlled by an adversary
- The rest nodes are risk-neutral and strategic: Maximizing the expected payoffs given by the designer
- Ground truth $\mathbf{X} \sim U(\mathbb{R}^d)$
- Each strategic node has a private signal
$$\mathbf{s}_i = \mathbf{X} + \mathbf{e}_i$$
  - $\mathbb{E}[\mathbf{e}_i] = \mathbf{0}$ and $\mathbf{e}_i$ has a bounded covariance matrix
- Key assumption: The adversary observes strategic nodes' private signals



Setting

- n (a large number of) nodes; εn nodes are controlled by an adversary
- The rest nodes are risk-neutral and strategic: Maximizing the expected payoffs given by the designer
- Ground truth $\mathbf{X} \sim U(\mathbb{R}^{d})$
- Each strategic node has a private signal

$$\mathbf{s}_i = \mathbf{X} + \mathbf{e}_i$$

  - $\mathbb{E}[\mathbf{e}_i] = \mathbf{0}$ and $\mathbf{e}_i$ has a bounded covariance matrix
- Key assumption: The adversary observes strategic nodes' private signals

Timing:

1. The designer announces a compensation mechanism
2. Each node submits a report
3. The designer pays each node and outputs a consensus

Setting

- n (a large number of) nodes; εn nodes are controlled by an adversary
- The rest nodes are risk-neutral and strategic: Maximizing the expected payoffs given by the designer
- Ground truth $\mathbf{X} \sim U(\mathbb{R}^d)$
- Each strategic node has a private signal
$$\mathbf{s}_i = \mathbf{X} + \mathbf{e}_i$$
  - $\mathbb{E}[\mathbf{e}_i] = \mathbf{0}$ and $\mathbf{e}_i$ has a bounded covariance matrix
- Key assumption: The adversary observes strategic nodes' private signals

Goals:

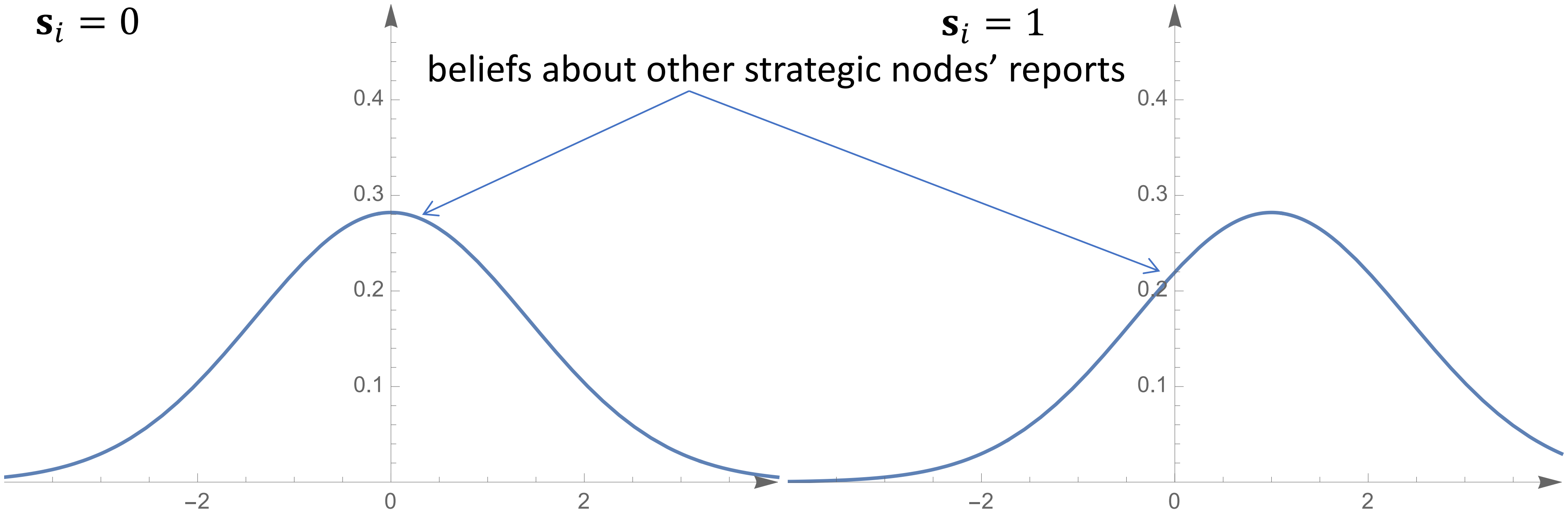
1. Find a robust compensation mechanism
2. Find a robust consensus $\widehat{\mathbf{X}}$ that is close to $\mathbf{X}$

robust = good given the adversary's any strategy

Part 1: (No) Robust compensation mechanism

No robust compensation mechanism

- Suppose $\mathbf{s}_i = \mathbf{X} + \mathcal{N}(0,1)$ and consider node i's decision problem



