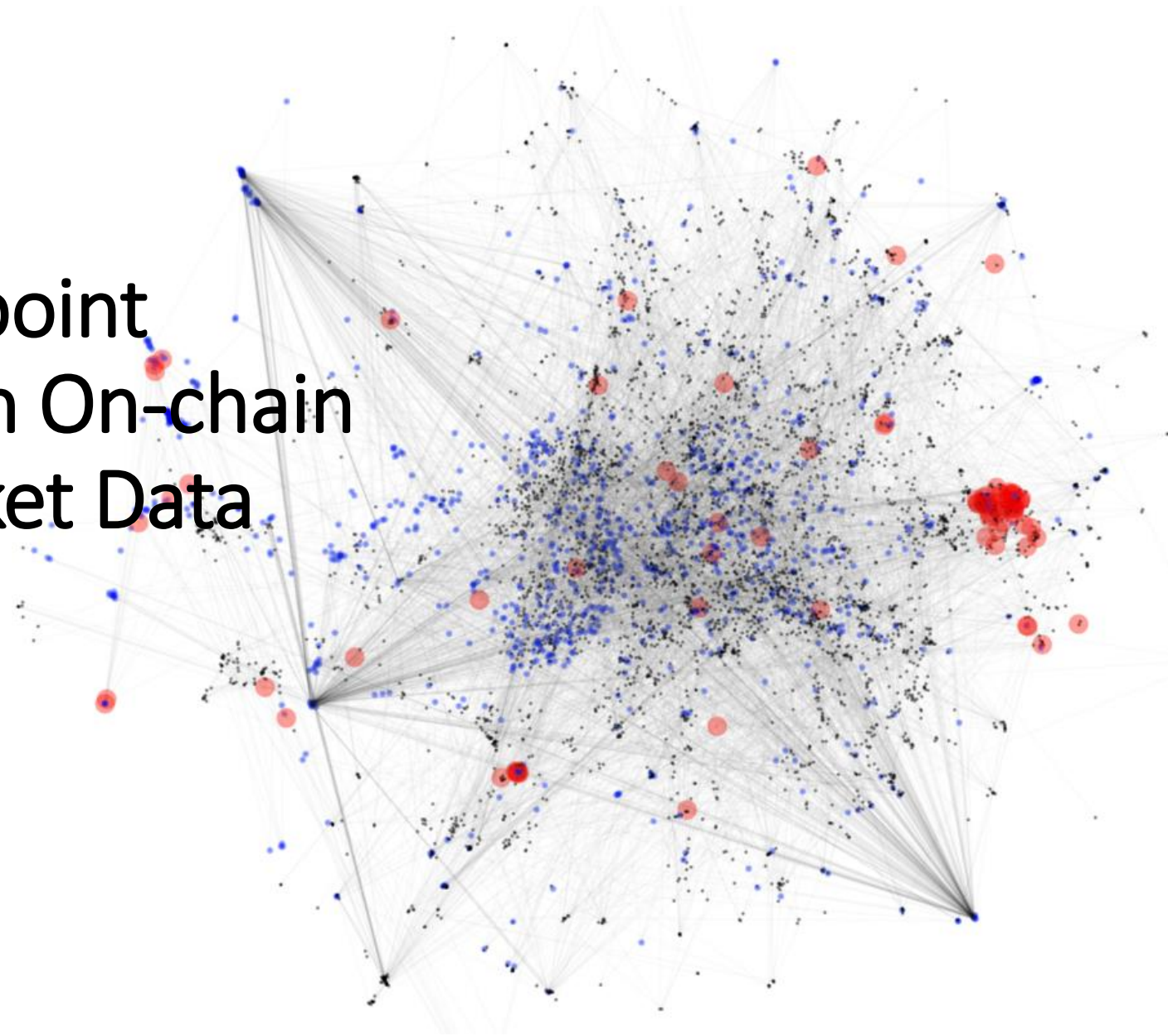
Oracle Counterpoint Relationships between On-chain and Off-chain Market Data

