DeFi Class Project

Dawn Song

Class Project

- 3-5 students per group (6 students per group is allowed)
- If you still have not formed a group and submitted the group formation information, you need to do it by this week
  - O.w., your class participation points will be deducted
  - Use edstem to find group members
  - Find groups of similar interest that you may want to join: potential project ideas spreadsheet
- Goal:
  - Hands-on, in-depth learning on a DeFi topic
  - Ideally a report/research paper that can be shared with and contribute to the community

Timeline

Group formation	9/13
Lab 1 out	10/01
Project proposal	10/04
Lab 1 due	10/11
Project milestone	11/01
Lab 2 out	11/02
Lab 2 due	11/22
Project presentation	12/02
Project final report	12/13

Project Proposal Form (Due 10/04/2021)

- Problem statement
- Project description
- Project artifacts
- Evaluation
- Expected outcome
- Project milestones and planned timeline
- Planned division of labor

Class Project Categories

- Systematization of Knowledge
- DeFi measurement/empirical study
- New design and implementation
- Others

Category I: Systematization of Knowledge (SoK)

- Goal:
  - Survey work in an area/on a topic
  - Establish a framework & extract insight
  - Conduct analysis and experiments/measurements as needed
- Example SoKs:
  - CeFi vs. DeFi — Comparing Centralized to Decentralized Finance, Qin et al.
  - SoK: Decentralized Finance, Werner et al.
- Project Evaluation:
  - Does it cover representative works in the area/on the topic?
  - What are the framework & insights?
  - Are analysis and/or experiments sufficient in supporting the insights?

Category I: Systematization of Knowledge (SoK)

- Sample project ideas:
  - SoK on DEX
  - SoK on general principles for writing secure smart contract
  - SoK on onchain portfolio management
  - SoK on DeFi insurance
  - SoK on scams in DeFi
  - SoK on secure wallet design
  - SoK on decentralized identity

Category II: DeFi Measurement/Empirical Study

- Goal:
  - Quantitatively understand a type of DeFi products (e.g., cross-chain bridge, yield aggregator) or a type of DeFi activity (e.g., MEV)
  - Study different aspects: Incentive structures, risks, stabilities, etc.
- Methodology
  - Crawl data (onchain and/or offchain)
  - Identify key metrics and questions for measurement
  - Analyze data
  - Extract insights
- Sample Paper: https://arxiv.org/pdf/2106.06389.pdf

Category II: DeFi Measurement/Empirical Study

- Project evaluation:
  - What are the key metrics and questions for measurement?
  - Is the data sufficient to measure the key metrics & answer the questions?
  - What are the insights?
  - Is the analysis repeatable?
- Sample project ideas: DeFi measurement on
  - Yield aggregators
  - DEX aggregators
  - Synthetic assets
  - Options
  - Asset management
  - NFT
  - Perpetuals
  - Algorithmic stablecoins
  - Insurance