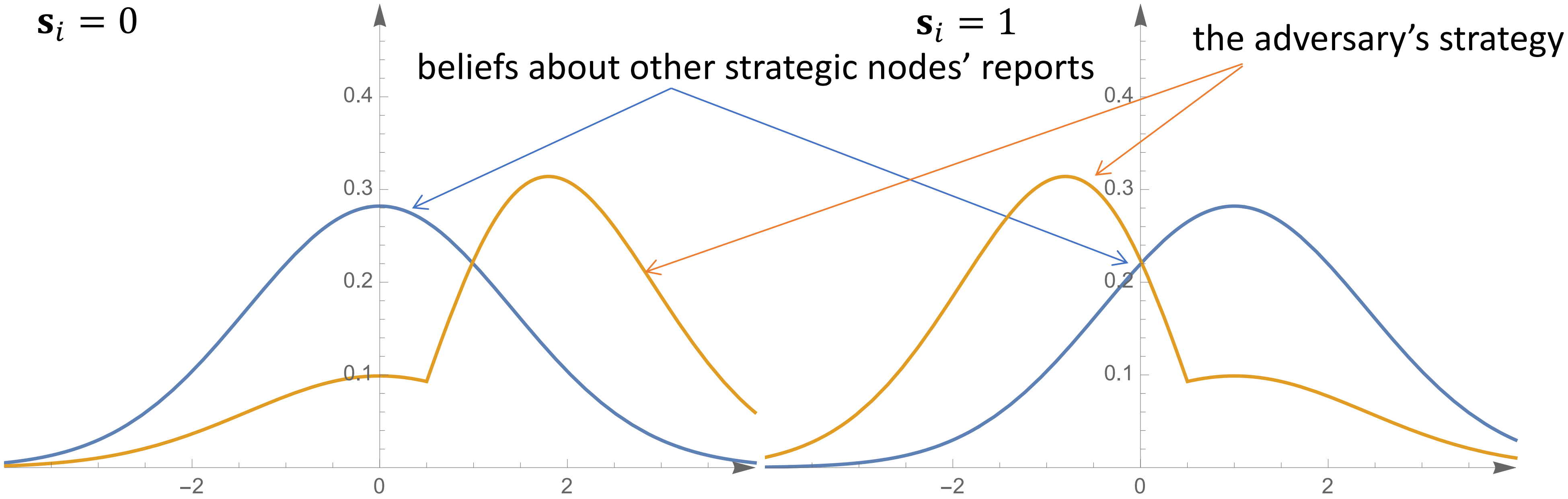
$\mathbf{s}_i = 0$

$\mathbf{s}_i = 1$

beliefs about other strategic nodes' reports

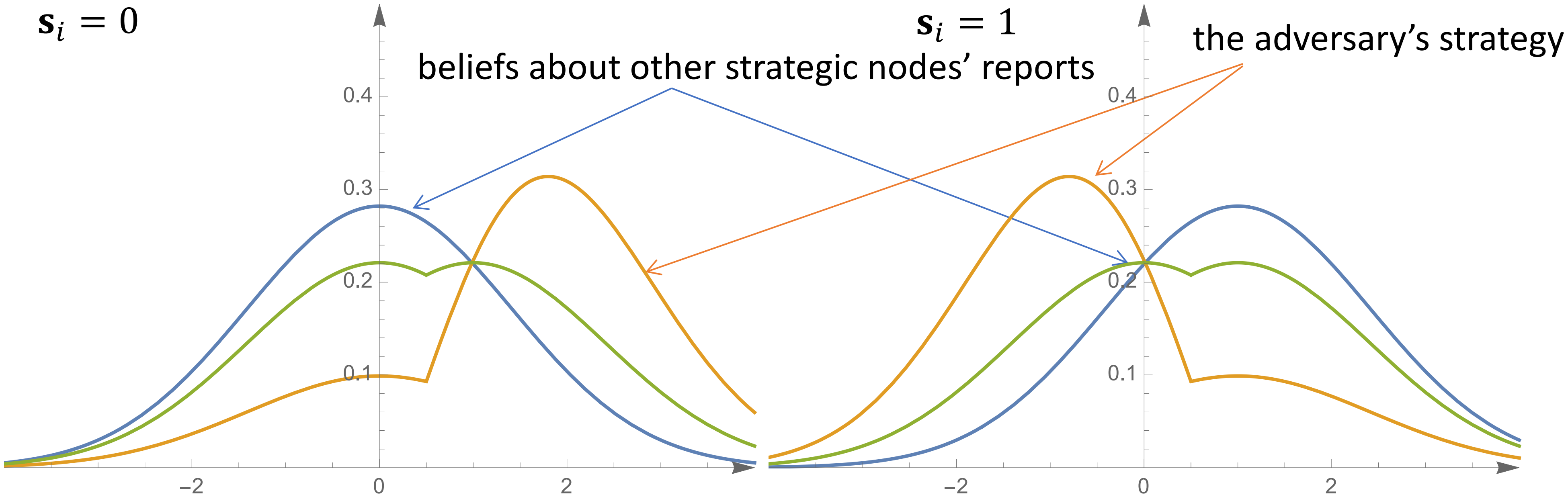
No robust compensation mechanism

- Suppose $\mathbf{s}_i = \mathbf{X} + \mathcal{N}(0,1)$ and consider node i's decision problem



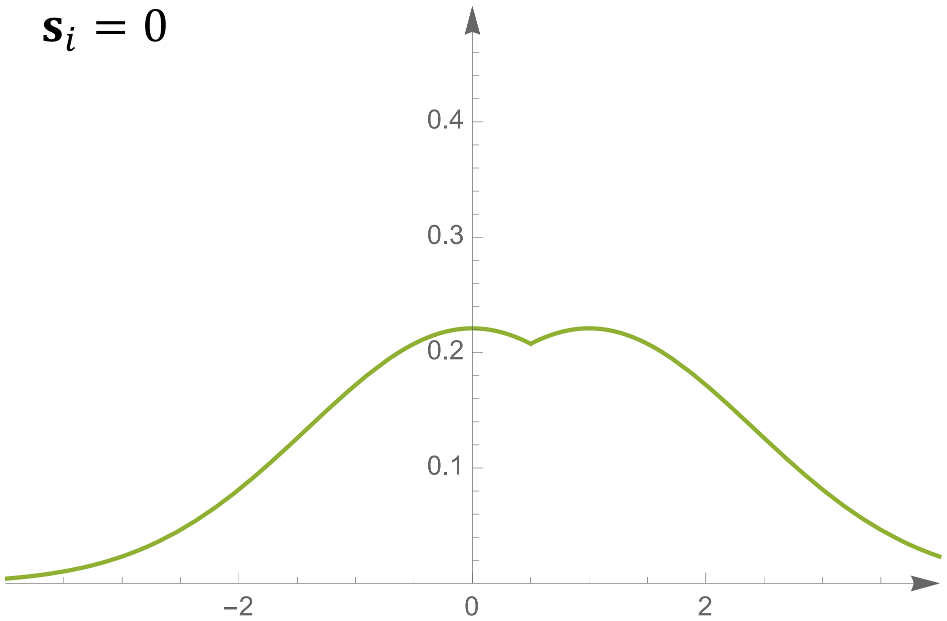
No robust compensation mechanism

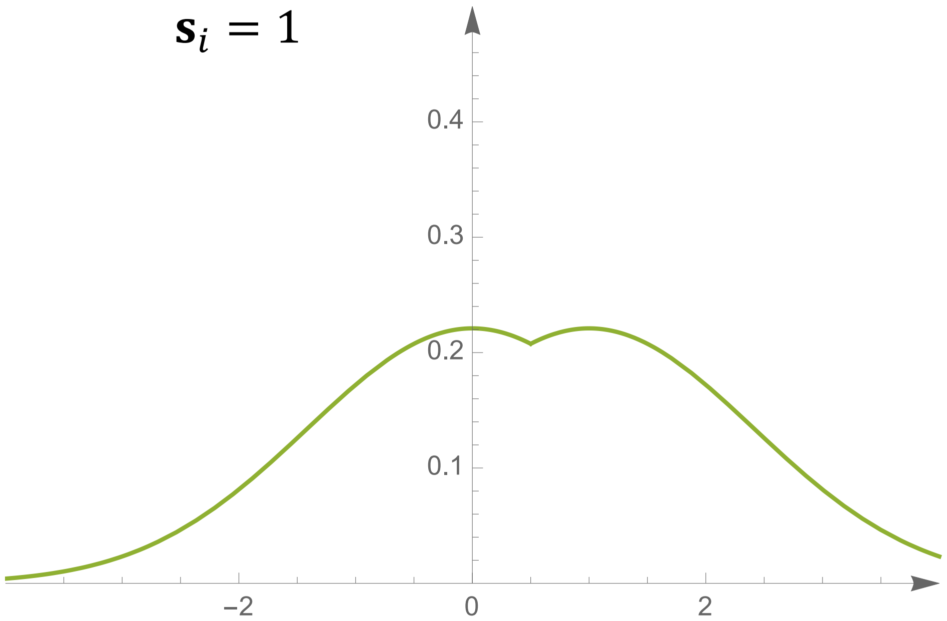
- Suppose $\mathbf{s}_i = \mathbf{X} + \mathcal{N}(0,1)$ and consider node i's decision problem
- Greenline $= (1-\varepsilon) *$ Blueline + $\varepsilon *$ Orangeline
- Node i's beliefs about other nodes' reports



No robust compensation mechanism

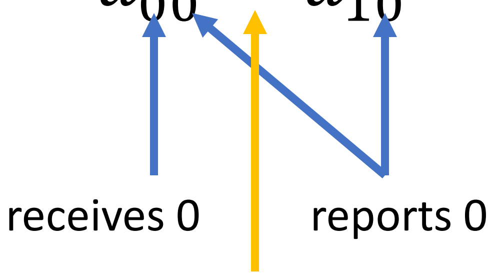
Lemma [implied by an observation in robust statistics]
Under a mild sufficient condition, the adversary has a reporting strategy such that even if node i may have different private information, node i's beliefs about other nodes' reports are unchanged.