Tammy Yang,

Ariah Klages-Mundt,

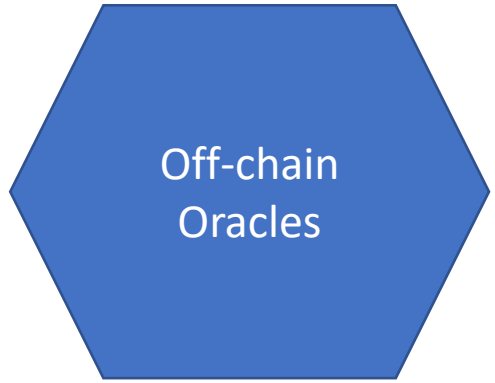
Lewis Gudgeon

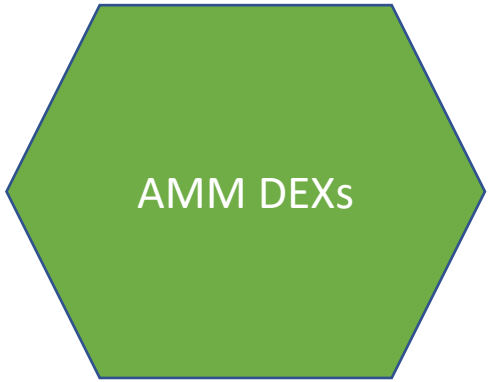


Obtaining price information on chain - Current

Oracles provided by off-chain services – e.g. Chainlink

- Simple, cheap
- Trust off-chain service is correct





Time weighted average prices from AMM DEXs, e.g., ETH/USDC

- Verifiable on-chain, costly to manipulate
- Trust stablecoin is at $1
- Slower

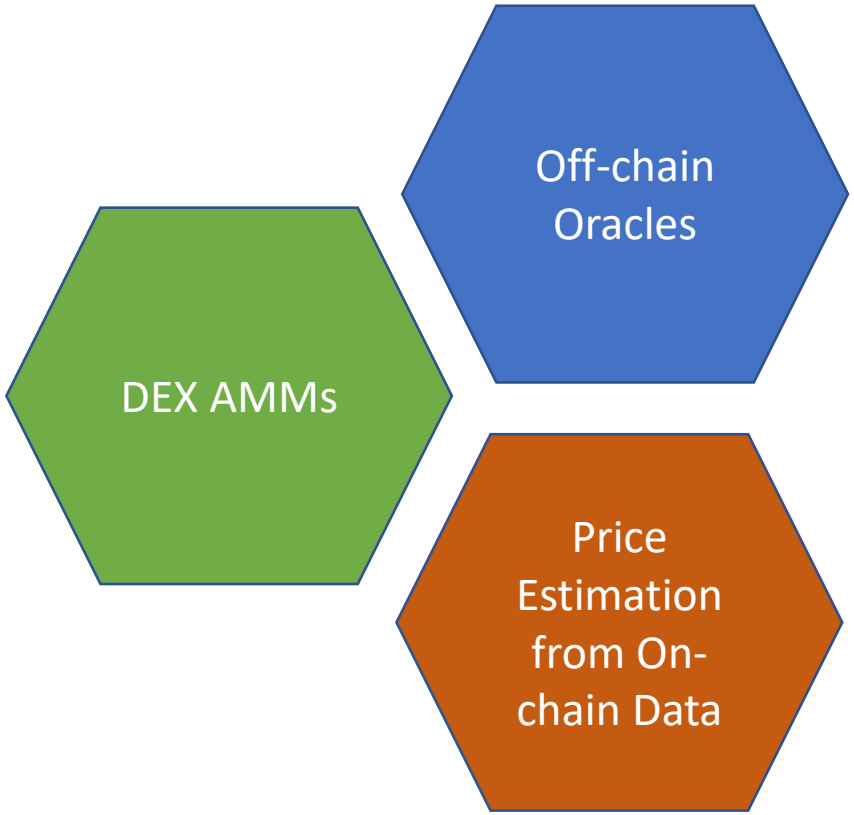
Project Overview

Goal

- To study empirical relationships between on-chain data and off-chain crypto price (e.g. ETH/USD, BTC/USD)

Motivation

- To develop an alternative to proxy off-chain crypto price that is verifiable on-chain