Example

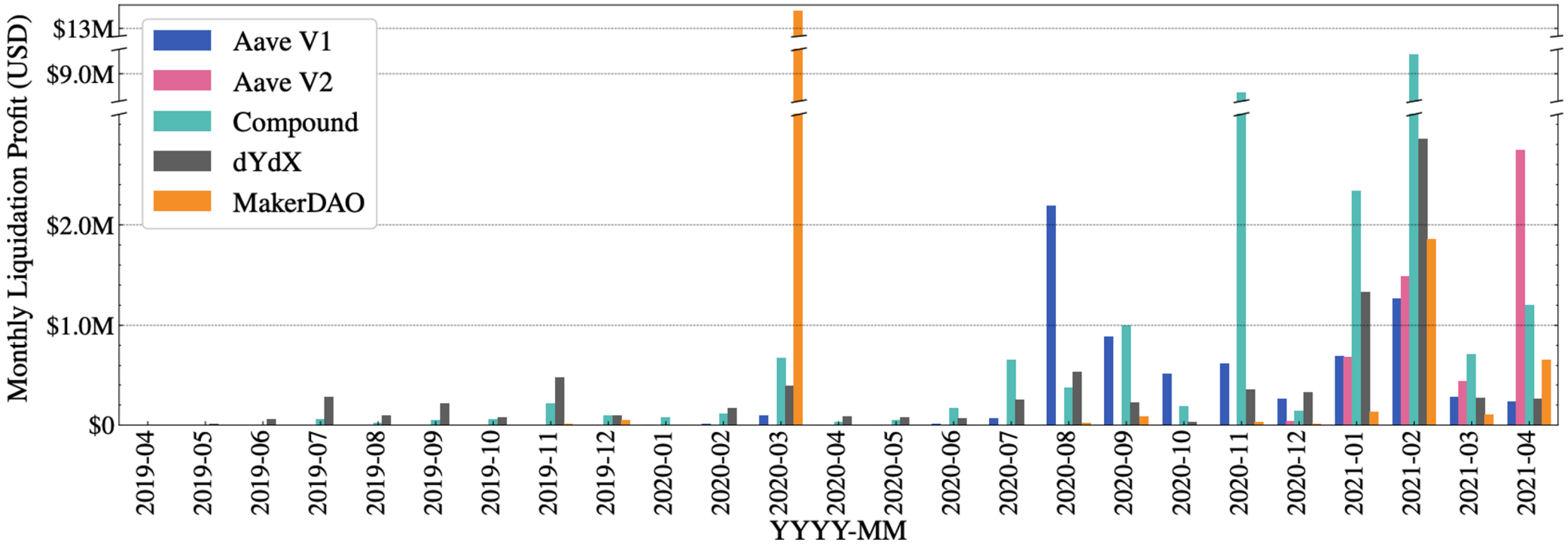


Figure 4: Monthly accumulated liquidator profit. We observe an outlier for MakerDAO in March, 2020, because the MakerDAO liquidation bots were faulty due to an excessive price decline of ETH. The outlier for Compound in November, 2020 is caused by an irregular price reported by a price oracle.

Sample project idea: DeFi Attacks Empirical Study

- Sample Paper: https://arxiv.org/abs/2003.03810
- Expectation:
  - Task 1 - Select a list of related attacks (e.g., on-chain price oracle manipulation)
  - Task 2 - Reproduce these attacks by forking the blockchain (similar to Lab 2 in this course), and perform optimisation to find the optimal attack vector.
  - Task 3 - Perform additional analysis to discover new findings that have not been made public via social media or articles.

Task 2 - Reproduce and Optimize

- Formulate DeFi actions in models

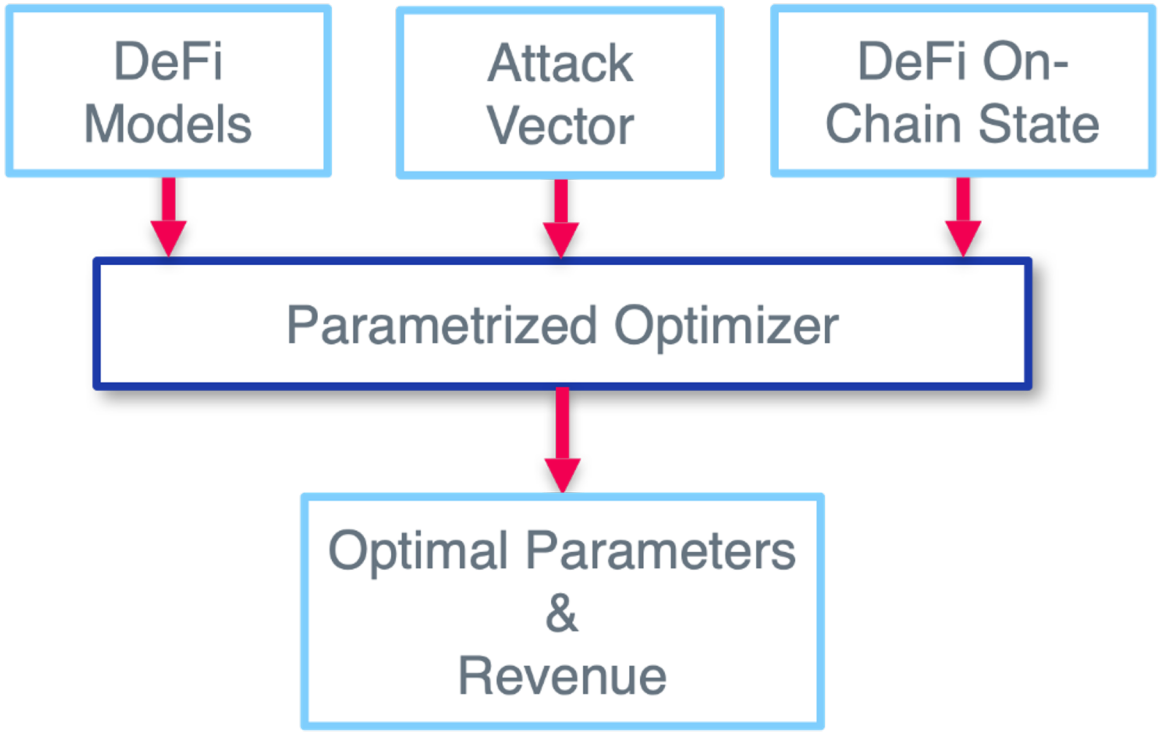
  ➢ Constant product AMM:

$$\Delta y = y - \frac{xy}{x + \Delta x}$$

- Construct a constrained optimization problem based on the attack vector

  ➢ Objective function: outcome profit

- Fetch the on-chain state that the attack is expected to be executed on.