$\mathbf{s}_i = 0$


$\mathbf{s}_i = 1$

No robust compensation mechanism

- $u_{00} = u_{10}$



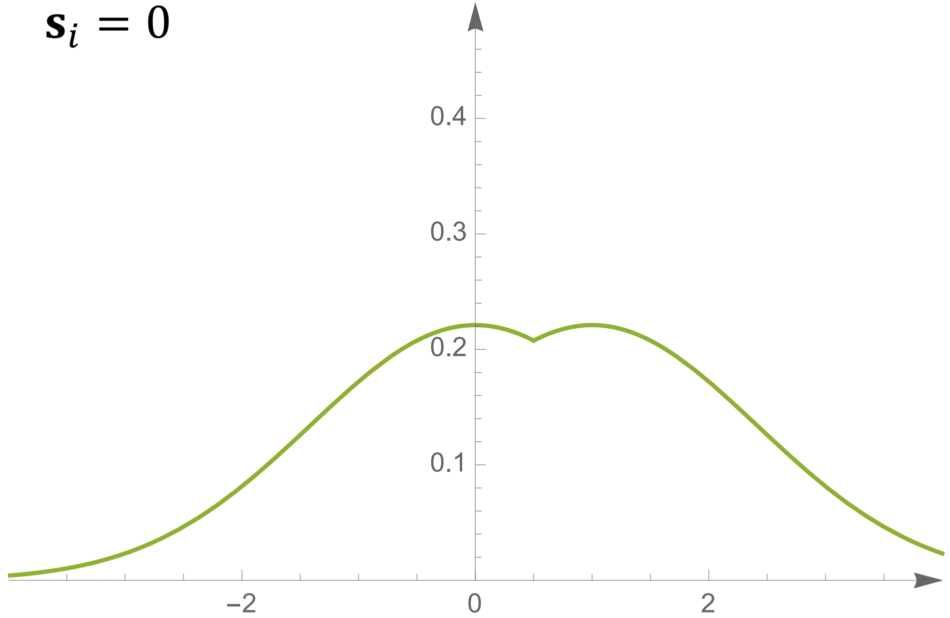
receives 0

reports 0

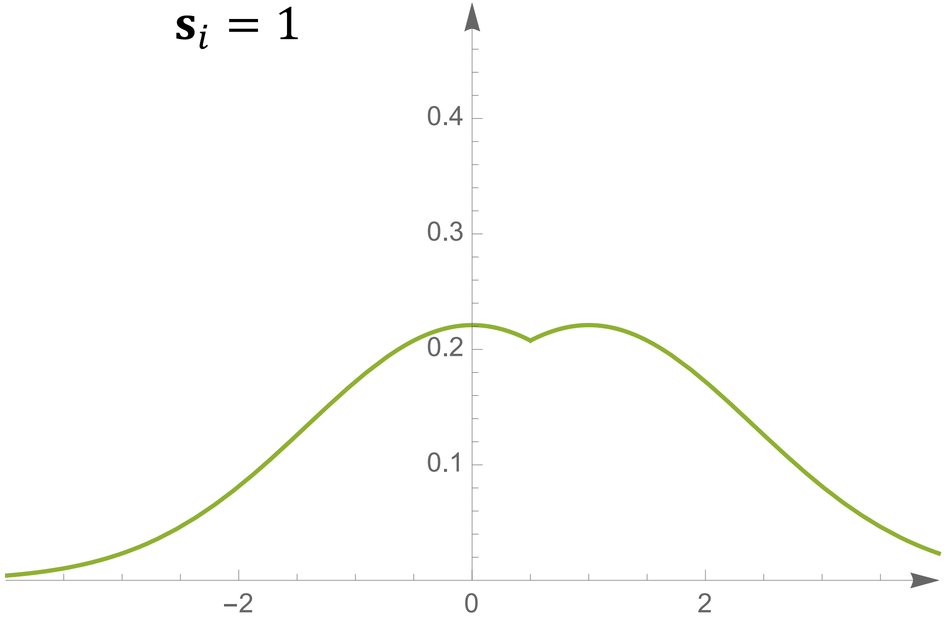
other nodes' reports are the same (the two green lines)

		Report $\mathbf{r}_i$	
		0	1
Private signal $\mathbf{s}_i$	0	u_{00}	u_{01}
	1	u_{10}	u_{11}

$\mathbf{s}_i = 0$

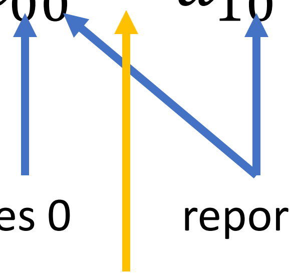


$\mathbf{s}_i = 1$



No robust compensation mechanism

- $u_{00} = u_{10} < u_{11}$

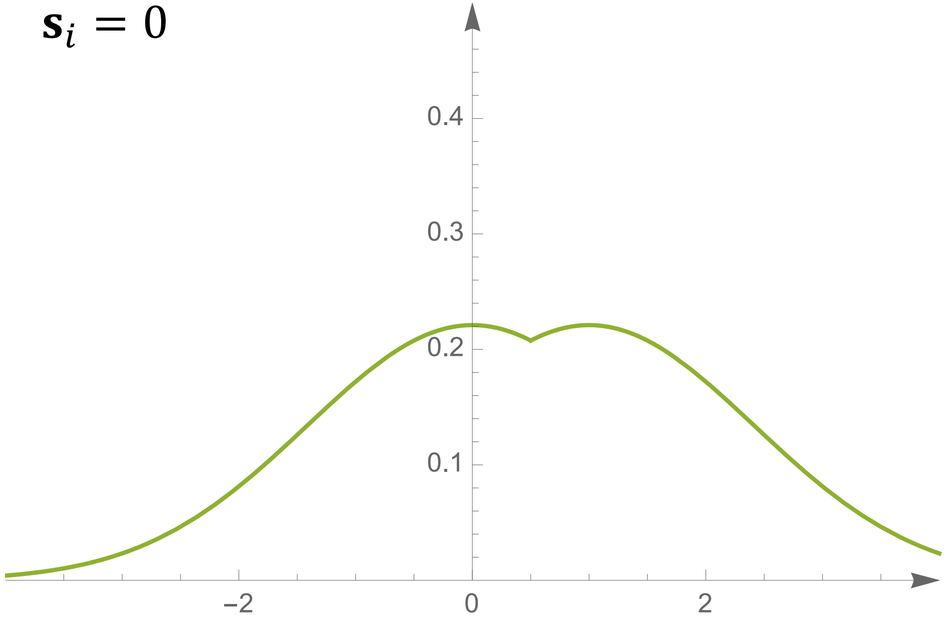


receives 0

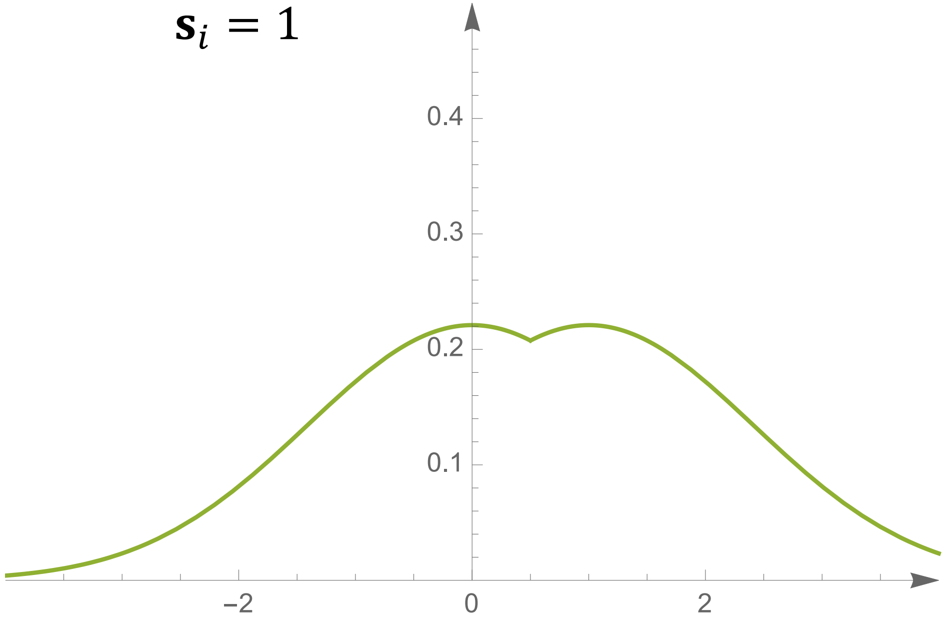
reports 0

other nodes’ reports are the same (the two green lines)