The Model

Ideal properties of *f*

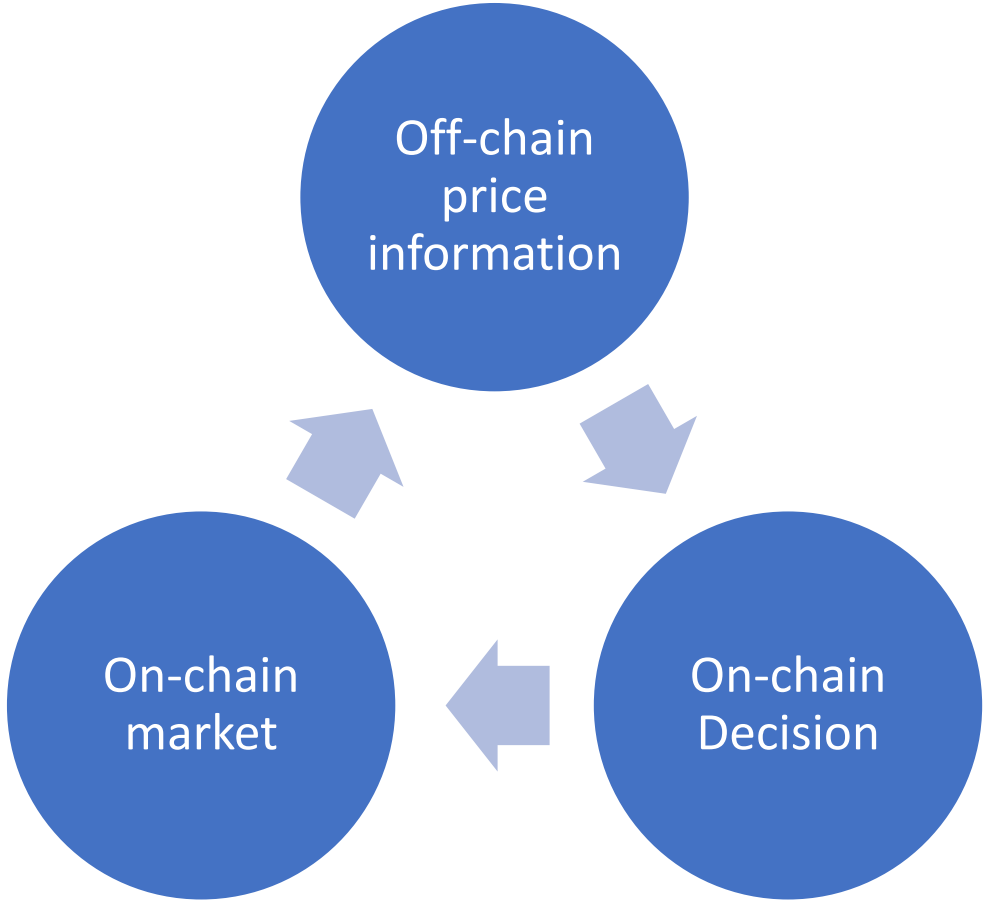
- Simple enough to be deployed on chain
- Difficult/costly to manipulate its output
- input features are verifiable on chain