Task 2 Example - Optimizing the bZx Attack

1. Borrow X ETH (bZx flash loan)
2. Convert $p1$ ETH to $f1(p1)$ sUSD (Uniswap)
3. Convert $p2$ ETH to $f2(p2)$ sUSD (Kyber)
4. Deposit $p3$ ETH for $f3(p3)$ sUSD (Synthetix)
5. Collateralize z sUSD to borrow $g(z)$ ETH
   $z = f1(p1) + f2(p2) + f3(p3)$
6. Repay X ETH (bZx flash loan)

Objective: $o = g\Big(f1(p1) + f2(p2) + f3(p3)\Big) - X$

s.t. $p1 + p2 + p3 < X$

Task 3 Example - Attack Window Analysis

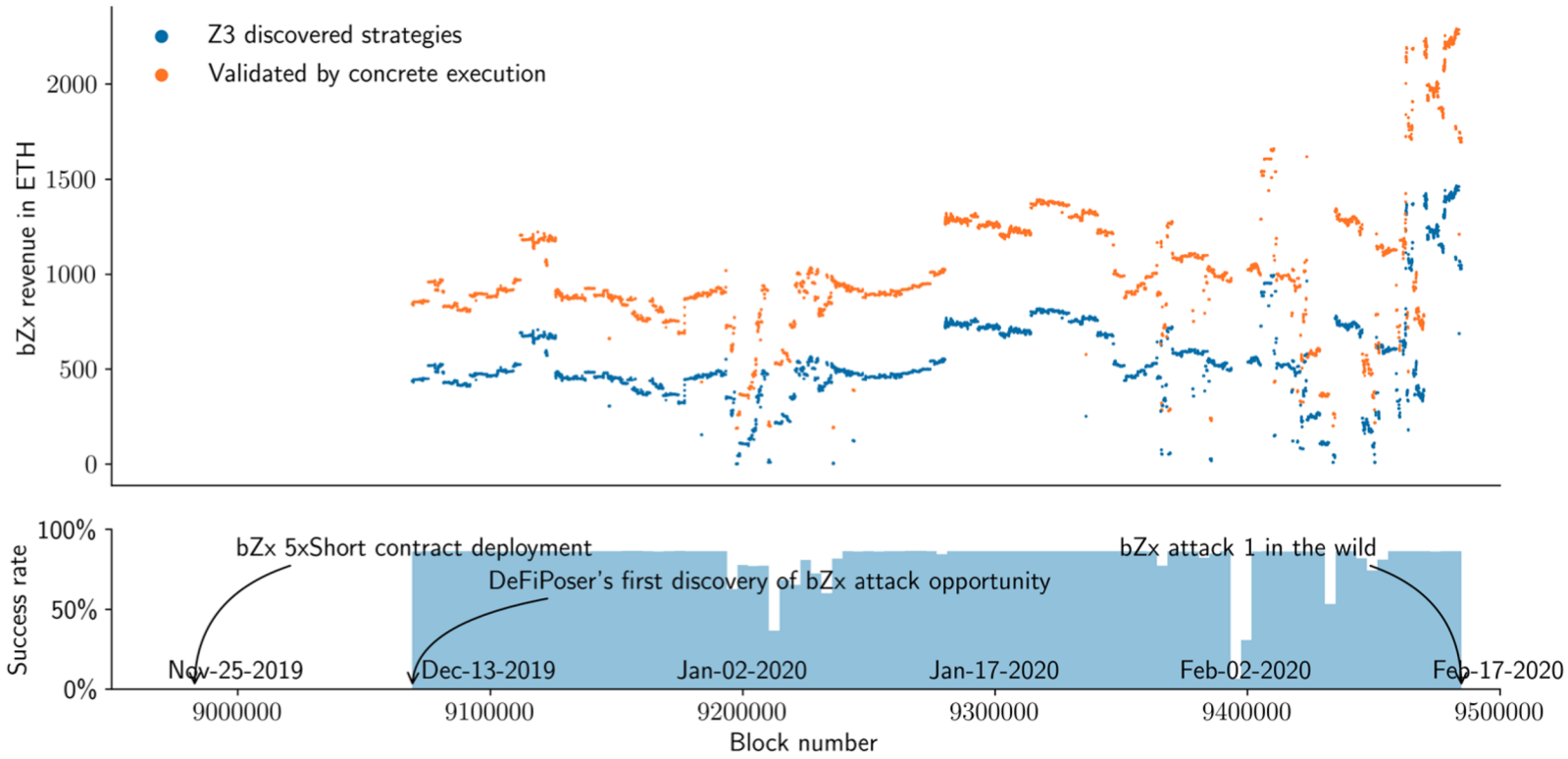


Fig. 16: Attack window analysis of the bZx attack. DEFIPOSER-SMT finds the first attack opportunity at block 9,069,000 (December 8th 2019). The opportunity lasted for 69 days, until the opportunity was exploited in block 9,484,687 (February 15th 2020). We visualize the difference between the profits from Z3 and concrete validation, along with the success rate (using block bin sizes of 100) of a Z3 strategy passing concrete validation. Note that the bZx loan interest rate formula is conservatively simplified in the encoding process, which explains why the Z3 anticipated revenue is lower than the concrete execution yield.

Category III: New Design & Implementation

- Goal:
  - Propose a new approach/solution to a problem in DeFi
  - Implement the approach/solution
  - Conduct simulation or experiments to evaluate the solution
- Project evaluation:
  - Is the problem clearly defined?
  - What is the new approach/solution?
  - Do the experiments properly evaluate the solution? How well does the solution improve over previous solutions?
- Sample project ideas:
  - New AMM design
  - New approach for decentralized identity
  - New design for privacy-preserving financial services