		Report $\mathbf{r}_i$	
		0	1
Private signal $\mathbf{s}_i$	0	u_{00}	u_{01}
	1	u_{10}	u_{11}



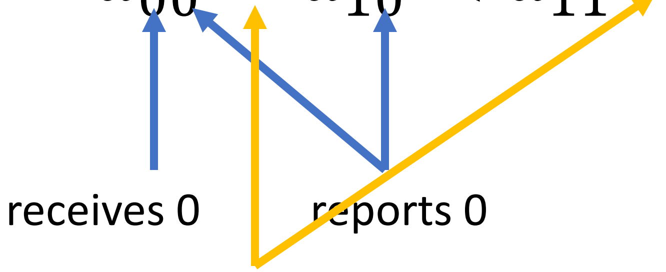
$\mathbf{s}_i = 0$



$\mathbf{s}_i = 1$

No robust compensation mechanism

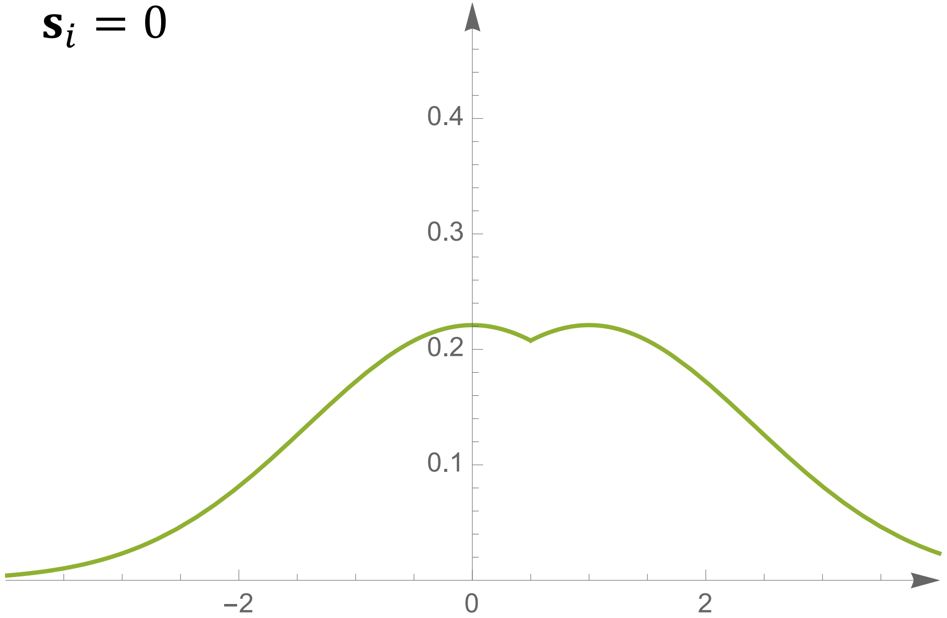
- $u_{00} = u_{10} < u_{11} = u_{01}$



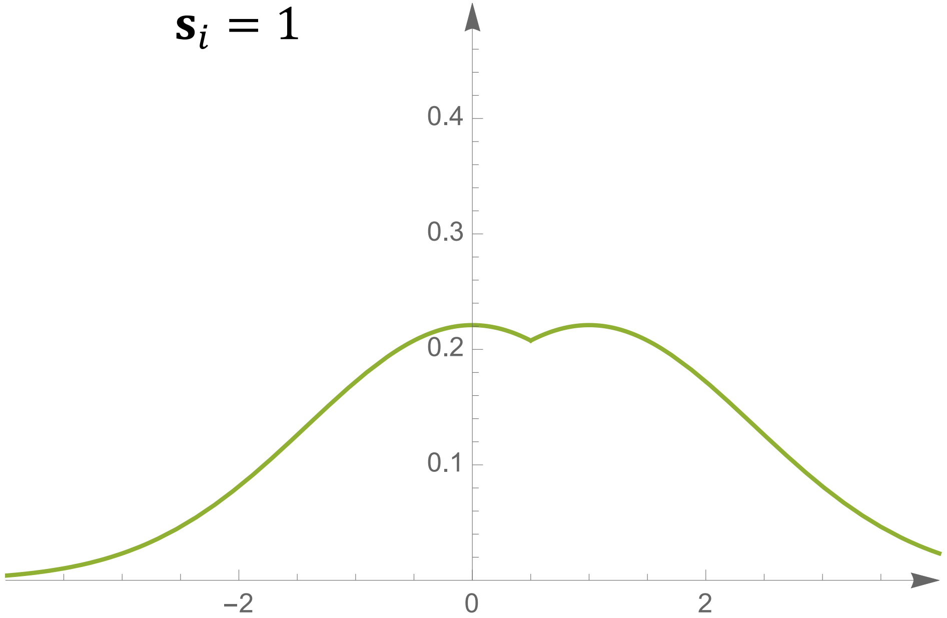
other nodes' reports are the same (the two green lines)

		Report $\mathbf{r}_i$	
		0	1
Private signal $\mathbf{s}_i$	0	u_{00}	u_{01}
	1	u_{10}	u_{11}