Key On-chain Features – Part of the Initial Selection

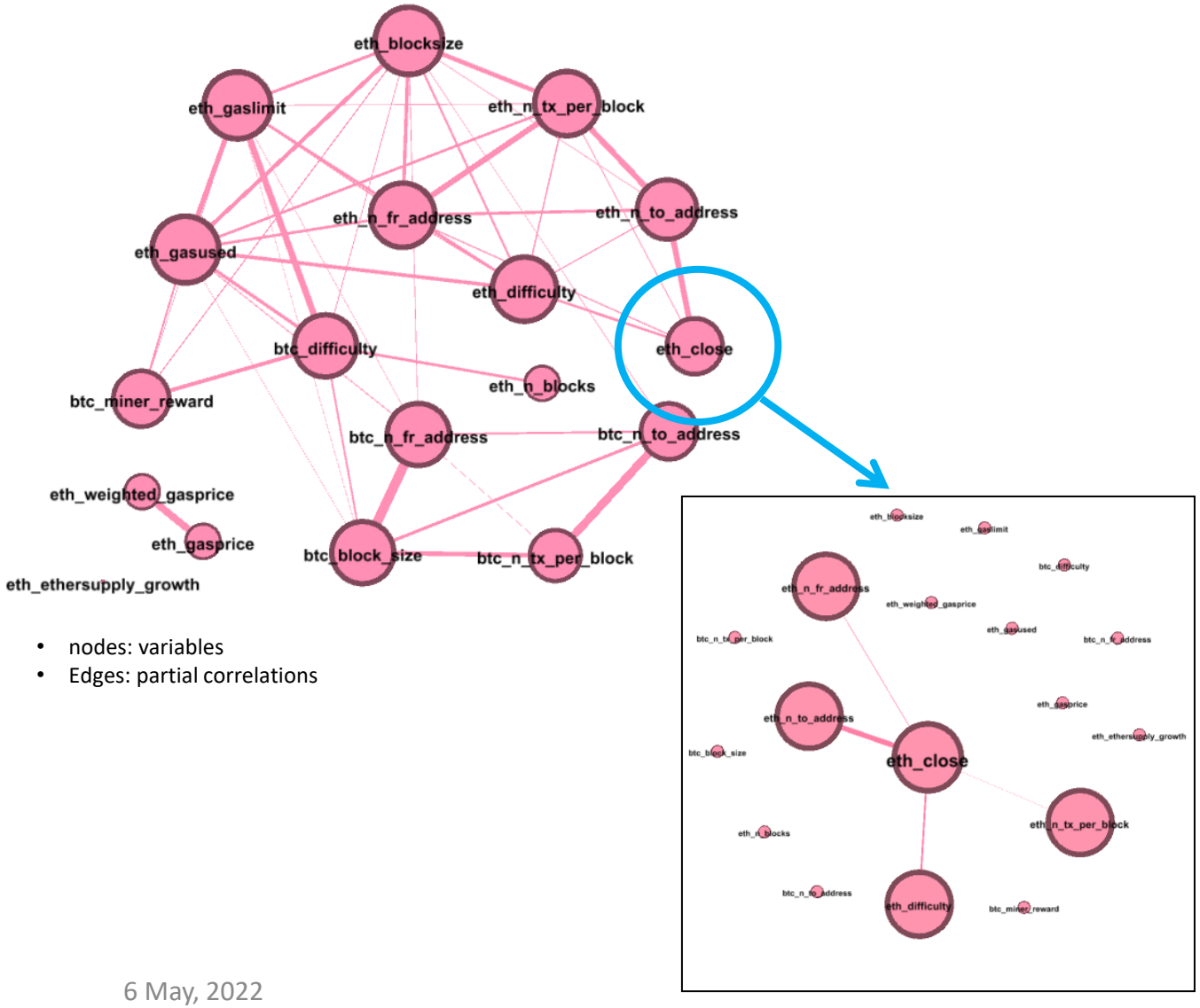
Basic	Economic	DeFi
• Difficulty • Number of senders/receivers • Number of transactions • Avg gas used • …	• Network congestion rate • Mining payoff • Computational burden of running full node • …	• Uniswap ETH trade volume • Uniswap stabecoin inflow • Uniswap stablecoin outflow

Rational

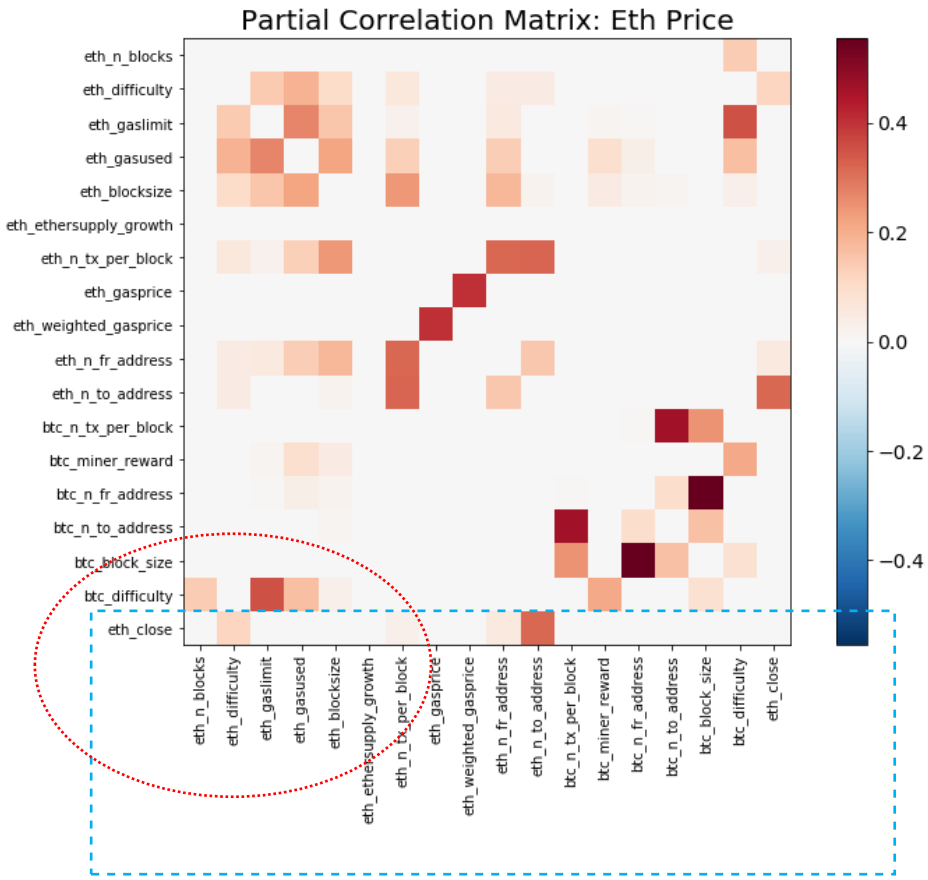
- Off-chain price information impacts how agents make decisions on-chain
- The decisions impacts on-chain markets output – which are observables on-chain
- Feed into our model to recover original off-chain price information