$\mathbf{s}_i = 0$

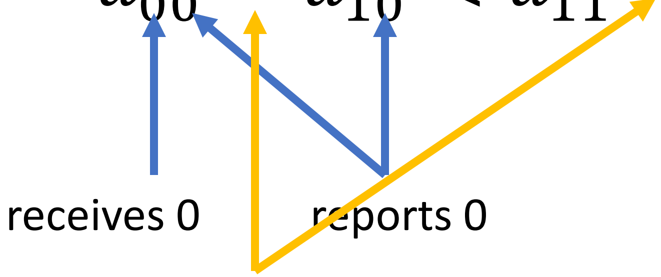


$\mathbf{s}_i = 1$



No robust compensation mechanism

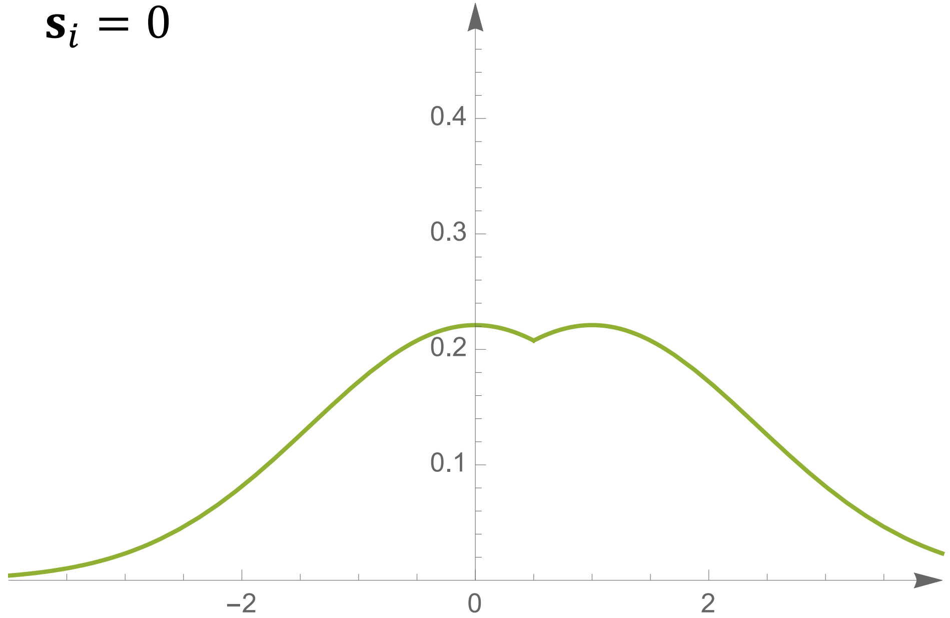
- $u_{00} = u_{10} < u_{11} = u_{01} < u_{00}$



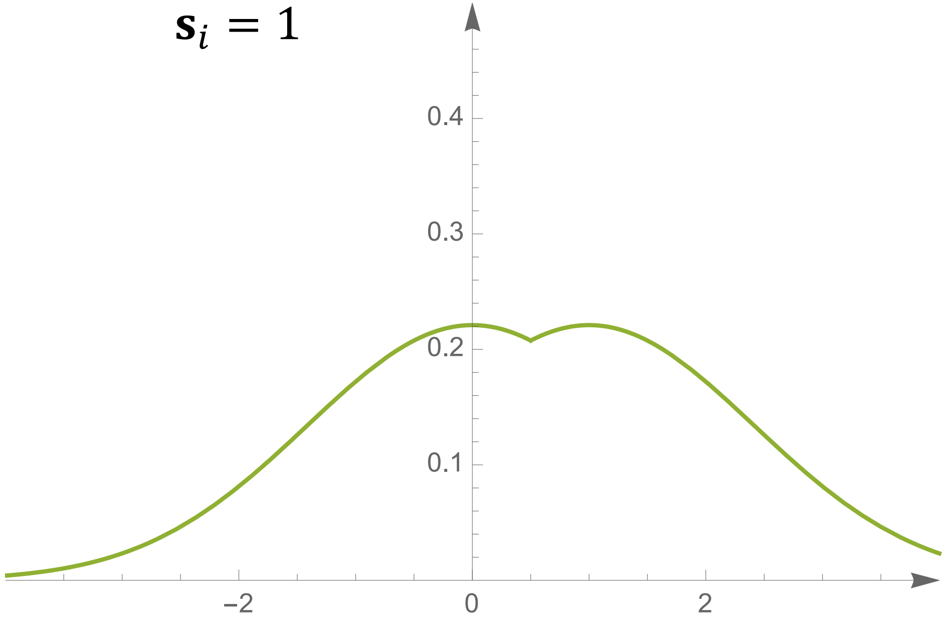
other nodes’ reports are the same (the two green lines)

		Report $\mathbf{r}_i$	
		0	1
Private signal $\mathbf{s}_i$	0	u_{00}	u_{01}
	1	u_{10}	u_{11}

$\mathbf{s}_i = 0$



$\mathbf{s}_i = 1$



No robust compensation mechanism

- Let $Q(\cdot;\mathbf{s})$ be a strategic node's posterior belief about another strategic node's private signal after observing $\mathbf{s}$
- Let d_{TV} denotes the total variation distance

$$d_{\mathrm{TV}}(P,P') \coloneqq \sup_{E\in\mathfrak{B}}[P(E)-P'(E)]$$

- Let $\mathcal{D}$ be the dataset of all reports

Theorem

If there are are two different signal realizations, $\mathbf{s}$ and $\mathbf{s}'$, such that

$$d_{\mathrm{TV}}\big(Q(\cdot;\mathbf{s}),Q(\cdot;\mathbf{s}')\big) \le \frac{\varepsilon}{1-\varepsilon},$$

then for any compensation mechanism $\mathcal{M}$ as a function of $\mathcal{D}$, $\mathcal{M}$ cannot be robust.

No robust compensation mechanism

- Let $Q(\cdot;\mathbf{s})$ be a strategic node's posterior belief about another strategic node's private signal after observing $\mathbf{s}$
- Let d_{TV} denotes the total variation distance

$$d_{\mathrm{TV}}(P,P') \coloneqq \sup_{E\in\mathfrak{B}}[P(E)-P'(E)]$$

- Let $\mathcal{D}$ be the dataset of all reports

the private signal's precision

Theorem

If there are are two different signal realizations, $\mathbf{s}$ and $\mathbf{s}'$, such that

$$\boxed{d_{\mathrm{TV}}\big(Q(\cdot;\mathbf{s}),Q(\cdot;\mathbf{s}')\big)} \le \boxed{\frac{\varepsilon}{1-\varepsilon}},$$

then for any compensation mechanism $\mathcal{M}$ as a function of $\mathcal{D}$, $\mathcal{M}$ cannot be robust.

the adversary's power

No robust compensation mechanism

- Economic intuition: Has to reward truth-telling and/or punish misreporting; but no way to check whether node i misreports or not given the adversary’s strategy

- Mathematical “intuition”: Data contamination breaks the stochastic relevance condition [which is the necessary condition to have a strict truth-telling eqm (P. Zhang and Chen, 2014)] 😎

Part 2: Robust consensus

Robust consensus: Overview

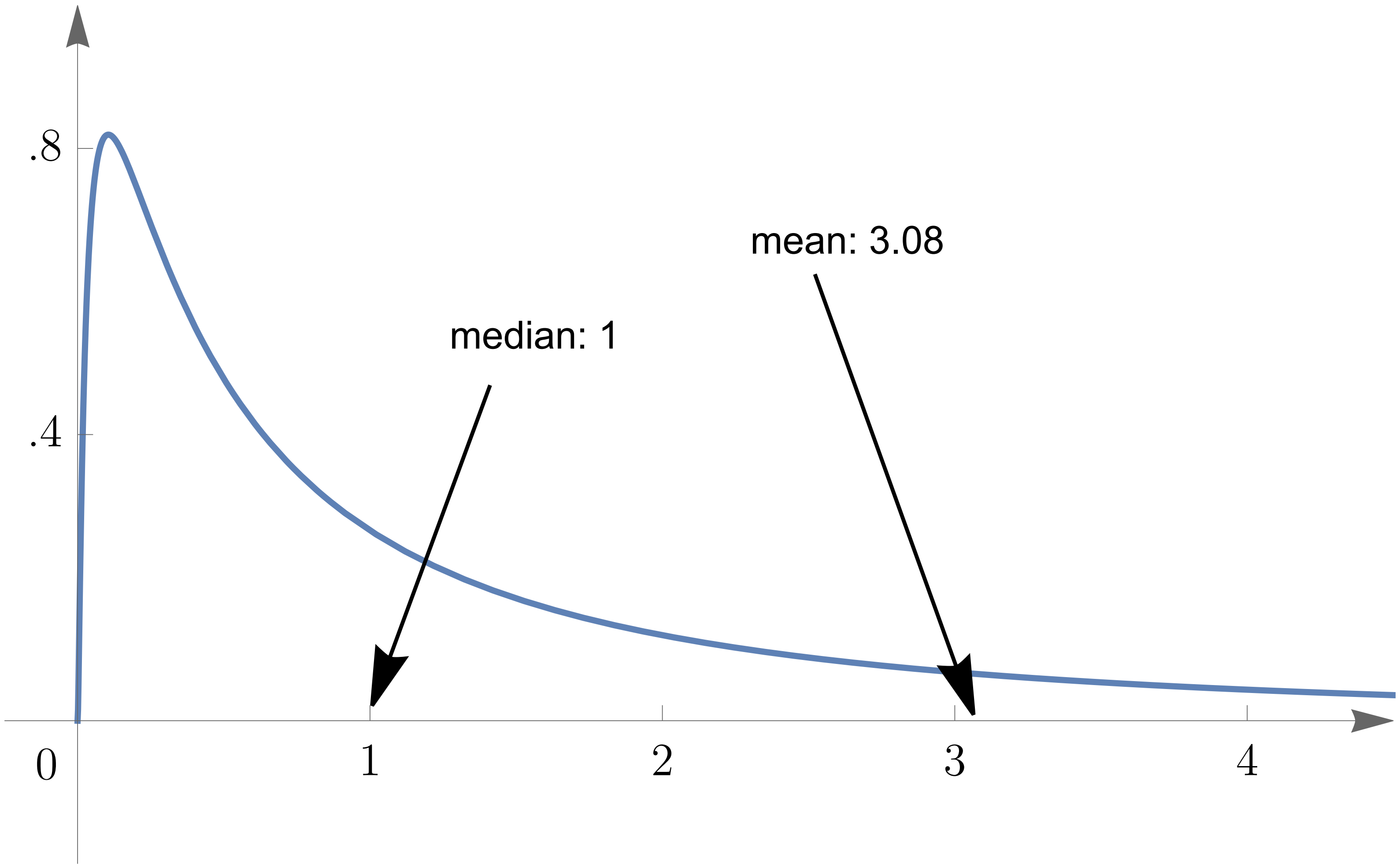
- The most popular consensus mechanism:

  Taking the (coordinate-wise) median

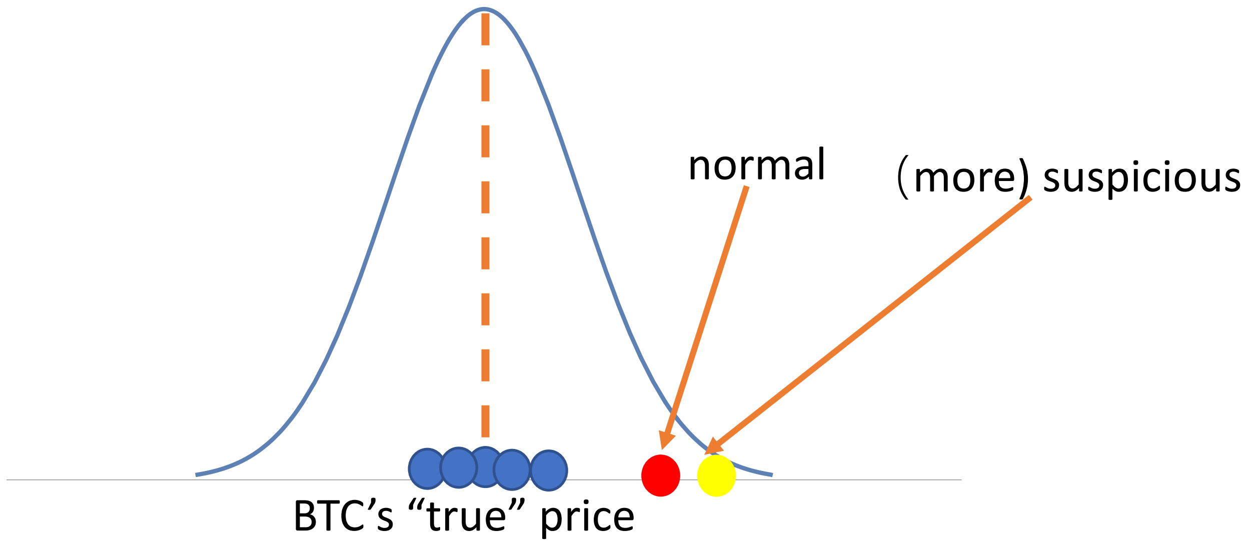
  - Bad if the noise term is asymmetric even without an adversary!
  - Not a bad estimator if symmetric; but is far from optimal under a multi-dimensional environment!
    - Even the best 1-d estimator can yield a L^2-norm error $\geq C\sqrt{\varepsilon d}$ (Folklore)

- Recent machine learning algorithms---unsupervised learning with contaminated datasets--- could yield a consensus that nearly achieves the error's theoretical lower bound without assuming symmetry!