Feature Analysis – Dependence



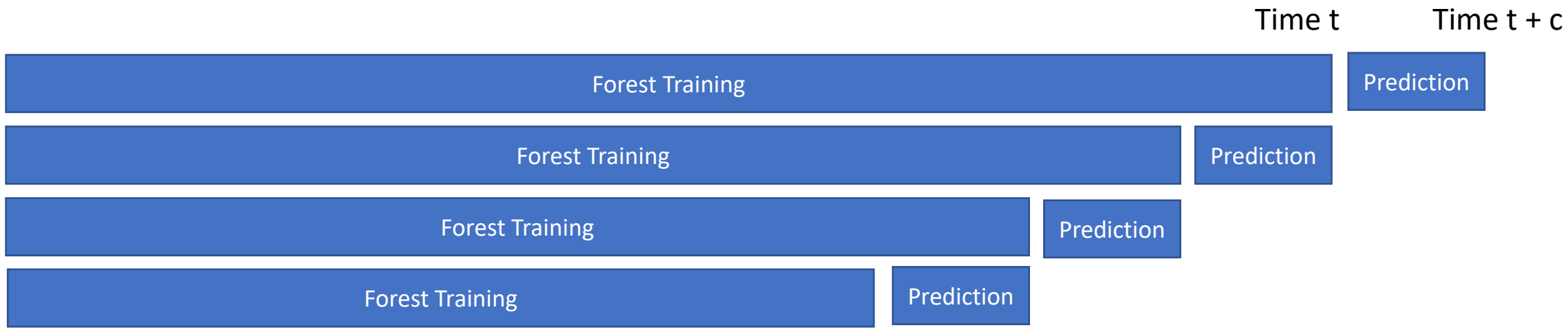
- nodes: variables
- Edges: partial correlations



Connected nodes to ETH price are:

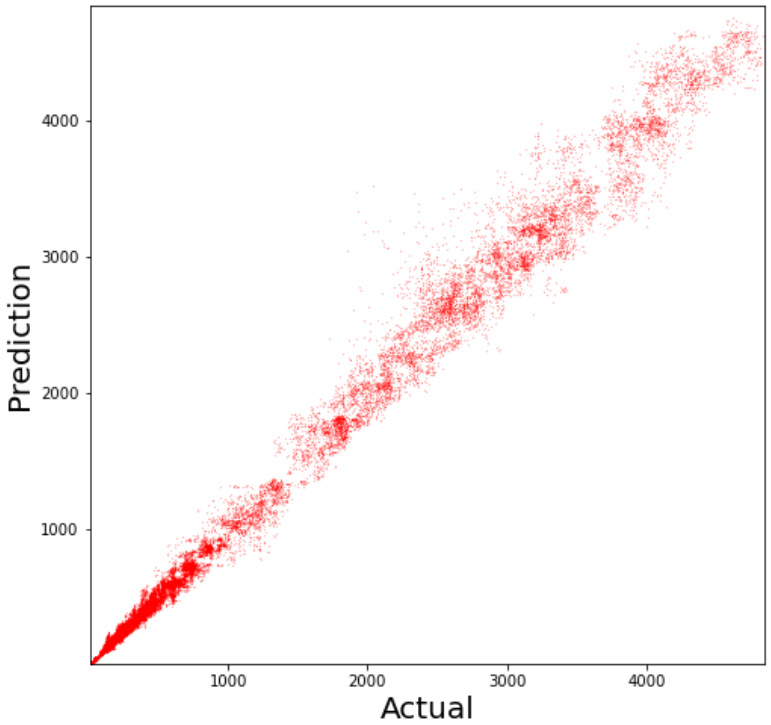
- eth_n_to_address
- eth_difficulty
- eth_n_fr_address
- Eth_n_tx_per_block

Model Training Approach – Rolling Forest

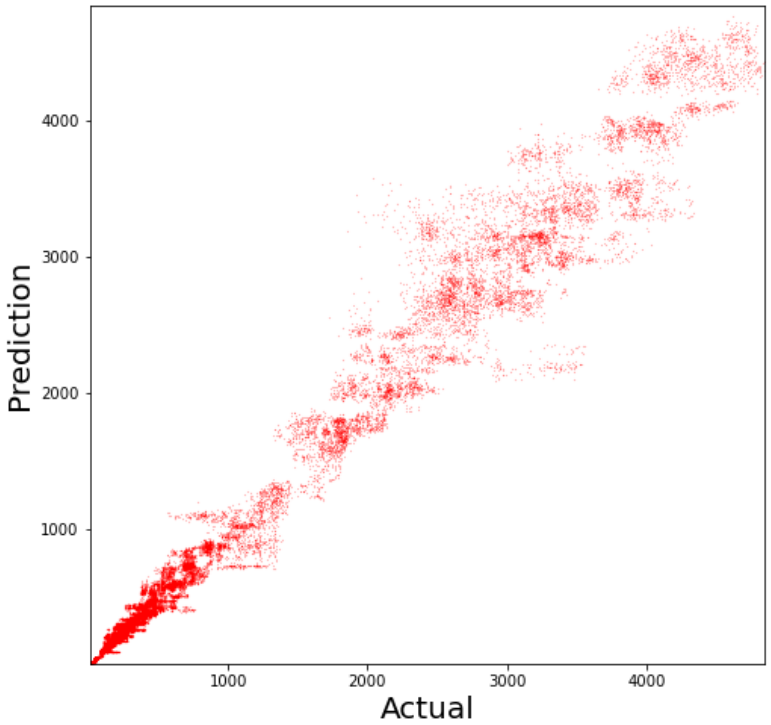


Model Performance

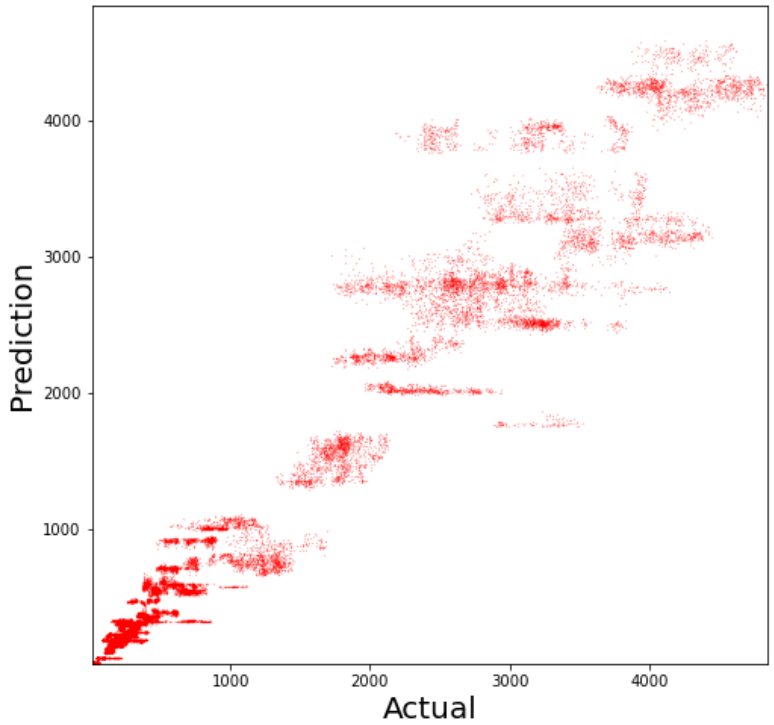
Model used for1-day, 1-week and 1-month price estimation



1-Day



1-Week



1-Month

Summary

- The model is not perfect but it shows strong potential
- It can be used to identify red flag on possible oracle issues

Potential Application

1st Layer: oracle prices (e.g., chainlink)

2nd Layer: use AMM TWAPs to check that oracle prices are consistent in relative sense

e.g., if have ETH/USD and DAI/USD, check that ETH/DAI = (ETH/USD)/(DAI/USD)

- note this doesn't assume that DAI = $1!

3rd Layer: check that ETH/USD price is consistent across alternative oracles

this is a check on absolute price level (e.g., all prices from layer A oracle aren't inflated together)