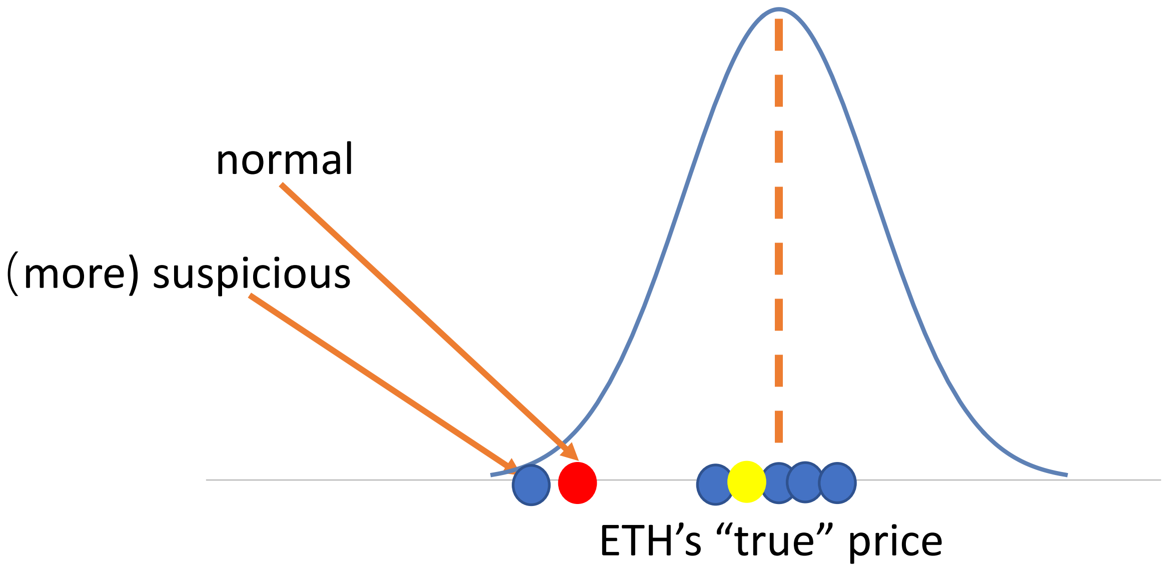
The current method may fail



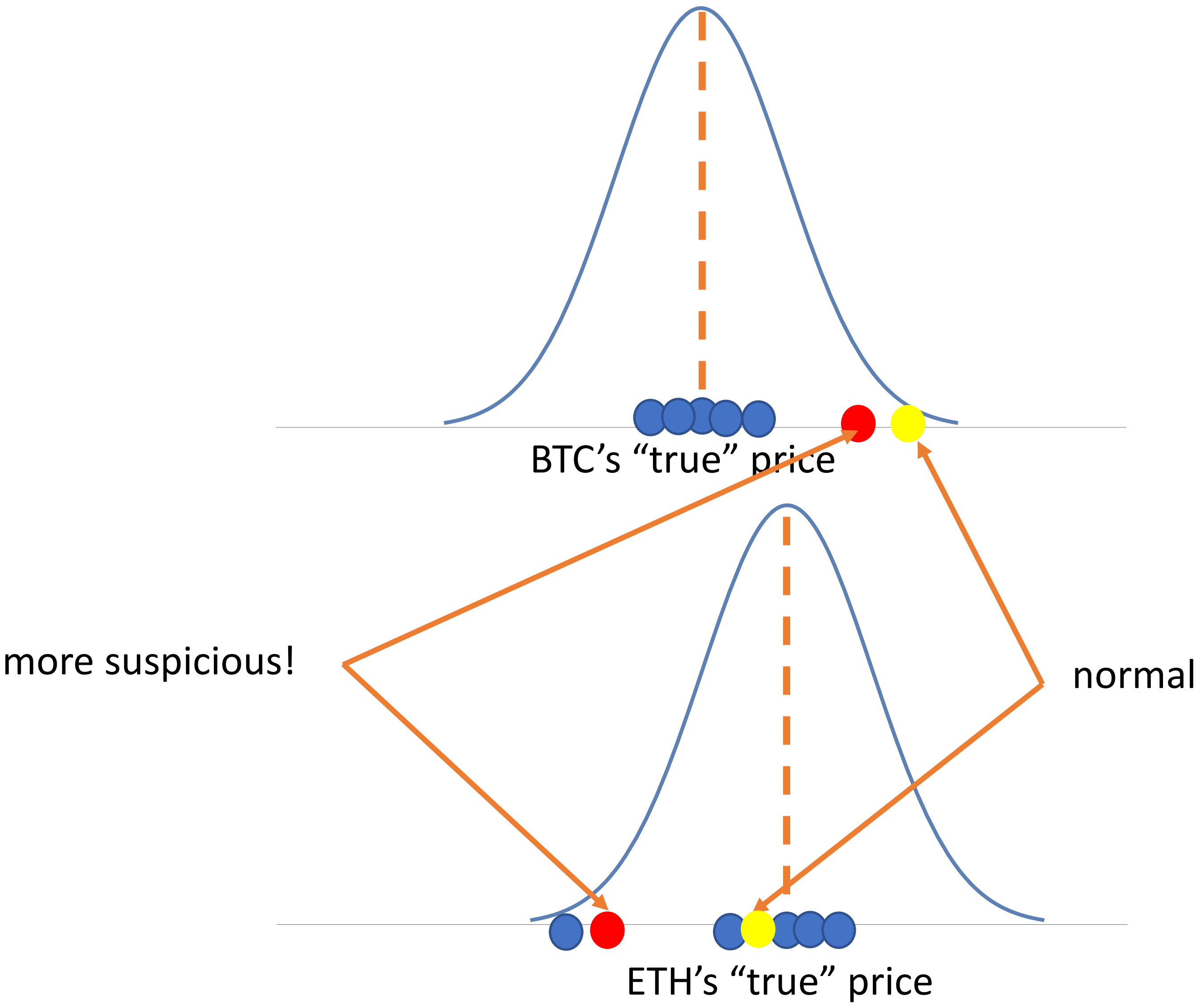
Robust consensus ($\varepsilon < 1/2$)



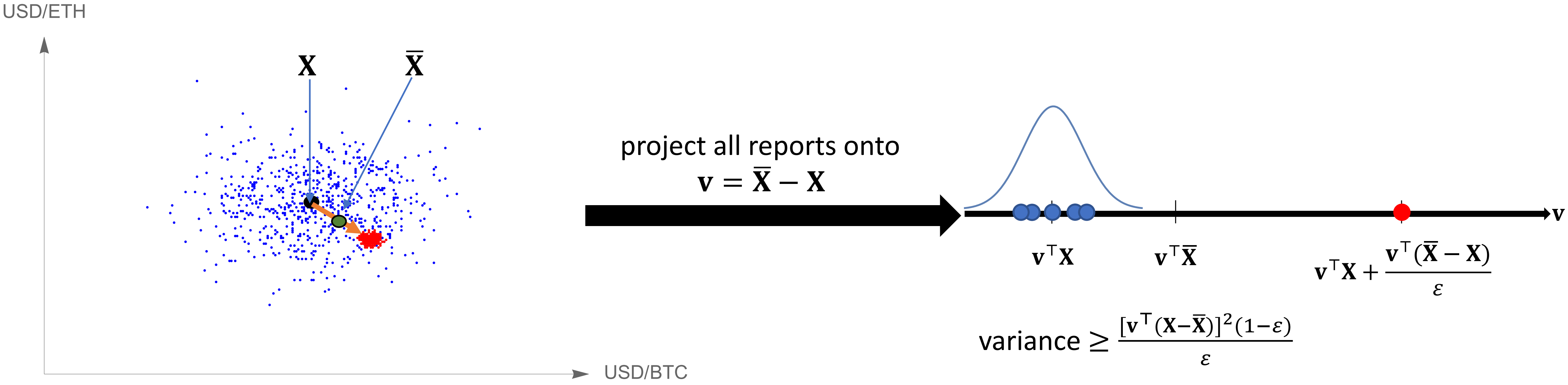
Robust consensus ($\varepsilon < 1/2$)



Robust consensus ($\varepsilon < 1/2$)



Robust consensus ($\varepsilon < 1/2$)

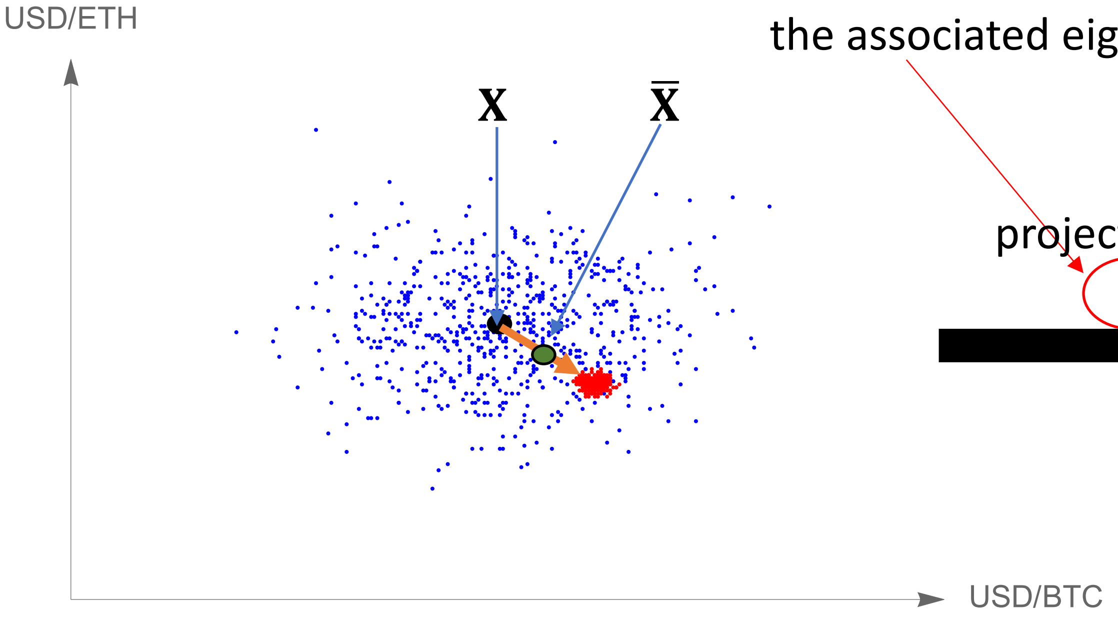

USD/ETH
$\mathbf{X}$
$\bar{\mathbf{X}}$
USD/BTC
$\mathbf{v}^\top \mathbf{X}$
$\mathbf{v}^\top \bar{\mathbf{X}}$
$\mathbf{v}^\top \mathbf{X} + \frac{\mathbf{v}^\top(\bar{\mathbf{X}} - \mathbf{X})}{\varepsilon}$
$\mathbf{v}$

project all reports onto
$\mathbf{v} = \bar{\mathbf{X}} - \mathbf{X}$

variance $\geq \frac{[\mathbf{v}^\top(\mathbf{X} - \bar{\mathbf{X}})]^2 (1-\varepsilon)}{\varepsilon}$

[The high-level idea (Diakonikolas et al., 2016, 2017; Diakonikolas and Kane, 2021): Using the covariance matrix!]

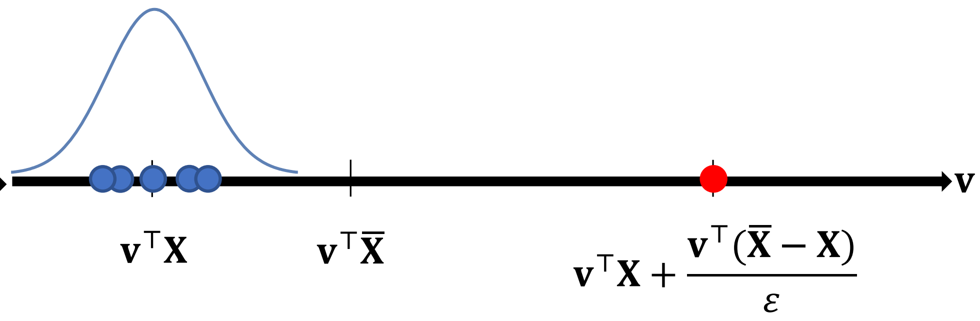
Robust consensus ($\varepsilon < 1/2$)



the associated eigenvector!

project all reports onto

$\mathbf{v} = \overline{\mathbf{X}} - \mathbf{X}$


$\mathbf{v}$
$\mathbf{v}^\top \mathbf{X}$
$\mathbf{v}^\top \overline{\mathbf{X}}$
$\mathbf{v}^\top \mathbf{X} + \frac{\mathbf{v}^\top (\overline{\mathbf{X}} - \mathbf{X})}{\varepsilon}$

variance $\geq \frac{[\mathbf{v}^\top (\mathbf{X} - \overline{\mathbf{X}})]^2 (1-\varepsilon)}{\varepsilon}$

the largest eigenvalue!

[The high-level idea (Diakonikolas et al., 2016, 2017; Diakonikolas and Kane, 2021): Using the covariance matrix!]

Robust consensus ($\varepsilon < 1/2$)

The filtering algorithm (Diakonikolas et al., 2016, 2017; Zhu et al., 2022)

1. Calculate the empirical covariance of the dataset $\mathcal{D}$ and find the largest eigenvalue

2. If the largest eigenvalue is small, then return the empirical mean of $\mathcal{D}$

3. Otherwise,
    - project $\mathcal{D}$ onto the eigenvector that is associated with the largest eigenvalue;
    - Downweight each point according to the distance between its projection and the projection of the empirical mean, and obtain a new dataset $\widetilde{\mathcal{D}}$;
    - replace $\mathcal{D}$ with $\widetilde{\mathcal{D}}$ and return to Step 1

Robust consensus ($\varepsilon < 1/2$)

theoretical lower bound

Theorem (Zhu et al., 2022)
The filtering algorithm will output a consensus $\hat{\mathbf{X}}$ such that

$$\left\|\hat{\mathbf{X}} - \mathbf{X}\right\|_2 \leq \boxed{\sigma\sqrt{\varepsilon}}\left(\frac{1}{\sqrt{1-\varepsilon}} + \frac{\sqrt{2}}{1-2\varepsilon}\right),$$

where σ^2 is an upper bound on the L^2-norm of the noise term’s covariance matrix.

Robust consensus ($\varepsilon < 1/2$)

theoretical lower bound

Theorem (Zhu et al., 2022)
The filtering algorithm will output a consensus $\widehat{\mathbf{X}}$ such that

$$\left\|\widehat{\mathbf{X}} - \mathbf{X}\right\|_2 \le \boxed{\sigma\sqrt{\varepsilon}}\left(\frac{1}{\sqrt{1-\varepsilon}} + \frac{\sqrt{2}}{1-2\varepsilon}\right),$$

where σ^2 is an upper bound on the L^2-norm of the noise term's covariance matrix.

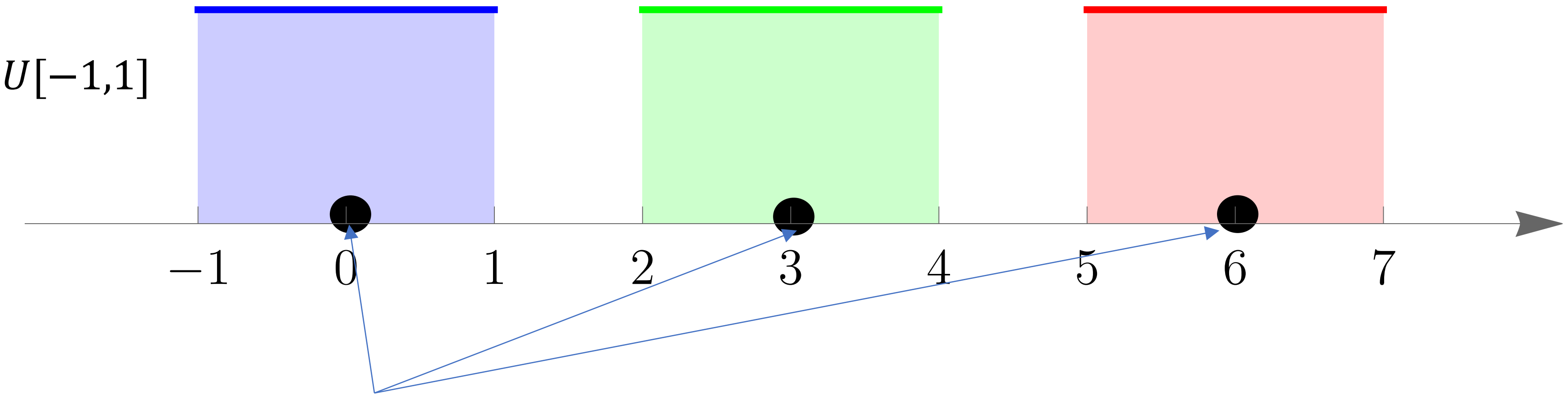
Best 1-d estimator: $\geq \sigma\sqrt{\varepsilon d}$

Robust consensus ($\varepsilon \geq 1/2$)

- Charikar et al. (2017)
  - There is no algorithm can return a unique consensus that is close to the ground truth
  - But we can return a list of candidates, in which at least one of them is “good”
  - A clever clustering algorithm

$\varepsilon = 2/3$

$\mathbf{s}_i = \mathbf{X} + U[-1,1]$



Which point is the ground truth?

Concluding remarks

- In general, no perfect decentralized solution to the oracle problem

- Machine learning can improve the consensus substantially

- All results also shed light on designing replacements for LIBOR

Thank you! ☺